Redaktion WinTotal
Autor: Ulrich Schlüter

 28.11.2005

Microsoft Exchange Server 2003 Service Pack 2

von Ulrich Schlüter, Autor des Buches

„Integrationshandbuch Microsoft-Netzwerk“

ISBN 3-89842-525-8 bei galileocomputing.de

Die neuen Features, die mit dem Exchange Server 2003 Service Pack 2 eingeführt werden, werden in Artikeln wie Top 10 Reasons to Install Exchange Server 2003 SP2 oder New Mobility Features in Exchange Server 2003 SP2 aufgezählt. Das Ziel der vorliegenden Abhandlung ist es, dem Exchange-Administrator eine zusammenfassende Anleitung für die Installation des Service Packs, die Erhöhung der maximalen Größe der Exchange-Datenbanken, die Wirkungsweise der verschiedenen Spamfilter sowie deren Konfiguration anzubieten. Die Abhandlung nennt außerdem Tools, um die Spamfilter zu testen und ausgefilterte E-Mails zu verwalten. Folgende Themen werden behandelt:

Das Microsoft Exchange Server 2003 Service Pack 2 installieren

Vorbereitung auf die Installation des Service Pack 2

Installation des Service Pack 2 und nachfolgende Schritte

Die maximale Datenbankgröße hochsetzen

Neue Standardwerte und Maximalwerte für die Datenbankgröße

Prüfung der Datenbankgröße

Die maximale Datenbankgröße über Einträge in der Registrierdatenbank neu festlegen

Spamfilter des Exchange 2003 Service Pack 2 einsetzen

Verhindern, dass der eigene Exchange-Server als Open Relay missbraucht wird

Was tun, wenn Ihr eigener SMTP-Server irrtümlich auf einer schwarzen Liste als

Spamversender eingetragen ist?

...

IMF Version 2 in Exchange 2003 SP2

Reihenfolge der Filter, die eine Eingangsnachricht durchläuft

IMF und POP Connector von Small Business Server 2003

SCL Spam Confidence Level

Spam-Nachrichtenbehandlung mit selbst versendeten Spamnachrichten testen

IMF konfigurieren und aktivieren

Die als SPAM erkannten und archivierten Mails einsehen und bearbeiten

Speicherort des Spamarchivs verlegen

IMF Archive Manager zum Verwalten des UCE-Archivs

IMF Companion als Alternative zum IMF Archive Manager

SCL-Werte von E-Mails in Outlook anzeigen

Das „Custom Weighting Feature“

Absenderkennungsfilterung

Verbindungsfilterung – Sperrlistenanbieter konfigurieren

Empfängerfilterung

Absenderfilterung

Unzustellbarkeitsberichte und Übermittlungsberichte temporär deaktivieren

Das Microsoft Exchange Server 2003 Service Pack 2 installieren

Vorbereitung auf die Installation des Service Pack 2

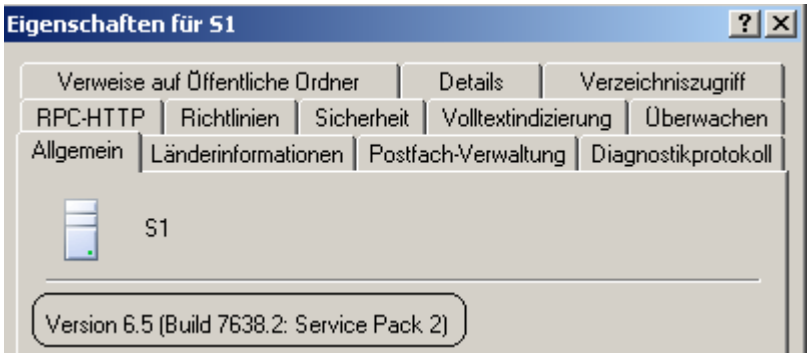
Sie können das Exchange Service Pack 2 von folgender Quelle herunterladen:

http://www.microsoft.com/downloads/details.aspx?FamilyId=535BEF85-3096-45F8-AA43-60F1F58B3C40&DisplayLang=de

...

Bevor Sie ein Exchange Service Pack installieren, sollten Sie sich sicher sein, welche Windows-Server-Version, welche Exchange-Version und welche Service Packs bereits installiert sind. Überprüfen Sie zuerst über „Systemsteuerung – Software“ den Versionsstand der Serverprodukte und darüber hinaus, ob bereits eine Vorversion des Intelligent Message Filter IMF oder aber Produkte von Drittanbietern für Datensicherung, Virenschutz oder Schutz vor Spam installiert sind. Stellen Sie über die Webseite des Herstellers oder durch Anfragen beim Hersteller sicher, ob Produkte von Drittanbietern (Virenschutz, Antispyware, Backup-Software) für Exchange 2003 SP2 freigegeben sind.

Die Version des Windows Servers und des installierten Windows Server Service Packs können Sie auch herausfinden, indem Sie im Menü des Windows Explorers auf das Fragezeichen und darunter auf „Info“ klicken. Wenn Sie jedoch den Exchange System-Manager starten und im Menü auf das Fragezeichen und dann auf „Info“ klicken, erhalten Sie keinen Hinweis über die Exchange-Version oder die Version des installierten Exchange Service Packs. Stattdessen wird die Version der Microsoft Management Console angezeigt. Da eine Exchange-Organisation aus mehreren Exchange-Servern bestehen kann, müssen Sie sich im Exchange-Manager zu demjenigen Exchange-Server hinhangeln, dessen Versionsstand Sie ermitteln wollen. Diesen Server klicken Sie mit der rechten Maustaste an und öffnen dessen Eigenschaften. In der Registerkarte „Allgemein“ wird die Exchange-Version und das installierte Service Pack angezeigt. Nach der Installation des Service Packs 2 steht dort „Version 6.5 Service Pack 2“.



Lesen Sie die „Frequently Asked Questions zu Exchange Server 2003 Service Pack“:

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2003/sp2/faq.mspx

Lesen Sie außerdem die Release Notes.

http://download.microsoft.com/download/f/b/5/fb5c54af-fe5c-48e9-be97-f9e8207325ab/Ex_2003_SP2_RelNotes.htm

Dort finden Sie unter anderen folgende wichtige Aussagen:

...

"If you are running Windows Server 2003, it is recommended that you ***install Windows Server 2003 Service Pack 1*** *(SP1)..."*

*"**Ensure that Hotfix 898060**, "Installing security update MS05-019 or Windows Server 2003 Service Pack 1 may cause network connectivity between clients and servers to fail Installing security update MS05-019 or Windows Server 2003 Service Pack 1 may cause network connectivity between clients and servers to fail," **has been installed** on your system. You can determine whether this hotfix is installed by running the Microsoft Exchange Server Best Practices Analyzer Tool, which checks for the hotfix being installed, and then reviewing the output log. If you do not run the Exchange Server Best Practices Analyzer, you must manually verify that Hotfix 898060 is installed on your system. If this hotfix is not on your system, you must install it now. This hotfix is applicable only to Windows Server 2003 customers who applied security update MS05019 or Windows Server 2003 SP1."*

"With Exchange Server 2003 Service Pack 2, we now include the Intelligent Message Filter; it is no longer a separate add-on to Exchange. As a result, we have to create an object within the Active Directory to store the IMF settings... In order to be able to create and validate that object, ***the following right is needed: - Exchange Administrator (or higher) on the Organization level****... After the first upgrade completes successfully, setup will check for the existence of the above AD object and allow customers to proceed with a more restricted permission set (i.e. Exchange Administrator role at the administrative group or higher, as per original permission requirements). So those elevated rights are needed only for the first Exchange 2003 SP2 installation in the Organization."*

*"**Before you enable Sender ID** on Exchange 2003 SP2 server, **make sure that you apply the Windows Server 2003 hotfix** that is referenced in Microsoft Knowledge Base article, Windows Server 2003 may stop responding when you enable Sender ID filtering on an SMTP virtual server in Exchange Server 2003 SP2."*

*"**Intelligent Message Filter is not cluster-aware** and cannot be installed on an Exchange server that is a member of a server cluster. The Intelligent Message Filter is not cluster-aware and cannot be installed on an Exchange server that is a member of a server cluster. However, it can run on front-end servers and Exchange Simple Mail Transfer Protocol (SMTP) gateways that are members of a network load-balanced cluster. It can also run on non-clustered Exchange Server 2003 computers."*

*"**Upgrade All Load-Balanced Front-End Servers to SP2 Together**."*

*"**Upgrade All Exchange Server 2003 Front-End Servers Before Upgrading Exchange Server 2003 Back-End Servers**."*

...

"A new version of the offline address book (OAB 4.0) has been introduced in Exchange Server 2003 SP2... You must have Microsoft Office Outlook 2003 Service Pack 2 (SP2) installed to realize this enhanced performance."

Beachten Sie weiterhin Folgendes:

- Wenn durch das Einspielen des Service Pack 2 erreicht werden soll, dass die maximale Größe der Exchange-Datenbanken erhöht werden kann, so müssen die Partitionen der Festplatten ausreichend dimensioniert sein. Eventuell müssen neue Festplatten beschafft und eingebaut werden.

- Die Hardware des Servers sollte generell so dimensioniert sein, dass die Gesamtperformance akzeptabel bleibt, wenn größere Exchange-Datenbanken verwaltet und gesichert werden müssen.

- Wenn mehrere Exchange Server 2003 eingesetzt werden, sollte sichergestellt sein, dass alle nacheinander zügig auf SP2 umgestellt werden können. Sie müssen damit rechnen, dass es Fehlermeldungen in den Ereignisprotokollen gibt, die erst dann verschwinden, wenn der letzte Exchange Server 2003 auf SP2 geupdatet wurde. Die Voraussetzungen dazu müssen auf allen Exchange Servern 2003 gegeben sein.

- Deinstallieren Sie ältere IMF-Versionen (IMF = Intelligent Message Filter), wenn Sie diese vorher zusätzlich zum Exchange Server 2003 installiert hatten. Das SP2 installiert eine neuere Version des IMF. Die Installationsroutine des SP2 bricht in der Regel mit einem entsprechenden Hinweis ab, wenn eine ältere IMF-Version installiert ist.

- Erstellen Sie ein Backup des Systemstatus und der Exchange-Datenbanken.

- Trennen Sie nach Möglichkeit den Exchange-Server vor dem Einspielen des SP2 vom restlichen Netzwerk, damit während des Installationsprozesses nicht ungeplant Updates automatisch eingespielt werden und damit kein Anwender während der Installation und den sich anschließenden Tests des Gesamtsystems (Exchange Server, Antiviren-Software, Antispy-Software etc.) auf sein Postfach zugreift. Der Exchange-Server sollte erst dann wieder mit dem Netz verbunden werden, wenn alle Tests erfolgreich verlaufen sind und damit sicher ist, dass nicht wieder zum alten Zustand zurückgekehrt werden muss.

- Stoppen Sie vor der Installation des Exchange 2003 SP2 alle Dienste von Drittanbieter-Software, die auf Exchange Server 2003 aufsetzt, wie Antivirensoftware oder Antispyware. Zwar erfordert das Einspielen des Service Pack 2 keinen Neustart des Servers. Dieser kann jedoch aus anderen Gründen während der Tests notwendig werden. Sie sollten deshalb erwägen, den Starttyp der Dienste von Drittprodukten temporär von „automatisch" auf „deaktiviert" umzustellen. Notieren Sie in diesem Fall, bei welchen Diensten der Starttyp umgestellt wurde, damit Sie später nicht vergessen, diese Änderungen rückgängig zu machen.

...

Installation des Service Pack 2 und nachfolgende Schritte

Die Installation des Service Pack 2 läuft mittels eines Assistenten ab. Sie setzt nicht voraus, dass das Service Pack 1 bereits installiert wurde. SP2 ist kumulativ, enthält also alle Fehlerbereinigungen, die SP1 enthielt. Nach erfolgter Installation ist kein Neustart des Servers erforderlich. Überprüfen Sie nach dem Einspielen des SP2, ob die Software von Drittanbietern fehlerfrei läuft. Dazu müssen deren Dienste eventuell wieder gestartet werden. Wurde der Starttyp der Dienste geändert, so müssen diese Änderungen wieder rückgängig gemacht werden.

Sollen die Maximalwerte der Exchange-Datenbanken erhöht werden, so fügen Sie jetzt die dazu notwendigen neuen Einträge in die Registrierdatenbank ein. Die Bereitstellung des Postfachspeichers muss dazu temporär aufgehoben werden. Eventuell müssen Postfachspeicher auch auf größere Partitionen verschoben werden.

Wird der Intelligent Message Filter IMF aktiviert und sollen ausgefilterte E-Mails archiviert werden, so müssen ebenfalls Änderungen in der Registrierdatenbank vorgenommen werden. Das Verzeichnis für die archivierten E-Mails sollte eventuell auf eine separate Partition verschoben werden, damit die Partition, auf der sich die Exchange-Datenbanken befinden, nicht unkontrolliert mit ausgefiltertem Spam vollläuft. Ein Tool zur weiteren Behandlung ausgefilterter Spammails wie z.B. der IMFArchiveManager sollte installiert und getestet werden.

Erst jetzt sollten Sie die Verbindung zum übrigen Netzwerk wieder herstellen und damit den Postfachzugriff seitens der Anwender ermöglichen. Erstellen Sie dann ein neues Backup des Exchange-Servers.

Die maximale Datenbankgröße hochsetzen

Neue Standardwerte und Maximalwerte für die Datenbankgröße

Die maximale Größe einer Exchange-Datenbank (Postfachspeicher oder Speicher für öffentliche Ordner) kann nach dem Einspielen von SP2 sowohl in der Exchange Server 2003 Standard Edition als auch in der Enterprise Edition durch Einträge in der Registrierdatenbank gesetzt werden. Bis Service Pack 1 waren die Maximalwerte hart codiert und konnten nicht verändert werden. Bei

...

der Enterprise Edition ist der Standardwert gleich dem Maximalwert und beträgt 8000 GB pro Datenbank, und zwar sowohl vor als auch nach dem Einspielen des SP2, jedoch mit dem Unterschied, dass nach dem Einspielen des SP2 der Maximalwert mittels des Registry-Eintrags **Database Size Limit in GB** bei Bedarf (Einsatz kleiner Festplatten) heruntergesetzt werden kann. Jedoch können bei der Enterprise Edition maximal 4 Speichergruppen mit jeweils 5 Postfachspeichern angelegt werden. Die Standard Edition unterstützt hingegen nur einen Postfachspeicher.

Exchange 2003-Version	Standardwert (hart codiert)	Maximale Größe
Standard Edition vor SP2	16 GB (nicht änderbar)	16 GB
Standard Edition mit SP2	18 GB (in Registry änderbar)	75 GB
Enterprise Edition vor SP2	8000 GB (nicht änderbar)	8000 GB
Enterprise Edition mit SP2	8000 GB (in Registry änderbar)	8000 GB

Im Gegensatz zur Enterprise Edition wurde bei der Standard Edition also ein Standardwert beibehalten, jedoch durch SP2 von 16 auf 18 GB hochgesetzt. Da der Standardwert für den ebenfalls neuen Registry-Wert **Database Size Buffer in Percentage** 10 Prozent beträgt, erfolgt die Warnung im Ereignisprotokoll also weiterhin bei ca.16 GB (18 GB abzüglich 10 %). Damit will Microsoft verhindern, dass es zum Desaster kommt, weil die Festplattengröße nicht den neuen Maximallimits angepasst wurde. Der Administrator soll zuerst sicherstellen, dass die Festplattenkapazität ausreichend ist, bevor er den Maximalwert höher als 18 GB einstellt.

Prüfung der Datenbankgröße

Die Prüfung der Datenbankgröße erfolgt ab SP2 aufgrund der logischen Größe der Datenbank und nicht mehr aufgrund der physischen Größe. Der durch gelöschte Objekte frei gewordene Speicherplatz zählt nicht mehr mit, sondern nur der belegte Speicherplatz. Überschreitet diese „Nettogröße“ den eingestellten Maximalwert, so muss keine Offline-Defragmentierung mittels des Werkzeugs Eseutil erfolgen. Dadurch allein würde die lizenzierte Datenbankgröße dann auch nicht wieder unterschritten.

Wird eine Exchange-Datenbank gestartet, so erfolgt zuerst eine Prüfung, ob die physikalische Größe der Datenbank (= Größe der edb-Datei + Größe der stm-Datei) die konfigurierte Datenbankgröße (z.B. 75 GB) überschreitet. Übersteigt diese physikalische Größe die konfigurierte Maximalgröße abzüglich des Puffers, der über den Registry-Eintrag „Database Size Warning Buffer“ festgelegt ist, so erfolgt zusätzlich eine Prüfung auf freie Speicherblöcke, die durch das Löschen von Objekten entstanden sind. Diese werden von der ermittelten physischen Datenbankgröße abgezogen, um die

...

logische Größe der Datenbank zu ermitteln. Diese zusätzliche Prüfung dauert einige Sekunden.

Danach wird die Datenbank alle 24 Stunden überprüft. Wird bei diesen Prüfungen zweimal hintereinander festgestellt, dass die logische Maximalgröße überschritten wurde, so wird die Datenbank erst bei der zweiten Überprüfung offline genommen. Der Administrator kann die Datenbank aber wieder online schalten und hat dann maximal 24 Stunden Zeit, deren Größe durch geeignete Maßnahmen zu korrigieren. Hatte er bis dahin als Maximalwert einen GB-Wert kleiner als 75 GB eingetragen, so kann er z.B. diesen Wert erhöhen.

Die maximale Datenbankgröße über Einträge in der Registrierdatenbank neu festlegen

Bevor Sie den Maximalwert für die Größe des Postfachspeichers unter Exchange Server 2003 Standard Edition hochsetzen, sollten Sie Folgendes bedenken:

- Eventuell reicht der freie Festplattenplatz nicht aus, so dass zuerst größere Festplatten in den Exchange-Server eingebaut werden müssen. Laut gängiger Empfehlungen sollte der freie Speicherplatz mindestens genauso groß sein wie die Größe der Exchange-Datenbanken, damit bei einer Reparatur mit dem Werkzeug Eseutil genug Platz zur Erzeugung der temporären Dateien verfügbar ist.

- Die Reparatur oder Offline-Defragmentierung des vor SP2 auf 16 Gigabyte begrenzten Postfachspeichers nimmt bei einer großen Exchange-Datenbank bereits eine erhebliche Zeit in Anspruch, abhängig von den Hardwarekomponenten des Servers und der Belastung durch Dienste und Zugriffe seitens der Anwender. Da es empfehlenswert ist, vorher eine separate Sicherung der Datenbank vorzunehmen, erhöht sich die Nichtverfügbarkeitsdauer des betroffenen Postfachspeichers um die dafür notwendige Sicherungszeit. Nimmt die Größe des Postfachspeichers auf maximal bis zu 75 GB zu, so erhöht sich entsprechend die Ausfallzeit, wenn die Datenbank beschädigt wird oder offline defragmentiert werden muss.

- Die Sicherung des Exchange-Servers dauert länger und benötigt mehr Bandkapazität. Auch die Wiederherstellung eines großen Postfachspeichers aus der Sicherung dauert länger.

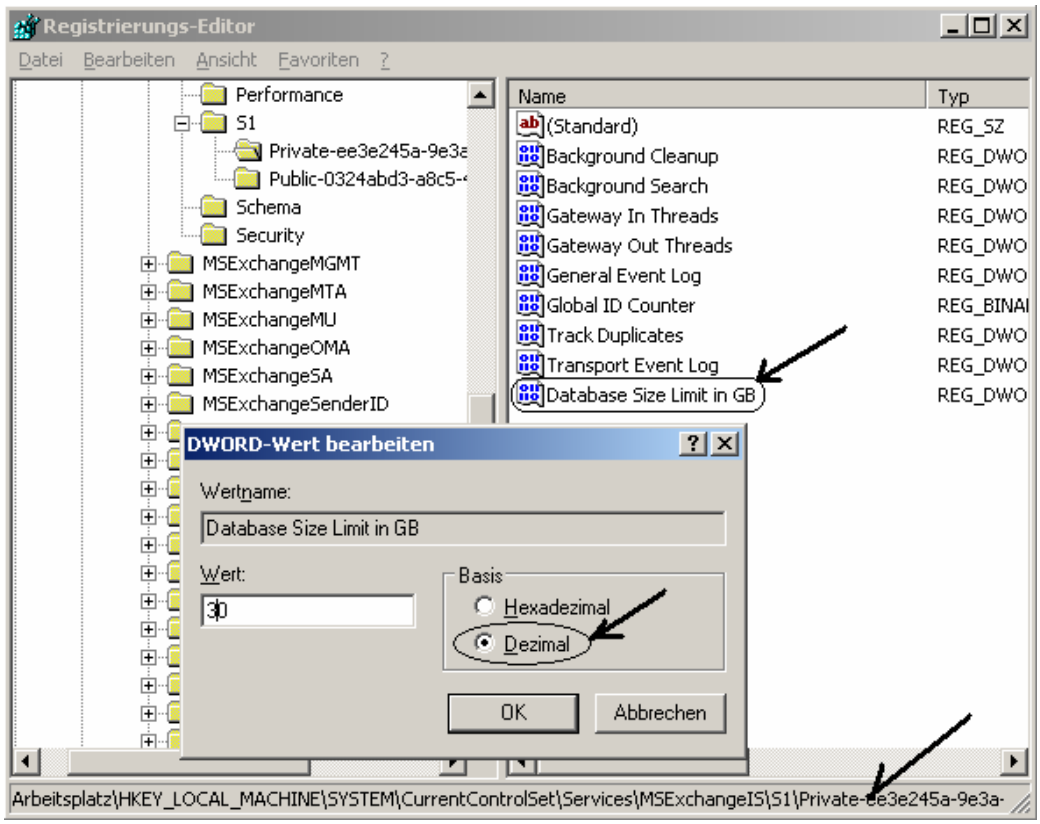
- Je größer die Exchange-Datenbanken sind, desto intensiver ist die Serverbelastung durch Zugriffe der Anwender und Verwaltungsaufgaben seitens des Servers. Eventuell reicht die Hardware nicht mehr aus, es kommt zu einem Performance-Einbruch. Serverhardware und Streamer müssen für größere Datenbanken ausreichend dimensioniert sein.

Es empfiehlt sich daher dringend, mit Bedacht vorzugehen und die Maximalgröße des Postfachspeichers in überschaubaren Etappen hochzusetzen, bei denen die Hardwareausstattung

...

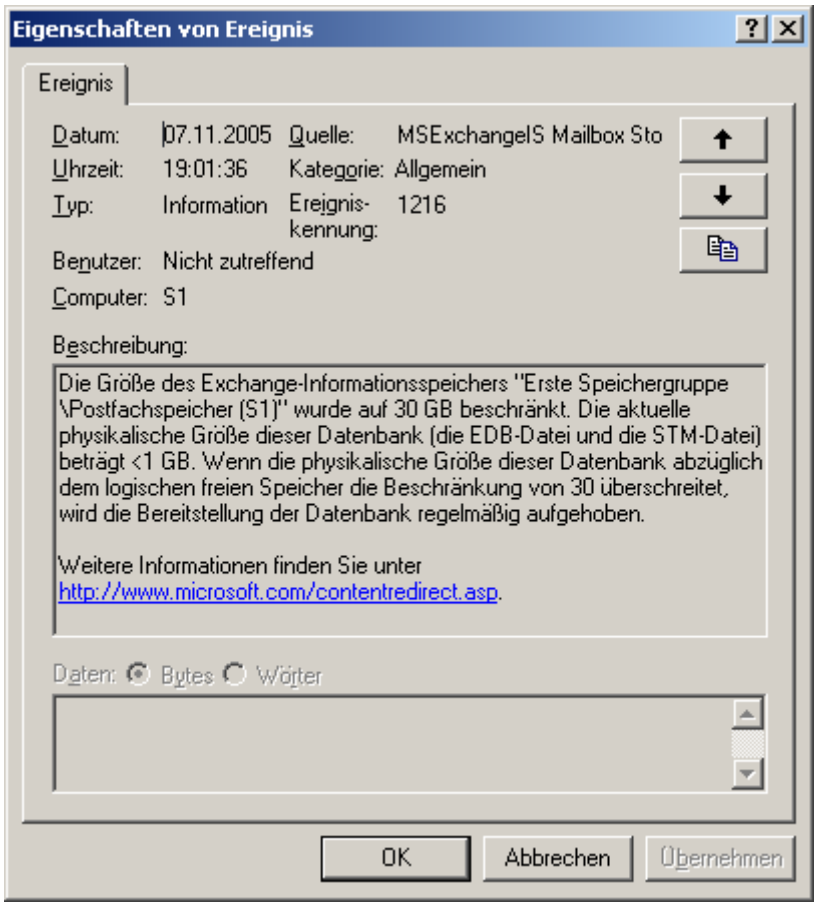
des Servers inklusive Sicherungsgeräte berücksichtigt wird. Das bedeutet gleichfalls, dass die Postfachkontingente der Anwender nur angemessen und in Etappen erhöht werden.

Nach der Installation des Service Pack 2 ist der Standardwert für die Größe des Postfachspeichers von 16 GB auf 18 GB erhöht. Er kann durch einen Registrierdatenbankwert auf maximal 75 GB erhöht werden. Dazu muss unter HKEY_LOCAL_Machine\SYSTEM\CurrentControl-Set\Services\MSExchangeIS\<Servername>\private GUID ein neuer DWORD-Wert mit dem Namen **Database Size Limit in GB** erstellt werden. Ändern Sie die Option „Basis“ zuerst in „Dezimal“, bevor Sie den gewünschten Maximalwert zwischen 18 und 75 eintragen.



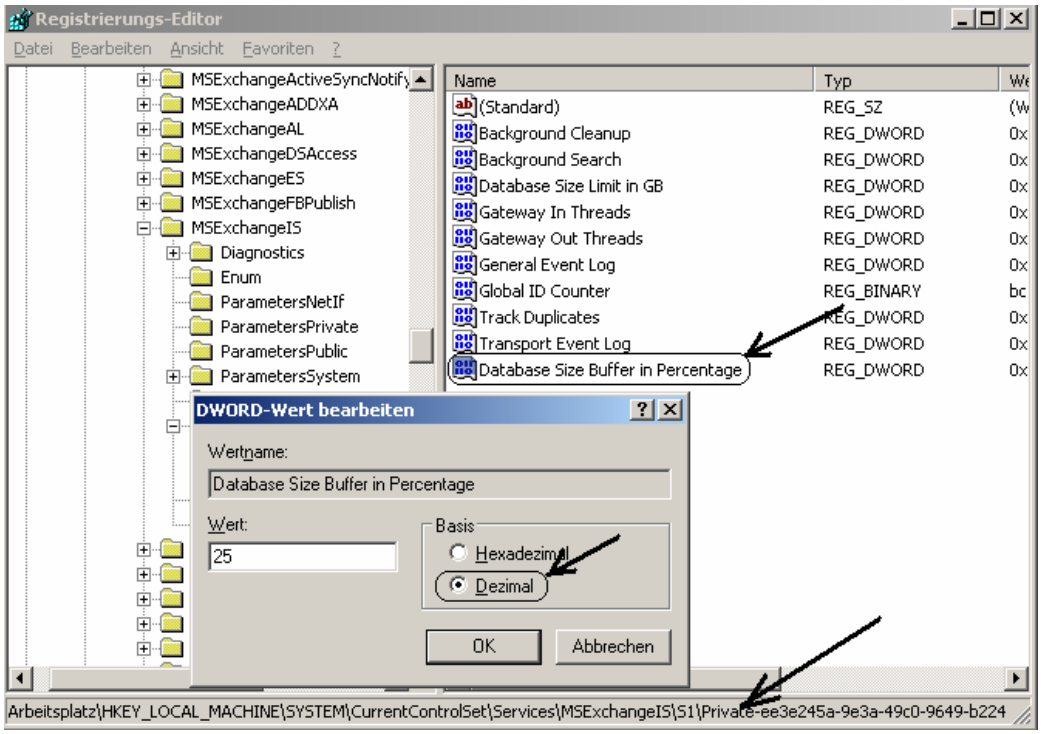
Damit der neue DWORD-Eintrag aktiv wird, muss die Bereitstellung des Postfachspeichers aufgehoben und dann wieder aktiviert werden. Dazu klicken Sie den Postfachspeicher im Exchange-Manager mit der rechten Maustaste an und wählen nacheinander die entsprechenden Befehle. Um zu überprüfen, ob die neue Beschränkung wirkt, öffnen Sie das Ereignisprotokoll. In der Kategorie „Anwendungen“ sollte nun ein Ereignis mit dem Text „Die Größe des Exchange-Informationsspeichers wurde auf x GB beschränkt“ stehen.

...



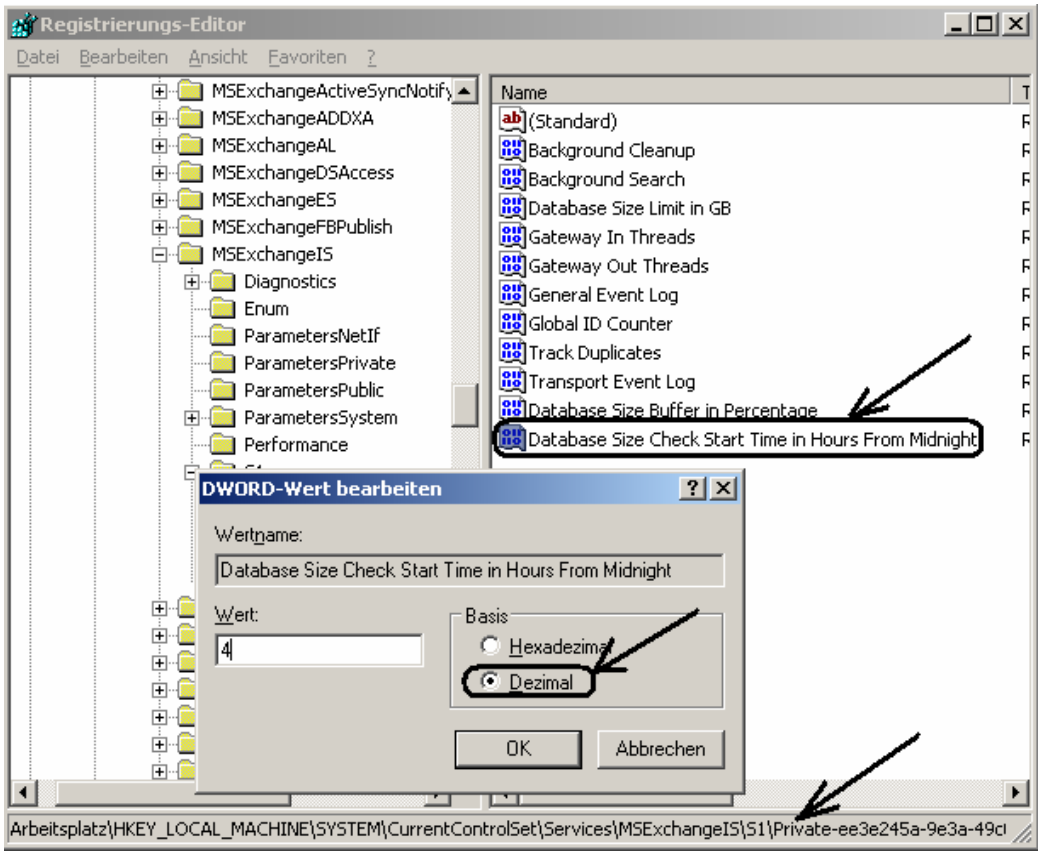
An derselben Stelle der Registrierdatenbank können Sie den DWORD-Wert **Database Size Buffer in Percentage** erstellen und z.B. dezimal mit „25“ belegen. Der Standardwert ist 10 und bedeutet, dass im Ereignisprotokoll eine Warnung erscheint, wenn 90 Prozent der eingestellten Maximalgröße des Postfachspeichers überschritten wurde. Bedenken Sie, dass Sie eine gewisse Zeit benötigen, um Gegenmaßnahmen zu ergreifen (Budget für mehr oder größere Festplatten durchsetzen, diese beschaffen und installieren…). Ein zu niedrig gesetzter Puffer wie 10 ist wahrscheinlich schneller durch weitere E-Mails ausgeschöpft, als Sie reagieren können!

...



Ein dritter DWORD-Wert namens **Database Size Check Start Time in Hours From Midnight** kann an derselben Stelle der Registrierdatenbank gesetzt werden. Wird er nicht explizit eingefügt, so wird die Datenbankgröße um 5 Uhr morgens überprüft. Soll diese Prüfung der Datenbank z.B. um 4 Uhr morgens ablaufen, so tragen Sie den dezimalen Wert „4“ ein.

...



Wird bei der Prüfung der Datenbankgröße festgestellt, dass der Maximalwert überschritten ist, so erscheint im Ereignisprotokoll unterhalb von „Anwendung“ ein Eintrag mit der ID 9689. Die Datenbank wird aber erst dann offline genommen, wenn bei der nächsten Prüfung 24 Stunden später der Maximalwert immer noch überschritten ist. Der Systemadministrator hat folglich 24 Stunden Zeit, Gegenmaßnahmen zu treffen. Pech nur, wenn samstagmorgens um 5 Uhr die erste Warnung im Ereignisprotokoll steht und der Administrator im Wochenende ist, und ein weiteres Argument dafür, den Registry-Wert „Database Size Buffer in Percentage“ nicht auf dem Standard 10 % zu belassen, sondern höher zu setzen.

Das Ändern der beiden zuletzt genannten Registry-Werte wird im Ereignisprotokoll nicht angezeigt. Doch auch hier gilt, dass die Bereitstellung der Datenbank aufgehoben und wieder aktiviert werden muss, damit die Änderungen wirksam werden.

Die drei Registry-Werte sind standardmäßig nicht vorhanden. Werden sie nicht mit dem Registrierdatenbank-Editor Regedit eingetragen, so gelten die im Programmiercode von Exchange Server verankerten Standardwerte. Sollen diese Werte geändert werden, so gibt es dafür derzeit keine direkte Unterstützung im Exchange System-Manager. Sie müssen also Regedit nutzen und bei mehreren Exchange-Servern die Werte pro Server setzen.

...

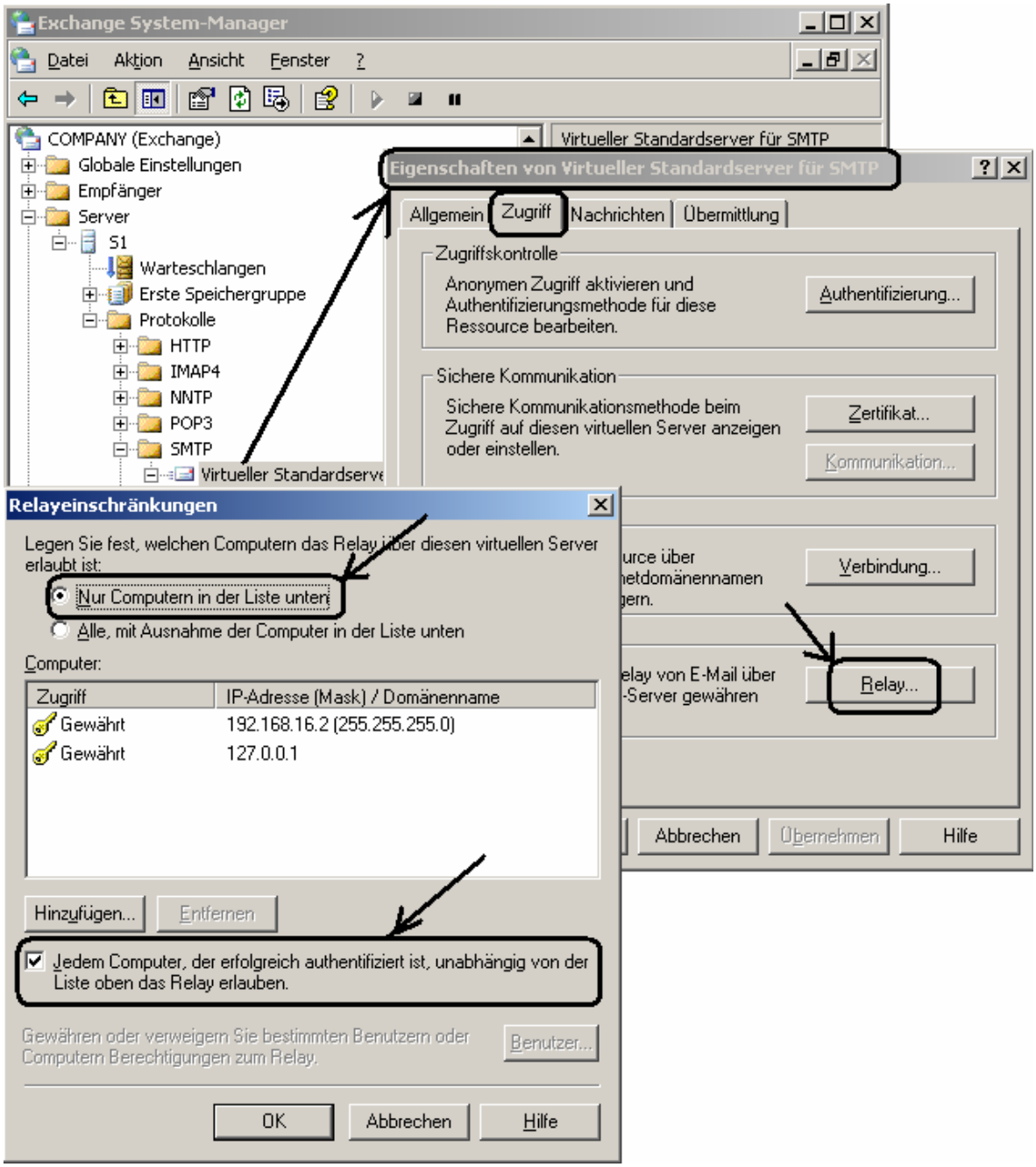
Wichtig: Wird ein Exchange-Server mittels des Setup-Wiederherstellungsparameters (setup.exe /disasterrecovery) repariert, so müssen die Registryänderungen manuell neu gesetzt werden.

Spamfilter des Exchange 2003 Service Pack 2 einsetzen

Verhindern, dass der eigene Exchange-Server als Open Relay missbraucht wird

Da das Versenden von Spam inzwischen in vielen Ländern verboten ist und drastisch bestraft wird, und natürlich, um nicht selbst die Kosten für den Versand von Massen-E-Mails zu tragen, nutzen Spammer fremde Computer („Zombies"), um Spammails zu verschicken. Dagegen nicht geschützte Computer werden dann zu Open Relays. Die Relaybeschränkungen sind im Exchange System-Manager in den Eigenschaften des virtuellen Standardservers für SMTP unter der Registerkarte „Zugriff" festgelegt:

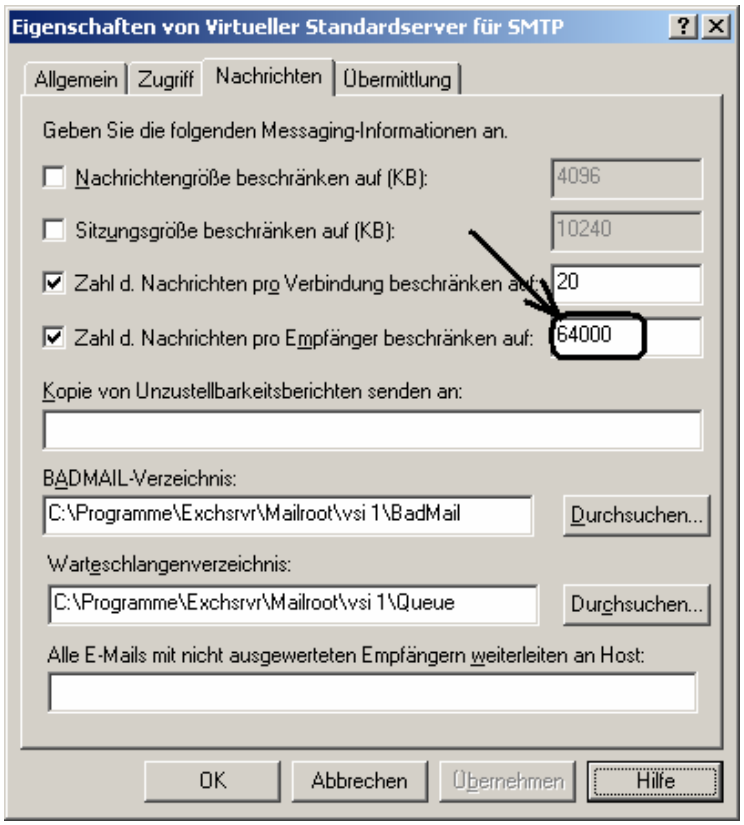
...



Durch die Voreinstellung „Nur Computern in der Liste unten“ ist standardmäßig abgesichert, dass der Exchange Server 2003 ohne Authentifizierung nicht als Open Relay missbraucht werden kann. Wenn man weitere virtuelle Standardserver für SMTP erstellt, sollte man die Relay-Einstellungen überprüfen, damit der eigene Exchange-Server nicht ungewollt zum Open Relay und später in öffentlichen Sperrlisten des Internets gelistet wird. **Die Passwörter der Benutzerkonten müssen stark sein** und nach einer bestimmten Anzahl von Hackversuchen (falschen Eingaben) das Benutzerkonto blockieren, damit ein Hacker nicht die Kontrolle über einen Computer der Domäne übernimmt und sich damit erfolgreich gegenüber dem Exchange-Server authentifizieren kann.

...

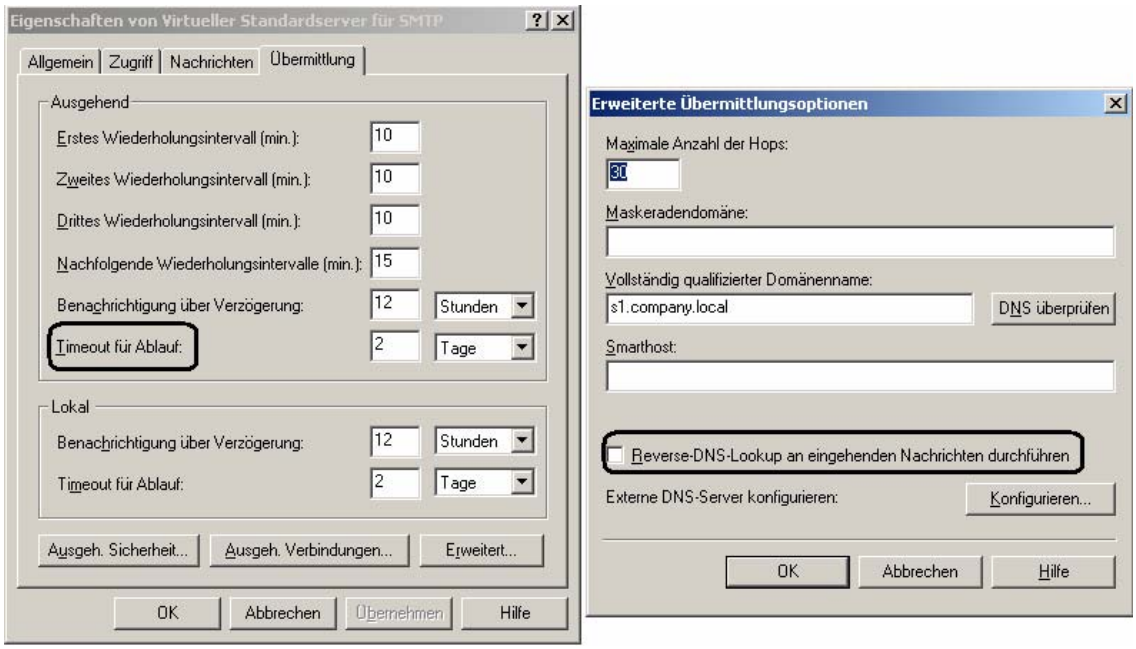
Eine weitere Maßnahme um zu verhindern, dass vom Exchange-Server Spammails verschickt werden, ist es, die **Höchstzahl der Empfänger einer pro Sitzung versendeten Nachricht zu beschränken**. Dazu öffnen Sie in den Eigenschaften des virtuellen Standardservers für SMTP die Registerkarte „Nachrichten“.



Der Standardwert 64000 ist zu hoch und sollte deutlich heruntergesetzt werden. SMTP-Standards verbieten aber, dass diese Höchstzahl auf einen Wert kleiner als 100 gesetzt wird.

Öffnen Sie bei dieser Gelegenheit einmal die Registerkarte „Übermittlung“:

...



Besteht der Verdacht, dass ein Hacker Zugriff auf den Exchange-Server bekommen hat, so können Sie temporär den „Timeout für Ablauf" heruntersetzen und z.B. das zweite Wiederholungsintervall für den Versand von E-Mails hochsetzen, damit vom Spammer bereits platzierte Nachrichten, die nicht zugestellt werden können, aus der Warteschlange getilgt werden. Klicken Sie auf die Schaltfläche „Erweitert", so können Sie die Option „**Reverse-DNS-Lookup an eingehenden Nachrichten durchführen**" aktivieren. Die IP-Adresse der eingehenden E-Mails wird dann automatisch zu einem Hostnamen aufgelöst, und dieser Hostname wird an den Header der E-Mail-Nachricht angefügt. Diese zusätzliche Information kann allein aus Beweissicherungsgründen wichtig werden, wenn man später rechtlich gegen einen Hacker vorgehen will.

Was tun, wenn Ihr eigener SMTP-Server irrtümlich auf einer schwarzen Liste als Spamversender eingetragen ist?

Wenn sich Ihre Absender beschweren, dass von ihnen versandte E-Mails beim Empfänger nicht ankommen, oder aber dass E-Mails von bestimmten Absendern nicht eingetroffen sind, obwohl diese E-Mails laut Auskunft des Versenders mit richtiger Empfängeradresse verschickt wurden, so sollten Sie überprüfen, ob Ihr eigener SMTP-Server oder aber der SMTP-Server des Versenders auf einer schwarzen Liste steht und damit geblockt wird. Unter www.kloth.net/services/dnsbl.php oder unter http://rbls.org/ tragen Sie die IP-Adresse des SMTP-Servers ein und erhalten dann eine Auflistung bekannter Webadressen mit schwarzen Listen sowie der Information, auf welchen dieser Listen der SMTP-Server eingetragen ist. Steht der SMTP-Server Ihrer eigenen Domäne auf einer dieser schwarzen Listen und wird dieser SMTP-Server von Ihrem Internet-Provider verwaltet, so müssen Sie den Provider umgehend auffordern, für Abhilfe zu sorgen. Die Sperrlistenanbieter bieten auf ihrer Webseite dazu in der Regel ein Formular an, jedoch kann es dauern, bis der irrtümlich eingetragene SMTP-Server von allen schwarzen Listen gelöscht ist. Hilfreich ist es dann, wenn in

...

weiser Voraussicht ein Ausfall-SMTP-Server konfiguriert wurde und einspringen kann.

IMF Version 2 in Exchange 2003 SP2

IMF (Intelligent Message Filter) schützt Ihren SMTP-Server vor Überflutung mit Spam. Spam ist übrigens die Abkürzung für „spiced pork and ham". Durch einen Sketch in Monty Python´s Flying Circus ist der Begriff aber ein Synonym für unverlangt per E-Mail zugesandte Werbung geworden. Wenn Ihr Internet-Provider selbst einen Spamfilter anbietet, sollten Sie zuerst diesen externen Spamfilter aktivieren und testen. Spammails werden dadurch bereits beim Provider ausgesondert und belasten dann weder die Leitung zum Provider noch Ihren Exchange-Server.

Reihenfolge der Filter, die eine Eingangsnachricht durchläuft

IMF scannt E-Mails, nachdem sie alle anderen Exchange-Filter durchlaufen haben, bevor sie aber in den Informationsspeicher gelangen. Diese anderen Filter können ein Verbindungsfilter, ein Empfängerfilter oder ein Absenderfilter sein. Eine hereinkommende Nachricht durchläuft also nacheinander folgende Filter, wenn sie aktiviert wurden:

- **Verbindungsfilter**: Nutzt die Sperrlisten von externen Blacklist-Anbietern oder selbst erstellte Sperrlisten.
- **Empfängerfilter**: Sperrt E-Mails an bestimmte E-Mail-Adressen wie z.B. info@com-pany.com oder auch an Empfänger, die nicht im Active Directory vorhanden sind.
- **Absenderfilter**: Sie können z.B. generell E-Mails ohne Absenderadresse verwerfen.
- **IMF Gateway-Schwellenwert**: Sortiert als Spam bewertete Nachrichten bereits aus, bevor sie in den Exchange-Informationsspeicher gelangen.
- **IMF Junk-E-Mail-Schwellenwert**: E-Mails mit einer Bewertungszahl größer als diesem Schwellenwert, die noch nicht durch den Gateway-Schwellenwert aussortiert wurden, landen beim Anwender im Outlook-Ordner Junk-E-Mail statt in dessen Posteingang.

Unter Outlook 2003 kann der Anwender schließlich noch über die Junk-E-Mail-Optionen sowohl eine Liste „Blockierte Absender" als auch eine Liste „Sichere Absender" pflegen, um vom IMF nicht als Spam klassifizierte Nachrichten auszusondern oder aber Nachrichten, die vom IMF Junk-E-Mail-Schwellenwert als Spam klassifiziert wurden und deshalb im Outlook Junk-E-Mail-Ordner landen würden, zukünftig wieder in den Posteingang einzustellen.

...

IMF und POP Connector von Small Business Server 2003

Der IMF von Exchange Server 2003 setzt voraus, dass eingehende E-Mails dem Exchange Server via SMTP übermittelt werden. Wird unter Small Business Server 2003 jedoch der integrierte POP Connector eingesetzt, so passieren diese E-Mails nicht den IMF. Der Artikel "HOW TO: Exchange Spam Filterung mit der Intelligenten Nachrichtenfilterung (IMF) bei POP basierter Emailabholung" bietet eine Lösung für dieses Problem:

http://dnn.sbsfaq.de/SBS2003/Exchange2003/HOWTOSpamFilterungmitIMFbeiPOPunddynIP/tabid/148/Default.aspx

SCL Spam Confidence Level

Der IMF klassifiziert eingehende E-Mails nach einer Bewertungszahl (Raw Score) zwischen 1 und 9 mit der Bezeichnung „**Spam Confidence Level**“, abgekürzt **SCL**. Je größer diese Zahl ist, desto wahrscheinlicher ist es, dass es eine Spammail ist. Wie wählt man den richtigen SCL-Schwellenwert aus? Setzt man den SCL-Schwellenwert zu klein (z.B. 2), so werden zu viele legitime Nachrichten als Spam bewertet und blockiert („falsche Positive“). Setzt man ihn zu hoch (z.B. 8), werden zu wenige Spammails als solche erkannt und folglich nicht ausgefiltert. Der Schwellenwert hängt stark vom betriebenen Geschäft ab. Beschäftigt sich das Unternehmen z.B. mit dem Vertrieb von Dessous, so würde ein niedriger Schwellenwert wahrscheinlich bewirken, dass wichtige Nachrichten von Lieferanten oder Kunden als Spam blockiert würden, weil sie Worte wie „Oberweite“ enthalten, die der Spamfilter als sexistisch deklarieren würde.

Es ist ratsam, nicht gleich mit einem zu niedrigem SCL-Schwellenwert für das Gateway zu beginnen und auch den Schwellenwert für die Junk-E-Mail-Konfiguration anfangs nicht zu niedrig zu setzen, damit nicht schlagartig zu viele „falsche Positive“ ausgefiltert werden und dann vom Administrator manuell an die Empfänger weitergeleitet werden müssen. Werden die durch Spamfilter ausgesonderten Nachrichten nicht zeitnah kontrolliert, so besteht die Gefahr, dass zeitkritische Geschäftsnachrichten unerkannt irgendwo im System hängen bleiben. Das führt sehr schnell dazu, dass die Anwender das Vertrauen in das Mailsystem verlieren, und in jedem Fall wird ein Anwender lieber die ein oder anderer unerwünschte Werbenachricht löschen, als sich unsicher zu sein, ob wichtige Geschäftsnachrichten abhanden kommen.

Spam-Nachrichtenbehandlung mit selbst versendeten Spamnachrichten testen

Um überhaupt feststellen zu können, ob und wie sich die verschiedenen Parameter des IMF auswirken, sollten Sie zuerst einen Weg finden, Spam-Testnachrichten an den Exchange Server zu versenden, ohne dass diese zuvor z.B. durch einen Spamfilter Ihres Providers ausgefiltert werden. Dazu können Sie ein Tool wie **Smtpsend** verwenden. Sie finden es auf der DVD des Buches „Integrationshandbuch Microsoft-Netzwerk“ im Verzeichnis Tool\SMTPsend oder unter

...

www.swsoft.co.uk. Kopieren Sie das Tool Smtpsend.exe nach C:\ auf den Exchange-Server und erzeugen Sie dort eine Datei test.txt mit folgendem Inhalt:

From: spamversender@spamcompany.com

To: administrator@company.local

Subject: Testnachricht mit dem Wort VIAGRA im Betreff

Kaufen Sie VIAGRA!

Die Syntax des Tools Smtpsend.exe zum Versenden einer Nachricht lautet:

smtpsend.exe Mailserver Absender Empfänger Nachrichtendatei

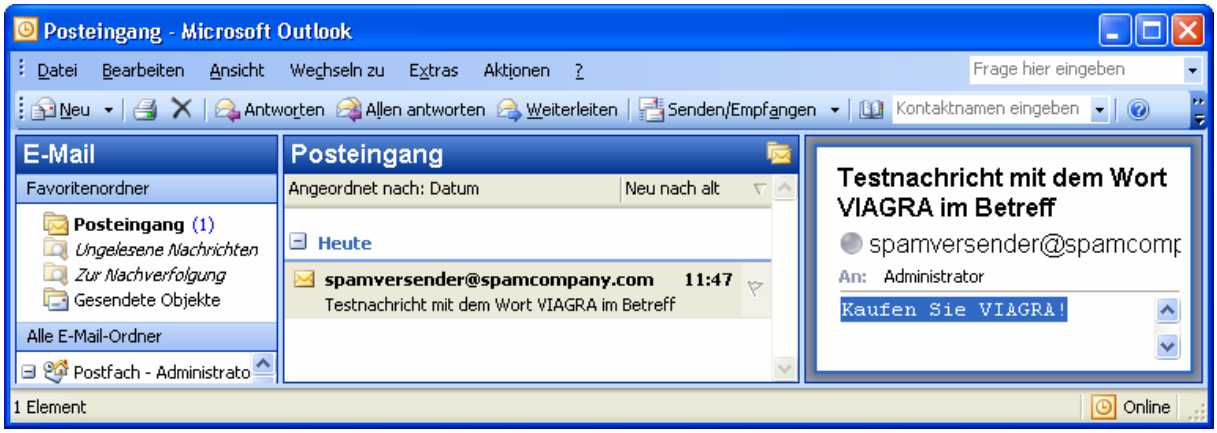
Als Nachrichtendatei verwenden wir die erzeugte Datei test.txt. Sie besteht aus einer From-Zeile, einer To-Zeile, einer Subject-Zeile und dem eigentlichen Nachrichtentext „Kaufen Sie VIAGRA!“, wobei der Nachrichtentext durch eine Leerzeile von der Subject-Zeile getrennt sein muss.

Öffnen Sie nun eine Command-Box („Start – Ausführen – cmd“) und wechseln Sie direkt nach C:\, um keine Verzeichnispfade eingeben zu müssen (das reduziert die möglichen Fehlerquellen). Hat der Exchange-Server die IP-Adresse 192.168.16.2 und der Administrator die SMTP-Adresse administrator@company.local, so senden Sie mit dem nachfolgenden Befehl den Inhalt der Nachrichtendatei test.txt an das Exchange-Postfach des Administrators:

smtpsend.exe 192.168.16.2 spamversender@spamcompany.local administrator@company.local test.txt

Wenn sich der Administrator der Domäne “Company” an einem Client anmeldet und Outlook startet, sollte diese Spam-Testnachricht angezeigt werden:

...



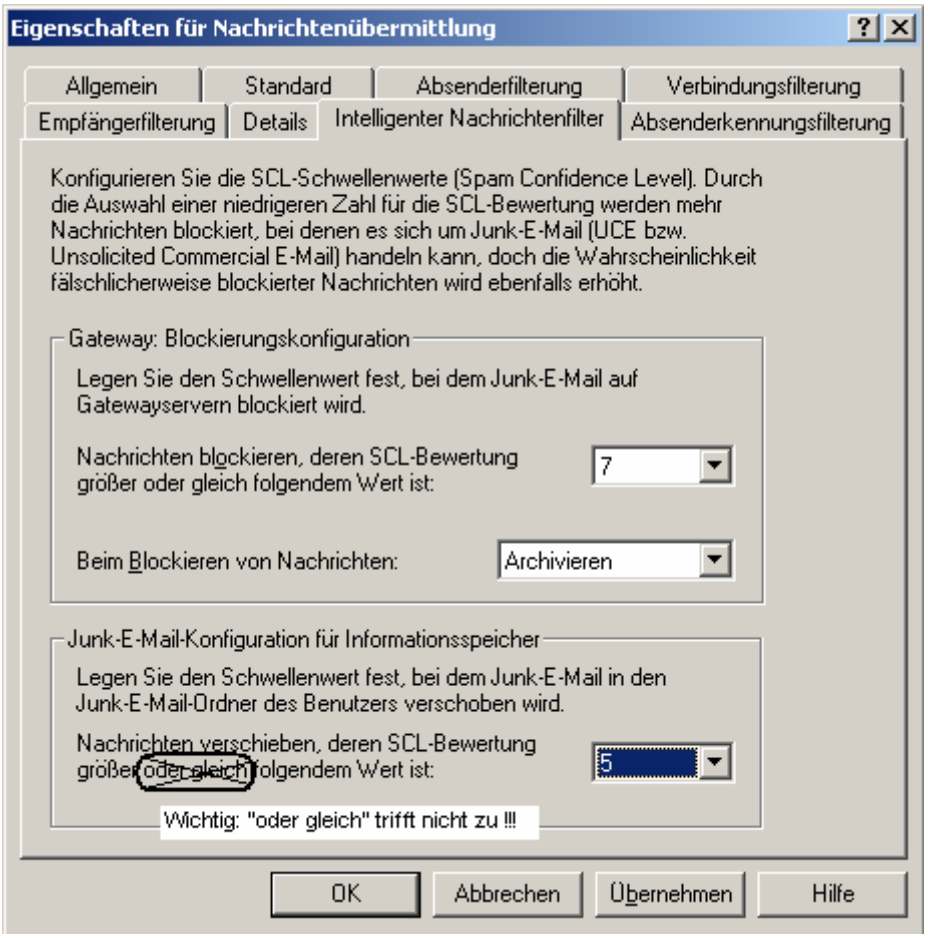
IMF konfigurieren und aktivieren

Der IMF ist standardmäßig deaktiviert. Öffnen Sie im Exchange System-Manager unter „Globale Einstellungen“ mit der rechten Maustaste die Eigenschaften der „Nachrichtenübermittlung“.

Das Fenster „Eigenschaften für Nachrichtenübermittlung“ bietet für alle Spamfilter eine Registerkarte, in der die Filter konfiguriert werden. Merken Sie sich an dieser Stelle: Die **Konfigurierung der verschiedenen Filter** erfolgt hier, die **Aktivierung** oder **Deaktivierung** der hier konfigurierten Filter erfolgt nicht hier, sondern über die Eigenschaften des virtuellen Standardservers für SMTP.

...

In der Registerkarte „Intelligenter Nachrichtenfilter“ stellen Sie nun einen SCL-Schwellenwert für das Gateway und für die Junk-E-Mail-Konfiguration ein. SCL ist die Abkürzung für „Spam Confidence Level“. Der Gateway SCL-Schwellenwert fängt alle E-Mails ab, die einen gleichgroßen oder höheren SCL-Wert haben. Solange im Feld „Beim Blockieren von Nachrichten“ die Einstellung „Keine Aktion“ nicht durch „Ablehnen“, „Archivieren“ oder „Löschen“ ersetzt wird, werden alle Nachrichten zugestellt. Sie sollten die Option „Archivieren“ auswählen.



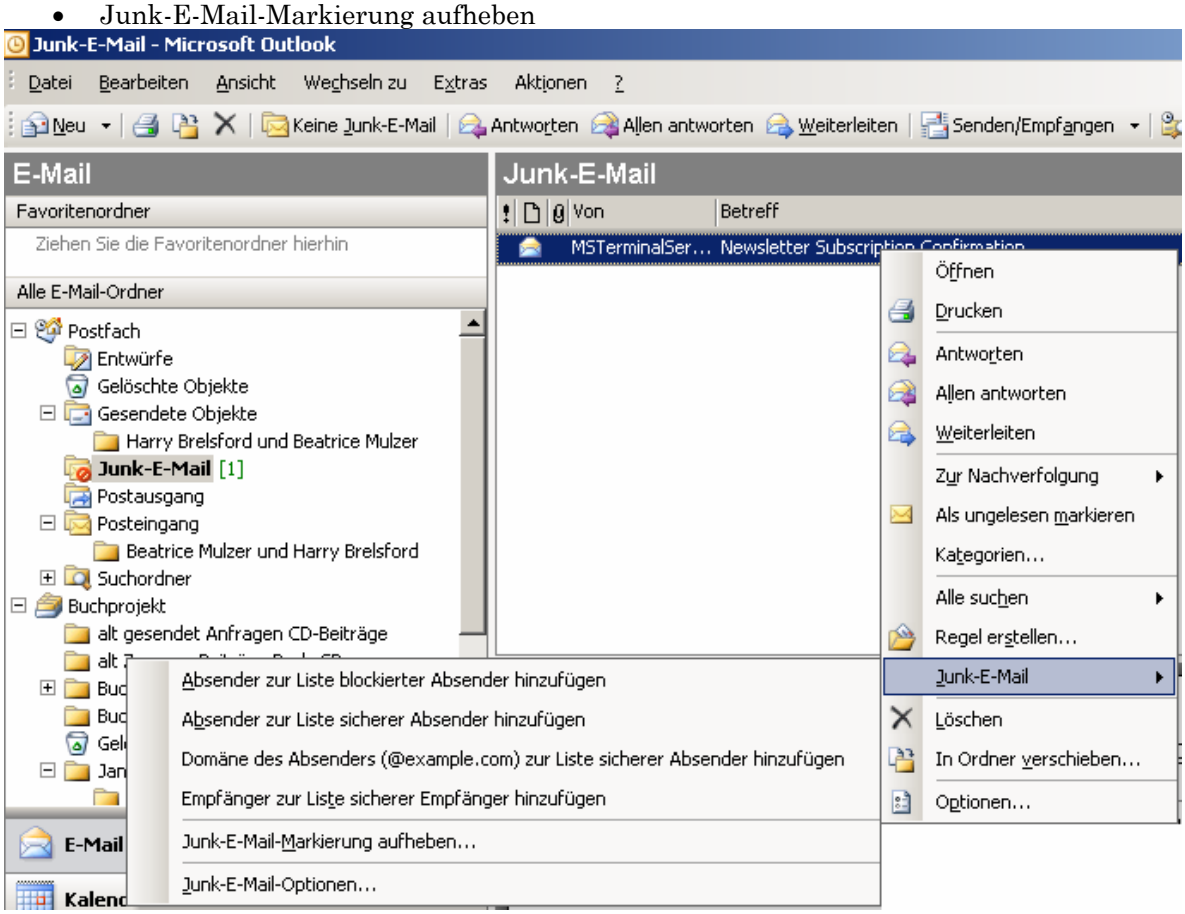
Es ist ratsam, nicht gleich mit einem zu niedrigem SCL-Schwellenwert für das Gateway zu beginnen und auch den Schwellenwert für die Junk-E-Mail-Konfiguration anfangs nicht zu niedrig zu setzen, damit nicht schlagartig zu viele „falsche Positive“ ausgefiltert werden und dann vom Administrator manuell an die Empfänger weitergeleitet werden müssen. Beginnen Sie stattdessen z.B. mit einem Gateway-Schwellenwert „7“ und setzen Sie diesen Wert schrittweise herunter, wenn weiterhin zu viele Spam-Nachrichten in die Postfächer der Anwender gelangen.

Der SCL-Schwellenwert für die Junk-E-Mail-Konfiguration gibt an, ab wann E-Mails, die vom ersten Schwellenwert nicht direkt abgefangen wurden, beim Anwender nicht mehr regulär im Posteingang erscheinen sollen, sondern stattdessen im Junk-E-Mail-Ordner von Outlook. Der Anwender muss dann selbst entscheiden, ob es sich um Spam handelt. Er kann dazu unter

...

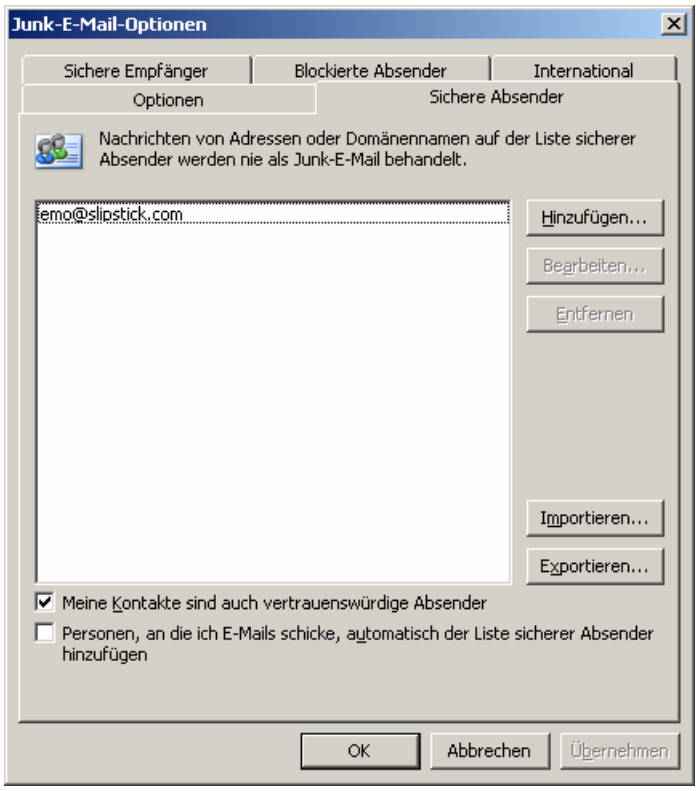
Outlook 2003 die betroffene Nachricht mit der rechten Maustaste anklicken und im Menüpunkt „Junk-E-Mail“ eine der folgenden Optionen wählen:

- Absender zur Liste blockierte Absender hinzufügen
- Absender zur Liste sicherer Absender hinzufügen
- Domäne des Absenders (@example.com) zur Liste sicherer Absender hinzufügen
- Empfänger zur Liste sicherer Empfänger hinzufügen
- Junk-E-Mail-Markierung aufheben



Außerdem kann der Anwender über die „Junk-E-Mail-Optionen“ selber eine Liste sicherer Absender (Whitelist) oder blockierter Absender (Blacklist) erstellen. Speziell über die von ihm gepflegte Liste der sicheren Absender kann der Anwender erreichen, dass E-Mails von bestimmten Absendern, deren SCL-Bewertung den vom Administrator eingetragenen zweiten Schwellenwert überschreiten, wieder im Posteingang statt im Ordner Junk-E-Mail erscheinen.

...



Wichtig: Die Anwender müssen im Umgang mit den Optionen des Ordners Junk-E-Mail geschult werden, bevor Sie den SCL-Schwellenwert der Junk-E-Mail-Konfiguration heruntersetzen. Sie sollten dazu eine bebilderte Kurzanleitung verfassen und an die Mitarbeiter verschicken.

Wird der Schwellenwert für die Junk-E-Mail-Konfiguration nicht mindestens 2 Einheiten kleiner als der Gateway-Schwellenwert gesetzt, so kommt nur der Gateway-SCL-Schwellenwert zum Tragen, da dann Mails mit einem SCL-Wert größer oder gleich dem Gateway-Schwellenwert gar nicht in das Postfach des Benutzers gelangen, sondern bereits abgefangen werden, bevor sie in den Postfachspeicher gelangen.

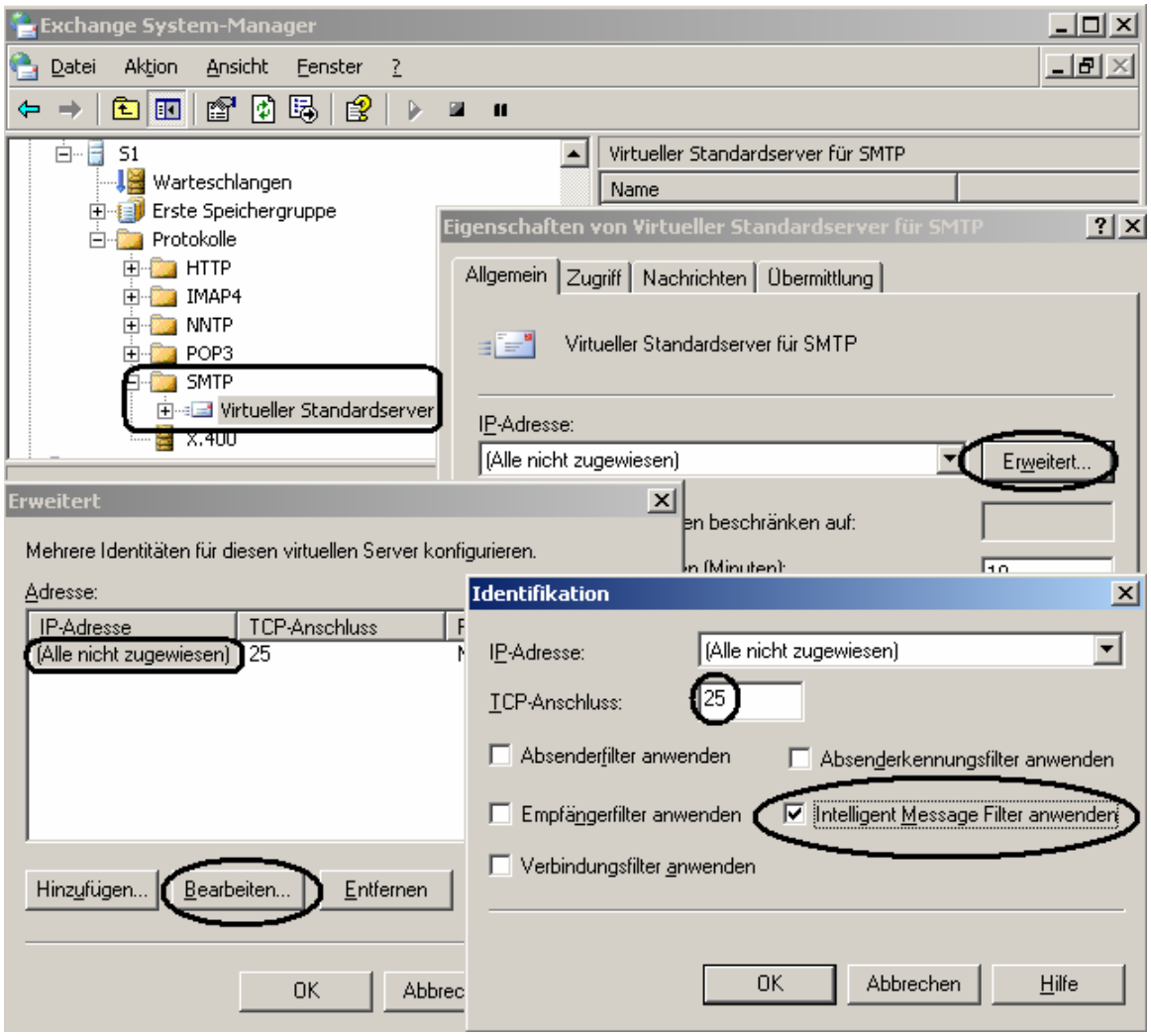
Wichtiger Hinweis:

In der Registerkarte „Intelligenter Nachrichtenfilter“ ist die Beschreibung „Nachrichten verschieben, deren SCL-Bewertung größer oder gleich folgendem Wert ist“ falsch!

Richtig ist, dass nur Nachrichten in den Outlook-Ordner „Junk-E-Mail“ verschoben werden, die **größer** (!!!) als der eingetragene SCL-Wert sind, und nicht solche mit einer SCL-Bewertung gleich dem eingetragenen Wert. Wir werden dieses später testen, indem wir unterschiedliche SCL-Schwellenwerte eingeben und Spam-Testnachrichten versenden. Beginnen Sie deshalb in der Testumgebung mit einem Wert, der zwei Einheiten unter dem Gateway-Schwellenwert liegt: z.B. „5“, wenn als Gateway-Schwellenwert „7“ gewählt wurde.

...

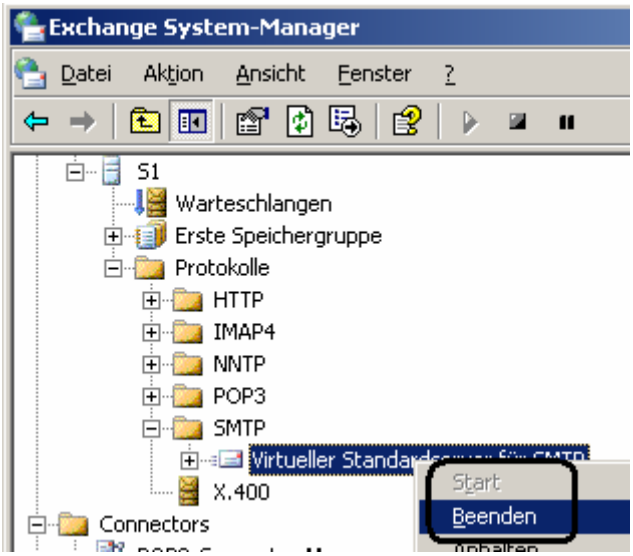
Um den IMF nun zu aktivieren, öffnen Sie im Exchange System-Manager unterhalb Ihres Exchange Servers die Protokolle, dort SMTP und über die rechte Maustaste die Eigenschaften des virtuellen Standardservers für SMTP. In der Registerkarte „Allgemein“ klicken Sie auf die Schaltfläche „Erweitert“, wählen die Identität des virtuellen Servers - in der Regel gibt es hier nur diejenige mit der Bezeichnung „(Alle nicht zugewiesenen)“ -, klicken auf „Bearbeiten“ und aktivieren im sich öffnenden Identifikationsfenster die Option „Intelligent Message Filter anwenden.“ Wenn im Feld TCP-Anschluss kein Port (i.d.R. der Port 25) eingetragen ist, erhalten Sie eine Meldung, dass mindestens ein Port angegeben sein muss.



Wie Sie den anderen Optionen des Fensters „Identifikation“ entnehmen können, werden an dieser Stelle des Exchange System-Managers alle Filter aktiviert oder deaktiviert, die unter „Globale Einstellungen – Nachrichtenübermittlung“ konfiguriert werden. Generell gilt hier: Um sicherzugehen, dass Änderungen an den Einstellungen eines virtuellen Standardservers für SMTP aktiv werden, sollten Sie den virtuellen Standardserver für SMTP über die rechte Maustaste zuerst

...

beenden und dann wieder starten.



Merken Sie außerdem: Änderungen an den SCL-Schwellenwerten eines Postfachspeichers werden generell erst dann wirksam, wenn die Bereitstellung des Postfachspeichers aufgehoben und er dann wieder bereitgestellt wird (Postfachspeicher mit der rechten Maustaste anklicken und die entsprechenden Befehle auswählen). Führen Sie diesen Schritt jetzt durch.

Die als SPAM erkannten und archivierten Mails einsehen und bearbeiten

Wurde in der Registerkarte „Intelligenter Nachrichtenfilter“ bei der Gateway-Konfiguration die Option „Archivieren“ ausgewählt, so werden als Spam deklarierte E-Mails standardmäßig im Ordner C:\Programme\Exchsrvr\Mailroot\vsi x\UceArchive abgelegt, wobei das Unterverzeichnis „vsi x“ für den x-ten „Virtuellen Standardserver für SMTP“ steht. Wurden weitere virtuelle SMTP-Server erzeugt (dazu klickt man mit der rechten Maustaste auf „Protokolle – SMTP“ und wählt den Befehl „Neu – Virtueller SMTP-Server“), so kann es hier weitere Unterverzeichnisse geben. Das Unterverzeichnis UceArchive wird jedoch erst erstellt, wenn die erste Spammail eingeht. UCE ist die Abkürzung für „unsolicited commercial e-mail“. Außerdem gibt es noch die Abkürzung UBE für „unsolicited bulk e-mail“.

Speicherort des Spamarchivs verlegen

...

Ist mit hohem Spamaufkommen zu rechnen, so sollten Sie das Spam-Archivverzeichnis UCEArchive auf eine separate Partition oder sogar eine andere Festplatte verlegen, damit die Partition, die die Exchange-Datenbanken enthält, nicht unkontrolliert volläuft. Dazu erstellen Sie in der Registrierdatenbank unter HKEY_Local_Machine\Software\Microsoft\Exchange\ContentFilter einen neuen Zeichenfolgewert namens **ArchiveDir** und geben einen vollständigen Pfad ein, z.B. E:\Spamarchiv.

Wenn nicht sichergestellt ist, dass ein Administrator täglich das Spamarchiv kontrolliert, kann es außerdem in eine den Anwendern zugängliche Freigabe verlegt werden. Die Anwender können dann selbst nachsehen, wenn sie den Verdacht haben, dass eine dringend erwartete Nachricht in das Spamarchiv aussortiert wurde. Diese Vorgehensweise muss jedoch mit der Unternehmensleitung vorher abgesprochen werden, da die Gefahr besteht, dass dann vertrauliche Nachrichten im Spamarchiv landen und für jeden Anwender einsehbar sind.

Es ist auch denkbar, ein Skript zu erstellen, das über den Taskmanager automatisch täglich abläuft und alle Inhalte des Spamarchivs löscht, die älter als z.B. 30 Tage sind. Beim del-Befehl gibt es leider keinen Parameter, um Dateien älter als x Tage zu löschen. Das Tool Robocopy des Windows Resource Kits ermöglicht aber z.B., Dateien älter als x Tage in ein anderes Verzeichnis zu verschieben, wo sie anschließend mit dem del-Befehl gelöscht werden können.

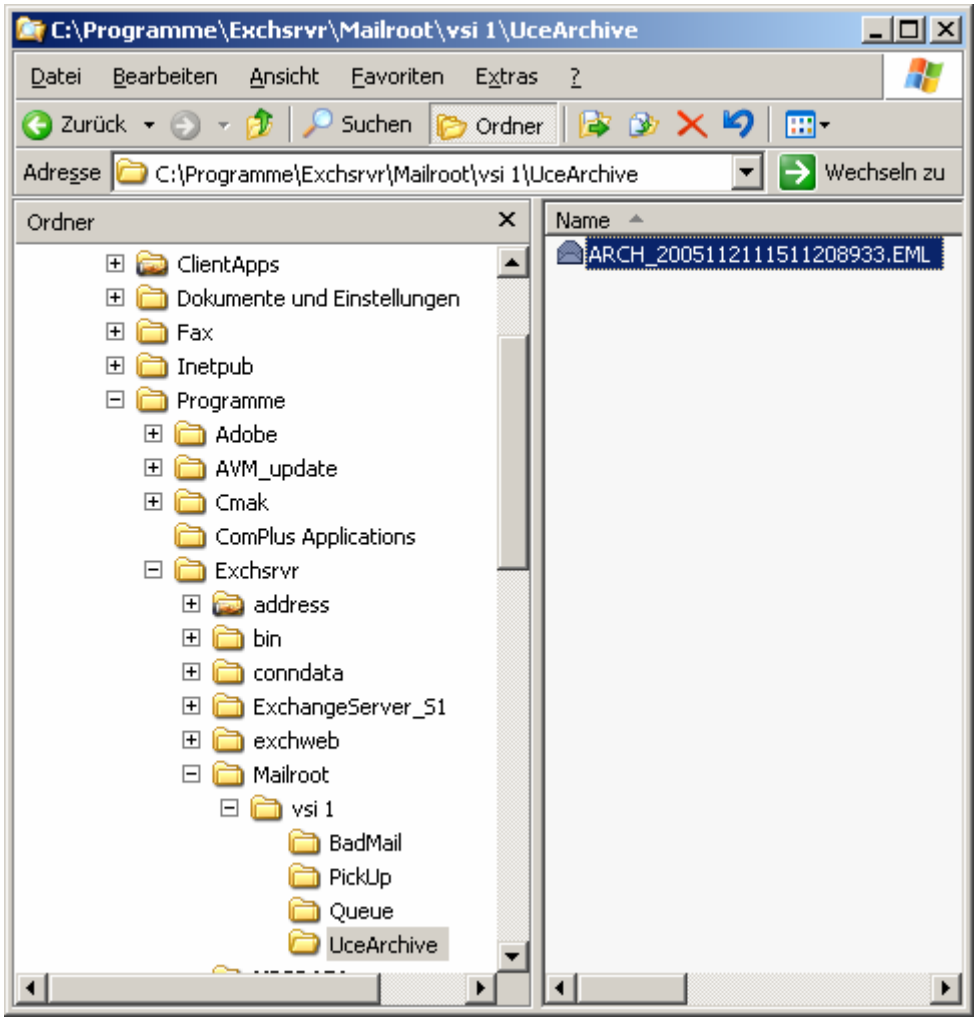
Das Unterverzeichnis UceArchive wird automatisch generiert, wenn die erste Spammail eingeht. Wollen Sie nicht auf den Eingang einer Spammail warten und IMF sofort testen, müssen Sie selbst Spam-Nachrichten an den Exchange-Server erfolgreich versenden, ohne dass diese zuvor z.B. durch einen Spamfilter Ihres Providers ausgefiltert werden. Dazu nutzen Sie erneut das Tool Smtpsend mit derselben Syntax wie zuvor:

smtpsend.exe 192.168.16.2 spamversender@spamcompany.local administrator@company.local test.txt

Hinweis: Lassen Sie die Command-Box offen, damit Sie den Befehl mit der Funktionstaste F3 später erneut absenden können, ohne ihn wieder einzutippen. Wir werden noch einige Tests mit unterschiedlichen SCL-Schwellenwerten durchführen.

Das Verzeichnis C:\Programme\Exchsrvr\Mailroot\vsi 1\UceArchive sollte jetzt erzeugt worden sein und die selbst zugesandte Spam-Nachricht enthalten:

...



Die in das UceArchive ausgefilterten Nachrichten müssen jedoch vom Administrator regelmäßig durchgesehen werden, um zu überprüfen, ob es sich wirklich um Spamnachrichten handelt oder um „falsche Positive“. Falsche Positive sind als Spam aussortierte Nachrichten, bei denen es sich in Wirklichkeit nicht um Spam handelt. Da es sich um wichtige Geschäftsinformationen handeln kann, müssen sie dem Anwender nachträglich zeitnah zugestellt werden, während die richtig als Spam erkannten Objekte des Verzeichnisses UceArchive regelmäßig gelöscht werden sollten, damit die Festplatte des Servers nicht vollläuft.

IMF Archive Manager zum Verwalten des UCE-Archivs

Im Spamarchiv ACEArchive werden die ausgesonderten Nachrichten als EML-Dateien abgelegt. Eine EML-Nachrichtendatei kann mit jedem Editor wie z.B. Notepad geöffnet werden. Ein Doppelklick öffnet diese Nachrichtendatei mit Outlook Express, und somit können neben der

...

Nachricht selbst auch Nachrichtenanhänge behandelt werden. Jedoch ist Outlook Express nicht als Client in Exchange Server eingebunden. Stellt man fest, dass eine als Spam ausgesonderte Nachricht eine wichtige Geschäftsnachricht ist und dem Anwender nachträglich zugestellt werden muss, so ist das aus Outlook Express heraus nicht möglich.

Nachdem eine EML-Datei des IMF-Archivs eingesehen wurde, kann sie im Windows Explorer gelöscht werden, denn sie ist nicht durch den Exchange Server oder durch IMF blockiert. Eine Nachricht, die irrtümlich als Spam aussortiert wurde, könnte nun in den SMTP Pickup-Ordner zurückverschoben werden, der sich standardmäßig unter „c:\Programme\exchsrvr\mailroot\vsi 1“ befindet. In dieses Verzeichnis stellt die IIS/Exchange SMTP Engine alle E-Mails zum weiteren Routing ein. Damit jedoch diese Nachricht nicht gleich wieder durch IMF in das Spamarchiv aussortiert wird, muss zuerst der SCL-Gateway-Schwellenwert niedriger eingestellt werden. Außerdem muss nach einer derartigen IMF-Änderung der Postfachspeicher neu gestartet werden.

Um die Nachrichten im IMF-Spamarchiv komfortabel bearbeiten (einsehen, löschen nachträglich zustellen) zu können, können Sie das kostenlose Tool IMF Archive Manager auf dem Exchange-Server installieren.

http://workspaces.gotdotnet.com/imfarchive

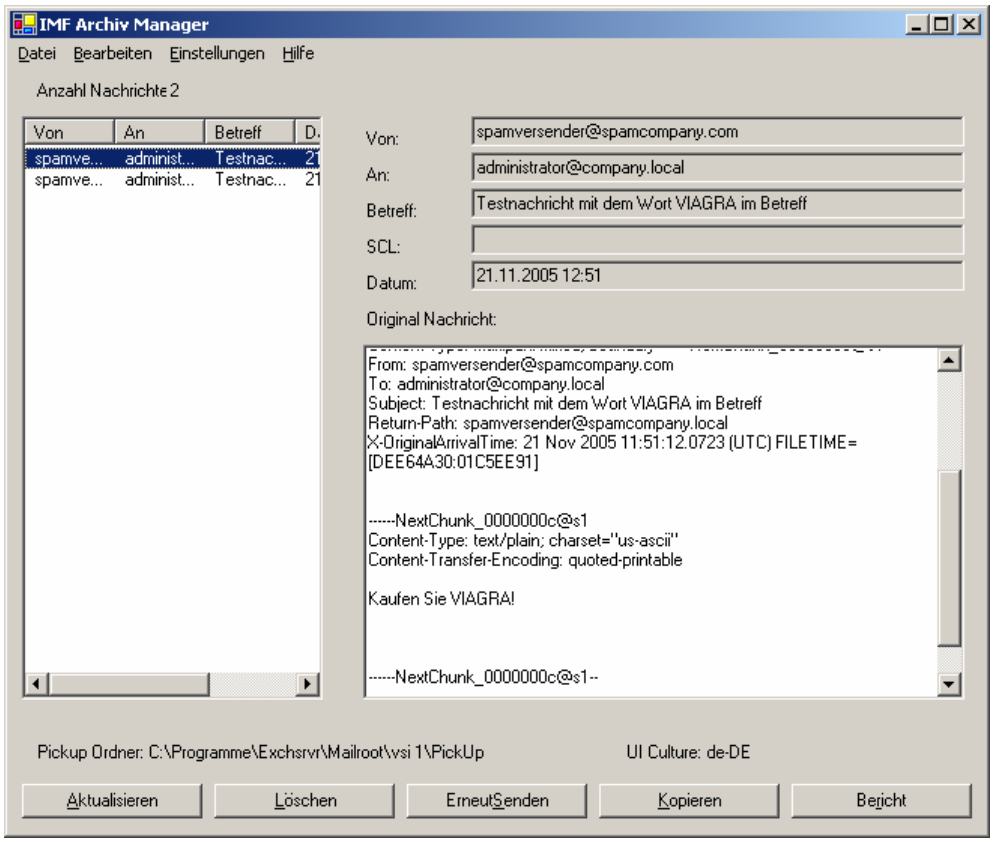
http://blogs.technet.com/exchange/archive/2004/05/26/142607.aspx

http://www.gotdotnet.com/workspaces/workspace.aspx?id=e8728572-3a4e-425a-9b26-a3fda0d06fee

http://www.slipstick.com/emo/2004/up040610.htm#monitor

Beim Start der Installationsdatei IMFFilterManager.exe müssen Sie den Ort des Verzeichnisses UceArchive sowie des Verzeichnisses Pickup angegeben. Beide Verzeichnisse finden Sie standardmäßig unter „C:\Programme\Exchsrvr\Mailroot\vsi 1“. Danach zeigt der IMF Archiv Manager die ausgefilterten Nachrichten und deren Inhalt an.

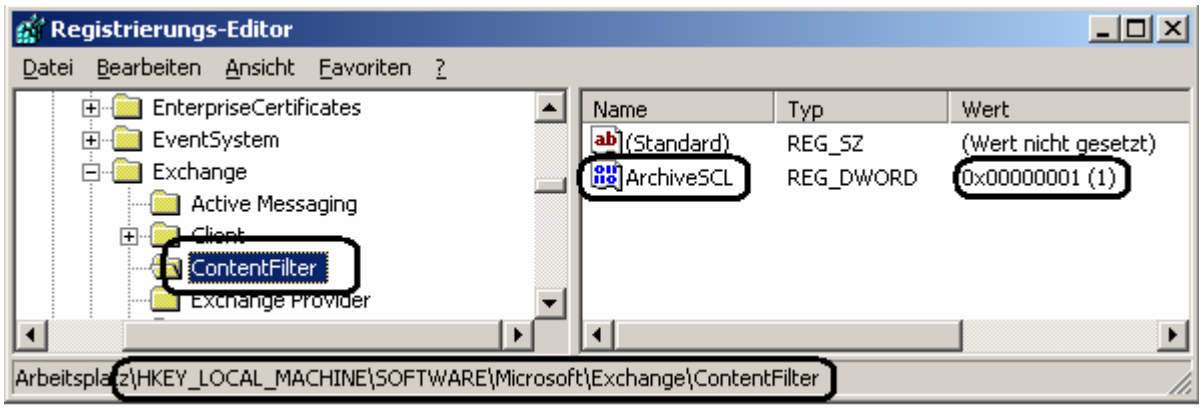
...



Stellen Sie im IMF Archiv Manager aufgrund des Inhalts einer Nachricht fest, dass es sich um eine „falsche Positive“ handelt, so klicken Sie auf „ErneutSenden“. Dadurch wird die Nachricht unverändert an den Empfänger gesendet und aus dem UceArchive entfernt. Die richtig als Spam gefilterten Nachrichten löschen Sie über die Schaltfläche „Löschen“. Über die Schaltfläche „Bericht“ kann eingestellt werden, dass ausgefilterte E-Mails an eine externe Adresse verschickt und anschließend im Spamarchiv gelöscht werden.

Standardmäßig zeigt der IMF Archiv Manager nicht den vom Gateway-Filter ermittelte SCL-Wert an. Das SCL-Feld ist in der obigen Abbildung leer. Um dieses zu ändern, müssen Sie eine weitere Änderung in der Registrierdatenbank des Exchange-Servers vornehmen. Erzeugen Sie unter HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange zuerst den neuen Schlüssel **ContentFilter**, legen Sie darunter den DWORD-Wert **ArchiveSCL** neu an und weisen Sie ihm den Wert „1“ zu:

...

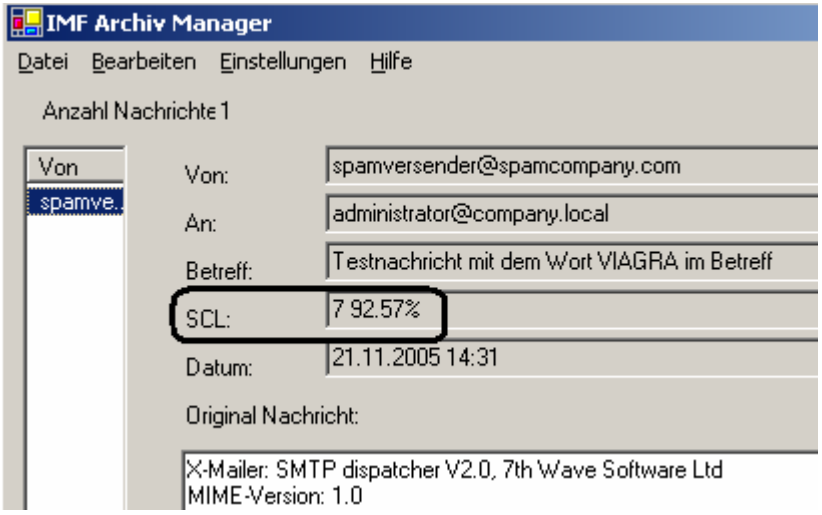


In den Release Notes des Exchange Server 2003 SP2 finden Sie dazu folgende Aussagen: *„Microsoft Exchange Intelligent Message Filter Exchange Server 2003 SP2 does not create the registry key named ContentFilter under HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange during an upgrade from Exchange Server 2003 or Exchange Server 2003 SP1, where Intelligent Message Filter version 1 was not previously installed. Therefore, to obtain an extended functionality (for example, change the Archive directory), you must manually create the HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange\ContentFilter key and restart the SMTP service.*

After the restart of SMTP, all the values created under this key are automatically picked up and no additional restarts of services are required. If you are upgrading the computer where Intelligent Message Filter version 1 was previously installed, no action is required because the registry key is preserved during the upgrade."

Beim SCL-Wert handelt es sich um eine Erweiterung des Nachrichtenkopfes. Setzt man den DWORD-Wert **ArchiveSCL** auf „0", so wird der SCL-Wert nicht mitgespeichert. Damit der neue Schlüssel ContentFilter wirkt, muss der SMTP-Dienst neu gestartet werden. Außerdem wird der SCL-Wert von bereits gefilterten Nachrichten nicht nachträglich angezeigt. Sie müssen deshalb mit dem Tool Smtpsend erneut eine Spammail erzeugen, um den Erfolg dieser Registry-Manipulation zu überprüfen.

...



Das Feld **SCL** zeigt jetzt nicht nur den SCL-Wert „7“ an, sondern dahinter die prozentuale Wahrscheinlichkeit, mit der es sich bei dieser Nachricht um Spam handelt.

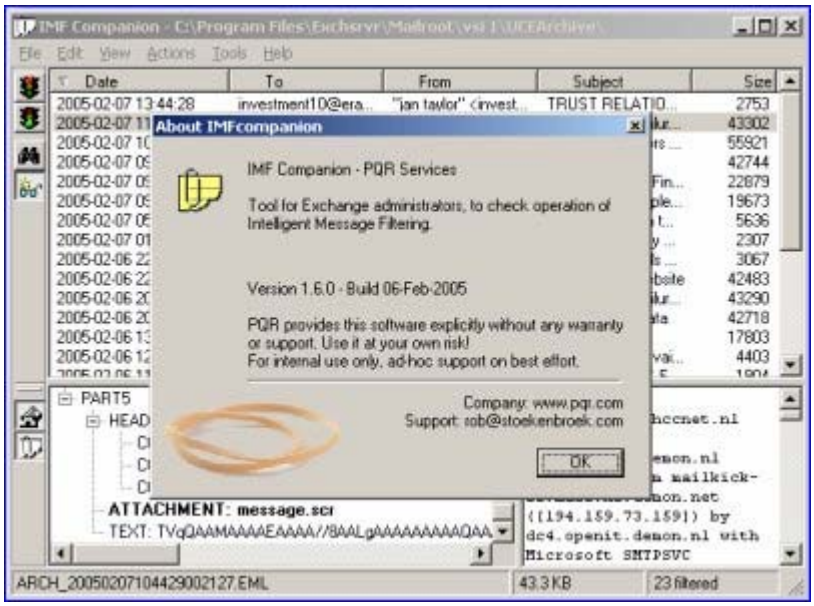
IMF Companion als Alternative zum IMF Archive Manager

Ein anderes kostenloses Tool zum Verwalten des Spamarchivs ist der IMF Companion.

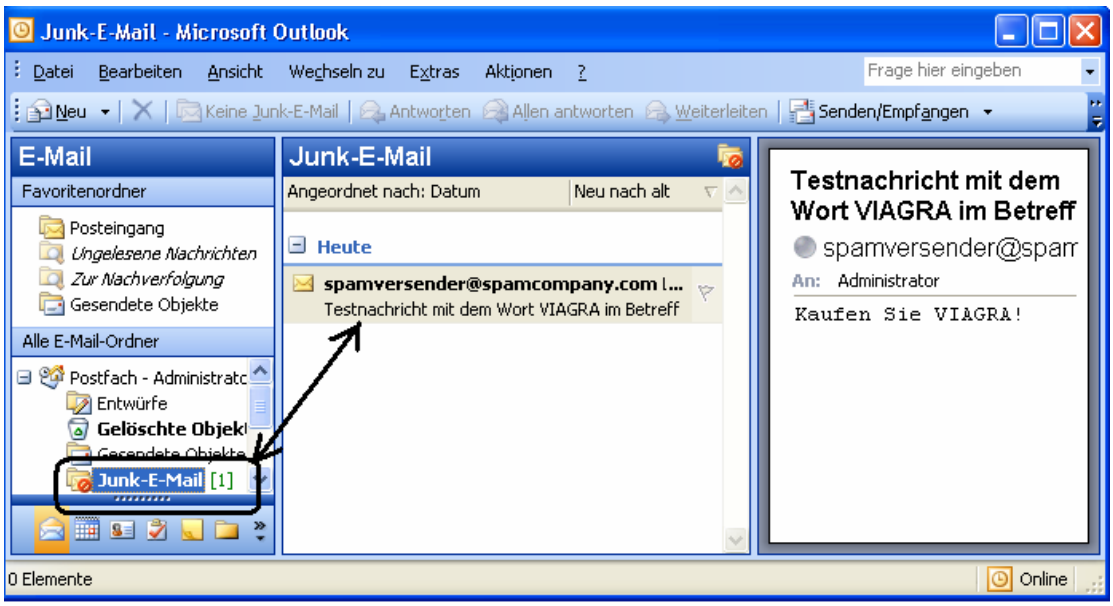
http://stoekenbroek.com/imfcompanion.htm

Es handelt sich im Gegensatz zum IMF Archive Manager um eine MSI-Datei mit sauberer Installationsroutine und eigenem Icon. Die Oberfläche wirkt aufgeräumter und die Spalten können besser eingesehen werden. Außerdem hat es eine Suchfunktion, dafür aber keine Berichtsfunktion und keine Spalte zum Anzeigen der SCL-Werte.

...



Mit der Erkenntnis, dass unsere Spam-Testnachricht den SCL-Wert „7“ aufweist, können wir nun testen, wie der zweite SCL-Wert für die Junk-E-Mail-Konfiguration wirkt. Dazu erhöhen Sie im Exchange System-Manager den Gateway-SCL-Wert von „7“ auf „8“ und belassen den SCL-Schwellenwert für die Junk-E-Mail-Konfiguration auf „5“. Die Bereitstellung des Postfachinformationsspeichers muss erneut aufgehoben und wieder aktiviert werden, damit diese Änderung aktiv wird. Versenden Sie dann erneut die Spam-Testnachricht mit dem Tool Smtpsend. Da deren SCL-Wert mit „7“ kleiner als der Gateway-SCL-Schwellenwert „8“ ist, landet die Nachricht dieses Mal nicht im Ordner UCEArchive des Exchange-Servers. Da der SCL-Wert „7“ der Testnachricht aber größer als der SCL-Schwellenwert „5“ der Junk-E-Mail-Konfiguration ist, wird die Nachricht beim Administrator unter Outlook in den Ordner Junk-E-Mail statt in den Posteingang eingestellt.



...

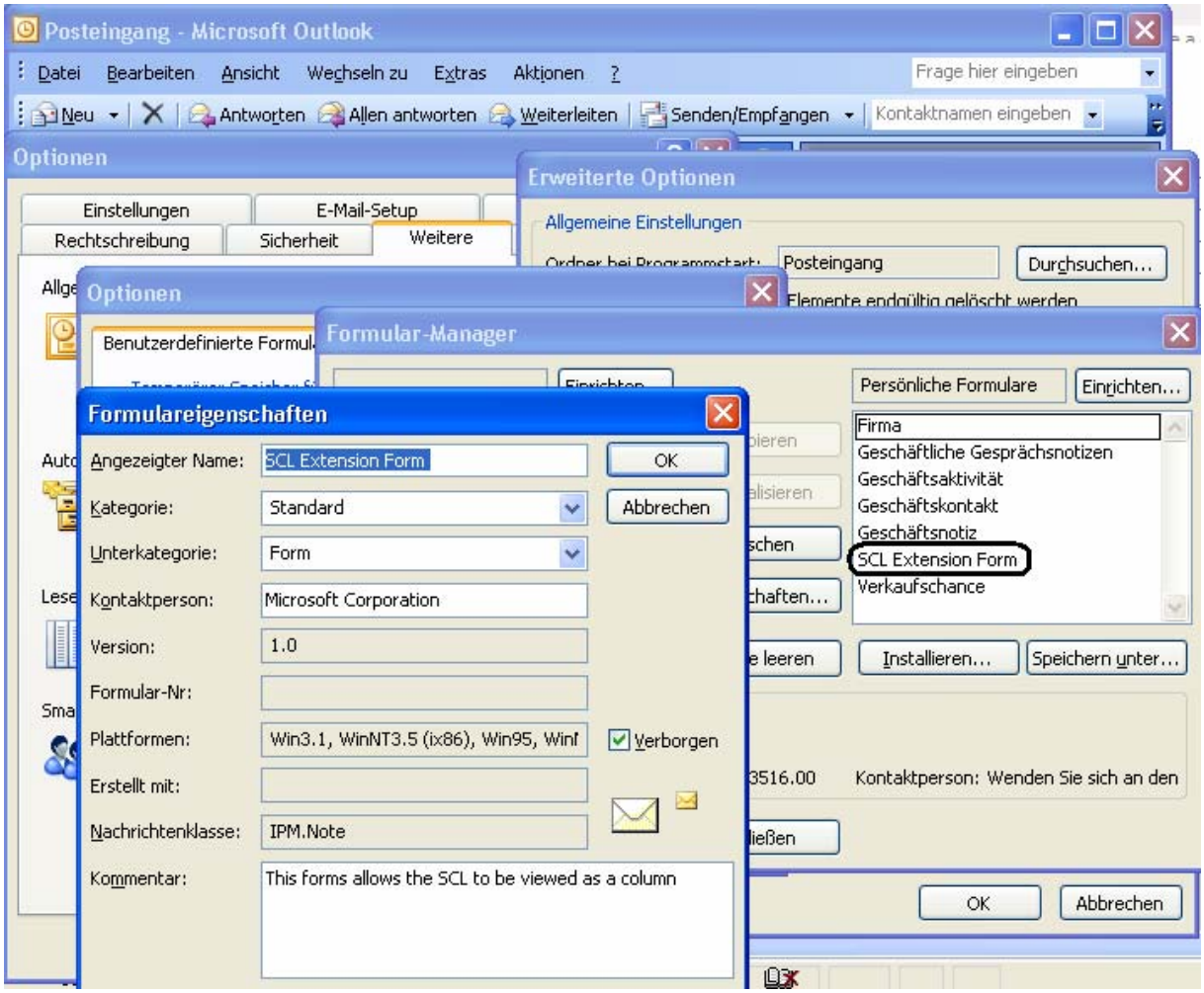
Zum Test setzen Sie nun den SCL-Schwellenwert der Junk-E-Mail-Konfiguration von „5“ auf „7“ hoch. Heben Sie die Bereitstellung des Postfachinformationsspeichers auf und stellen Sie ihn wieder bereit, damit diese Änderung wirksam wird. Wenn Sie nun erneut die Spam-Testnachricht versenden, so wird sie unter Outlook im Posteingang erscheinen und nicht im Ordner Junk-E-Mail. Damit ist bewiesen, dass der SCL-Schwellenwert für die Junk-E-Mail-Konfiguration nicht wirkt, wenn er gleich groß wie der SCL-Wert einer Spam-E-Mail ist, sondern nur dann, wenn er kleiner ist.

SCL-Werte von E-Mails in Outlook anzeigen

Im Outlookordner Junk-E-Mail werden die SCL-Werte von Spammails ebenfalls standardmäßig nicht angezeigt. Das wäre jedoch für den Administrator zur Feinjustierung der SCL-Schwellenwerte von IMF sehr hilfreich. Der Administrator könnte dann zuerst eine Zeit lang in Outlook die SCL-Werte daraufhin beurteilen, ab welchem Schwellenwert eine vertretbare Anzahl von „falschen Positiven“ irrtümlich als Spam ausgefiltert werden.

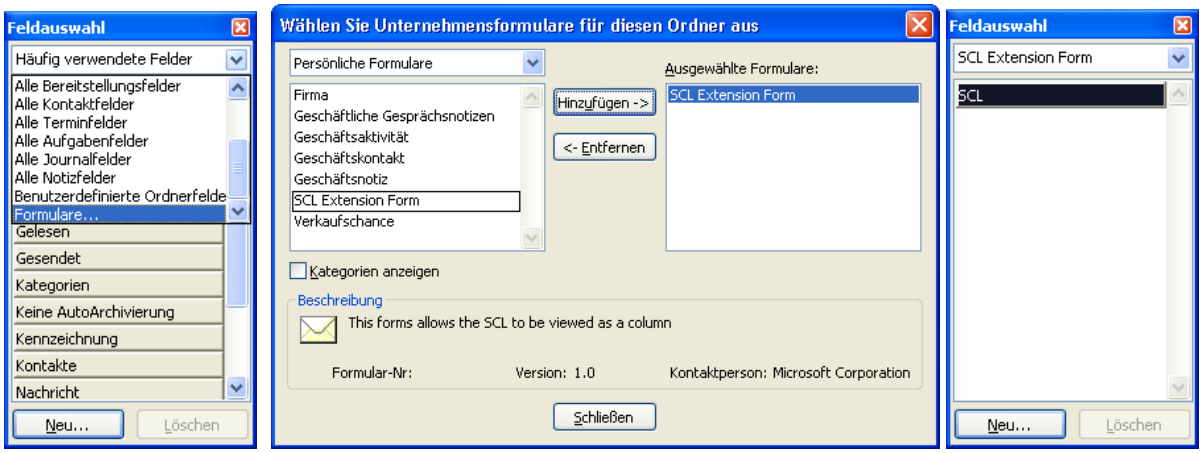
Unter http://www.smallbizserver.net/Default.aspx?tabid=69 können Sie aber das zusätzliche Outlook-Benutzerformular **scl.cfg** als Datei „Controlling SCL Rates Outlook.zip“ herunterladen. Entpacken Sie die Datei scl.cfg und kopieren Sie diese Outlook-Formulardatei in das Verzeichnis C:\Programme\Microsoft Outlook\Office 11\Forms\1031. Sie müssen das neue Formular zuerst in Outlook 2003 installieren. Öffnen Sie dazu unter „Extras – Optionen“ die Registerkarte „Weitere“, klicken Sie auf die Schaltfläche „Erweiterte Optionen“, dann auf „Benutzerformulare“ und „Formulare verwalten“. Wählen Sie „Installieren“, dann die Datei scl.cfg.

...

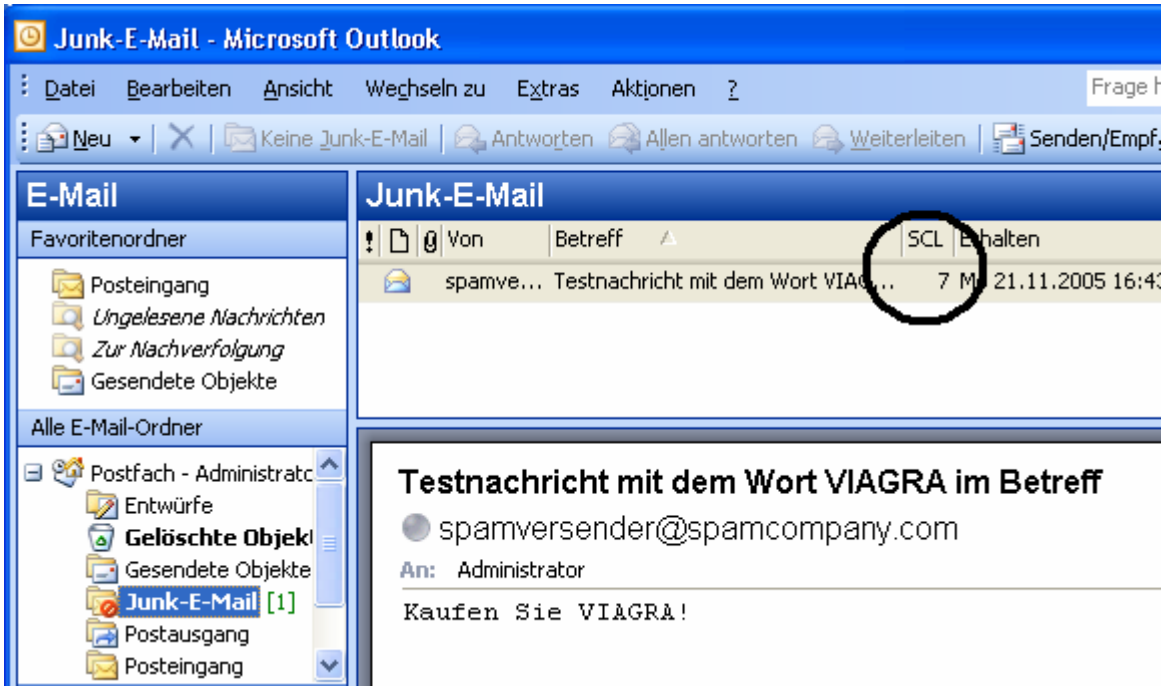


Schließen Sie die Outlook-Optionsfenster. Über „Extras – Lesebereich“ sollten Sie eventuell das Nachrichtenvorschaufenster ganz ausblenden oder die Option „unten“ wählen, um zusätzliche Spalten besser einsehen zu können. Im Ordner Junk-E-Mail klicken Sie nun die Spaltenüberschriftenzeile mit der rechten Maustaste an und wählen „Feldauswahl“. Wählen Sie in der Scroll-Leiste zuerst die Kategorie „Formulare“ aus und fügen Sie das Feld **SCL Extension Form** hinzu:

...



Im Fenster „Feldauswahl“ erscheint nun das Feld mit der Bezeichnung „SCL“. Ziehen Sie es mit der linken gedrückten Maustaste in die Zeile mit den Spaltenüberschriften.



Sie können in Outlook über „Ansicht – Anordnen nach – Aktuelle Ansicht – Ansichten definieren“ auch eine benutzerdefinierte Ansicht erstellen, dieser Ansicht die Bezeichnung „SCL-Spambewertung“ geben und die SCL-Spalte in diese neu definierte Ansicht aufnehmen. Damit können Sie dann auch in anderen Outlook-Ordnern diese Ansicht schnell auswählen und wieder abwählen.

...

Das „Custom Weighting Feature“

In den „Microsoft Exchange Server 2003 Service Pack 2 Release Notes“ wird das Custom Weighting Feature beschrieben. Der Administrator kann damit festlegen, ob der IMF-Filter nur die Betreffzeilen der Nachrichten, den Nachrichtentext oder beides auf Spam-Phrasen überprüft. Dieses Feature kann nicht über eine Benutzeroberfläche konfiguriert werden, sondern über eine Datei namens MSExchange.UceContentFilter.xml. Im genannten Artikel wird eine Beispieldatei gelistet und beschrieben.

Absenderkennungsfilterung

Das Exchange Server 2003 Service Pack 2 bietet neben dem „intelligenten Nachrichtenfilter“ (IMF) als weiteren Spamfilter die Absenderkennungsfilterung (Sender ID Filtering) an. Dieser Filter soll verifizieren, dass eine Nachricht wirklich von der Internet-Domäne verschickt wurde, von der sie laut Absenderadresse zu stammen vorgibt. Einige Gründe sprechen jedoch dafür, diesen Filter zumindest vorerst nicht zu aktivieren:

- Der Einsatz des Absenderkennungsfilters setzt voraus, dass Ihre externen Korrespondenzpartner einen SPF-Eintrag in den DNS-Datensatz (DNS Record) des SMTP-Servers einpflegen bzw. von deren Internet-Provider einpflegen lassen, was bisher oft nicht der Fall ist. Ein Mailserver, auf dem die Absenderkennungsfilterung aktiviert ist, überprüft bei jeder eingehenden Nachricht, ob die IP-Adresse, von der diese Nachricht stammt, im DNS Record der Absenderdomäne eingetragen ist. Dazu sendet der Mailserver eine Anfrage an die Absenderdomäne.

- Sie selbst sollten ebenfalls einen SPF-Eintrag in den DNS Record Ihres SMTP-Servers einpflegen bzw. Ihren Internet-Provider dazu beauftragen.

- Fällt die Gegenabfrage des Mailservers nach einem SPF-Eintrag im DNS Record der Domäne des Versenders negativ aus, so **kann** es sich um Spam handeln, **muss aber nicht**. Genauso gut ist es möglich, dass der Versender bisher noch keinen SPF-Eintrag im DNS Record vornehmen ließ oder aber diesen anzupassen vergaß, als er z.B. den Provider wechselte oder aus Redundanzgründen (Ausfall eines SMTP-Servers) einen alternativen SMTP-Server hinzufügte. Deshalb sollte in der Registerkarte „Absenderkennungsfilter“ als mögliche Reaktion auf Fehler beim Überprüfen der Absenderkennung vorerst auf keinen Fall eine der beiden Optionen „Löschen“ oder „Ablehnen“ gewählt werden. Folglich bleibt nur die Option „Annehmen“ übrig. Damit ist aber nichts gewonnen. Stattdessen steigt die Belastung der Internetanbindung durch die zusätzlichen Sicherheitsabfragen und die Rückantworten.

...

- Man kann in Outlook ein Benutzerformular installieren (Näheres z.B. unter http://blogs.technet.com/exchange/archive/2005/10/13/412487.aspx), mit dem der Wert der Sender ID in einer zusätzlichen Spalte angezeigt wird. Schaut man sich nach einiger Zeit die Sender ID-Werte von neu eingegangenen Nachrichten an, so stellt man fest, dass bei einem Großteil der Nachrichten der Wert „5“ angezeigt wird. Sie werden diesen Wert z.B. häufig bei Newslettern finden, die Sie abonniert haben. Er bedeutet, dass für die versendende Domäne bisher kein Sender ID-Record veröffentlicht wurde. Ein Wert „4“ steht für einen „soft fail“ und tritt oft auf, wenn es sich um gehostete Mailserver handelt. Anhand derartiger Beobachtungen kommt man schnell zu dem Schluss, dass der Absendererkennungsfilter wenig aussagefähig ist.

- Es ist technisch möglich, dass gewiefte Spamversender auch den Mechanismus Absenderkennungsfilterung aushebeln. Ebenso ist denkbar, dass Spamversender selbst falsche SPF-Einträge in DNS Records eintragen. Professionelle Spamversender werden nicht in Ländern aktiv, in denen der Spamversand rechtlich verfolgt wird, sondern oft irgendwo auf der Erde, wo derartigen Dingen seitens der Behörden bewusst nicht nachgegangen wird oder es den Mitarbeitern der in Frage kommenden Behörden schlichtweg am Know-how fehlt, um den ständig neuen und intelligenteren Tricks der technisch bestens versierten Spamversender Paroli zu bieten.

- Mit jedem zusätzlich aktivierten und konfigurierten Filter wachsen die möglichen Fehlerquellen, z.B. durch falsche Konfiguration. Die Wirkungsweise und das Zusammenspiel der eigenen Filter und der vom Internet-Provider vorgenommenen Maßnahmen werden immer undurchsichtiger. Hinzu kommt, dass durch das Einspielen von später veröffentlichten Service Packs oder Hotfixes sich neue Probleme einstellen können. Ein Systemadministrator, der sich nicht ausschließlich um das E-Mail-Geschäft kümmert, verliert dann schnell den Überblick. Werden die durch Spamfilter ausgesonderten Nachrichten nicht zeitnah kontrolliert, so besteht die Gefahr, dass zeitkritische Geschäftsnachrichten unerkannt irgendwo im System hängen bleiben. Das führt sehr schnell dazu, dass die Anwender das Vertrauen in das Mailsystem verlieren, und in jedem Fall wird ein Anwender lieber die ein oder anderer unerwünschte Werbenachricht löschen, als sich unsicher zu sein, ob wichtige Geschäftsnachrichten abhanden kommen.

Aus den genannten Bedenken wird die Konfiguration des Absenderkennungsfilters deshalb in dieser Abhandlung nicht weiter beschrieben. Stattdessen finden Sie nachfolgend Links zum Thema „Absenderkennungsfilter“ bzw. „Sender ID Filter“:

„Configuring and enabling Sender ID filtering in Exchange 2003 SP2“

http://www.msexchange.org/tutorials/Exchange_Server_2003

http://blogs.technet.com/exchange/archive/2005/10.aspx

http://www.anti-spamtools.org/SenderIDEmailPolicyTool/Default.aspx

You Had Me At EHLO... : Sender ID:

...

http://blogs.technet.com/exchange/archive/2005/10/13/412487.aspx

Sender ID Tool:
http://www.anti-spamtools.org/SenderIDEmailPolicyTool/Default.aspx

Tool zum Anzeigen der wirklichen Versenderadresse:

http://cameron-webb.com/blog/archive/2005/10/20/639.aspx

Cfg-Datei zum Anzeigen des SCL-Wertes:

http://www.slipstick.com/emo/2004/up040610.htm#monitor

Sender ID Framework Overview: Verification System Aims to Reduce Spam and Increase Safety Online:
http://www.microsoft.com/mscorp/safety/technologies/senderid/overview.mspx

Sender ID Technology: Information for IT Professionals:
http://www.microsoft.com/mscorp/safety/technologies/senderid/technology.mspx

Sender ID Resources: Tools and Information About the Technology:
http://www.microsoft.com/mscorp/safety/technologies/senderid/resources.mspx

Beachten Sie außerdem den folgenden Hinweis aus den „Microsoft Exchange Server 2003 Service Pack 2 Release Notes“:

Before you enable Sender ID on Exchange 2003 SP2 server, make sure that you apply the Windows Server 2003 hotfix that is referenced in Microsoft Knowledge Base article,

„Windows Server 2003 may stop responding when you enable Sender ID filtering on an SMTP virtual server in Exchange Server 2003 SP2.”

Verbindungsfilterung – Sperrlistenanbieter konfigurieren

Im Internet gibt es Anbieter von Sperrlisten (Blacklist), in denen die IP-Adressen von SMTP-Servern eingetragen sind, die von diesen Anbietern als Spamversender betrachtet werden. Diese Anbieter stellen ihre Listen entweder kostenlos oder entgeltlich zur Verfügung. Viele Internet-Provider bedienen sich solcher Sperrlisten, um die Spamflut einzudämmen. Bezieht Ihr Exchange-Server seine Eingangsnachrichten von einem Internet-Provider, der bereits gängige Sperrlisten nutzt, so können Sie auf die Einrichtung von Verbindungsfiltern auf Ihrem Exchange-Server eventuell verzichten. Unter www.kloth.net/services/dnsbl.php oder unter http://rbls.org/ können Sie überprüfen, ob ein SMTP-Server in einer DNS-Blacklist steht. Dazu tragen Sie die IP-Adresse des SMTP-Servers ein und erhalten dann eine Auflistung bekannter Webadressen mit schwarzen Listen.

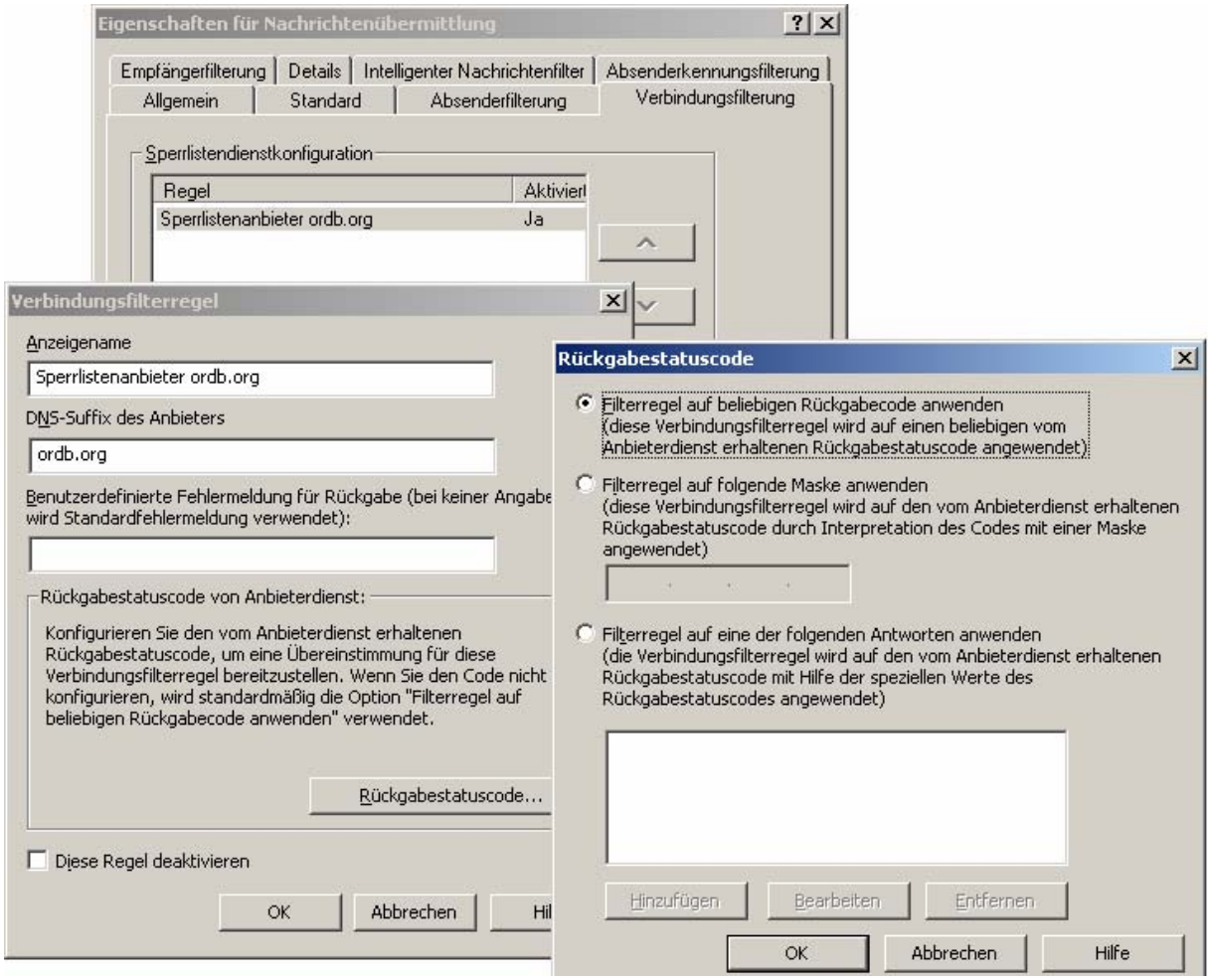
...

Eine Liste von RBL-Anbietern (RBL = Relay Blacklist) findet man unter www.email-policy.com/spam-black-lists.htm. Dort findet man auch Infos, ob das Angebot kostenpflichtig ist und welche Return Codes eine Anfrage an die Sperrliste liefert. Bekannte Anbieter derartiger Sperrlisten sind z.B. ordb.org, blackholes.wirehub.net, bl.spamcop.net, list.dsbl.org, relays.ordb.org, relays.visi.com, sbl.spamhaus.org oder xbl.spamhaus.org

Daneben gibt es die Möglichkeit, selbst IP-Adressen von SMTP-Servern anzugeben, von denen Sie eingehenden E-Mails immer (globale Annahmeliste, „Whitelist“) oder nie (globale Verweigerungsliste, „Blacklist“) annehmen wollen. Wenn Sie sowohl Sperrlistendienste als auch selbst definierte Annahme- oder Verweigerungslisten einsetzen, so haben die letzteren bei der Behandlung durch IMF Vorrang vor den Listen der externen Anbieter. Haben Sie also die IP-Adresse eines SMTP-Servers in die globale Verweigerungsliste aufgenommen, so werden eingehende E-Mails dieses SMTP-Servers auch dann geblockt, wenn er nicht auf einer Sperrliste eines externen Anbieters eingetragen ist.

Sie konfigurieren die Verbindungsfilterung im Exchange System-Manager, indem Sie in den Eigenschaften von „Globale Einstellungen – Nachrichtenübermittlung“ die Registerkarte „Verbindungsfilterung“ öffnen.

...



Im Feld „DNS Suffix des Anbieters“ tragen Sie den DNS Suffix des RBL-Anbieters ein (z.B. ordb.org). Im Feld „Benutzerdefinierte Fehlermeldung für Rückgabe“ kann die Standardfehlermeldung "<IP-Adresse> wurde blockiert durch <Connection Filter Rule Name>" geändert werden.

Werden von solchen Listen falsche Positive geblockt, so kann man diese SMTP-Server als Ausnahmen über die Schaltfläche „Annehmen“ in der Registerkarte „Verbindungsfilter“ als einzelne IP-Adressen oder als IP-Adressbereiche eintragen. Über die Schaltfläche „Ausnahmen“ können außerdem Domänennamen wieder zugelassen werden (z.B. durch Hinzufügen von *@abc.com). Über die Schaltfläche „Verweigern“ können Sie selbst eine Schwarze Liste erstellen.

Ist die IP-Adresse eines SMTP-Servers in der Sperrliste eines hinzugefügten Sperrlistenanbieters eingetragen, so gibt dieser Anbieter einen Statuscode an den Exchange-Server zurück. Dieser Statuscode enthält den Grund, warum der SMTP-Server als Spamversender gelistet ist. Standardmäßig blockiert der Exchange-Server E-Mails mit beliebigem Statuscode. Dieses Verhalten kann aber über die Schaltfläche „Rückgabestatuscode“ eingeschränkt werden. Der RBL Provider (RBL = Relay Blacklist) gibt als Antwort „Host Not Found“ zurück, wenn die IP-Adresse des angefragten SMTP-Servers bei ihm nicht gelistet ist, oder aber einen Code von „127.0.0.1“ bis

...

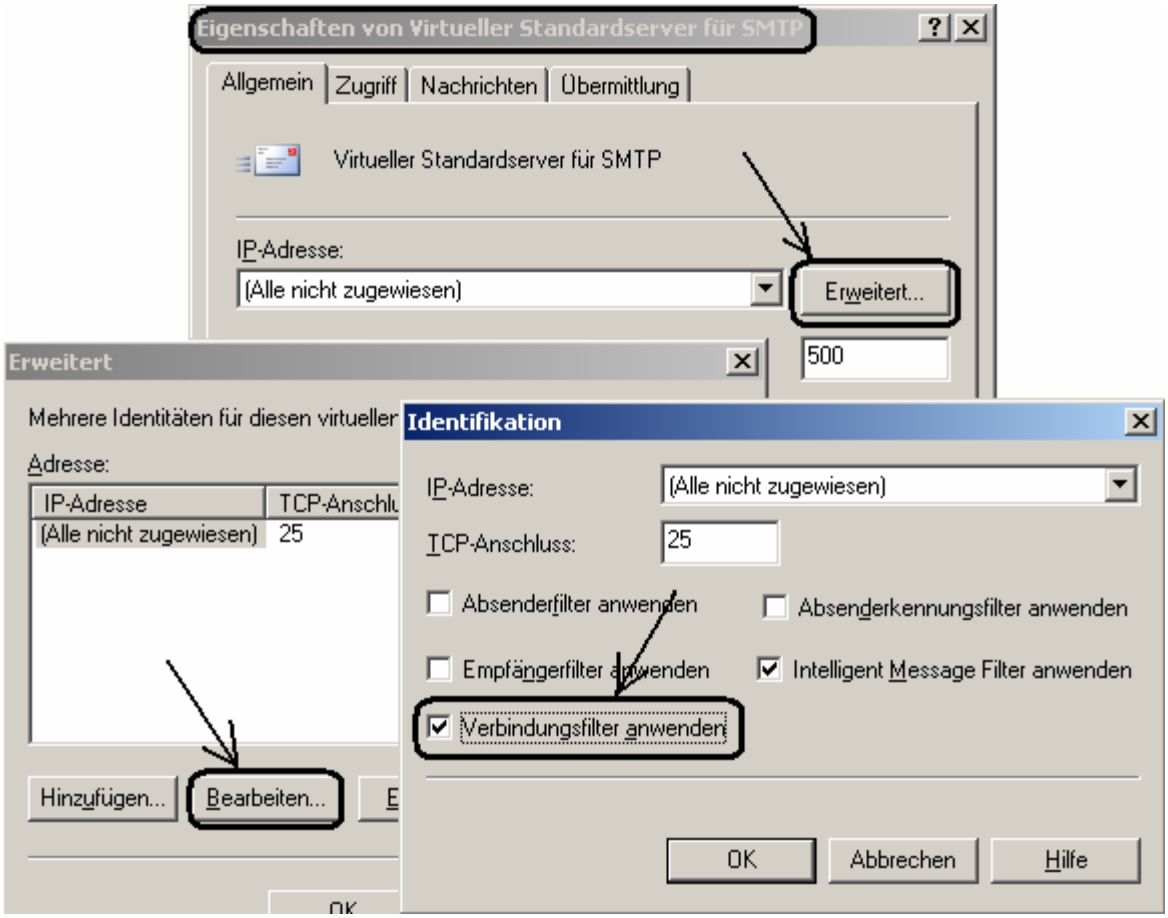
„127.0.0.9“, wobei dessen Bedeutung von Anbieter zu Anbieter variieren kann. Gängige Bedeutungen sind:

127.0.0.2	open relay
127.0.0.3	dialup spam source
127.0.0.4	confirmed spam source
127.0.0.5	smarthosts
127.0.0.6	spamware software developer or spamvertized site
127.0.0.7	listserver
127.0.0.8	insecure formail.cgi scripts
127.0.0.9	open proxy server

Unter http://www.email-policy.com/spam-black-lists.htm finden Sie nicht nur eine Liste von RBL-Providern, sondern auch die von diesen Providern zurückgegebenen Statuscodes.

Der konfigurierte Verbindungsfilter muss wie jeder andere Filter aktiviert werden. Dazu öffnen Sie die Eigenschaften des „Virtuellen Standardservers für SMTP“, klicken in der Registerkarte „Allgemein“ auf die Schaltfläche „Erweitert“, im nächsten Fenster auf die Schaltfläche „Bearbeiten“ und aktivieren im sich öffnenden Identifikationsfenster die Option „Verbindungsfilter anwenden“.

...

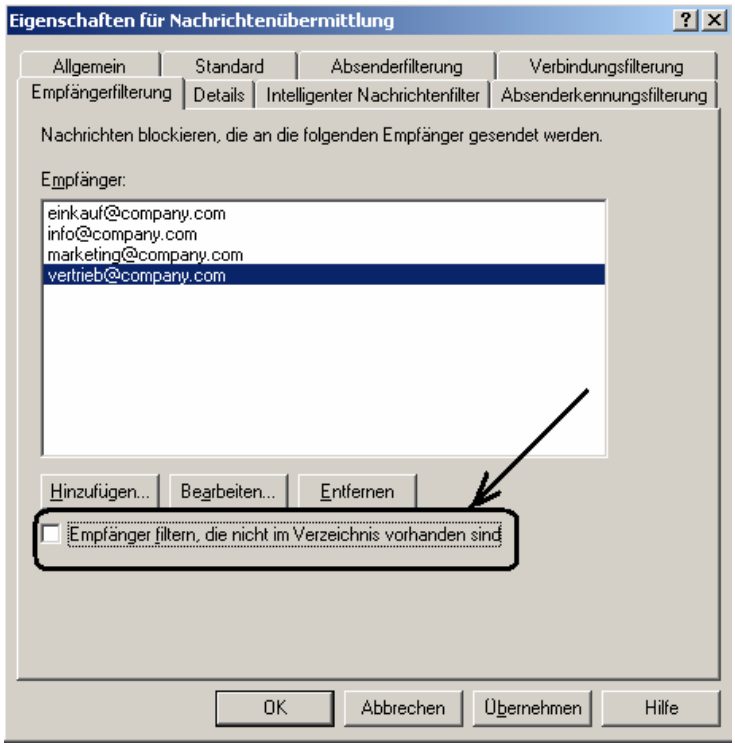


Weitere Informationen finden Sie unter „How to configure connection filtering to use Realtime Block Lists (RBLs) and how to configure recipient filtering in Exchange 2003", http://support.microsoft.com/default.aspx?scid=kb;en-us;823866.

Empfängerfilterung

Sowohl die Empfängerfilterung als auch die Absenderfilterung werden über die gleichnamigen Registerkarten in den Eigenschaften der Nachrichtenübermittlung konfiguriert, müssen dann aber über die Eigenschaften des virtuellen Standardservers für SMTP aktiviert werden. Um wirkungsvoll Wörterbuchattacken (der Spamversender testet aufgrund eines Wörterbuches allgemein bekannte Empfänger wie tom@company.com, thomas@company.com) abzuwehren, kann in der Konfiguration des Empfängerfilters die Option „Empfänger filtern, die nicht im Verzeichnis vorhanden sind" aktiviert werden.

...

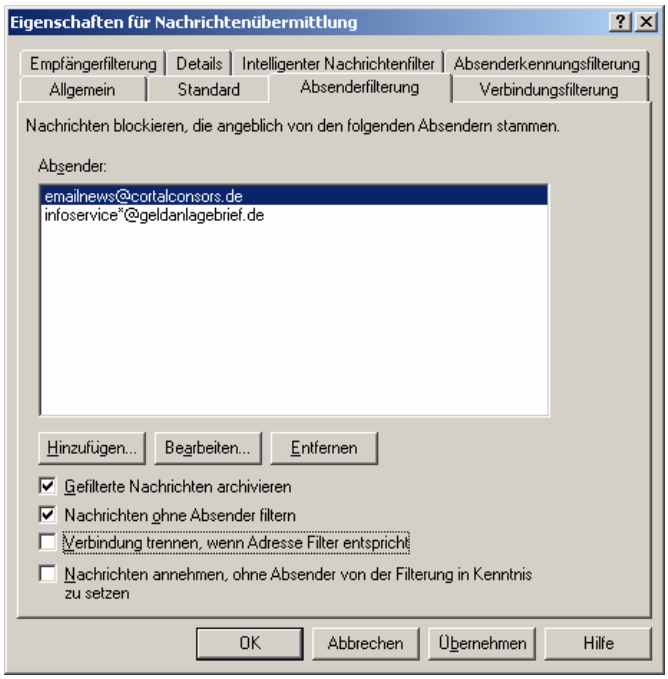


Der Exchange-Server verwirft dann eingehende Nachrichten an Empfängeradressen, die nicht im Active Directory existieren.

Absenderfilterung

In der Registerkarte „Absenderfilterung“ können Einzeladressen wie info@spamversender.de oder ganze Versenderdomänen wie *@spamversender.de eingetragen werden. Sie können z.B. die Absenderadresse von bestimmten Newslettern eintragen, wenn unterbunden werden soll, dass Mitarbeiter diese Newsletter während der Arbeitszeit lesen.

...



Interessant ist hier besonders die Option „**Nachrichten ohne Absender filtern**“, da immer mehr Spams ohne „Von“-Feld eintreffen. Die Option „Gefilterte Nachrichten archivieren“ stellt die gefilterten Nachrichten nicht in den IMF-Archivordner UCEArchive, sondern in das Verzeichnis C:\Programme\Exchsrvr\Mailroot\vsi 1\Filter ein. Der Unterverzeichnis „Filter“ wird beim ersten Eingang einer so gefilterten Nachricht erstellt. Sie können dieses mit dem Tool Smtp erneut testen: Erstellen Sie eine Datei C:\Test2.txt mit folgendem Inhalt

From:

To: administrator@company.local

Subject: Testnachricht ohne Absenderadresse

Diese Nachricht enthält keine Absenderadresse

Verwenden Sie folgende Syntax zum Versenden der Test2.txt, bei der der Parameter für die Absenderadresse durch doppelte Anführungszeichen ersetzt wurde:

Smtpsend 192.168.16.2 "" administrator@company.local test2.txt

...

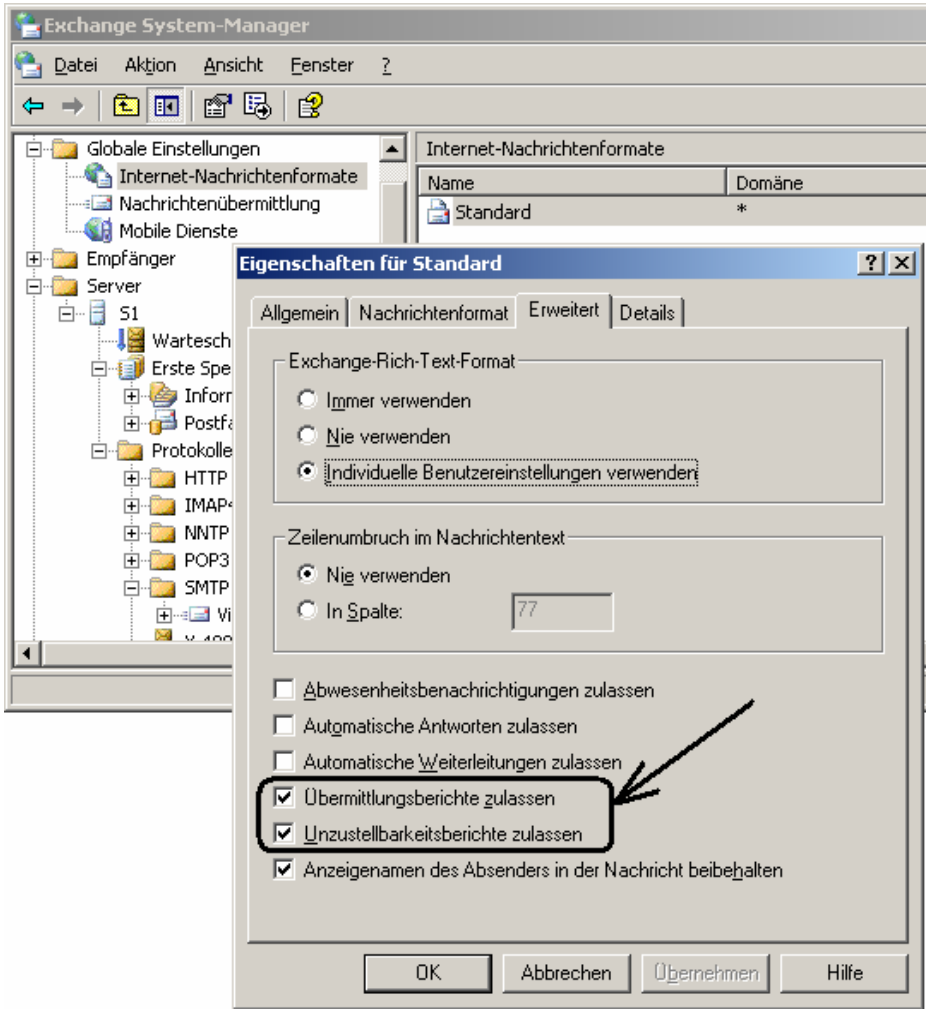
Unzustellbarkeitsberichte und Übermittlungsberichte temporär deaktivieren

Neben den Spamfiltern gibt es noch weitere Möglichkeiten, sich vor Spamattacken zu schützen. Einige Spamversender nutzen z.B. die Unzustellbarkeitsberichte (NDR = non-delivery reports), die ein Exchange Server versendet, wenn eine eingehende E-Mail aufgrund eines nicht bekannten Postfachs nicht zugestellt werden kann. Der Versender soll so informiert werden, dass seine Nachricht das Ziel nicht erreicht hat, um z.B. eine falsch eingetippte Empfängeradresse korrigieren zu können. Daneben gibt es die Übermittlungsberichte (delivery reports), die dann an den Absender versendet werden, wenn dieser beim Verfassen der E-Mail unter Outlook die Option „Die Übermittlung dieser Nachricht bestätigen" gewählt hatte. Diese Optionen sind unter Exchange Server 2003 standardmäßig aktiviert und können bei einer speziellen Spamattacke ausgenutzt werden, um Positivlisten zu generieren - Adresslisten, an die dann später erfolgreich Werbung verschickt werden kann.

Hinzu kommt Folgendes: Antispam-Software filtert oft keine Unzustellbarkeitsnachrichten. Ein Spamversender könnte diesen Umstand ausnutzen, seine Werbung in Form von Pixel statt als Buchstaben an nicht existente E-Mail-Adressen des Zielserver versenden (Spamfilter suchen nach Textphrasen, können diese aber nicht finden, wenn statt Buchstaben Bilder verschickt werden) und als Absenderadresse die eigentlichen Adressen der gewünschten Empfänger einsetzen. Der Zielserver stellt fest, dass es die Zieladresse nicht gibt, und sendet die Nachricht mitsamt der Werbung in Form einer Unzustellbarkeitsberichts an die gefälschte Absenderadresse weiter. Durch diese Vorgehensweise könnte der Spamversender versuchen zu verhindern, dass er selbst auf eine Sperrliste (Blacklist) gerät.

Wenn Sie feststellen, dass Ihr Exchange-Server das Ziel eines solchen Angriffs ist, so können Sie temporär die Erstellung von Unzustellbarkeitsberichten oder Übermittlungsberichten deaktivieren. Dazu öffnen Sie im Exchange System-Manager unter „Globale Einstellungen – Internet-Nachrichtenformate" die Eigenschaften von „Standard" und deaktivieren in der Registerkarte „Erweitert" die beiden Optionen „Übermittlungsberichte zulassen" und „Unzustellbarkeitsberichte zulassen".

...



Nicht standardmäßig aktiviert sind unter Exchange Server 2003 die Optionen „Abwesenheitsbenachrichtigungen zulassen“, „Automatische Antworten zulassen“ und „Automatische Weiterleitungen zulassen“, die Sie ebenfalls an dieser Stelle des Exchange System-Managers finden. Alle Optionen betreffen nur den externen Versand von automatisch erzeugten Nachrichten. Intern kann der Abwesenheitsassistent von Outlook deshalb wirksam eingesetzt werden, wenn die Option „Abwesenheitsbenachrichtigungen zulassen“ hier abgewählt wurde.

Zusammenfassung - Folgende Informationen sollten Sie griffbereit haben:

...

Den Versionsstand eines Exchange-Servers ermitteln Sie im Exchange System-Manager über die Registerkarte „Allgemein“ in den Eigenschaften des betreffenden Exchange-Servers.

Gibt es Exchange 2003 Front-End- und Back-End-Server, so muss das Service Pack 2 zuerst auf den Frond-End-Servern installiert werden.

Produkte von Drittanbietern müssen auf Kompatibilität mit dem Exchange 2003 Service Pack 2 untersucht werden.

Die Standardgröße des Postfachspeichers eines Exchange Servers 2003 Standard Edition mit SP2 beträgt 18 GB und kann über den DWORD-Eintrag **Database Size Limit in GB**

in der Registrierdatenbank auf maximal 75 GB erhöht werden. Dieser DWORD-Wert muss dann unter HKEY_LOCAL_Machine\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<Server-name>\private GUID mit Regedit erstellt werden. An gleicher Stelle können zusätzlich die beiden DWORD-Werte **Database Size Buffer in Percentage** (dessen hartcodierte Standardeinstellung ist 10) und **Database Size Check Start Time in Hours From Midnight** (hartcodiert ist 4 für 4 Uhr morgens) eingefügt werden.

Wird ein Exchange Server mittels des Setup-Wiederherstellungsparameters (setup.exe /disasterrecovery) repariert, so müssen die Registryänderungen manuell neu gesetzt werden.

Überschreitet die logische Datenbankgröße (Größe der edb-Datei + Größe der stm-Datei abzüglich der als gelöscht markierten Speicherblöcke) die maximale Größe der Datenbank, so erfolgt eine Warnung im Ereignisprotokoll. Hat der Administrator innerhalb 24 Stunden keine Gegenmaßnahmen getroffen, so wird die Datenbank offline genommen.

Stellen Sie über die Relaybeschränkungen (Exchange System-Manager - Eigenschaften des virtuellen Standardservers für SMTP - Registerkarte „Zugriff“) sicher, dass Ihr Exchange-Server nicht als Open Relay missbraucht wird.

In der Registerkarte „Nachrichten“ können Sie außerdem die Höchstzahl der Empfänger einer pro Sitzung versendeten Nachricht beschränken.

In der Registerkarte „Übermittlung“ können Sie über die Schaltfläche „Erweitert“ die Option „Reverse-DNS-Lookup an eingehenden Nachrichten durchführen“ aktivieren.

Unter www.kloth.net/services/dnsbl.php oder unter http://rbls.org/ können Sie überprüfen, ob ein SMTP-Server in Sperrlisten (Blacklist) gelistet ist. Ist Ihr eigener SMTP-Server dort gelistet, so

...

können Sie über die Webseite des Sperrlistenanbieters in der Regel online die Löschung von der Liste beantragen.

IMF kann nicht auf dem Knoten eines Clusters aktiviert werden.

Wird unter Small Business Server 2003 der integrierte POP Connector verwendet, so wirkt der IMF nicht.

Eine hereinkommende Nachricht durchläuft also nacheinander folgende Filter, wenn sie aktiviert wurden: **Verbindungsfilter – Empfängerfilter – Absenderfilter - IMF Gateway-Schwellenwert - IMF Junk-E-Mail-Schwellenwert**

Die Spamfilter werden zwar im Exchange System-Manager unter „Globale Einstellungen – Nachrichtenübermittlung“ konfiguriert, müssen aber über die Eigenschaften des virtuellen Standardservers für SMTP aktiviert oder deaktiviert werden. Änderungen werden oft erst dann wirksam, wenn die Bereitstellung der Datenbank aufgehoben und wieder aktiviert wird bzw. wenn der virtuelle Standardserver für SMTP beendet und wieder gestartet wird.

In der Registerkarte „Intelligenter Nachrichtenfilter“ ist die Beschreibung „Nachrichten verschieben, deren SCL-Bewertung größer oder gleich folgendem Wert ist“ falsch!

Richtig ist, dass nur Nachrichten in den Outlook-Ordner „Junk-E-Mail“ verschoben werden, die **größer** (!!!) als der eingetragene SCL-Wert sind, und nicht solche mit einer SCL-Bewertung gleich dem eingetragenen Wert.

Als Spam ausgefilterte E-Mails werden entweder auf dem Exchange-Server im Verzeichnis C:\Programme\Exchsrvr\Mailroot\vsi x\UceArchive oder unter Outlook im Ordner Junk-E-Mail archiviert. Um den Archivordner auf dem Exchange-Server zu verschieben, muss in der Registry unter HKEY_Local_Machine\Software\Microsoft\Exchange\ContentFilter der Zeichenfolgewert **ArchiveDir** erstellt werden. Dort wird der gewünschte Pfad und Ordnername eingetragen.

Mit dem kostenlosen Tool IMF Archive Manager können die in das Spamarchiv des Servers eingestellten E-Mails eingesehen, gelöscht oder nachträglich zugestellt werden.

http://workspaces.gotdotnet.com/imfarchive

Sollen die SCL-Werte der dort archivierten E-Mails angezeigt werden, so muss in der Registry unter HKEY_LOCAL_MACHINE\Software\Microsoft\Exchange zuerst der Schlüssel **ContentFilter** neu erstellt werden. Darunter muss dann der DWORD-Wert **ArchiveSCL** neu erstellt und auf „1“

...

gesetzt werden.

Eine Alternative ist das Tool IMF Companion.

http://stoekenbroek.com/imfcompanion.htm

Um die SCL-Werte von E-Mails unter Outlook in einer neuen Spalte anzuzeigen, kann das Outlook-Benutzerformular **scl.cfg** installiert werden.

Unter http://www.email-policy.com/spam-black-lists.htm finden Sie nicht nur eine Liste von RBL-Providern, sondern auch die von diesen Providern zurückgegebenen Statuscodes.

Um Wörterbuchattacken abzuwehren, kann in der Konfiguration des Empfängerfilters die Option „Empfänger filtern, die nicht im Verzeichnis vorhanden sind“ aktiviert werden.

Über die Absenderfilterung können Sie z.B. den Empfang bestimmter Newsletter und generell den Empfang von Nachrichten ohne Absenderangabe abstellen.

Wenn der Verdacht besteht, dass Spamversender die von Ihrem Exchange-Server automatisch versendeten Unzustellbarkeitsberichte oder Übermittlungsberichte für Spamattacken ausnutzen, so können Sie über „Globale Einstellungen – Internet-Nachrichtenformate“ in den Eigenschaften von „Standard“ und dort in der Registerkarte „Erweitert“ die beiden Optionen „Übermittlungsberichte zulassen“ und „Unzustellbarkeitsberichte zulassen“ temporär deaktivieren.

Literatur

Im Artikel „What's New in Exchange Server 2003“ (http://go.microsoft.com/fwlink/?LinkId=47591) wurden seitens Microsoft folgende Kapitel hinzugefügt oder bezüglich des Service Pack 2 ergänzt:

- Administration Features in Exchange Server 2003
- Enabling or Disabling MAPI Access for a Specific User
- Enabling Direct Push Technology
- Managing Security Settings for Mobile Clients

...

- Remote Wiping of Mobile Devices
- Global Address List Search for Mobile Clients
- Certificate-Based Authentication and S/MIME on Mobile Devices
- Tracking Public Folder Deletions
- Manually Stopping and Resuming Replication
- Synchronizing the Public Folder Hierarchy
- Using the Manage Public Folders Settings Wizard
- Moving Public Folder Content to a Different Server
- Performance and Scalability Features of Exchange Server 2003
- Improved Offline Address Book Performance
- Transport and Message Flow Features of Exchange Server 2003
- Step 3: Specifying the Servers to Exclude from Connection Filtering
- Sender ID Filtering
- Intelligent Message Filtering
- Understanding How Enabled Filters Are Applied
- Storage Features of Exchange Server 2003
- Database Size Limit Configuration and Management
- Schema Changes in Exchange Server 2003

zusätzliche Literatur:

How Outlook 2003 SP2 and Exchange Server 2003 SP2 OAB Version 4 Work Together

http://www.microsoft.com/technet/prodtechnol/exchange/2003/insider/outlook-oab.mspx

OAB Version 4 in Exchange Server 2003 Service Pack 2

http://www.microsoft.com/technet/prodtechnol/exchange/2003/insider/oab4.mspx

Offline Address Book - Things to Consider

http://www.microsoft.com/technet/prodtechnol/exchange/2003/insider/offlineadd-consider.mspx

Exchange 2003 SP2 Webcasts
Top 10 Reasons to Install Exchange Server 2003 SP2
Exchange Server 2003 SP2 Release Notes
Frequently Asked Questions About Exchange Server 2003 SP2 page

What Is New in Exchange Server 2003
Exchange Server 2003 Support for Mobile Device

New Mobility Features in Exchange Server 2003 SP2

Messaging and Security Feature Pack for Windows Mobile 5.0

How to configure connection filtering to use Realtime Block Lists (RBLs) and how to configure recipient filtering in Exchange 2003

http://support.microsoft.com/default.aspx?scid=kb;en-us;823866

...

HOW TO: Exchange Spam Filterung mit der Intelligenten Nachrichtenfilterung (IMF) bei POP basierter Emailabholung

http://dnn.sbsfaq.de/SBS2003/Exchange2003/HOWTOSpamFilterungmitIMFbeiPOPunddynIP/tabid/148/Default.aspx