

G DATA MailSecurity

Bedienung

Inhalt

Allgemeines	5
Ein paar Worte vorab	5
Der Supportrahmen	6
Vor der Installation	11
Grundlegende Vorgehensweise	11
Systemvoraussetzungen	14
Installation.....	15
G DATA MailSecurity MailGateway	17
G DATA MailSecurity Administrator	19
Erster Programmstart (Kennwortvergabe)	19
Weitere Programmstarts (Zugangskennwort)	20
Aufbau G DATA MailSecurity Administrator.....	21
Status-Bereich	23
Filter-Bereich	26
Warteschlangen-Bereich	38
Aktivität-Bereich	39
Virenfunde-Bereich	40
Optionen-Bereich.....	41
Eingehend (SMTP)	41
Ausgehend (SMTP)	43
Eingehend (POP3)	44
Virenprüfung	46
Scanparameter	52
Warteschlange	56
Erweitert	58

Spamfilter-Bereich	60
Filter	60
Whitelist	63
Blacklist	64
Realtime Blacklists	65
Schlüsselwörter (Betreff)	66
Schlüsselwörter (Mailtext)	67
Inhaltsfilter	68
Profi-Einstellungen	69
Internet Update-Bereich	70
Einstellungen	70
Virensignaturen	72
Programmdateien	72
Anhang	73
Problemlösungen (FAQ)	73
Index	74

Allgemeines

■ Ein paar Worte vorab

Der sichere Viren- und Spamschutz für Ihre Mail-Korrespondenz. **G DATA MailSecurity** arbeitet als **Gateway** unabhängig von Ihrem **Mailserver**, ist daher mit beliebiger **Mailserver-Software** unter **Windows** wie auch **Linux** kombinierbar und schützt Ihre **SMTP**- oder **POP3**-basierte Korrespondenz sicher vor Viren, Spam, Phishing und anderen Schädlingen - bevor sie Ihren Server erreichen.

Wir wünschen Ihnen viel Vergnügen und ein erfolgreiches Arbeiten mit **G DATA MailSecurity**!

Ihr **G DATA**-Team

■ Führende Technologie

- Neue DoubleScan-Technologie: Preisgekrönte Virenerkennung dank zweier Virens Scanner-Module
- Neue ressourcenschonende Netzwerktechnik mit Multithreading
- OutbreakShield blockiert infizierte Mails schon 0,5 bis 2 Minuten nach Virenausbruch
- Durchsucht nahezu alle Formate gepackter Dateien und Archive
- Erkennt und entfernt alle Virenarten wie Script-, Makro- und Dateiviren
- Permanenter Schutz vor Viren, Würmern, Trojanern, Backdoors und Malware
- Preisgekrönter Schutz vor Spam und Phishing
- Heuristik entdeckt unbekannte Viren

■ HighTech für höchste Sicherheit

- E-Mail Virenprüfung für eingehende und ausgehende Mails
- Prüft SMTP- und POP3-basierte Mailkorrespondenz
- Für beliebige Mailserver wie Exchange, Notes etc.
- Mailserver Betriebssystem-unabhängig (z. B. Windows oder Linux)
- Frei definierbare Contentfilter

■ Der Supportrahmen

G DATA MailSecurity ist das Softwarepaket zum Komplettschutz Ihres Mailverkehrs. Folgende **Supportleistungen** ergänzen die Funktionalität unserer Software:

■ G DATA PremiumHotline

Die **PremiumHotline** für **G DATA MailSecurity Mehrfach- und Netzwerklizenzen** steht allen **registrierten Kunden** jederzeit zur Verfügung. Sie hilft bei allen Problemen, die im Zusammenhang mit dem Produkt auftreten telefonisch, per Fax oder Internet.

Tel.: **0180 11 55 190** *(4,09 Cent/Minute a. d. deutschen Festnetz. Aus dem Mobilfunknetz können ggf. abweichende Preise gelten)*

Fax: **0234 9762 162**

E-Mail: **business-support@gdata.de**

Die **Registriernummer** finden Sie auf der Rückseite des Benutzerhandbuches. Wenn Sie die Software online gekauft haben, erhalten Sie die **Registriernummer** in einer gesonderten E-Mail. Über das **Online-Registrierungsformular** können Sie diese eingeben und erhalten auf diese Weise sofort online ein Kennwort, mit dem Sie Ihre persönlichen **Internet-Updates** downloaden können. Viele Fragen sind auch schon in der **Online-Datenbank** für häufig gestellte Fragen (**FAQ**) zum **G DATA MailSecurity** beantwortet worden: **www.gdata.de**

Überprüfen Sie vor dem Gespräch mit der Hotline bitte, wie Ihr Computer/Netzwerk ausgestattet ist. Wichtig sind dabei vor allem folgende Informationen:

- die **Versionsnummern** des **Administrators** und des **MailGateways** (diese finden Sie im **Hilfe**-Menü des **Administrators** unter „**Info**“)
- die **G DATA MailSecurity-Registrierungsnummer** oder den **Benutzernamen** für das **Internet-Update**. Die **Registrierungsnummer** befindet sich auf der Rückseite des Benutzerhandbuchs. Der Benutzername wird Ihnen bei der **Online-Registrierung** übermittelt.
- genaue **Windows-Version** (Client/Server)
- Verwendeter **Mailserver** und **Zusatzprogramme**

Mit diesen Angaben wird das Gespräch mit den Hotline-Mitarbeitern kürzer, effektiver und erfolgreicher verlaufen. Bitte richten Sie es für die Beratung möglichst so ein, dass Telefon in der Nähe eines Rechners zu haben, auf dem Sie die Administratorsoftware für den Managementserver installiert haben.. Bitte richten Sie es für die Beratung möglichst so ein, dass Telefon in der Nähe des Computers zu haben, auf dem sich **G DATA MailSecurity** befindet.

■ PremiumSupport-Verlängerungen

Mit dem **PremiumSupport** erhalten Sie mit Durchführung der **Online-Registrierung** für ein Jahr lang stündlich aktualisierte Virendaten per **Internet-Update** zur Virenbekämpfung. Auf Wunsch erhalten Sie weitergehende Informationen (z.B. über **Upgrades** der **ManagementServer-Software** und aktuelle **Virenwarnungen**) per E-Mail. Der **PremiumSupport** kann natürlich von Jahr zu Jahr verlängert werden. Kontaktieren Sie uns einfach unter

Tel.: **0234 / 9762-170** (Mo. bis Fr. von 9 bis 17 Uhr)

Fax: **0234 / 9762-299**

E-Mail: **b-vertrieb@gdata.de**

- *Selbstverständlich wird unser Business-Vertrieb Ihre Anfragen bestmöglich bearbeiten und Sie individuell beraten. Haben Sie bitte Verständnis dafür, dass **technische Fragen** zur vorliegenden Software nur über unser **ServiceCenter** bearbeitet werden können.*

■ Ebenfalls erhältlich: G DATA AntiVirus Enterprise

G DATA AntiVirus Enterprise kombiniert den E-Mail Virenschutz von **G DATA MailSecurity** mit der Client-/Server-Lösung **G DATA AntiVirus**, dem vollautomatischen Virenschutz für Windows-Netzwerke.

G DATA AntiVirus besteht aus einer zentralen TCP/IP basierten Steuereinheit – dem **G DATA AntiVirus ManagementServer** - und den **G DATA AntiVirus Clients**, deren Virenschutzfunktionen für den Anwender „unsichtbar“ auf Fileservern und Workstations im Hintergrund ablaufen. Die Bedienung der Clients von der Installation über Virensuchen bis zu Einstellungen ändern vollzieht der Netzwerkadministrator komplett ferngesteuert.

G DATA AntiVirus Enterprise schützt somit Ihr gesamtes Unternehmen umfassend vor Viren.

Nähere Informationen erhalten Sie vom **G DATA** Business-Vertrieb.

Tel.: **0234 / 9762-170** (Mo. bis Fr. von 9 bis 17 Uhr)

Fax: **0234 / 9762-299**

E-Mail: **b-vertrieb@gdata.de**

- ▣ *Selbstverständlich wird unser Business-Vertrieb Ihre Anfragen bestmöglich bearbeiten und Sie individuell beraten. Haben Sie bitte Verständnis dafür, dass **technische Fragen** zur vorliegenden Software nur über unser **ServiceCenter** bearbeitet werden können.*

■ Lizenzvereinbarungen

Nachfolgend sind die Vertragsbedingungen für die Benutzung von "**G DATA MailSecurity**" durch den Endverbraucher (im Folgenden auch: „Lizenznehmer“), aufgeführt.

1. Gegenstand des Vertrages

Gegenstand des Vertrages ist **G DATA MailSecurity** und die Programmbeschreibung. Sie werden im Folgenden auch als „Software“ bezeichnet. **G DATA** macht darauf aufmerksam, dass es nach dem Stand der Technik nicht möglich ist, Computersoftware so zu erstellen, dass sie in allen Anwendungen und Kombinationen fehlerfrei arbeitet.

2. Umfang der Benutzung

G DATA gewährt Ihnen für die Dauer dieses Vertrages das einfache, nicht ausschließliche und persönliche Recht (im Folgenden auch als „Lizenz“ bezeichnet), die Software auf einem vertraglich vereinbarten Anzahl von Computern zu benutzen. Ist dieser Computer ein Mehrbenutzersystem, so gilt dieses Benutzungsrecht für alle Benutzer dieses einen Systems. Als Lizenznehmer dürfen Sie Software in körperlicher Form (d.h. auf einem Datenträger abgespeichert) von einem Computer auf einen anderen Computer übertragen, vorausgesetzt, dass sie zu irgendeinem Zeitpunkt auf immer nur auf der vertraglich vereinbarten Anzahl von Computern genutzt wird. Eine weitergehende Nutzung ist nicht zulässig.

3. Besondere Beschränkungen

Dem Lizenznehmer ist untersagt, ohne vorherige schriftliche Einwilligung von **G DATA** die Software abzuändern.

4. Inhaberschaft an Rechten

Sie erhalten mit dem Erwerb des Produktes nur Eigentum an dem körperlichen Datenträger, auf dem die Software aufgezeichnet ist und auf die mittels Supportrahmen vereinbarten Updates. Ein Erwerb von Rechten an der Software selbst ist nicht damit verbunden. **G DATA** behält sich insbesondere alle Veröffentlichungs-, Vervielfältigungs-, Bearbeitungs- und Verwertungsrechte an der Software vor.

5. Vervielfältigung

Die Software und das zugehörige Schriftmaterial sind urheberrechtlich geschützt. Das Anfertigen einer Sicherheitskopie, die jedoch nicht an Dritte weitergegeben werden darf, ist erlaubt.

6. Dauer des Vertrages

Der Vertrag läuft auf unbestimmte Zeit. Das Recht des Lizenznehmers zur Benutzung der Software erlischt automatisch und ohne Kündigung, wenn er eine Bedingung dieses Vertrages verletzt. Bei Beendigung des Nutzungsrechtes ist er verpflichtet, die Original CD-ROM einschließlich etwaiger UPDATES/UPGRADES sowie das schriftliche Material zu vernichten.

7. Schadensersatz bei Vertragsverletzung

G DATA macht darauf aufmerksam, dass Sie für alle Schäden aufgrund von Urheberrechtsverletzungen haften, die **G DATA** aus einer Verletzung dieser Vertragsbestimmungen durch Sie entstehen.

8. Änderungen und Aktualisierungen

Es haben jeweils unsere neuesten Servicebedingungen Gültigkeit. Die Servicebedingungen können jederzeit, ohne Ankündigung und ohne Angabe von Gründen geändert werden.

9. Gewährleistung & Haftung von G DATA

a) **G DATA** gewährleistet gegenüber dem ursprünglichen Lizenznehmer, dass zum Zeitpunkt der Übergabe der Datenträger (CD-ROM), auf dem die Software aufgezeichnet ist, unter normalen Betriebsbedingungen und bei normaler Instandhaltung in Materialausführung fehlerfrei ist.

b) Sollte der Datenträger (die CD-ROM) fehlerhaft sein, so kann der Erwerber Ersatzlieferung während der Gewährleistungszeit von 6 Monaten ab Lieferung verlangen. Er muss dazu die CD-ROM und eine Kopie der Rechnung/Quittung an **G DATA** zurücksenden.

c) Als den vorstehend unter 1. genannten Gründen übernimmt **G DATA** keine Haftung für die Fehlerfreiheit der Software. Insbesondere übernimmt **G DATA** keine Gewähr dafür, dass die Software den Anforderungen und Zwecken des Erwerbers genügt oder mit anderen von ihm ausgewählten Programmen zusammenarbeitet. Die Verantwortung für die richtige Auswahl und die Folgen der Benutzung der Software sowie der damit beabsichtigten oder erzielten Ergebnisse trägt der Erwerber. Das gleiche gilt für das die Software begleitende, schriftliche Material. Ist die Software nicht im Sinne von 1. grundsätzlich brauchbar, so hat der Erwerber das Recht, den Vertrag rückgängig zu machen. Das gleiche Recht hat **G DATA**, wenn die Herstellung von im Sinne von 1. brauchbarer Software mit angemessenem Aufwand nicht möglich ist.

d) **G DATA** haftet nicht für Schäden, es sei denn, dass ein Schaden durch Vorsatz oder grobe Fahrlässigkeit seitens **G DATA** verursacht worden ist. Gegenüber Kaufleuten wird auch die Haftung für grobe Fahrlässigkeit ausgeschlossen. Die maximale Entschädigungsleistung beträgt den Kaufpreis der Software.

10. Gerichtsstand

Alleiniger Gerichtsstand bei allen aus dem Vertragsverhältnis mittelbar oder unmittelbar sich ergebenden Streitigkeiten ist nach unserer Wahl der Sitz unserer Firma oder der Sitz des Käufers.

11. Schlussbestimmungen

Sind einzelne Bestimmungen dieser Lizenzvereinbarung ungültig, so bleiben die übrigen Bestimmungen wirksam. Anstelle der ungültigen Bestimmung gilt eine ihrem wirtschaftlichen Zweck möglichst nahekommende, wirksame Bestimmung als vereinbart.

Vor der Installation

■ Grundlegende Vorgehensweise

G DATA MailSecurity ist das Softwarepaket zum Komplettschutz Ihrer **E-Mail-Kommunikation**. Es umfasst:

- **G DATA MailSecurity Mailgateway:** Das **Mailgateway** ist der High-End Virenschutz für Ihre Mail-Korrespondenz und verriegelt so den Haupt-Verbreitungsweg moderner Viren effizient und sicher. Es arbeitet als **Gateway** unabhängig von Ihrem Mailserver und ist daher mit beliebiger Mailserver-Software unter Windows, wie auch Linux kombinierbar.
- **G DATA MailSecurity Administrator: Steuerungssoftware** für das Mail-Gateway.

Das Programm ist ein **Mailgateway** für SMTP und POP3 mit integriertem Virenschutz.

- **SMTP:** Eingehende Mails werden nicht mehr an den Mail-Server sondern an das **G DATA MailSecurity Mail Gateway** geschickt. Nach der Virenprüfung werden Sie von dort an den Mail-Server weitergeleitet. **G DATA MailSecurity** kann natürlich auch die ausgehenden Mails prüfen. Dazu wird der Mail-Server so konfiguriert, dass er die Mails nicht mehr direkt versendet sondern erst an **G DATA MailSecurity** weiterleitet. Das Programm kümmert sich dann um die weitere Verarbeitung.
- **POP3:** Sie können **G DATA MailSecurity** auch verwenden, wenn Sie Ihre Mails via POP3 abholen. **G DATA MailSecurity** holt die Mails stellvertretend für das anfordernde Programm ab, prüft sie auf Viren und leitet sie dann an das Programm weiter.

Vor der Installation sollten Sie sich natürlich Gedanken darüber machen, wo im Netzwerk Sie **G DATA MailSecurity** installieren. Während Sie die **G DATA MailSecurity-Administratorsoftware** von jedem Punkt des Netzwerks aus verwenden können, benötigt die Installation des eigentlichen **Mail Gateways** einiger Vorüberlegungen. Generell sollte sich das **MailGateway** am besten direkt hinter Ihrer **Netzwerk-Firewall** befinden (soweit vorhanden), d.h. dass der **SMTP/POP3-Datenstrom** aus dem Internet über die **Firewall** direkt zum **MailGateway** geleitet und von dort weiter verteilt wird.

- *Bitte beachten Sie, dass Sie gegebenenfalls Ihre **Firewall-Konfigurationen (IP-Adresse und/oder Port)** verändern müssen, damit der **E-Mailverkehr** über das **G DATA MailSecurity MailGateway** abgewickelt wird.*

Prinzipiell können Sie das **G DATA MailSecurity Mail Gateway** auf einem eigenen Rechner installieren, der dann für das gesamte Netzwerk als **MailGateway** fungiert, es ist aber auch möglich, **G DATA MailSecurity** auf dem Rechner einzusetzen, der gleich-

zeitig als **Mail-Server** dient. Dabei ist zu beachten, dass eine gemeinsame Installation auf einem einzigen Rechner bei starkem Mail-Aufkommen zu Verzögerungen führen kann, da sowohl die Verwaltung permanenter E-Mail-Kommunikation, als auch die immanenten Virenanalyse sehr rechenintensive Vorgänge sind.

■ Installation des MailGateways auf dem Mail-Server (SMTP)

Wenn Ihr SMTP-Server die Änderung der Port-Nummer erlaubt, können Sie **G DATA MailSecurity** auch auf demselben Rechner installieren, wie Ihren **SMTP-Server**. In diesem Fall vergeben Sie bitte für Ihren Original-Mailserver einen neue **Port-Nummer** (z.B. 7100 oder höher). Das **G DATA MailSecurity** MailGateway verwendet dann weiterhin den Port 25 zur Verarbeitung der eingehenden Mails.

- ▣ *Sollten Sie **G DATA MailSecurity** auf demselben Rechner wie **Microsoft Exchange 5.5** installieren, kann das **G DATA MailSecurity** Setup automatisch den **Port** für eingehende Mails umstellen. Dazu wird der **SMTP-Eintrag** in der Datei `\winnt\system32\drivers\etc\services` verändert und der Internet Mail Dienst von Microsoft **Exchange** neu gestartet. Beispiel:*

Konfiguration Mail-Server

Port für eingehende Mails: 7100 (Beispiel)

Nachrichtenübermittlung: Alle Nachrichten zum Host weiterleiten: 127.0.0.1

Konfiguration G DATA MailSecurity MailGateway (Eingehended (SMTP))

Port, auf dem die Mails eingehen: 25

DNS zum Versenden der Mails verwenden: AUS

Mails an diesen SMTP-Server weiterleiten: 127.0.0.1

Port: 7100 (Beispiel)

Konfiguration G DATA MailSecurity MailGateway (Ausgehend (SMTP))

Ausgehende Mail verarbeiten: EIN

IP-Adressen der Server, die ausgehende Mails senden können:

127.0.0.1;<IP Mail-Server>

DNS zum Versenden der Mails verwenden: EIN

Bezeichnungen

<IP Mail-Server> = IP-Adresse des Rechners, auf dem der Mail-Server installiert ist.

<IP G DATA MailSecurity> = IP-Adresse des Rechners, auf dem **G DATA MailSecurity** installiert ist

■ Installation des MailGateways auf separatem Rechner (SMTP)

Hierbei müssen eingehende Mails an das **G DATA MailSecurity MailGateway** gesendet werden (nicht an den **Mail-Server**). Das kann über unterschiedliche Methoden erreicht werden:

- a) den **MX-Record** im **DNS-Eintrag** anpassen
- b) **Umleitung** an der **Firewall** definieren (falls vorhanden)
- c) die **IP-Adresse** des Mail-Servers ändern und dem Rechner mit dem **G DATA MailSecurity MailGateway** die originale IP-Adresse des Mail-Servers zuweisen

▣ *Beispiel:*

Konfiguration Mail-Server

Port für eingehende Mails: 25

Nachrichtenübermittlung: Alle Nachrichten zum Host weiterleiten: <IP G DATA MailSecurity>

Konfiguration G DATA MailSecurity MailGateway (Eingehend (SMTP))

Port, auf dem die Mails eingehen: 25

DNS zum Versenden der Mails verwenden: AUS

Mails an diesen SMTP-Server weiterleiten: <IP Mail-Server>

Port: 25

Konfiguration G DATA MailSecurity MailGateway (Ausgehend (SMTP))

Ausgehende Mail verarbeiten: EIN

IP-Adressen der Server, die ausgehende Mails senden können: <IP Mail-Server>

DNS zum Versenden der Mails verwenden: EIN

Bezeichnungen

<IP Mail-Server> = IP-Adresse des Rechners, auf dem der **Mail-Server** installiert ist.

<IP G DATA MailSecurity> = IP-Adresse des Rechners, auf dem das **G DATA MailSecurity MailGateway** installiert ist

■ Systemvoraussetzungen

Für die Nutzung von **G DATA MailSecurity** müssen Sie folgenden Festplattenspeicherplatz veranschlagen:

- Mail Gateway: 20 MB zzgl. zwischengespeicherter Mails (Empfehlung: mind. 50 MB frei)
 - Administrator: 2 MB

 - **Voraussetzungen für die Nutzung des G DATA MailSecurity Administrators:** Pentium PC mit Betriebssystem **Windows XP, Windows 2000, Windows Vista** oder Windows **Server 2003**, 32 MB RAM
 - **Voraussetzungen für das G DATA MailSecurity Mail Gateway:** Pentium PC mit Betriebssystem **Windows XP, Windows 2000, Windows Vista** oder Windows **Server 2003**, 256 MB RAM, CD-ROM-Laufwerk, Internetzugang
- ***G DATA MailSecurity ist auch auf 64 Bit Windows-Betriebssystemen lauffähig.***

Installation

Schließen Sie bitte alle anderen Programme, bevor Sie mit der Installation von **G DATA MailSecurity** beginnen. Es kann zu Fehlfunktionen oder einem Abbruch kommen, falls z.B. Programme geöffnet sind, die auf Daten zugreifen, die **G DATA MailSecurity** zur Installation benötigt. Beachten Sie bitte auch, dass für eine Installation ausreichender **Festplattenspeicherplatz** auf Ihrem System zur Verfügung steht. Sollte während der Installation nicht genügend Speicherplatz zur Verfügung stehen, weist Sie das Installationsprogramm von **G DATA MailSecurity** darauf hin.



Die **Installation** von **G DATA MailSecurity** ist ausgesprochen unkompliziert. Starten Sie einfach Ihr Windows und legen dann die **G DATA MailSecurity-CD-ROM** in Ihr CD-ROM-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster, welches Ihnen folgende Optionen bietet:

- **Installieren:** Hiermit starten Sie die Installation von **G DATA MailSecurity** auf Ihrem Computer.
- **Durchsuchen:** Über den Windows-Explorer können Sie hier die Verzeichnisse der **G DATA MailSecurity-CD-ROM** sichten.
- **Abbrechen:** Über diesen Eintrag können Sie die den Autostart-Bildschirm schließen, ohne eine Aktion durchzuführen.

■ *Sollten Sie die Autostart-Funktion Ihres CD-ROM-Laufwerks nicht aktiviert haben, kann **G DATA MailSecurity** den Installationsvorgang nicht automatisch starten. Klicken Sie dann im „**Start-Menü**“ von Windows auf*

*„Ausführen“, tippen in dem erscheinenden Fenster e:\setup.exe ein und klicken auf OK. Auf diese Weise öffnet sich ebenfalls der Einstiegsbildschirm für die **G DATA MailSecurity-Installation**. - Der Eintrag „e:“ bezeichnet den **Laufwerksbuchstaben** Ihres CD-ROM-Laufwerks. Sollten Sie Ihr CD-ROM-Laufwerk auf einem anderen Laufwerksbuchstaben angemeldet haben, geben Sie statt „e:“ bitte den entsprechenden Laufwerksbuchstaben an.*

Folgen Sie nun einfach den einzelnen Schritten des Installationsassistenten und installieren Sie über den Button „**G DATA MailSecurity**“ das **MailGateway** auf dem Rechner den Sie dafür verwenden möchten. Das kann im besten Fall ein speziell dafür abgestellter **MailGateway-Rechner** sein, aber auch der **Mail-Server-Rechner** selber bzw. irgendeine anderer Computer, der im Netzwerk administrative Aufgaben übernehmen kann. Bitte beachten Sie in diesem Zusammenhang die **Mindest-Systemvoraussetzungen** die für den Betrieb des MailGateways notwendig sind.

G DATA MailSecurity MailGateway

Nach Abschluss der Installation steht Ihnen die **MailGateway-Software** zur Verfügung. Neben der eigentlichen Software, die im Hintergrund läuft, wurde automatisch der **Administrator** installiert, über den Sie vollen Zugriff auf die Funktionen und Optionen des **MailGateways** haben. Diesen **Administrator** finden Sie bei einer Standardinstallation unter „**Start > Programme > G DATA MailSecurity > G DATA MailSecurity**“. Die Einstellungs- und Einflussmöglichkeiten, die Ihnen über den Administrator zur Verfügung stehen, werden in den folgenden **Kapiteln** ausführlich erläutert.

- ▣ Sie können das **MailGateway** auch über jeden anderen Rechner warten, der die Systemvoraussetzungen für das **G DATA MailSecurity Administrator-Tool** erfüllt. Wenn Sie das **MailGateway** also über einen anderen Rechner im Netzwerk ansteuern möchten, installieren Sie dort einfach den **Administrator** ohne die eigentliche **MailGateway-Software**. Starten Sie dazu einfach erneut das **Setup** und wählen den Button „**G DATA MailSecurity Administrator**“ aus.
- ▣ *Wenn Sie die **Administrator-Software** beenden, schließen Sie damit nicht das **MailGateway**. Dieses bleibt weiterhin im **Hintergrund** aktiv und steuert die Prozesse, die von Ihnen eingestellt wurden.*

Der Empfang und Versand von E-Mails wird in der Regel über die beiden Protokolle SMTP und POP3 abgewickelt. Dabei dient **SMTP (= Simple Mail Transfer Protokoll)** dazu, Mails an beliebige Empfänger zu verschicken, während **POP3 (= Post Office Protokoll 3)** als übergeordnetes Protokoll dazu verwendet wird, eingegangene Mails in einem speziellen „Postfach“ abzulegen, auf welches nur der spezielle Empfänger mittels eines Passwortes Zugriff hat.

Je nachdem, wie Ihr Netzwerk aufgebaut ist, kann **G DATA MailSecurity** nun an verschiedenen Knotenpunkten greifen, um eingehende Mails auf Virenbefall zu überprüfen:

- Wenn Sie im Netzwerk einen **SMTP-Server** verwenden, kann **G DATA MailSecurity** eingehende Mails schon vor dem Erreichen des Mail-Servers überprüfen. Hierzu steht Ihnen die Funktion „**Prüfung eingehender Mails (SMTP)**“ im **Status-Bereich** zur Verfügung..
- Wenn Sie Ihre Mails z.B. über einen aushäusigen Server direkt als **POP3-Mails** bekommen (z.B. über ein **POP3-Sammelkonto**), kann **G DATA MailSecurity** auch hier eingreifen, um die POP3-Mails vor dem Öffnen durch den Empfänger auf Virenbefall überprüfen. Hierzu steht Ihnen die Funktion „**Prüfung eingehender Mails (POP3)**“ im **Status-Bereich** zur Verfügung.

Selbstverständlich kann **G DATA MailSecurity** auch all Ihre ausgehenden Mails vor dem Versand an die Empfänger auf Virenbefall überprüfen. Da für das Versenden von Mails nur das **SMTP-Protokoll** Verwendung findet, gibt es hier logischerweise keine **POP3-Variante**. Hier steht Ihnen die Funktion „**Prüfung ausgehender Mails (SMTP)**“ im **Status-Bereich** zur Verfügung.

G DATA MailSecurity Administrator

Der **G DATA MailSecurity Administrator** ist die Steuerungssoftware für das **G DATA MailSecurity MailGateway**, das - vom Systemadministrator zentral gesteuert - den gesamten SMTP- und POP3 basierten E-Mailverkehr mit und in Ihrem gesamten Netzwerk sichert. Der **Administrator** kann passwortgeschützt von jedem Rechner unter Windows gestartet werden. Als ferngesteuerte Jobs sind alle denkbaren Einstellungsänderungen am Virens scanner und Virensignatur-Updates möglich.

■ Erster Programmstart (Kennwortvergabe)



Sie können das AdministratorTool zur Steuerung des **MailGateways** mit einem Klick auf den Eintrag „**G DATA MailSecurity Administrator**“ in der Programmgruppe „**Start > (Alle) Programme > G DATA MailSecurity**“ des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem **Server** und dem **Kennwort** gefragt.

G DATA MailSecurity Administrator

Geben Sie als Server bitte den Namen oder die IP-Adresse des Rechners ein, auf dem G DATA MailSecurity installiert ist.

Server: JENSWISTA2

Kennwort: |

OK Abbrechen Hilfe

Geben Sie in dem Feld „**Server**“, den **Computernamen** oder die **IP-Adresse** des Computers ein, auf dem das **MailGateway** installiert wurde. Da Sie jetzt noch kein Kennwort vergeben haben, klicken ohne Eingabe eines Kennworts einfach auf den **OK-Button**. Es öffnet sich ein **Kennworteingabefenster**, in dem Sie unter „**Neues Kennwort**“ ein neues Kennwort für den **G DATA MailSecurity Administrator** vergeben können.

Kennwort eingeben

Geben Sie bitte ein Kennwort für künftige Anmeldungen ein.

Neues Kennwort: |

Neues Kennwort bestätigen: |

OK Abbrechen

Sie bestätigen das eingegebenen Kennwort durch erneutes Eintippen im Feld „**Neues Kennwort bestätigen**“ und klicken dann auf **OK**.

- Sie können das Kennwort jederzeit im Bereich „Optionen“ in der Karteikarte „**Erweitert**“ mit einem Klick auf den Button „**Kennwort ändern**“ neu vergeben.

■ Weitere Programmstarts (Zugangskennwort)

Sie können das AdministratorTool zur Steuerung des **MailGateways** mit einem Klick auf den Eintrag „**G DATA MailSecurity Administrator**“ in der Programmgruppe „**Start > (Alle) Programme > G DATA MailSecurity**“ des Startmenüs aufrufen. Beim Starten des Administrators werden Sie nach dem **Server** und dem **Kennwort** gefragt.



Geben Sie in dem Feld „**Server**“, den **Computernamen** oder die **IP-Adresse** des Computers ein, auf dem das **MailGateway** installiert wurde.

Aufbau G DATA MailSecurity Administrator

Die Bedienung von **G DATA MailSecurity** ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links im **G DATA MailSecurity Administrator** angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen **Programmbereich** und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen. Folgende **Programmbereiche** stehen Ihnen zur Verfügung:



Status-Bereich



Filter-Bereich



Warteschlangen-Bereich



Aktivität-Bereich



Virenfunde-Bereich

Außerdem finden Sie in der oberen Menüleiste der Programmoberfläche übergreifende Funktionen und Einstellungsmöglichkeiten.



Optionen-Bereich: Hier können Sie grundlegende Einstellungen zum Betrieb Ihres **G DATA MailSecurity** verändern und an individuelle Bedürfnisse anpassen.



Spamfilter-Bereich: Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren.



Internet Update-Bereich: Im Internet Update-Bereich können Sie grundlegende Einstellungen zum automatischen Download von aktuellen Virensignaturen aus dem Internet vornehmen. Sie können die Zeitplanungen für diese Downloads individuellen Bedürfnissen anpassen und außerdem Updates der Programmdateien von **G DATA MailSecurity** durchführen.



Virenlexikon-Bereich: Über diesen Button werden sie direkt mit dem großen **AntiVirusLab-Virenlexikon** (www.antiviruslab.com) verbunden. Diese umfangreiche **Online-Lexikon** beinhaltet Informationen zu aktuellen Viren und bietet ein umfangreiches **Archiv**, in dem schon bekannte Viren und ihre Schadfunktionen ausführlich erläutert werden.




Hilfe-Bereich: Hier rufen Sie die **Online-Hilfe** zum Produkt auf.




Info-Bereich: Hier erhalten Sie Informationen zur **Programmversion**.

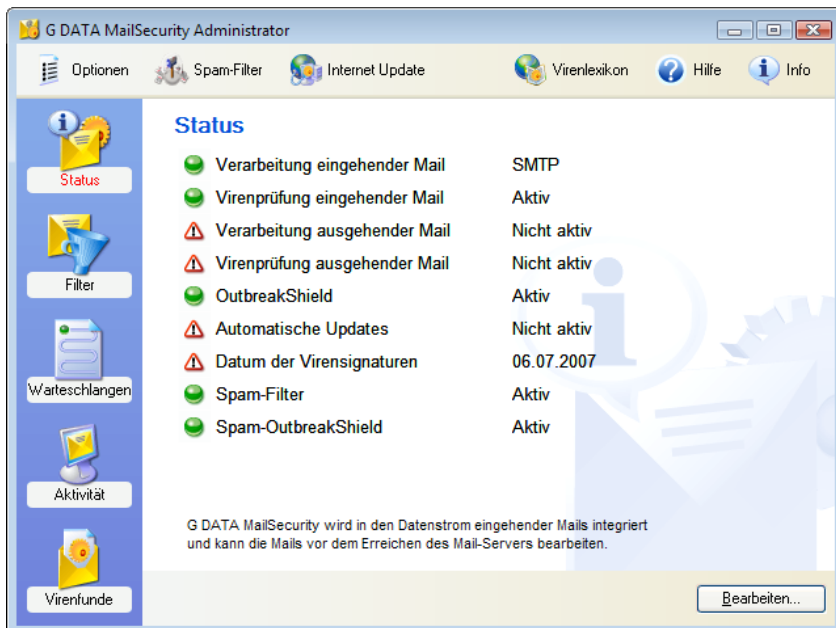
■ Status-Bereich

Im Status-Bereich des **Administrators** erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und des **MailGateways**. Diese finden sich rechts vom jeweiligen Eintrag als Text-, Zahl- oder Datumsangabe.

 Solange Ihr **G DATA MailSecurity** optimal für den Schutz vor Computerviren konfiguriert ist, finden Sie links vor den hier aufgeführten Einträgen ein grünes **Ampelsymbol**.

 Sollte eine Komponente nicht optimal eingestellt sein (z.B. veraltete Virensignaturen, abgeschaltete Virenprüfung), weist Sie ein **Achtung-Symbol** darauf hin.

Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken des „**Bearbeiten...**“-Buttons) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit **Achtung-Symbol** optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Ampelsymbol.



Komponente	Status	Wert
Verarbeitung eingehender Mail	Aktiv	SMTP
Virenprüfung eingehender Mail	Aktiv	Aktiv
Verarbeitung ausgehender Mail	Nicht aktiv	Nicht aktiv
Virenprüfung ausgehender Mail	Nicht aktiv	Nicht aktiv
OutbreakShield	Aktiv	Aktiv
Automatische Updates	Nicht aktiv	Nicht aktiv
Datum der Virensignaturen	Nicht aktiv	06.07.2007
Spam-Filter	Aktiv	Aktiv
Spam-OutbreakShield	Aktiv	Aktiv

G DATA MailSecurity wird in den Datenstrom eingehender Mails integriert und kann die Mails vor dem Erreichen des Mail-Servers bearbeiten.

[Bearbeiten...](#)

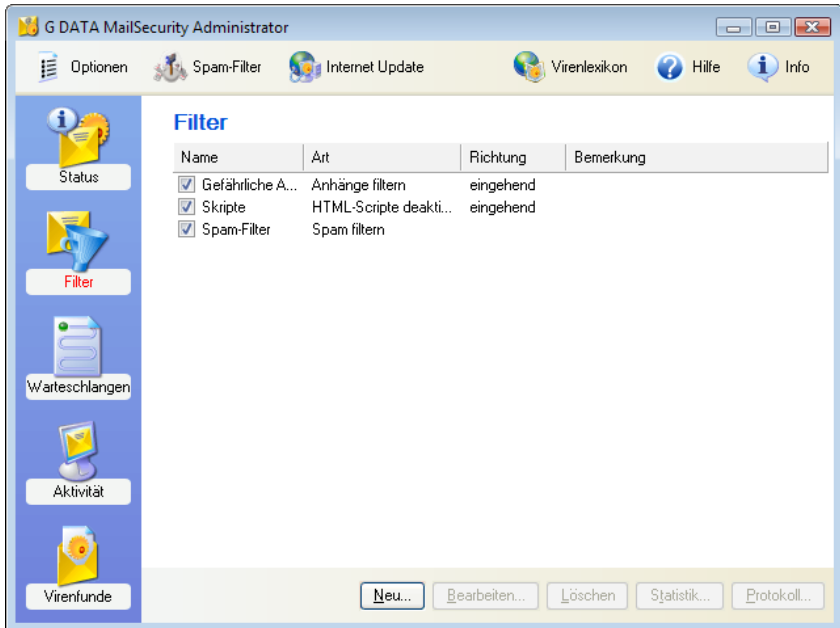
Folgende Einträge stehen Ihnen zur Verfügung

- **Verarbeitung eingehender Mails:** Die Verarbeitung **eingehender Mails** sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Eingehend (SMTP)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung eingehender Mails:** Die Prüfung **eingehender Mails verhindert**, dass infizierte Dateien in Ihr Netz gelangen. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Virenprüfung**) und können die Prüfung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Verarbeitung ausgehender Mails:** Die Verarbeitung **ausgehender Mails** sorgt dafür, dass Mails vor der Weitergabe an den Empfänger durch das MailGateway überprüft werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Ausgehend (SMTP)**) und können die Verarbeitung eingehender Mails an individuelle Bedürfnisse anpassen.
- **Virenprüfung ausgehender Mails:** Die Prüfung **ausgehender Mails** verhindert, dass aus Ihrem Netz infizierte Dateien verschickt werden. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Optionen > Virenprüfung**) und können die Prüfung ausgehender Mails an individuelle Bedürfnisse anpassen.
- **OutbreakShield:** Mit dem **OutbreakShield** können Schädlinge in **Massenmails** schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht.
- **Automatische Updates:** Die **Virensignaturen** können selbstständig aktualisiert werden. Sie sollten die Option für automatische **Updates** generell aktiviert haben. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Internet Update**) und können die Updatefrequenz an individuelle Bedürfnisse anpassen.
- **Datum der Virensignaturen:** Je aktueller die **Virensignaturen**, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten und diesen Prozess möglichst automatisieren. Wenn Sie einen Doppelklick auf diesen Eintrag ausführen, gelangen Sie in das dazugehörige Einstellungsfenster (Menüleiste: **Internet Update**) und können auch direkt ein Internet Update (unabhängig von etwaigen Zeitplänen) durchführen.

- **Spam-Filter:** Über den **Spam-Filter** haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren.
- **Spam-OutbreakShield:** Mit dem **Spam-OutbreakShield** können Massenmails schnell und sicher erkannt und bekämpft werden. Das Spam-OutbreakShield erfragt dabei vor dem Abruf von Mails über das Internet besondere Häufungen von verdächtigen Mails ab und lässt diese gar nicht erst in das Postfach des Empfängers gelangen.

■ Filter-Bereich

Im Filter-Bereich können Sie auf komfortable Weise Filter nutzen, die ein- und ausgehende Mails blocken oder automatisch möglicherweise gefährlichen Inhalte aus Mails entfernen. Dazu können Sie über den **„Neu-Button“** im neue Filterregeln anlegen oder über den **„Bearbeiten-Button“** vorhandene Filter bearbeiten.



Die erstellten Filter werden in der Liste im Filter-Bereich angezeigt und können über die **Häkchenfelder** links vom jeweiligen Eintrag beliebig an- bzw. abgeschaltet werden. Wenn sich ein Häkchen im Häkchenfeld befindet, ist der jeweilige Filter aktiv. Wenn sich kein Häkchen im Häkchenfeld befindet, ist der Filter nicht aktiv. Um einen Filter endgültig zu löschen, markieren Sie diesen bitte mit einem einfachen Mausklick und verwenden dann den **„Löschen-Button“**.

- *Selbstverständlich ist Ihr Netzwerk auch unabhängig von individuellen Filterregeln vor Virenbefall geschützt, da **G DATA MailSecurity** ständig im Hintergrund eingehende und ausgehende Mails überprüft. **Filterregeln** dienen eher dazu, Ihre E-Mail-Accounts vor unerwünschten Mails, Spam und unsicheren Scripten zu bewahren und potentielle Virenherde schon vor der eigentlichen Virenerkennung durch **G DATA MailSecurity** zu minimieren.*

- Für den **Spam-Filter** gibt es ein Protokoll mit einer Liste, in der die als Spam eingestuftten Mails aufgelistet sind. Sie können dieses **Protokoll** im **Filter-Bereich** über den Button „**Protokoll**“ aufrufen, wenn Sie den Filter namens „**Spam-Filter**“ in der Filterliste mit der Maus markieren. Dem Protokoll kann man auch entnehmen, welche Kriterien für die Einstufung als Spam verantwortlich waren (**Spam-Index-Werte**).

Datum/Uhrzeit	Spamwahrs...	Sender	Empfänger	Betreff	Spam-Index
04.05.2007 13:33	Verdacht	a_sadiq@nokia...		We bring forwa...	12
04.05.2007 13:33	Sehr hoch	Shanna.Rivers...		job: just for you.	42
04.05.2007 13:31	Sehr hoch	smokiestricket...		Special offer	30
04.05.2007 13:30	Hoch	a_randall@adte...		Just \$0.87 per ...	17
04.05.2007 13:26	Sehr hoch	bllon@lovelet...		Intuitive Standard	27
04.05.2007 13:24	Sehr hoch	xhjuxedjyxr@...		Hey I missed yo...	31
04.05.2007 13:22	Sehr hoch	hhlbnovn@net.th		Ragland	39
04.05.2007 13:21	Sehr hoch	icidhxvfm@co...		Sehen Sie G7Q ...	31
04.05.2007 13:20	Sehr hoch	lupfvuady@co...		Verpassen Sie d...	33
04.05.2007 13:20	Sehr hoch	dnconsultfem...		re:Can't find go...	20
04.05.2007 13:18	Sehr hoch	zlighttower@ep...		You can be with...	24
04.05.2007 13:15	Sehr hoch	Dana@ritches...		Low-price Viagr...	40
04.05.2007 13:13	Sehr hoch	darth91@leil.is		CIALLis Soft is u...	44
04.05.2007 13:13	Sehr hoch	Jewel@uk.york...		Would you like /...	32
04.05.2007 13:10	Verdacht	PoloLeone13492...		¡¡¡EEI v aEEÖÖ...	14
04.05.2007 13:09	Sehr hoch	givobushiq@ya...		Harder and Ple...	34
04.05.2007 13:09	Sehr hoch	hglzptlygoyf@...		Longer...Harder	34
04.05.2007 13:09	Sehr hoch	jeeqjujh@hotmail...		Does 8 inches	34
04.05.2007 13:08	Sehr hoch	gazneffs@cod...		Try out all night...	29
04.05.2007 13:08	Sehr hoch	eadeviston@n...		Don't spend a l...	33

Hier können Sie ggf. bei einer fälschlichen Einstufung einer Mail als Spam den **OutbreakShield-Server** online darüber informieren, dass hier eine **Fehlkennung („False Positive“)** vorliegt. Die Mail wird dann vom OutbreakShield erneut geprüft und - falls sie tatsächlich fälschlicherweise als Spam erkannt wurde - des Weiteren als unbedenklich eingestuft.

- **Achtung:** Hierbei wird lediglich eine Prüfsumme übermittelt und nicht der Inhalt dieser Mail.

Spam

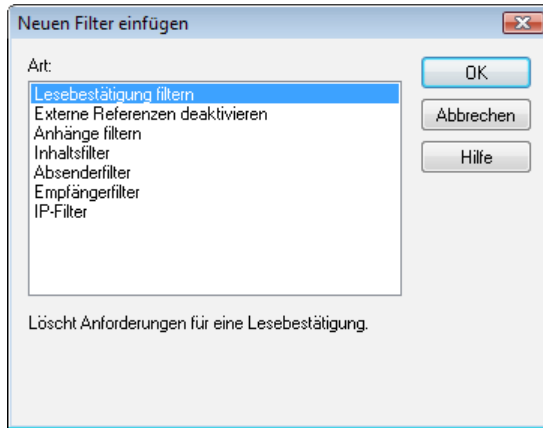
Datum/Uhrzeit: 04.05.2007 13:09

Absender: jeeqjujh@hotmail.com
 Empfänger: hotline@gdata.de
 Betreff: Does 8 inches Enough 4 U?

Spamwahrscheinlichkeit: Sehr hoch
 Spam-Index: 34
 Spam-Index-Details: Blacklist: 14, Mailtext: 5, OutbreakShield: 15

Kein Spam? Schließen

Wenn Sie einen neuen Filter anlegen, öffnet sich ein **Auswahlfenster**, in dem Sie den grundlegenden **Filtertyp** festlegen können. Alle weiteren Angaben zum zu erstellenden Filter können Sie dann in einem dem Filtertyp angepassten **Assistentenfenster** angeben. Auf diese Weise erstellen Sie auf sehr komfortable Weise Filter gegen jede erdenkliche Gefährdung.



Folgende Filtertypen stehen Ihnen zur Verfügung. Diese werden in den folgenden Abschnitten ausführlich erläutert:

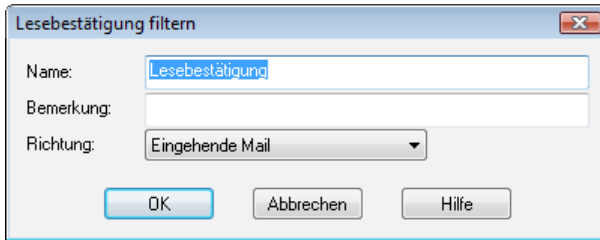
- **Lesebestätigung filtern**
- **HTML-Scripte deaktivieren**
- **Externe Referenzen deaktivieren**
- **Anhänge filtern**
- **Inhaltsfilter**
- **Absenderfilter**
- **Empfängerfilter**
- **Spam filtern**
- **IP-Filter**

Generell können Sie bei allen Filtertypen unter „**Name**“ einen aussagekräftigen Namen für den jeweiligen Filter angeben, mit dem dieser Filter dann in der Liste des Filter-Bereichs angezeigt wird und Sie können unter „**Bemerkung**“ interne Bemerkungen und Notizen zu dem betreffenden Filter angeben.

Unter „**Richtung**“ können Sie generell bestimmen, ob eine Filterregel nur für eingehende Mails, nur für ausgehende Mails oder beide Richtungen gelten soll.

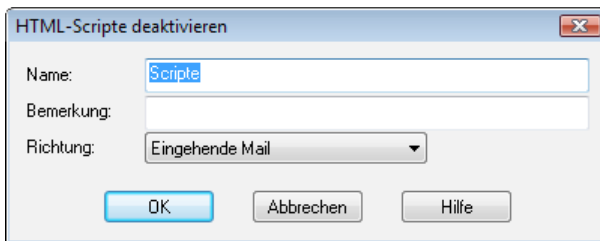
■ Lesebestätigung filtern

Dieser Filter löscht Anforderungen für eine Lesebestätigung. Dabei handelt es sich um eine **Rückantwortmail**, die automatisch abgeschickt wird, sobald der Empfänger eine solche Mail mit Lesebestätigung gelesen hat.



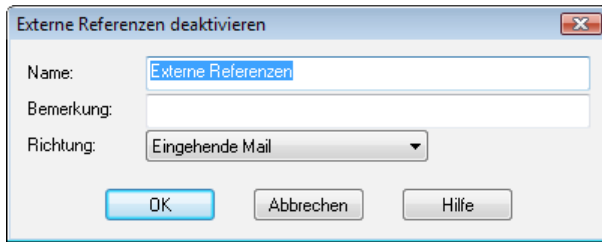
■ HTML-Skripte deaktivieren

Dieser Filter deaktiviert Skripte im **HTML-Teil einer Mail**. Skripte, die in einer Internetseite durchaus einen Sinn haben mögen, sind - wenn sie in eine HTML-Mail eingebunden sind - eher störend. In manchen Fällen werden HTML-Skripte auch aktiv dazu verwendet, Rechner zu infizieren, wobei Skripte die Möglichkeit haben, sich nicht erst durch das Öffnen einer infizierten Anlage weiterzuverbreiten, sondern alleine schon in der **Vorschauansicht** einer Mail wirksam werden können.



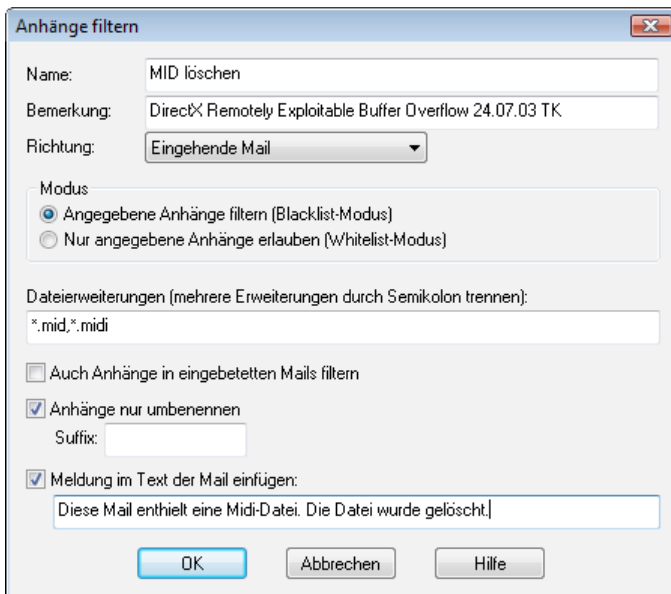
■ Externe Referenzen deaktivieren

Viele Newsletter und Produktinformationen im HTML-Mailformat beinhalten **Links**, die erst dann ausgeführt und angezeigt werden, wenn die Mail geöffnet wird. Dies können z.B. Grafiken sein, die nicht mit der Mail versandt wurden, sondern erst über einen **Hyperlink** automatisch nachgeladen werden. Da es sich hierbei nicht nur um ‚harmlose‘ Grafiken handeln kann, sondern durchaus auch um **Schadroutinen**, ist es durchaus sinnvoll, diese Referenzen zu deaktivieren. Der eigentliche Mail-Text ist von dieser Deaktivierung nicht betroffen.



■ Anhänge filtern

Beim Filtern von Anhängen haben Sie eine große Auswahl von Möglichkeiten, um **Mail-Anhänge (= Attachments)** und Anlagen zu filtern. Die meisten E-Mailviren verbreiten sich über solche Attachments, die in den meisten Fällen mehr oder minder gut verborgene ausführbare Dateien enthalten. Dabei kann es sich um eine klassische **EXE-Datei** handeln, die ein Schadprogramm enthält, aber auch um **VBS-Skripte**, die sich unter bestimmten Voraussetzungen sogar hinter vermeintlich sicheren Grafik-, Film- oder Musikdateien verbergen. Generell sollte jeder Anwender bei der Ausführung von Mail-Anhängen große Vorsicht walten lassen und im Zweifelsfall lieber noch einmal eine Rückfrage beim Absender einer Mail durchführen, bevor er eine Datei ausführt, die er nicht ausdrücklich angefordert hat.



Unter „**Dateierweiterungen**“ können Sie die **Dateiendungen** aufzählen, auf die Sie den jeweiligen Filter anwenden möchten. Dabei können Sie z.B. alle **ausführbaren Dateien** (z.B. **EXE** und **COM**-Dateien) in einem Filter zusammenfassen, aber auch andere Formate (z.B. **MPEG**, **AVI**, **MP3**, **JPEG**, **JPG**, **GIF** etc.) filtern, wenn diese aufgrund Ihrer Größe eine Belastung für den Mailserver darstellen. Selbstverständlich können Sie auch beliebige **Archivdateien** (z.B. **ZIP**, **RAR** oder **CAB**) filtern.

Trennen Sie bitte alle Dateierweiterungen einer Filtergruppe durch **Semikolon**, z.B. „*.exe;*.dll“.

Über die Funktion „**Auch Anhänge in eingebetteten Mails filtern**“ sorgen Sie dafür, dass die Filterung der unter „**Dateierweiterungen**“ ausgewählten Anlagentypen auch in Mails stattfindet, die selber eine Anlage einer Mail darstellen. Diese Option sollte generell aktiviert sein.

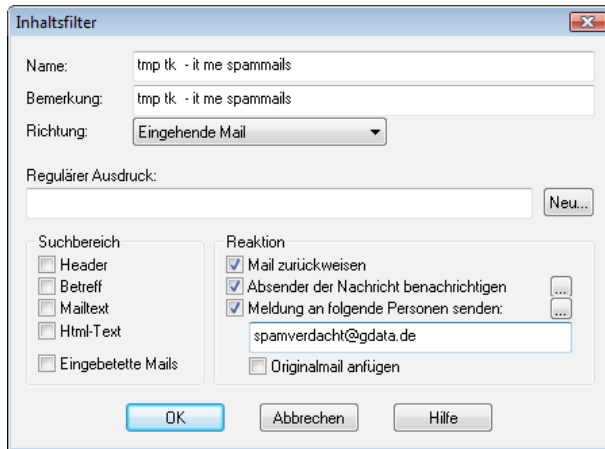
Über „**Anhänge nur umbenennen**“ werden die zu filternden Anlagen nicht automatisch gelöscht, sondern nur umbenannt. Dies ist z.B. bei ausführbaren Dateien (wie z.B. EXE und COM) durchaus sinnvoll, aber auch bei Microsoft Office-Dateien, die möglicherweise ausführbare **Scripte** und **Makros** enthalten könnten. Durch das Umbenennen einer Anlage kann Sie nicht unbedacht durch einfachen Mausklick geöffnet werden, sondern muss vom Empfänger erst abgespeichert und ggf. wieder umbenannt werden, bevor er sie verwenden kann. Wenn das „**Häkchen bei Anhänge nur umbenennen**“ nicht gesetzt ist, werden die entsprechenden Anhänge direkt gelöscht.

Unter „**Suffix**“ geben Sie die Zeichenfolge ein, mit der Sie die eigentliche **Dateiendung erweitern** möchten, auf diese Weise wird die **Ausführbarkeit** einer Datei durch einfaches Anklicken verhindert (z.B. „*.exe.danger“).

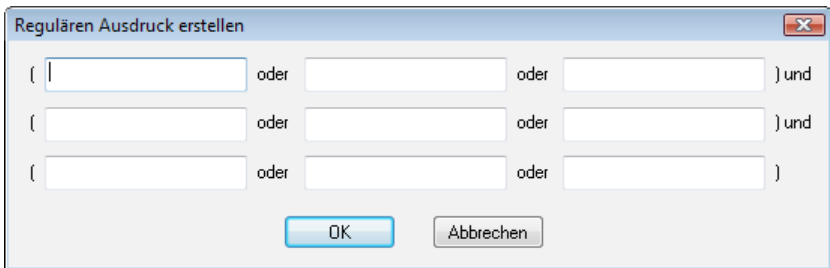
Unter „**Meldung im Text der Mail einfügen**“ können Sie den Empfänger der gefilterten Mail darüber informieren, dass ein Anhang aufgrund einer Filterregel gelöscht oder umbenannt wurde.

■ Inhaltsfilter

Über den Inhaltsfilter können Sie E-Mails, die bestimmte Themen oder Texte enthalten auf bequeme Weise blocken. Geben Sie dazu unter „**Regulärer Ausdruck**“ einfach die **Schlüsselwörter** und **Ausdrücke** ein, auf die **G DATA MailSecurity** reagieren soll und geben Sie unter „**Suchbereich**“ an, in welchen Bereichen einer Mail nach diesen Ausdrücken gesucht werden soll. Unter „**Reaktion**“ können Sie festlegen, ob Mails mit entsprechendem Inhalt nicht an den Empfänger übermittelt werden sollen (**Mail zurückweisen**) und/oder ob der Absender der Mail und andere Personen über die „**Aktivierung des Content Filters**“ informiert werden.



Über den „**Neu-Button**“ rechts vom Eingabefeld für „**Regulärer Ausdruck**“ können Sie auf bequeme Weise Text eingeben, der eine Filteraktion hervorruft. Dabei können Sie Text auf beliebige Weise mit den **logischen Operatoren UND und ODER** verknüpfen.



- Wenn Sie z.B. **sex** „**ODER**“ **drugs** „**ODER**“ **rock’n’roll** eingeben „**UND**“ **wein** „**ODER**“ **weib** „**ODER**“ **gesang**, würde der Filter bei einer Mail, die z.B. die Begriffe „**drugs**“ und „**wein**“ enthält, aktiviert werden, nicht aber bei einer Mail, die nur den Begriff „**drugs**“ oder nur den Begriff „**wein**“ enthält. Der logische Operator „**UND**“ setzt also voraus, dass alle mit „**UND**“ verknüpften Elemente vorhanden sind, der logische Operator „**ODER**“ setzt lediglich voraus, dass ein Element vorhanden ist.

Sie können auch ohne die Eingabehilfe unter **Regulärer Ausdruck** beliebige **Suchbegriffe** miteinander kombinieren. Geben Sie dazu einfach die Suchbegriffe ein und verknüpfen diese mit den logischen Operatoren:

ODER entspricht dem Trennstrich (AltGr + <) = |
UND entspricht dem Kaufmanns-Und (Shift + 6) = &

Sie können den Text für die Funktionen „**Absender benachrichtigen**“ und „**Meldung an folgende Personen senden**“ individuell gestalten. Klicken Sie dazu einfach auf den „**•••-Button**“ rechts von der jeweiligen Reaktion. Dabei können Sie auch **Platzhalter** verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen.

The dialog box titled "Absender benachrichtigen" has a "Betreff:" field containing "Nicht zugestellt: %u". The "Mailtext:" area contains the text "Die Nachricht wurde vom Systemadministrator zurückgewiesen." Below this is a "Platzhalter:" list with the following items: %s Absender, %r Empfänger, %c Cc, %d Datum, %u Betreff, %h Header, and %i Absender-IP. At the bottom are "OK" and "Abbrechen" buttons.

The dialog box titled "Meldung" has a "Betreff:" field containing "Nachricht zurückgewiesen". The "Mailtext:" area contains the text "G DATA MailSecurity hat folgende Nachricht zurückgewiesen:" followed by a list of fields: Absender: %s, Empfänger: %r, Cc: %c, Datum: %d, and Betreff: %u. Below this is a "Platzhalter:" list with the following items: %s Absender, %r Empfänger, %c Cc, %d Datum, %u Betreff, %h Header, and %i Absender-IP. At the bottom are "OK" and "Abbrechen" buttons.

Im frei definierbaren Text für den „**Betreff**“ und den „**Mailtext**“ stehen Ihnen folgende „Platzhalter“ (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

- %s** **Absender**
- %r** **Empfänger**
- %c** **Cc**
- %d** **Datum**
- %u** **Betreff**

■ Absenderfilter

Über den Absenderfilter können Sie E-Mails, die von bestimmten Absendern kommen, auf bequeme Weise blocken. Geben Sie dazu unter „**Adressen/Domains**“ einfach die E-Mail-Adressen oder **Domain-Namen** ein, auf die **G DATA MailSecurity** reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen.

- Sie können auch Mails ohne Absenderangabe automatisch ausfiltern.*

Unter „**Reaktion**“ können Sie festlegen, ob Mails mit entsprechendem Inhalt nicht an den Empfänger übermittelt werden sollen (**Mail zurückweisen**) und/oder ob der Absender der Mail und andere Personen über die Aktivierung des Content Filters informiert werden.

Absenderfilter

Name:

Bemerkung:

Richtung:

Adressen/Domains (mehrere Einträge durch Semikolon trennen):

Mails ohne Absender filtern

Reaktion

Mail zurückweisen

Absender der Nachricht benachrichtigen

Meldung an folgende Personen senden:

Originalmail anfügen

OK Abbrechen Hilfe

Sie können den Text für die Funktionen „**Absender benachrichtigen**“ und „**Meldung an folgende Personen senden**“ individuell gestalten. Klicken Sie dazu einfach auf den „...-Button“ rechts von der jeweiligen „Reaktion“. Dabei können Sie auch „**Platzhalter**“ verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den **Benachrichtigungstext** übernehmen. Lesen Sie hierzu auch die Ausführungen im Abschnitt „**Inhaltsfilter**“.

■ Empfängerfilter

Über den Empfängerfilter können Sie E-Mails für bestimmte Empfänger auf bequeme Weise blocken. Geben Sie dazu unter „**Adressen/Domains**“ einfach die E-Mail-Adressen oder **Domain-Namen** ein, auf die **G DATA MailSecurity** reagieren soll. Mehrere Einträge können Sie durch Semikolon voneinander trennen.

- *Sie können auch Mails mit **leerem Empfängerfeld** (also Mails, die nur **Bcc-** und/oder **Cc-Empfänger** enthalten) automatisch ausfiltern.*

Unter „**Reaktion**“ können Sie festlegen, ob Mails mit entsprechendem Inhalt nicht an den Empfänger übermittelt werden sollen (**Mail zurückweisen**) und/oder ob der Absender der Mail und andere Personen über die Aktivierung des Content Filters informiert werden.

Empfängerfilter

Name:

Bemerkung:

Richtung:

Adressen/Domains (mehrere Einträge durch Semikolon trennen):

Mails mit nur Cc- oder Bcc-Empfängern filtern (leeres Empfängerfeld)

Reaktion

Mail zurückweisen

Absender der Nachricht benachrichtigen

Meldung an folgende Personen senden:

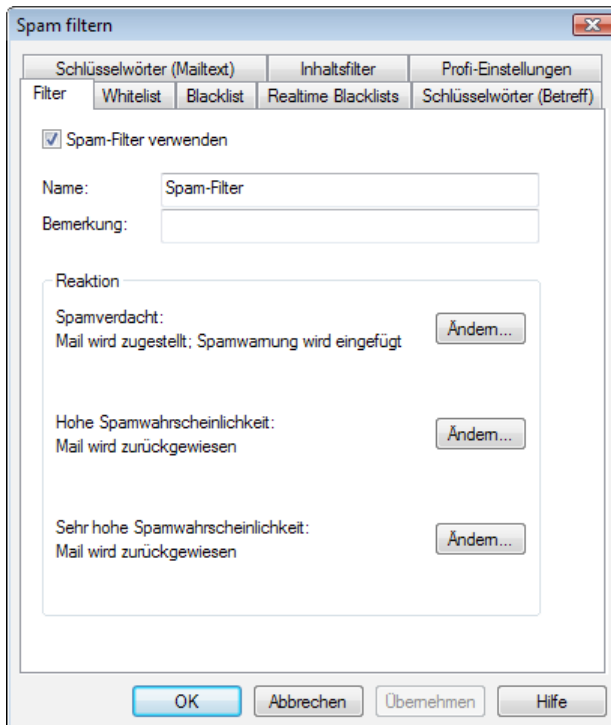
Originalmail anfügen

OK Abbrechen Hilfe

Sie können den Text für die Funktionen „**Absender benachrichtigen**“ und „**Meldung an folgende Personen senden**“ individuell gestalten. Klicken Sie dazu einfach auf den „...-Button“ rechts von der jeweiligen Reaktion. Dabei können Sie auch „**Platzhalter**“ verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen. Lesen Sie hierzu auch die Ausführungen im Abschnitt „**Inhaltsfilter**“.

■ Spam filtern

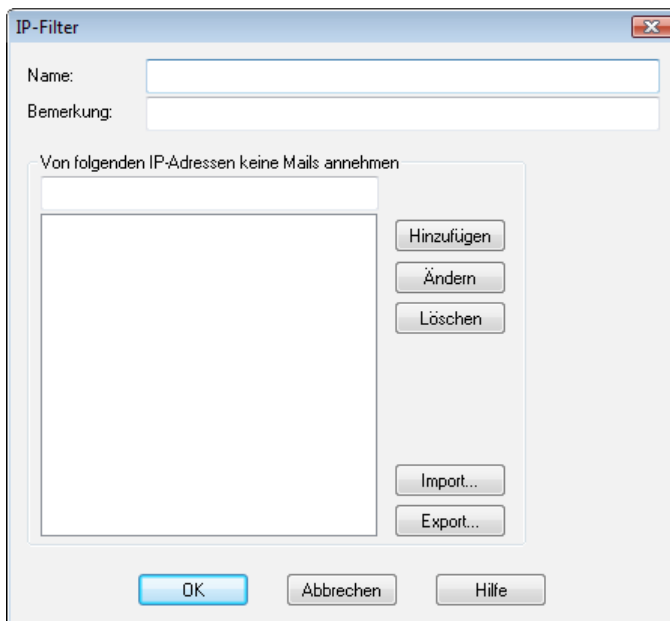
Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. **Massenmailversendern**) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen. Die Funktionsweise und Einstellungsmöglichkeiten des Spamfilters werden im Kapitel „**Spamfilter-Bereich**“ ausführlich erläutert.



■ IP-Filter

Der IP-Filter unterbindet den Empfang von Mails, die von bestimmten **Servern** abgesendet werden. Geben Sie hier unter „**Name**“ und „**Bemerkung**“ Informationen dazu ein, wieso sie die jeweiligen **IP-Adressen** sperren möchten und dann jede einzelne IP-Adresse unter „**Von folgenden IP-Adressen keine Mails annehmen**“ ein. Klicken Sie auf „**Hinzufügen**“ und die aktuell eingetragene IP-Adresse wird in die Liste der gesperrten IP-Adressen übernommen.

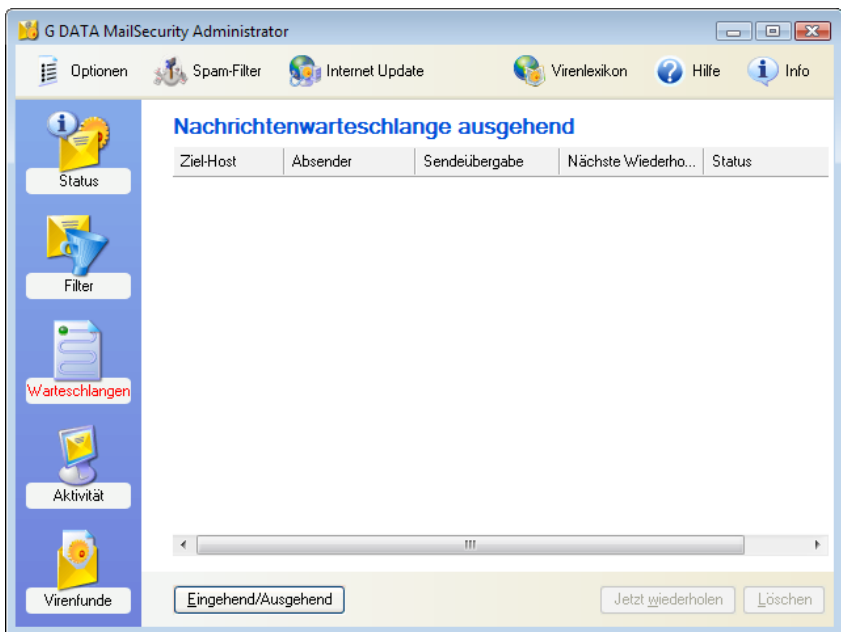
- *Sie können die Liste der IP-Adressen auch als txt-Datei **exportieren** oder eine entsprechende txt-Liste mit IP-Adressen **importieren**.*



The screenshot shows a dialog box titled "IP-Filter" with a standard Windows window border. At the top, there are two text input fields: "Name:" and "Bemerkung:". Below these is a section titled "Von folgenden IP-Adressen keine Mails annehmen" which contains a large empty list box. To the right of the list box are five buttons: "Hinzufügen", "Ändern", "Löschen", "Import...", and "Export...". At the bottom of the dialog are three buttons: "OK", "Abbrechen", and "Hilfe".

■ Warteschlangen-Bereich

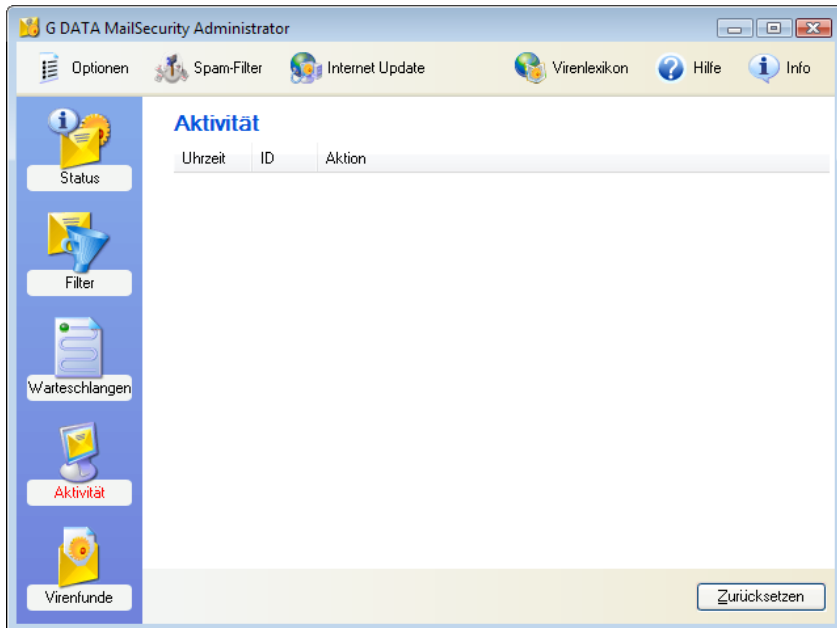
Im Warteschlangen-Bereich haben Sie jederzeit Überblick über eingehende und ausgehende Mails, die im MailGateway auflaufen und auf Viren und/oder Content überprüft werden. Die Mails werden in der Regel sofort weitergeleitet, durch das MailGateway nur minimal **verzögert** und dann auch sofort wieder aus der Warteschlangen-Liste gelöscht. Sobald eine Mail nicht **zustellbar** ist oder sich **Verzögerungen** in der **Zustellung** ergeben (weil der jeweilige Server z.B. momentan nicht erreichbar ist), erfolgt in der Warteschlangenliste ein entsprechender Eintrag. **G DATA MailSecurity** versucht dann in einstellbaren **Abständen** (unter „**Optionen > Warteschlange**“) die Mail erneut zu verschicken. Eine nicht erfolgte oder verzögerte **Mailzustellung** wird auf diese Weise jederzeit dokumentiert.



Über den Button „**Eingehend/Ausgehend**“ wechseln Sie von der „**Listenansicht für eingehende Mails**“ zur „**Listenansicht für ausgehende Mails**“. Über den Button „**Jetzt wiederholen**“ können Sie eine markierte Mail, die nicht zugestellt werden konnte - unabhängig von den „**Zeitvorgaben**“, die Sie für eine erneute Zustellung unter „**Optionen > Warteschlange**“ definiert haben - erneut zustellen. Mit dem „**Löschen-Button**“ entfernen Sie eine nicht zustellbare Mail endgültig aus der **Queue**.

■ Aktivität-Bereich

Im Aktivität-Bereich haben Sie jederzeit Überblick über die von **G DATA MailSecurity** durchgeführten Aktionen. Diese werden mit **Uhrzeit, ID** und **Aktionsbeschreibung** in der **Aktivität-Liste** aufgelistet. Mit dem **Scrollbalken** rechts können Sie in dem Protokoll auf und abscrollen. Über den „**Zurücksetzen-Button**“ löschen Sie das bis dahin erzeugte Protokoll und **G DATA MailSecurity** beginnt die Aufzeichnung der Aktivitäten erneut.



- Über die **ID** können Sie die protokollierten Aktionen eindeutig einzelnen Mails zuordnen. So gehören Vorgänge mit gleicher ID immer zusammen (z.B. 12345 Lade Mail, 12345 Verarbeite Mail, 12345 Sende Mail).

■ Virenfunde-Bereich

Im Virenfunde-Bereich werden sie detailliert darüber informiert, wann **G DATA MailSecurity** eine infizierte Mail ermittelt hat, welche Maßnahmen dahingehend erfolgten (Status: Virenbestandteile gelöscht, Anlage entfernt, Mail nicht weitergeleitet etc.), um welche Art von Virus es sich handelt und wer die eigentlichen Sender und Empfänger dieser betreffenden Mail sind.

Datum/Uhrzeit	Virus	Status	Sender	Empfänger
04.05.2007 13:44	W32/Sober.AT...	Nachricht gelös...	<Postmaster@h...	mailserver@gda
04.05.2007 13:39	W32/Sober.AT...	Nachricht gelös...	<Webmaster@w...	listening@gdata
04.05.2007 13:39	W32/Netsky.P...	Nachricht gelös...	<idqct@mail.com>	newsletter@gda
04.05.2007 13:26	W32/Sober.AT...	Nachricht gelös...	<Webmaster@m...	hotline@gdata.c
04.05.2007 13:20	W32/Sober.AT...	Nachricht gelös...	<Postmaster@a...	electronicpartne
04.05.2007 13:18	W32/Sober.AT...	Nachricht gelös...	<Webmaster@a...	address@gdata.
04.05.2007 13:15	W32/Sober.AT...	Nachricht gelös...	<Postmaster@h...	e-user@gdata.d
04.05.2007 13:09	W32/Sober.AT...	Nachricht gelös...	<Webmaster@h...	silver-certs@gde
04.05.2007 13:09	W32/Sober.AT...	Nachricht gelös...	<Postmaster@w...	XPost@gdata.di
04.05.2007 13:08	W32/Sober.AT...	Nachricht gelös...	<Hostmaster@m...	listening338@gc
04.05.2007 13:06	W32/Sober.AT...	Nachricht gelös...	<Hostmaster@m...	mortbay@gdata.
04.05.2007 13:04	W32/Sober.AT...	Nachricht gelös...	<Hostmaster@h...	mailserver7541..
04.05.2007 13:03	W32/Sober.AT...	Nachricht gelös...	<Postmaster@h...	Z-Account@gde
04.05.2007 13:02	W32/Sober.AT...	Nachricht gelös...	<Postmaster@mi...	e-user@gdata.d
04.05.2007 12:59	W32/Sober.AT...	Nachricht gelös...	<Webmaster@h...	silver-certs@gde
04.05.2007 12:58	W32/Sober.AT...	Nachricht gelös...	<Webmaster@g...	email9370@gda

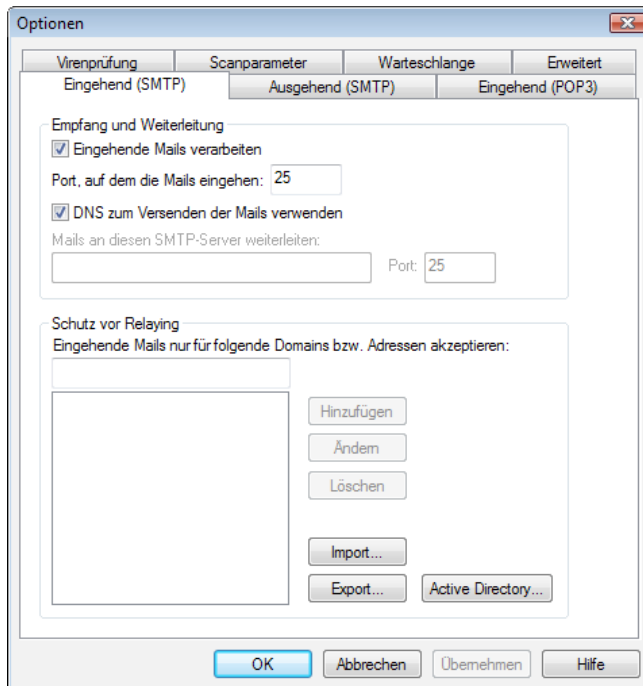
Über den „**Vireninformation-Button**“ können Sie die Internetseite des **AntiVirusLab** aufrufen, um detaillierte Informationen zum gefundenen Virus zu erhalten. Über „**Löschen**“ entfernen Sie die jeweils ausgewählte Virenmeldung aus der Virenfunde-Liste.

Optionen-Bereich

Im **Optionen-Bereich** können Sie umfangreiche Einstellungen vornehmen, um **G DATA MailSecurity** optimal auf die Gegebenheiten anzupassen, die in Ihrem **Netzwerk** existieren. Dazu stehen Ihnen verschiedene thematisch untergliederte **Einstellungsbereiche** in verschiedenen **Karteikarten** zur Verfügung, die Sie durch Anklicken des jeweiligen **Karteireiters** in den Vordergrund holen. Allgemein gilt, dass Sie mit dem „**OK-Button**“ durchgeführte Änderungen übernehmen und den Optionen-Bereich schließen, über „**Abbrechen**“ werden keine Änderungen übernommen und mit dem „**Übernehmen-Button**“ werden die bis dahin durchgeführten Änderungen im Optionen-Bereich ins Programm übernommen, ohne, dass der Optionen-Bereich geschlossen wird. Die Einstellungen, die Sie in den einzelnen Karteikarten vornehmen können, werden Ihnen in den folgenden Kapiteln ausführlich erläutert.

■ Eingehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



■ Empfang und Weiterleitung

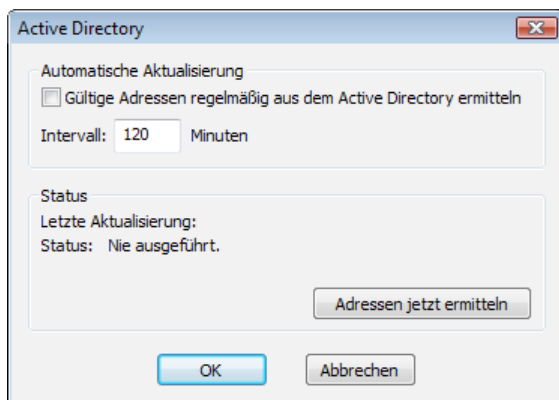
Unter **“Port, auf dem die Mails eingehen“** müssen Sie den Port angeben, den Sie für eingehende Mails in Ihrem Netzwerk verwenden. Zur **Weiterleitung der eingehenden Mails an Ihren Mail-Server** deaktivieren Sie bitte die Option **„DNS zum Versenden der Mails verwenden“** und geben Sie unter **„Mails an diesen SMTP-Server weiterleiten“** den gewünschten Server an. Geben Sie bitte auch den **„Port“** an, über den die Mails an den **SMTP-Server** weitergeleitet werden sollen.

■ Schutz vor Relaying

Um einen Missbrauch Ihres Mail-Servers zu unterbinden, können und sollten Sie unter **“Eingehende Mails nur für folgende Domains akzeptieren“** die Domains festlegen, an die **SMTP-Mails** versendet werden dürfen. Auf diese Weise kann Ihr Server nicht zur **Weiterleitung** von SPAM-Mails an andere Domains missbraucht werden.

- **Achtung:** Wenn Sie hier keine **Domains** eintragen, werden auch keine Mails angenommen. Sollen alle Mails von allen Domains angenommen werden, muss hier ein **„*.“** (Sternchen Punkt Sternchen) hinzugefügt werden.

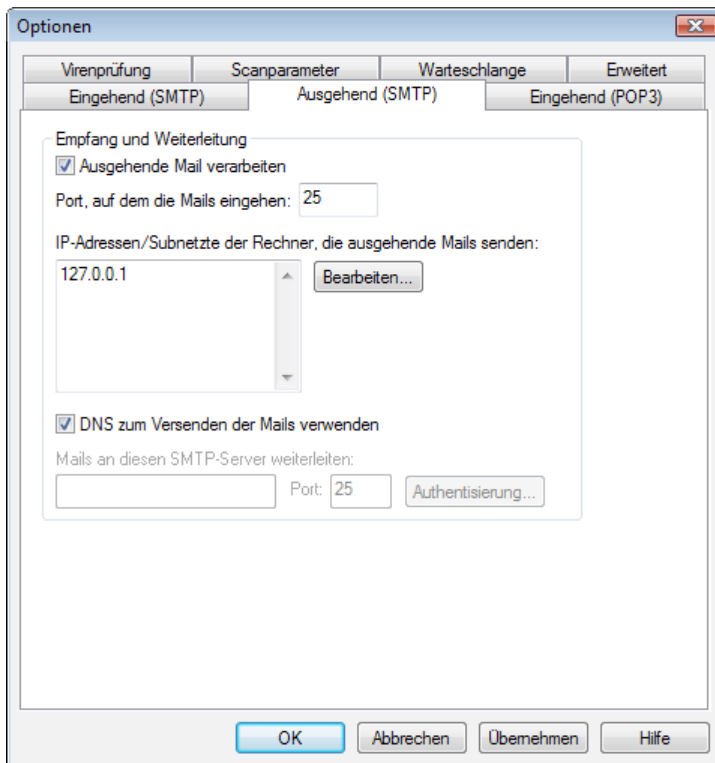
Der **Relay-Schutz** kann wahlweise auch über eine Liste von gültigen E-Mail-Adressen realisiert werden. Mails für Empfänger, die nicht auf der Liste stehen, werden nicht angenommen. Um die Pflege dieser Mailadressen zu automatisieren, können diese automatisch und periodisch aus dem **ActiveDirectory** gelesen werden. Für die ActiveDirectory-Anbindung wird mindestens das **.Net-Framework 1.1** benötigt.



- **Active Directory** ist eine in **Microsoft Windows** (XP, 2000, 2003 Server, Vista) verwendete **Datenbank**, in der vom Administrator Informationen zu Objekten (z.B. Diensten, Ressourcen oder Benutzern) im Netzwerk zentral organisiert, bereitgestellt und überwacht werden können.

■ Ausgehend (SMTP)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle ausgehender SMTP-Mails auf Ihrem Mail-Server vorzunehmen.



■ Empfang und Weiterleitung

Über das Häkchenfeld **“Ausgehende Mail verarbeiten”** legen Sie grundlegend fest, ob Sie ausgehende SMTP-Mails auf Virenbefall kontrollieren möchten oder nicht. Unter **„IP-Adressen der Server, die ausgehende Mails senden“** können Sie festlegen, von welchen IP-Adressen die zu überprüfenden Mails kommen. Wenn

mehrere IP-Adressen dafür in Frage kommen, trennen Sie bitte die einzelnen IP-Adressen durch ein Komma voneinander ab.

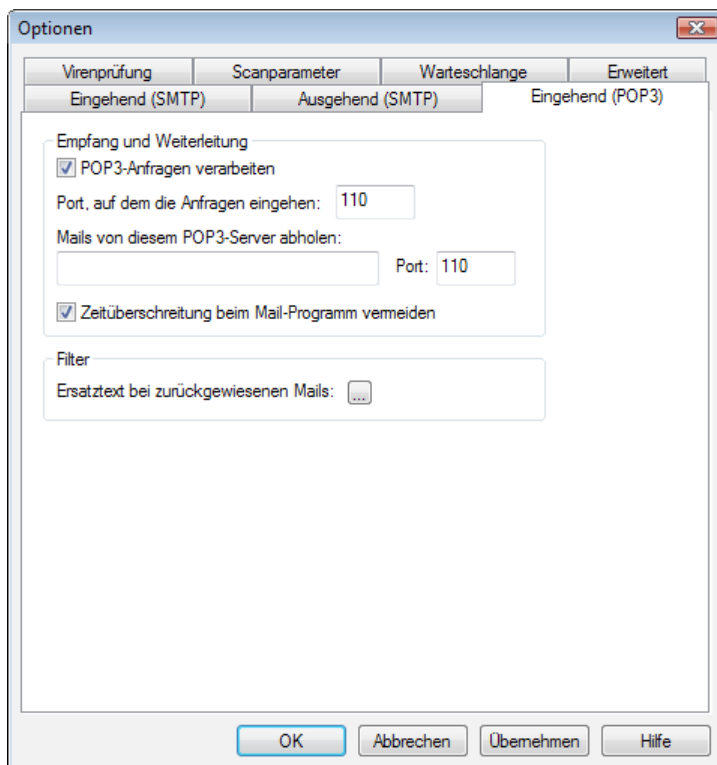
Diese Eingabe ist nötig, damit das MailGateway eingehende und ausgehende Mails voneinander unterscheiden kann.

Unter „**Port, auf dem die Mails eingehen**“ müssen Sie den Port angeben, über den Sie ausgehende Mails über das MailGateway empfangen.

Aktivieren Sie den Eintrag „**DNS zum Versenden der Mails verwenden**“, damit die Mails direkt an den für die **Zieldomäne** zuständigen Mailserver geschickt wird. Wenn Sie die Mails indirekt über ein **Relay** (z.B. einen Provider) versenden möchten, deaktivieren Sie „**DNS zum Versenden der Mails verwenden**“ und geben Sie unter „**Mails an diesen SMTP-Server weiterleiten**“ das Relay an

■ Eingehend (POP3)

In diesem Bereich haben Sie die Möglichkeit, alle notwendigen Einstellungen zur Virenkontrolle eingehender POP3-Mails auf Ihrem Mail-Server vorzunehmen.



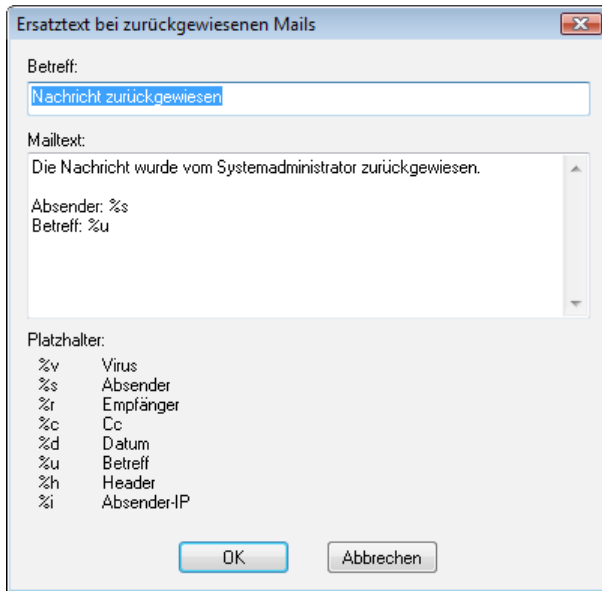
Unter „**POP3-Anfragen verarbeiten**“ aktivieren Sie die Möglichkeit, über **G DATA MailSecurity** Ihrer **POP3-Mails** vom entsprechenden POP3-Server abzuholen, auf Viren zu überprüfen und über Ihren Mail-Server an die Empfänger weiterzuleiten. Sie müssen dazu den „**Port**“ angeben, den Ihr Mailprogramm für POP3-Anfragen verwendet (in der Regel Port 110) und unter „**Mails von diesem POP3-Server abholen**“ den POP3-Server angeben, von dem Sie die Mails abholen (z.B. pop3.mail-dienstanbieter.de). Mit der Funktion „**Zeitüberschreitung beim Mail-Programm vermeiden**“ überbrücken Sie die Zeit, die **G DATA MailSecurity** zum Überprüfen der E-Mails benötigt und verhindern so, dass der Empfänger beim Abruf seiner POP3-Mails möglicherweise vom Mail-Programm einen „**TimeOut-Fehler**“ erhält, weil die Daten nicht sofort zur Verfügung stehen (sondern je nach Mail-Aufkommen erst ein paar Sekunden verzögert).

- ▣ **POP3-basierte Mailprogramme** können manuell konfiguriert werden. Verwenden Sie dabei in Ihrem Mail-Programm „127.0.0.1“ bzw. den **Server Ihres MailGateways** als eingehenden POP3-Server und schreiben Sie den Namen des externen Mail-Servers mit einem Doppelpunkt getrennt vor den Benutzernamen. Also z.B. statt „**POP3-Server:mail.xxx.de/Benutzername: Erika Musterfrau**“ schreiben Sie: „**POP3-Server:127.0.0.1/Benutzername: mail.xxx.de:Erika Musterfrau**“. Um eine **manuelle Konfiguration** durchzuführen, informieren Sie sich bitte auch in der Bedienungsanleitung Ihres Mail-Programms über die notwendigen Schritte für eine manuelle Konfiguration.

■ Filter

Wenn **POP3-Mails** auf Grund einer **Content-Prüfung** oder auf Grund eines Virenbefalls zurückgewiesen werden, kann der Absender dieser Nachricht automatisch darüber informiert werden. Der Ersatztext bei zurückgewiesenen Mails lautet dabei: „Die Nachricht wurde vom Systemadministrator zurückgewiesen“.

Sie können den **Text für diese Benachrichtigungsfunktionen** aber auch individuell gestalten. Klicken Sie dazu einfach auf den „...-Button“ rechts von der **Benachrichtigungsoption**. Dabei können Sie auch **Platzhalter** verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den **Benachrichtigungstext** übernehmen.

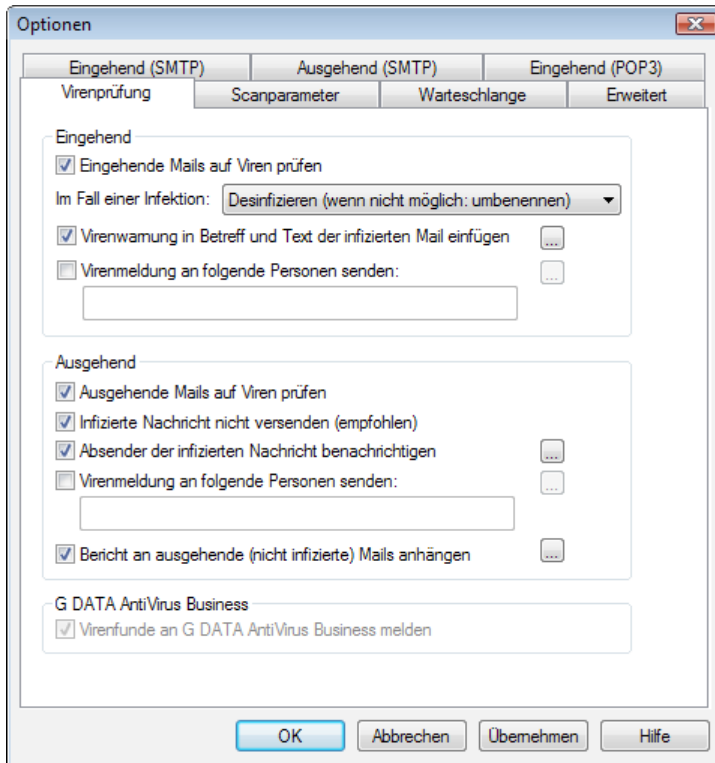


Im frei definierbaren Text für den **Betreff** und den **Mailtext** stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

%v	Virus
%s	Absender
%r	Empfänger
%c	Cc
%d	Datum
%u	Betreff
%h	Header
%i	Absender-IP

■ Virenprüfung

Bei der Virenprüfung haben Sie die Möglichkeit, Virenprüfungsoptionen für ein- und ausgehende Mails einzustellen:



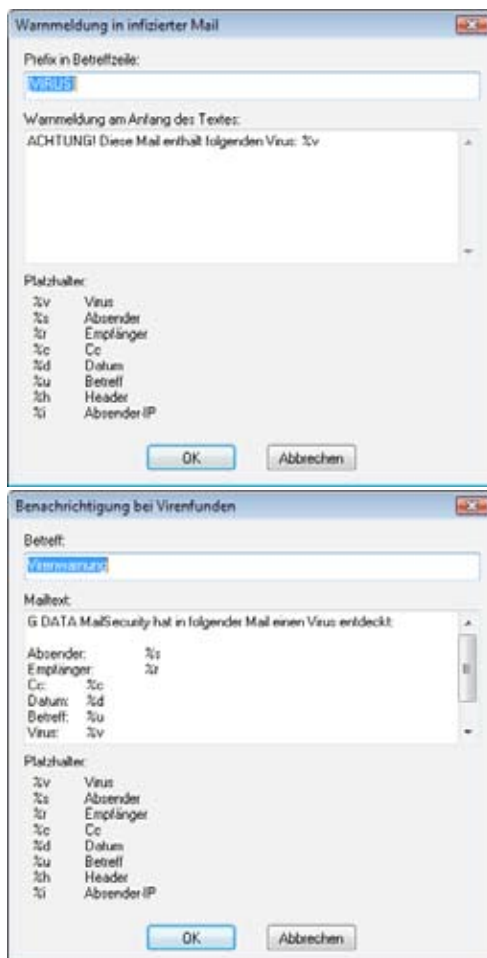
■ Eingehend

Grundsätzlich sollten Sie natürlich die Funktion **“Eingehende Mails auf Viren prüfen”** aktiviert haben und auch darauf achten, welche Option Sie **„im Fall einer Infektion“** nutzen möchten.

- **Nur protokollieren**
- **Desinfizieren (wenn nicht möglich: nur protokollieren)**
- **Desinfizieren (wenn nicht möglich: umbenennen)**
- **Desinfizieren (wenn nicht möglich: löschen)**
- **Infizierte Anhänge umbenennen**
- **Infizierte Anhänge löschen**
- **Nachricht löschen**

Optionen, in denen nur ein **„Protokollieren“** eingehender Viren stattfindet, sollten Sie nur dann verwenden, wenn Sie Ihr System auf andere Weise permanent vor

Virenbefall geschützt haben (z.B. mit dem Client/Server-basierten Virenschutz **G DATA AntiVirus**). Bei **Virenfunden** haben Sie eine große Anzahl von **Benachrichtigungsoptionen**. So können Sie eine **Virenwarnung in Betreff** und **Text** der infizierten Mail einfügen, um den Empfänger einer solchen Mail zu informieren. Auch können Sie eine **Meldung über den Virenfund** an bestimmte Personen senden, also z.B. Systemverwalter oder zuständige Mitarbeiter davon in Kenntnis setzen, dass ein Virus an eine E-Mail-Adresse in ihrem Netzwerk verschickt wurde. Mehrere **Empfängeradressen** trennen Sie bitte mit einem Semikolon voneinander ab. Sie können den **Text für die Benachrichtigungsfunktionen** individuell gestalten. Klicken Sie dazu einfach auf den „...-Button“ rechts Benachrichtigungsoption. Dabei können Sie auch **Platzhalter** verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den Benachrichtigungstext übernehmen.



Im frei definierbaren Text für den „**Betreff**“ und den „**Mailtext**“ stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

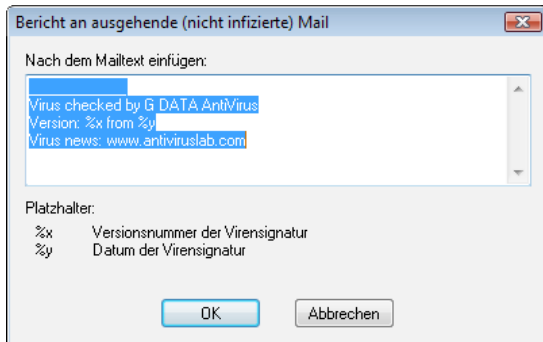
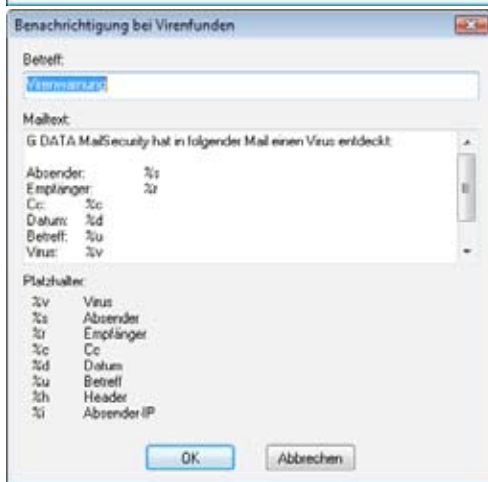
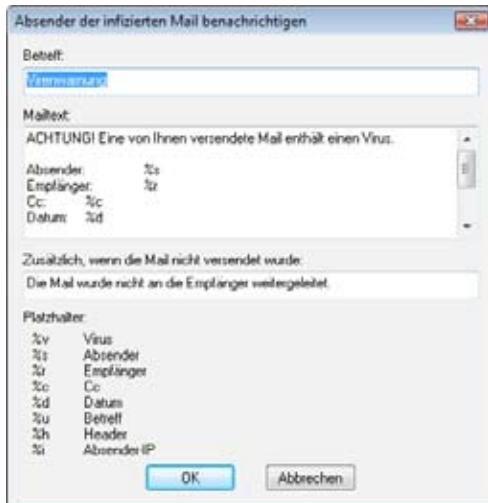
%v	Virus
%s	Absender
%r	Empfänger
%c	Cc
%d	Datum
%u	Betreff
%h	Header
%i	Absender-IP

■ Ausgehend

Grundsätzlich sollten Sie natürlich die Funktion „**Ausgehende Mails auf Viren prüfen**“ aktiviert haben und die Funktion „**Infizierte Nachricht nicht versenden**“ standardmäßig eingeschaltet haben. Auf diese Weise verlässt kein Virus Ihr Netzwerk und richtet möglicherweise bei Geschäftspartnern Schaden.

Bei **Virenfunden** haben Sie eine große Anzahl von **Benachrichtigungsoptionen**. So können Sie den „**Absender der infizierten Mail benachrichtigen**“ und unter „**Virenmeldung an folgende Personen senden**“ z.B. **Systemverwalter** oder zuständige Mitarbeiter davon in Kenntnis setzen, dass aus Ihrem Netzwerk ein Virus verschickt werden sollte. Mehrere **Empfängeradressen** trennen Sie bitte mit einem Semikolon voneinander ab.

Sie können den Text für die Benachrichtigungsfunktionen individuell gestalten. Klicken Sie dazu einfach auf den „...-Button“ rechts. Dabei können Sie auch „Platzhalter“ verwenden, die entsprechende Angaben zur zurückgewiesenen Mail in den **Benachrichtigungstext** übernehmen.



Im frei definierbaren Text für den „**Betreff**“ und den „**Mailtext**“ stehen Ihnen folgende Platzhalter (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

%v	Virus
%s	Absender
%r	Empfänger
%c	Cc
%d	Datum
%u	Betreff
%h	Header
%i	Absender-IP

Zusätzlich haben Sie unter „**Bericht an ausgehende (nicht infizierte) Mails anhängen**“ die Möglichkeit, von **G DATA MailSecurity** geprüfte Mails mit einem Bericht am Ende des Mailtextes zu versehen, in dem explizit darauf hingewiesen wird, dass diese Mail von **G DATA MailSecurity** geprüft wurde.

Die standardisierte Meldung lautet dabei:

*Virus checked by G DATA AntiVirus
Version: %x from %y
Virus news: www.antiviruslab.com*

Wobei die beiden Variablen %x und %y folgende Bedeutung haben:

%x	Versionsnummer der Virensignatur
%y	Datum der Virensignatur

Selbstverständlich können Sie diesen Bericht aber auch individuell verändern oder ganz weglassen.

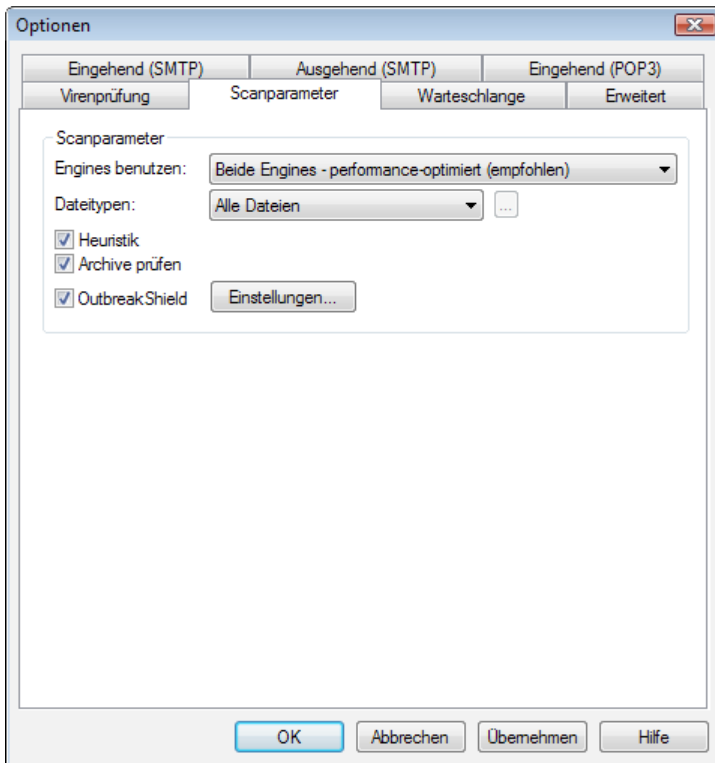
■ **G DATA AntiVirus Business**

Wenn Sie den Client/Server basierten Virenschutz **G DATA AntiVirus** (z.B. im Rahmen der **G DATA AntiVirus Business-** oder **G DATA AntiVirus Enterprise-Lösung**) installiert haben, können Sie über das Setzen des Häkchens bei „**Virenfunde an G DATA AntiVirus Business melden**“ dafür sorgen, dass die

Client/Server-basierte AntiVirensoftware **G DATA AntiVirus** über Virenfunde des **MailGateways** benachrichtigt wird und Ihnen auf diese Weise einen umfassenden Überblick über die Virenbelastung bzw. -gefährdung Ihres Netzwerkes liefert.

■ Scanparameter

In diesem Bereich können Sie die **Virenerkennungsleistung von G DATA MailSecurity optimieren** und an persönliche Erfordernisse anpassen. Generell gilt, dass durch eine Verringerung der Virenerkennungsleistung die **Performance** des Gesamtsystems steigt, während eine Erhöhung der Virenerkennungsleistung möglicherweise leichte **Einbußen in der Performance** mit sich bringen kann. Hier ist von Fall zu Fall abzuwägen.



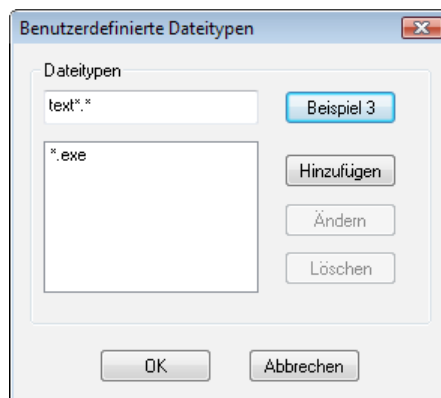
■ Engines benutzen

G DATA MailSecurity arbeitet mit zwei AntiViren-Engines, zwei grundsätzlich unabhängig voneinander operierenden **Virenanalyseeinheiten**. Unter „**Engines benutzen**“ stellen Sie ein, wie diese miteinander kooperieren. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der **Virenprophylaxe**. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen.

■ Dateitypen

Unter „**Dateitypen**“ können Sie festlegen, welche Dateitypen von **G DATA MailSecurity** auf Viren untersucht werden sollen. Wir empfehlen hier die **automatische Typ-Erkennung** über die automatisch nur die Dateien geprüft werden, die theoretisch auch einen Virus enthalten können.

Wenn Sie selber die Dateitypen definieren möchten, für die eine Virenprüfung erfolgen soll, verwenden Sie die Funktion „**benutzerdefiniert**“. Durch Anklicken des „...-Buttons“ können Sie dann eine Dialogbox öffnen, in der Sie die gewünschten Dateitypen ins obere Eingabefeld eintragen und dann über den „**Hinzufügen-Button**“ in die Liste der benutzerdefinierten Dateitypen übernehmen.



Sie können dabei auch mit **Platzhaltern** arbeiten, also Zeichen oder Zeichenketten durch die folgenden Symbole ersetzen:

- ? Das **Fragezeichen-Symbol** ist Stellvertreter für einzelne Zeichen.
- * Das **Sternchen-Symbol** ist Stellvertreter für ganze Zeichenfolgen.

Um z.B. sämtliche Dateien mit der Dateieindung „.exe“ prüfen zu lassen, geben Sie also *.exe ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu überprüfen (z.B. *.xlr, *.xls), geben Sie einfach *.xl? ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu prüfen, geben Sie beispielsweise text*.* ein.

■ Heuristik

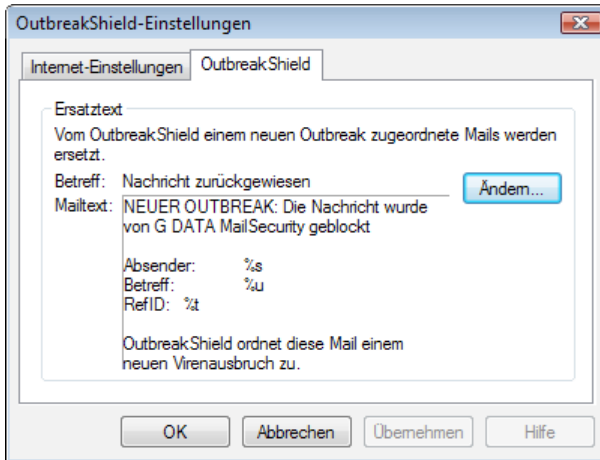
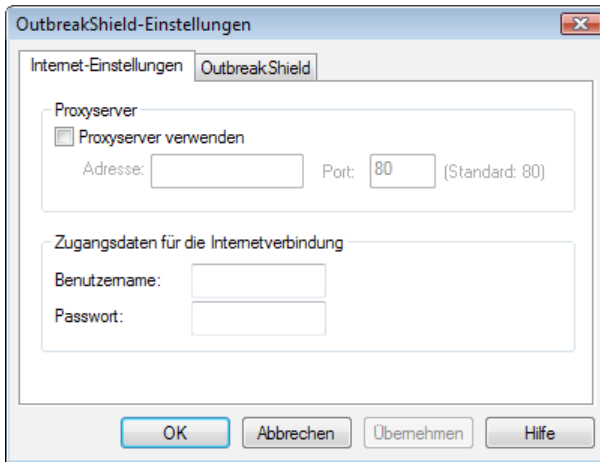
In der „**Heuristik-Analyse**“ werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist einerseits ein weiteres Sicherheitsplus, andererseits kann sie in seltenen Fällen auch einen Fehlalarm erzeugen.

■ Archive prüfen

Das Überprüfen **gepackter Dateien in Archiven** sollten generell aktiviert sein.

■ OutbreakShield

Mit dem „**OutbreakShield**“ können Schädlinge in **Massenmails** schon erkannt und bekämpft werden, bevor aktualisierte Signaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Signaturen besteht. Wenn Sie „OutbreakShield“ verwenden möchten, geben Sie über den Button „**Einstellungen**“ an, ob Sie einen **Proxyserver** verwenden und gegebenenfalls - um OutbreakShield einen jederzeitigen Zugang zum Internet zu ermöglichen - die **Zugangsdaten für Ihre Internetverbindung**. Auf der Registerkarte „**OutbreakShield**“ können Sie den Text der Mail definieren, den ein **Mailempfänger** enthält, wenn eine an ihn gerichtete Massenmail zurückgewiesen wurde.



- Da das OutbreakShield auf Grund seiner eigenständigen Architektur infizierte Mailanhänge nicht desinfizieren, umbenennen oder in die Quarantäne verschieben kann, informiert der Ersatztext den Anwender darüber, dass ihm die verdächtige bzw. infizierte Mail nicht zugestellt wurde. Eine Meldung über vom OutbreakShield zurückgewiesene Mails entfällt, wenn Sie auf der Karteikarte „**Virenprüfung**“ unter „**Im Falle einer Infektion**“ den Punkt „**Nachricht löschen**“ auswählen. In diesem Fall werden alle infizierten Mails, inklusive derer, die ausschließlich vom OutbreakShield erkannt werden, direkt gelöscht.

■ Warteschlange

In diesem Bereich können Sie festlegen, wie oft und in welchen Abständen der **erneute Versand von Mails** erfolgen soll, die vom MailGateway nicht an den entsprechenden Mailserver weitergeleitet werden können.

Mails können sich dabei aus verschiedenen Gründen in der Warteschlange befinden. So kann z.B. der Mailserver, an den Sie nach der Virenprüfung weitergeleitet werden sollen.

- *Generell gelangen Mails erst nach der **Virenüberprüfung** durch **G DATA MailSecurity** in die Warteschlange.*

The image shows a screenshot of a software configuration window titled 'Optionen'. The window has a tabbed interface with four tabs: 'Eingehend (SMTP)', 'Ausgehend (SMTP)', 'Eingehend (POP3)', and 'Erweitert'. The 'Warteschlange' tab is currently selected. The window contains the following settings:

- Nicht zustellbare Nachrichten**
 - Wiederholungsintervall (Stunden):
 - Fehlerwartezeit (Stunden):
 - Absender von Nachrichten in der Warteschlange alle Stunden benachrichtigen (0=aus).
 -
- Größenbegrenzung**
 - Größe der Warteschlange begrenzen
 - Maximale Anzahl von Nachrichten:

At the bottom of the window, there are four buttons: 'OK', 'Abbrechen', 'Übernehmen', and 'Hilfe'.

■ Nicht zustellbare Nachrichten

Geben Sie unter **“Wiederholungsintervall“** an, in welchen Abständen **G DATA MailSecurity** einen neuen **Versendeversuch** unternehmen soll. So bedeutet z.B. die Angabe 1, 1, 1, 4, dass **G DATA MailSecurity** die ersten drei Stunden stündlich versucht, die Mail zu verschicken und von da an regelmäßig im Abstand von 4 Stunden. Unter Fehlerwartezeit legen Sie fest, wann die Versendung der Mail endgültig abgebrochen und die Mail gelöscht wird.

Sie können **„Absender von Nachrichten in der Warteschlangen alle x Stunden benachrichtigen“**, wobei x ein ganzzahliger Stundenwert sein muss. Wenn Sie die Absender einer nicht zustellbaren Nachricht nicht regelmäßig informieren möchten, geben Sie hier einfach eine 0 ein.

- *Auch wenn Sie die regelmäßige Benachrichtigung von Absendern nicht weitergeleiteter Mails abschalten, wird der Absender natürlich dennoch informiert, wenn seine Mail endgültig nicht zugestellt und von Server gelöscht wurde.*

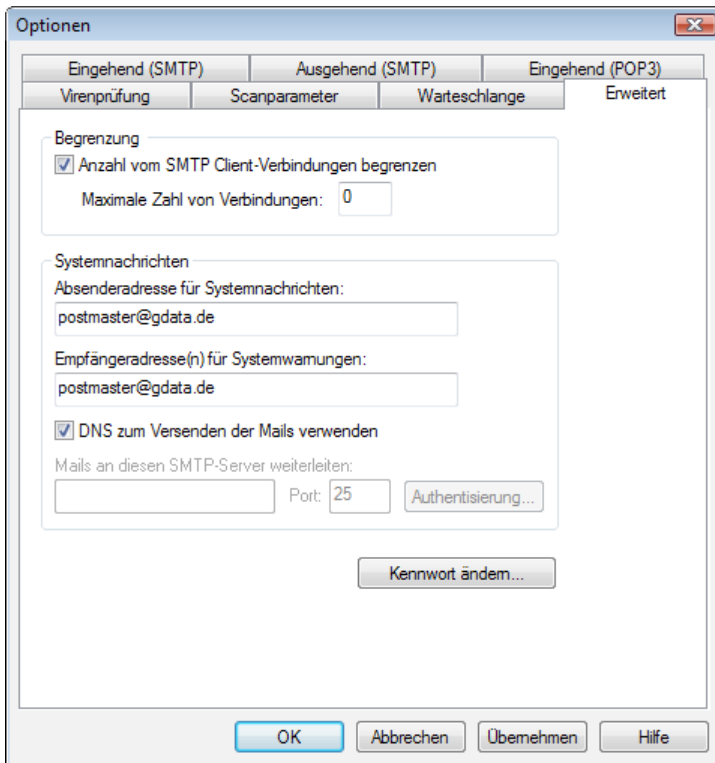
Über den Button **„Auf Standardwerte zurücksetzen“** können Sie die **Standardeinstellungen** im Bereich Warteschlange wiederherstellen. Diese Einstellungen haben sich in der Praxis bewährt.

■ Größenbegrenzung

Die **Größe der Warteschlange** kann auf Wunsch begrenzt werden. Dies dient dem Schutz vor **Denial of Service-Attacken**. Sollte die Größenbeschränkung überschritten werden, werden keine weiteren Mails mehr in die **Warteschlange** aufgenommen.

■ Erweitert

Im Erweitert-Bereich können Sie **globale Einstellungen** von **G DATA MailSecurity** verändern.



■ Begrenzung

Um die **Anzahl der SMTP-Verbindungen** zu begrenzen, die **G DATA MailSecurity** gleichzeitig verarbeitet, setzen Sie bitte das Häkchen vor „**Anzahl von SMTP Client-Verbindungen begrenzen**“. **G DATA MailSecurity** lässt dann nur die maximale Zahl von Verbindungen zu, die Sie vorgeben. Auf diese Weise können Sie die Mailfilterung an die Leistung der Hardware anpassen, die Sie für das MailGateway verwenden.

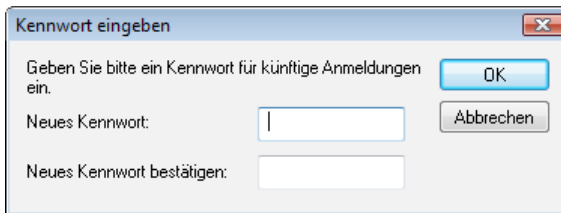
■ Systemnachrichten

Die Absenderadresse für Systemnachrichten ist die Mail-Adresse, die z.B. dazu verwendet wird, Absender und Empfänger virenfizierter Mails zu informieren

oder darüber zu informieren, dass sich ihre Mails in der Warteschlange befinden. **G DATA MailSecurity Systemwarnungen** sind unabhängig von den allgemeinen Mitteilungen bei Virenfunden. Bei einer Systemwarnung handelt es sich in der Regel um eher globale Informationen, die nicht mit einer einzelnen möglicherweise infizierten Mail in Zusammenhang stehen. So würde **G DATA MailSecurity** z.B. eine Systemwarnung verschicken, wenn die Virenkontrolle aus irgendwelchen Gründen nicht mehr gewährleistet ist. Die **Empfängeradresse(n)** für Systemwarnungen können durchaus identisch mit den Adressen sein, die Sie unter Eingehend/Ausgehend (SMTP, POP3) verwenden.

■ Kennwort ändern

Hier können Sie das **Administrator-Passwort** ändern, das Sie beim ersten Start von **G DATA MailSecurity** vergeben haben. Geben Sie dazu einfach das momentan aktuelle Passwort unter „**Altes Kennwort**“ ein und dann unter „**Neues Kennwort**“ und „**Neues Kennwort bestätigen**“ das neue Kennwort. Mit Anklicken des OK-Buttons wird die Kennwortänderung durchgeführt.



The image shows a dialog box titled "Kennwort eingeben" (Enter password). The dialog has a standard Windows-style title bar with a close button (X) in the top right corner. The main content area contains the following text and controls:

- Text: "Geben Sie bitte ein Kennwort für künftige Anmeldungen ein." (Please enter a password for future logins.)
- Text: "Neues Kennwort:" (New password:)
- Text: "Neues Kennwort bestätigen:" (Confirm new password:)
- Buttons: "OK" (highlighted in blue), "Abbrechen" (Cancel), and "OK" (highlighted in blue).

There are two empty text input fields: one for the "Neues Kennwort:" label and one for the "Neues Kennwort bestätigen:" label. The "OK" button is highlighted in blue, indicating it is the default action.

Spamfilter-Bereich

Über den **Spam-Filter** haben Sie umfangreiche Einstellungsmöglichkeiten, um Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Dazu stehen Ihnen mehrere Karteikarten zur Verfügung, in denen Ihnen alle relevanten Einstellungsmöglichkeiten thematisch gegliedert zur Verfügung stehen.

■ Filter

Geben Sie unter **„Name“** und **„Bemerkung“** an, wie Sie den Filter nennen möchten und welche zusätzlichen Informationen hierzu vielleicht nötig sind. Unter **„Reaktion“** können Sie bestimmen, wie der Spam-Filter mit Mails umgehen soll, die möglicherweise Spam enthalten. Dabei können Sie drei Abstufungen vornehmen, die davon beeinflusst werden, wie hoch **G DATA MailSecurity** die Wahrscheinlichkeit dafür ansetzt, dass es sich bei der betreffenden E-Mail um Spam handelt.

Spam filtern

Schlüsselwörter (Mailtext) Inhaltsfilter Profi-Einstellungen

Filter Whitelist Blacklist Realtime Blacklists Schlüsselwörter (Betreff)

Spam-Filter verwenden

Name: Spam-Filter

Bemerkung:

Reaktion

Spamverdacht:
Mail wird zugestellt; Spamwarnung wird eingefügt

Hohe Spamwahrscheinlichkeit:
Mail wird zurückgewiesen

Sehr hohe Spamwahrscheinlichkeit:
Mail wird zurückgewiesen

Unter „**Spamverdacht**“ wird der Umgang mit den Mails geregelt, in denen **G DATA MailSecurity** einzelne Spam-Elemente findet. Dabei muss es sich nicht generell um Spam handeln, sondern in seltenen Fällen möglicherweise auch um **Newsletter-Mails** oder **Sammelmailings**, die vom Empfänger durchaus erwünscht sind. Hier empfiehlt es sich, den Empfänger auf den Spam-Verdacht hinzuweisen. Unter „**Hohe Spamwahrscheinlichkeit**“ werden die Mails zusammengefasst, die viele Merkmale für Spam in sich vereinen und nur in sehr seltenen Fällen vom Empfänger wirklich erwünscht sind. Unter „**Sehr hohe Spamwahrscheinlichkeit**“ finden sich die Mails, die alle Kriterien einer Spam-Mail erfüllen. Hier handelt es sich so gut wie nie um gewünschte E-Mails und das Zurückweisen von derart gestalteten Mails ist in den meisten Fällen empfehlenswert.

- *Tippt: Mit einer Weiterleitung solcher Mails an G DATA verbessern Sie die Spamerkennung! Sie können diese Option aber natürlich auch abschalten*

Jede dieser drei abgestuften Reaktionen können Sie individuell gestalten.

Reaktion bei Spamverdacht

Mail zurückweisen

Spamwarnung in Betreff und Text der Mail einfügen

Prefix in Betreffzeile:

[SPAM]

Meldung in Text:

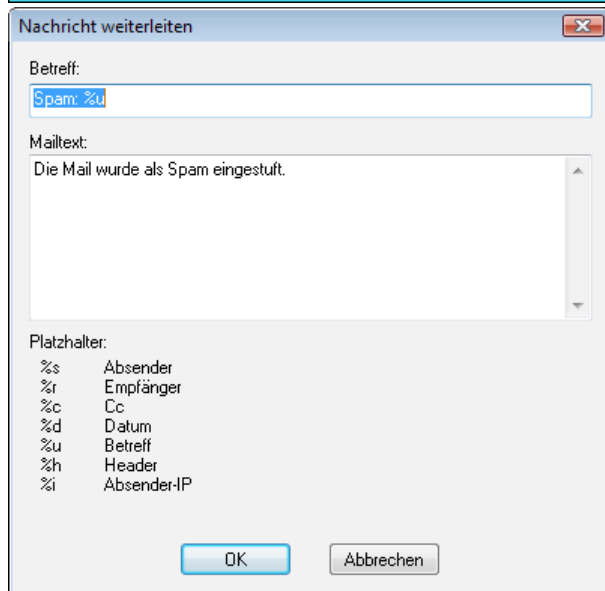
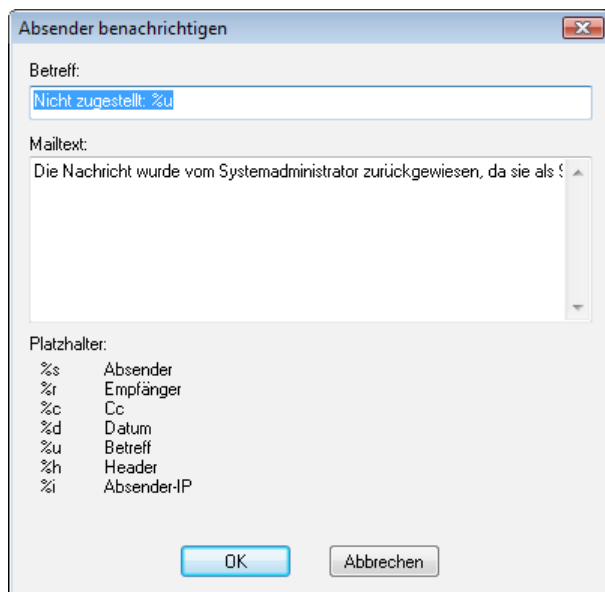
Absender der Nachricht benachrichtigen

An folgende Personen weiterleiten:

OK Abbrechen

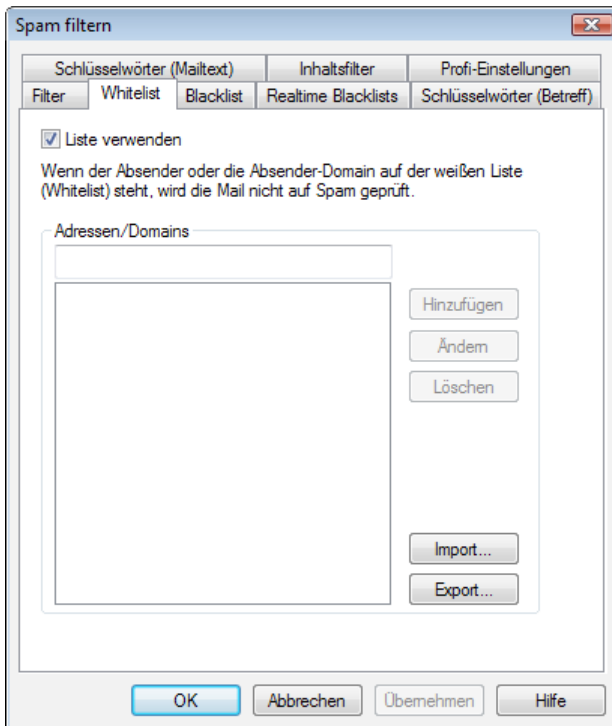
So haben Sie über „**Mail zurückweisen**“ die Möglichkeit, die Mail gar nicht erst auf Ihren Mail-Server gelangen zu lassen. Der Empfänger erhält diese Mail dann erst gar nicht. Über „**Spamwarnung in Betreff und Text der infizierten Mail einfügen**“ können Sie einen Empfänger einer als Spam identifizierten Mail davon in Kenntnis setzen, dass es sich um Spam handelt. Über die Option „**Absender der Nachricht benachrichtigen**“ können Sie eine automatische Antwortmail an den Absender der als Spam erkannten Mail verschicken, in der Sie diesen darauf hinweisen können, dass seine Mail als Spam erkannt wurde. Da gerade bei Spam viele Mailadressen aber nur einmal verwendet werden, sollten Sie sich überlegen, ob Sie

diese Funktion aktivieren. Über die Option „**An folgende Personen weiterleiten**“ können Sie als Spam verdächtige Mails auch automatisch weiterleiten, z.B. an den Systemadministrator.



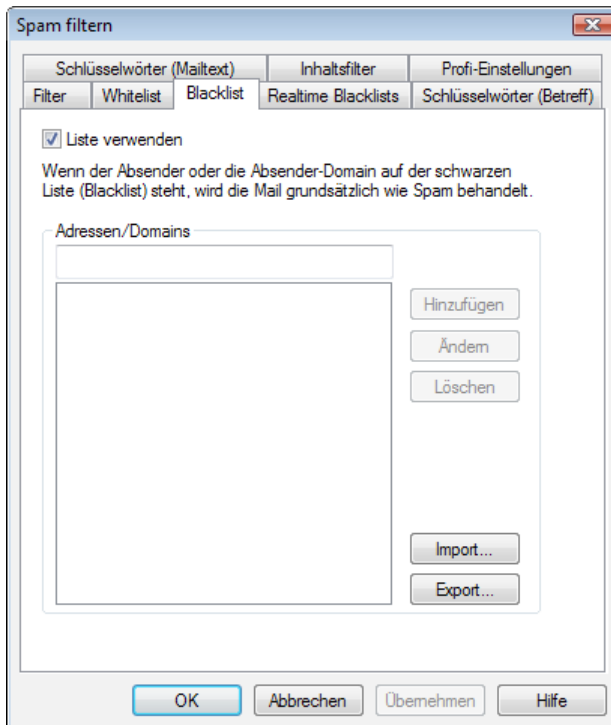
■ Whitelist

Über die Whitelist können Sie bestimmte **Absender-Adressen** oder Domains explizit vom **Spamverdacht** ausnehmen. Geben Sie dazu einfach in das Feld „**Adressen/Domains**“ die gewünschte E-Mail-Adresse (z.B. newsletter@gdata.de) oder **Domain** (z.B. gdata.de) ein, die Sie vom Spamverdacht ausnehmen möchten und **G DATA MailSecurity** behandelt Mails von diesem Absender bzw. dieser **Absenderdomain** nicht als Spam. Über den „**Import-Button**“ können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Whitelist einfügen. Die Adressen und Domains müssen in so einer **Liste** in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über den „**Export-Button**“ können Sie eine solche Whitelist auch als Textdatei exportieren.



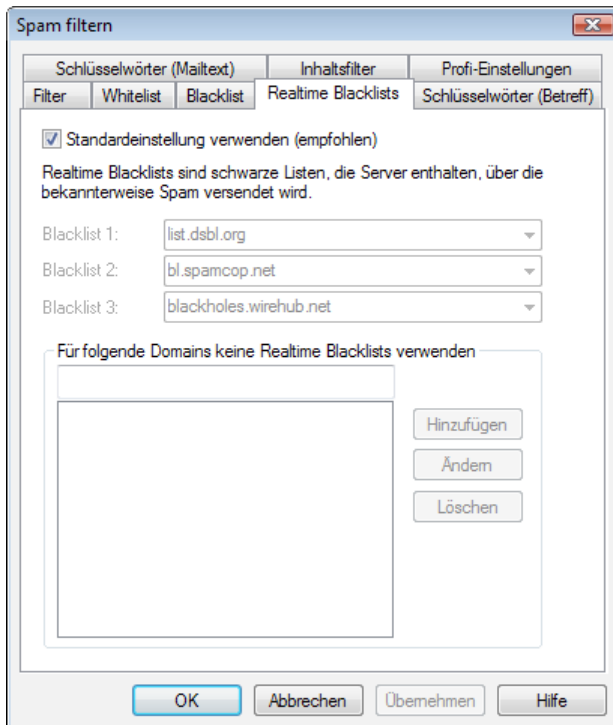
■ Blacklist

Über die Blacklist können Sie bestimmte Absender-Adressen oder Domains explizit unter Spamverdacht setzen. Geben Sie dazu einfach in das Feld **„Adressen/ Domains“** die gewünschte E-Mail-Adresse (z.B. newsletter@megaspam.de.vu) oder **Domain** (z.B. megaspam.de.vu) ein, die Sie unter Spamverdacht setzen möchten und **G DATA MailSecurity** behandelt Mails von diesem Absender bzw. dieser **Absenderdomain** generell als **„Mails mit sehr hoher Spamwahrscheinlichkeit“**. Über den **„Import-Button“** können Sie auch vorgefertigte Listen von E-Mail-Adressen oder Domains in die Blacklist einfügen. Die Adressen und Domains müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über den **„Export-Button“** können Sie eine solche Blacklist auch als Textdatei exportieren.



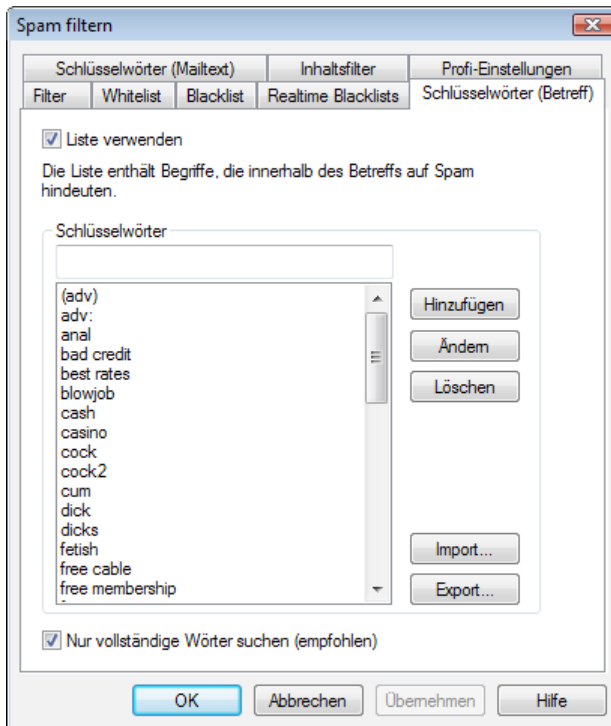
■ Realtime Blacklists

Im Internet finden sich **schwarze Listen**, die **IP-Adressen** von Servern enthalten, über die bekanntermaßen Spam verschickt wird. **G DATA MailSecurity** ermittelt durch **DNS-Anfragen** an die **RBLs (Realtime Blacklists)**, ob der sendende Server gelistet ist. Falls ja, erhöht sich die Spamwahrscheinlichkeit. Generell sollten Sie hier die Standardeinstellung verwenden, können allerdings auch unter Blacklist 1, 2 und 3 eigene Adressen für Blacklists aus dem Internet vergeben.



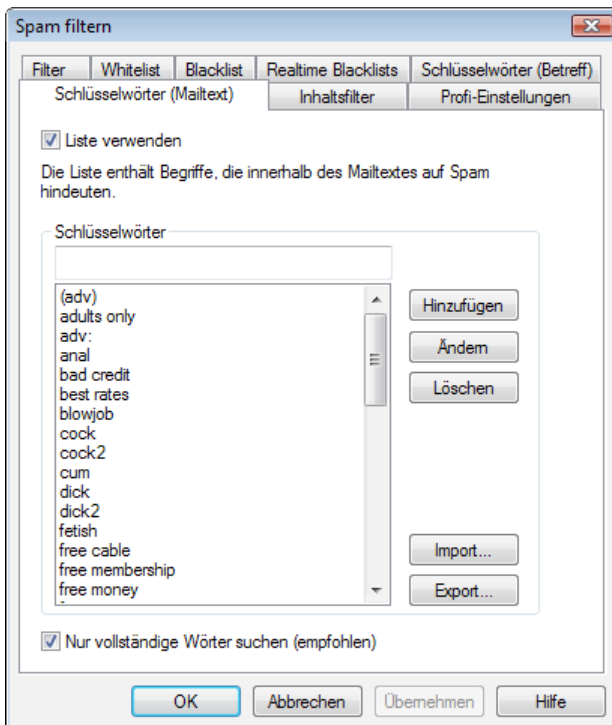
■ Schlüsselwörter (Betreff)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der in der Betreffzeile verwendeten Wörter unter **Spamverdacht** stellen. Wenn mindestens einer der Begriffe in der Betreffzeile vorkommt, erhöht sich die Spamwahrscheinlichkeit. Diese **Liste** können Sie über die Buttons **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern. Über den „**Import-Button**“ können Sie auch vorgefertigte Listen von **Schlüsselwörtern** in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache **txt-Datei** verwendet, wie sie z.B. auch mit dem Windows **Notepad** erstellt werden kann. Über den „**Export-Button**“ können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über das Häkchen vor „**Nur vollständige Wörter suchen**“ können Sie festlegen, dass **G DATA MailSecurity** die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie „cash“ unter Spamverdacht fallen, während z.B. die gemeinen Cashew-Kerne weiterhin unbeanstandet bleiben.



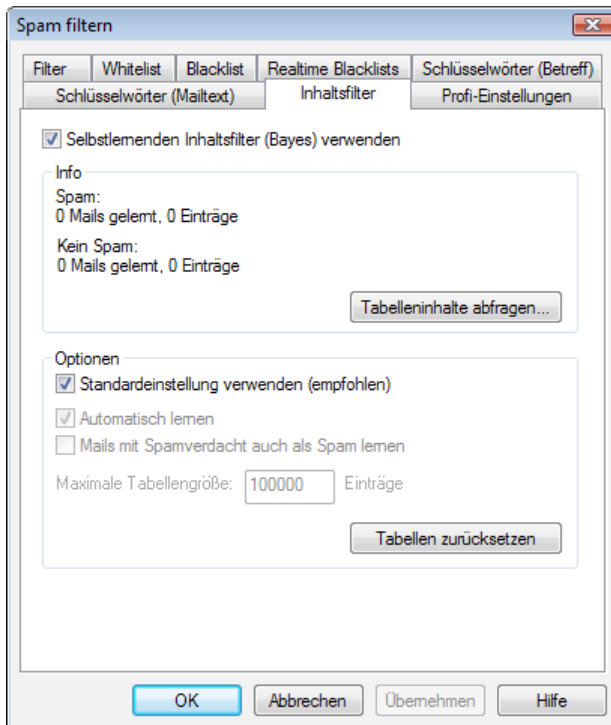
■ Schlüsselwörter (Mailtext)

Über die Liste der Schlüsselwörter können Sie Mails auch anhand der im Mailtext verwendeten Wörter unter Spamverdacht stellen. Wenn mindestens einer der Begriffe im Mailtext vorkommt, erhöht sich die **Spamwahrscheinlichkeit**. Diese Liste können Sie über die Buttons „**Hinzufügen**“, „**Ändern**“ und „**Löschen**“ beliebig verändern. Über den „**Import-Button**“ können Sie auch vorgefertigte Listen von Schlüsselwörtern in Ihre Liste einfügen. Die Einträge müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows **Notepad** erstellt werden kann. Über den „**Export-Button**“ können Sie eine solche Liste von **Schlüsselwörtern** auch als Textdatei exportieren. Über das Häkchen vor „**Nur vollständige Wörter suchen**“ können Sie festlegen, dass **G DATA MailSecurity** die Betreffzeile einer Mail nur nach ganzen Wörtern durchsucht, so würde z.B. ein Begriff wie „cash“ unter Spamverdacht fallen, während z.B. die gemeinen Cashew-Kerne weiterhin unbeanstandet bleiben.



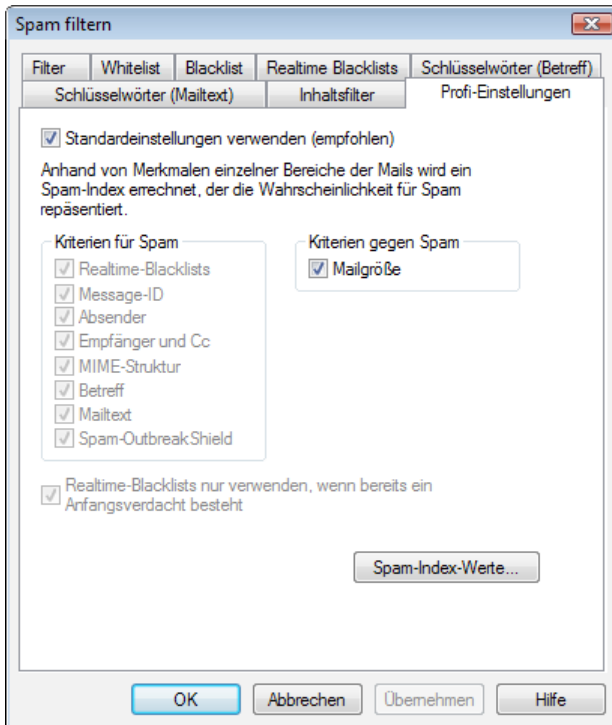
■ Inhaltsfilter

Beim Inhaltsfilter handelt es sich um einen **selbstlernenden Filter** auf Basis der **Bayes-Methode**, der auf Grund der im Mailtext verwendeten Worte eine **Spamwahrscheinlichkeit** berechnet. Dabei arbeitet dieser Filter nicht allein auf Basis feststehender Wortlisten, sondern lernt bei jeder neu empfangenen Mail weiter dazu. Über den Button „**Tabelleninhalte abfragen**“ können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer Mail als Spam verwendet. Über den Button „**Tabellen zurücksetzen**“ löschen Sie alle gelernten Tabelleninhalte und der selbstlernende Inhaltsfilter startet den **Lernvorgang** erneut von Beginn an.



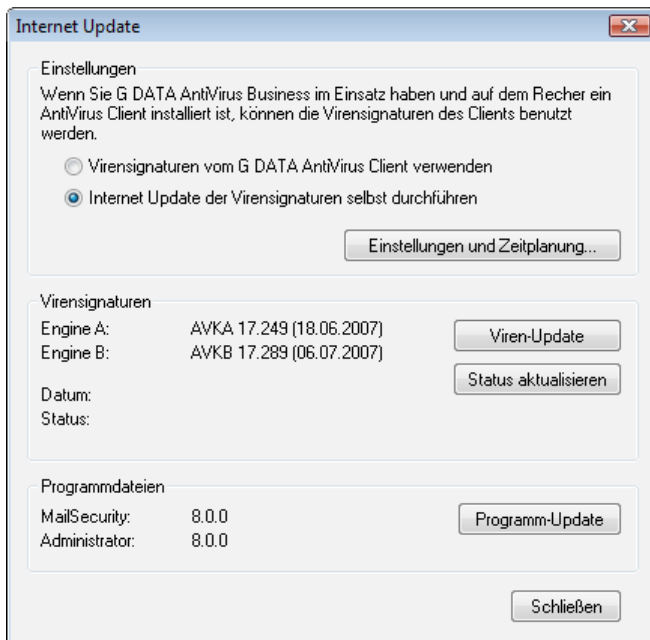
■ Profi-Einstellungen

In diesem Bereich können Sie die Spamerkennung von **G DATA MailSecurity** sehr detailliert verändern und an die Gegebenheiten Ihres Mailservers anpassen. Generell empfiehlt es sich hier jedoch, die **Standardeinstellungen** zu verwenden. In den Profi-Einstellungen sollten Sie nur dann Veränderungen vornehmen, wenn Sie sich in der Thematik auskennen und genau wissen, was Sie tun.



Internet Update-Bereich

Im **Internet Update-Bereich** können Sie umfangreiche Einstellungen vornehmen, um **G DATA MailSecurity** optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren.



■ Einstellungen

Hier können Sie grundlegende Einstellungen für das Internet Update vorgeben. Wenn Sie (z.B. im Rahmen der **G DATA AntiVirus Business**-Lösung) parallel zu **G DATA MailSecurity** das Client/Server-basierte **G DATA AntiVirus** verwenden, können Sie sich über „**Virensignaturen vom G DATA AntiVirus Client verwenden**“ den doppelten Download der Virensignaturen sparen und diese direkt von **G DATA AntiVirus** erhalten, dass diese schon auf Ihrem Server gespeichert hat. Über „**Internet Update der Virensignaturen selbst durchführen**“ führt **G DATA MailSecurity** diesen Vorgang selbstständig durch.

Über den Button „**Einstellungen und Zeitplanung**“ gelangen Sie in einen Bereich, in dem Sie sämtliche notwendigen Einstellungen für manuelle und automatische Internet Updates eingeben können.

Geben Sie unter „**Zugangsdaten**“ den **Benutzernamen** und das **Passwort**) ein, die Sie bei der Anmeldung von **G DATA MailSecurity** erhalten haben. Klicken Sie auf den Button „**Am Server anmelden**“, wenn Sie sich noch nicht am **G DATA**-Server angemeldet haben. Mit Hilfe dieser Daten werden Sie vom **G DATA**-Server erkannt und das **Update der Virensignaturen** kann vollautomatisch erfolgen.

- *Wenn Sie noch keine Anmeldung am Server durchgeführt haben, können Sie diese jetzt nachholen. Geben Sie einfach die **Anmeldenummer** ein (- Sie finden diese auf der Rückseite des Benutzerhandbuches -), Ihre **Kundendaten** und klicken Sie auf „**Senden**“. Sofort werden Ihnen die **Zugangsdaten (Benutzername und Passwort)** angezeigt. Sie sollten sich diese Daten aufschreiben und diese sicher verwahren. Für die Anmeldung am Server ist natürlich (- wie auch für das Internet-Update der Virensignaturen -) eine **Internetverbindung** notwendig.*

Falls Sie einen Rechner hinter einer **Firewall** verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen **Proxyserver**. Sie sollten diese Einstellung nur ändern, wenn das Internet-Update nicht funktioniert. Wenden Sie sich wegen der **Proxy-Adresse** gegebenenfalls an Ihren Internetzugangsanbieter.

Die Zugangsdaten für die Internetverbindung (Benutzernamen und Passwort) sind gerade beim automatischen Internet-Update per Zeitplan sehr wichtig. Ohne diese Angaben kann keine automatische Verbindung mit dem Internet erfolgen. Achten Sie bitte auch darauf, dass Sie in Ihren allgemeinen Interneteinstellungen (z.B. für Ihr Mailprogramm oder Ihren Internetbrowser) die automatische Einwahl ermöglichen. Ohne die automatische Einwahl startet **G DATA MailSecurity** zwar den Internet-Update-Vorgang, muss dann aber darauf warten, dass Sie den Aufbau der Internetverbindung mit „OK“ bestätigen.

Über die Karteikarte „**Zeitplanung Viren-Update**“ können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter „**Ausführen**“ geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter „**Zeitpunkt**“ und „**Wochentage**“ spezifizieren.

- *Unter „**Täglich**“ können Sie mit Hilfe der Angaben unter „**Wochentage**“ z.B. bestimmen, dass Ihr Rechner nur an Werktagen das Update durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Um unter „**Zeitpunkt**“ Daten- und Zeiteinträge zu ändern, markieren Sie einfach das Element, das Sie ändern möchten (z.B. Tag, Stunde, Monat, Jahr) mit der Maus und nutzen dann die Pfeiltasten oder die kleinen Pfeilsymbole rechts vom Eingabefeld, um sich im jeweiligen Element chronologisch zu bewegen.*

Geben Sie bitte unter „**Benutzerkonto**“ ein Benutzerkonto auf dem MailGateway-Rechner an, für das ein Zugang zum Internet besteht.

- **Achtung:** Bitte verwechseln Sie nicht die Angaben, die Sie in den Karteikarten **Zugangsdaten** und **Benutzerkonto** tätigen.

■ Virensignaturen

Über die Buttons „**Viren-Update**“ und „**Status aktualisieren**“ können Sie auch unabhängig von den Vorgaben, die Sie unter Zeitplanung vorgenommen haben, ein aktuelles Virensignaturupdate starten.

■ Programmdateien

Über den Button „**Programm-Update**“ können Sie auch die Programmdateien von **G DATA MailSecurity** aktualisieren, sobald sich hier Änderungen und Verbesserungen ergeben.

■ Problemlösungen (FAQ)

In diesem Bereich finden Sie Antworten zu Fragestellungen, die bei der Arbeit mit **G DATA MailSecurity** möglicherweise auftreten könnten.

Ich verwende AVM Ken! und möchte G DATA MailSecurity auf dem gleichen Rechner wie den Ken!-Server installieren

Detaillierte Anleitungen hierzu erhalten Sie von unserem **Support-Team**.

Ich verwende einen Exchange-Server 2000 und möchte G DATA MailSecurity auf dem gleichen Rechner wie den Exchange-Server installieren. Wie kann ich im Exchange-Server die Ports für eingehende und ausgehende Mails umstellen?

Detaillierte Anleitungen hierzu erhalten Sie von unserem **Support-Team**.

■ Index

A

Abbrechen 41
Abbrechen: 15
Absender 31, 45, 47, 49
Absender-Adressen 63
Absender-IP 45, 47, 49
Absender benachrichtigen 31, 34, 35
Absender der infizierten Mail benachrichtigen 49
Absender der Nachricht benachrichtigen 60
Absenderdomain 63, 64
Absenderfilter 26, 34
Absender von Nachrichten in der Warteschlangen
alle x Stunden benachrichtigen 57
Abständen 38
Achtung 26, 42, 70
Achtung-Symbol 23
ActiveDirectory 42
Administrator 17, 19, 20
Administrator-Passwort 59
Administrator-Software 17
Administrator-Tool 17
Administrators 6, 23
Adressen/Domains 34, 35, 63, 64
Adressen/Domains\; Domain-Namen 35
Aktionsbeschreibung 38, 39
Aktivierung des Content Filters 31
Aktivität-Bereich 21, 38, 39
Aktivität-Liste 38, 39
Allgemeines 5
Altes Kennwort 59
Ampelsymbol. 23
Am Server anmelden 70
Ändern 66, 67
An folgende Personen weiterleiten 60
Anhang 72
Anhänge filtern 26, 30
Anhänge nur umbenennen 30
Anmeldenummer 70
AntiVirusLab 38, 40
AntiVirusLab-Virenlexikon 21
Anzahl der SMTP-Verbindungen 58
Anzahl von SMTP Client-Verbindungen begrenzen 58
Archiv 21
Archivdateien 30
Archive prüfen 54
Assistentenfenster 26

Auch Anhänge in eingebetteten Mails filtern 30
Auf Standardwerte zurücksetzen 57
Ausdrücke 31
ausführbaren Dateien 30
Ausführbarkeit 30
Ausführen 15, 70
Ausgehend 49
Ausgehend (SMTP) 43
Ausgehende Mails auf Viren prüfen 49
Ausgehende Mail verarbeiten 12, 13, 43
ausgehender Mails 23
Auswahlfenster 26
automatische Typ-Erkennung 53
Automatische Updates: 23
AVI 30

B

b-vertrieb@gdata.de 7
Bayes-Methode 68
Bcc 35
Bearbeiten-Button 26
Bearbeiten... 23
Begrenzung 58
Bemerkung 26, 37, 60
Benachrichtigungsoption 45
Benachrichtigungsoptionen 47, 49
Benachrichtigungstext 34, 45, 49
benutzerdefiniert 53
Benutzerkonto 70
Benutzernamen 6, 70
Bericht an ausgehende (nicht infizierte) Mails
anhängen 49
Betreff 31, 45, 47, 49
Bezeichnungen 12, 13
Blacklist 64
business-support@gdata.de 6

C

CAB 30
Cc 31, 35, 45, 47, 49
Clients 7
COM 30
Computernamen 19, 20
Content-Prüfung 45

D

Dateiendung 30
Dateiendungen 30
Dateierweiterungen 30
Dateitypen 53
Datenbank 42
Datum 31, 45, 47, 49
Datum der Virensignatur 49
Datum der Virensignaturen: 23
Denial of Service-Attacken 57
Der Supportrahmen 6
Desinfizieren (wenn nicht möglich: löschen) 47
Desinfizieren (wenn nicht möglich: nur protokollieren) 47
Desinfizieren (wenn nicht möglich: umbenennen) 47
DNS-Anfragen 65
DNS-Eintrag 13
DNS zum Versenden der Mails verwenden 12, 13, 42, 43
Domain 63, 64
Domain-Namen 34
Domains 42
drugs 31
Durchsuchen: 15

E

E-Mail 6, 7
E-Mail-Kommunikation 11
E-Mailverkehr 11
e: 15
e:.exe 15
Ebenfalls erhältlich: G DATA AntiVirus Enterprise 7
Einbußen in der Performance 52
Eingehend 47
Eingehend (POP3) 44
Eingehend (SMTP) 41
Eingehend/Ausgehend 38
Eingehende Mails auf Viren prüfen 47
Eingehende Mails nur für folgende Domains akzeptieren 42
eingehender Mails 23
eingehender Mails verhindert 23
Ein paar Worte vorab 5
Einstellungen 54, 70
Einstellungen und Zeitplanung 70
Einstellungsbereiche 41
Empfänger 31, 45, 47, 49

Empfängeradresse(n) 58
Empfängeradressen 47, 49
Empfängerfilter 26, 35
Empfang und Weiterleitung 42, 43, 45
Engines benutzen 53
erneute Versand von Mails 56
Erster Programmstart (Kennwortvergabe) 19
erweitern 30
Erweitert 19, 58
Exchange 12
EXE 30
EXE-Datei 30
Export-Button 63, 64, 66, 67
exportieren 37
Externe Referenzen deaktivieren 26, 29

F

FAQ 6
Fax 6, 7
Fehlennung („False Positive“) 26
Festplattenspeicherplatz 15
Filter 45, 60
Filter-Bereich 21, 26
Filterregeln 26
Filtertyp 26
Firewall 11, 13, 70
Firewall-Konfigurationen 11
Fragezeichen-Symbol 53
Führende Technologie 6

G

Gateway 5, 11
G DATA 5, 7, 70
G DATA AntiVirus 7, 47, 51, 70
G DATA AntiVirus Business 51, 70
G DATA AntiVirus Business- 51
G DATA AntiVirus Business-\\; G DATA AntiVirus Enterprise-Lösung 51
G DATA AntiVirus Enterprise 7
G DATA AntiVirus ManagementServer 7
G DATA MailSecurity 5, 6, 7, 8, 11, 12, 13, 14, 15, 17, 19, 20, 21, 23, 26, 31, 34, 35, 38, 41, 45, 49, 53, 56, 57, 58, 59, 60, 63, 64, 65, 66, 67, 69, 70, 72, 73
G DATA MailSecurity-Administratorsoftware 11
G DATA MailSecurity-CD-ROM 15
G DATA MailSecurity-Installation 15
G DATA MailSecurity-Registrierungsnummer 6

- G DATA MailSecurity\; 64 Bit Windows-Betriebssystemen 14; MailGateway 11
- G DATA MailSecurity Administrator 11, 17, 19, 21
- G DATA MailSecurity MailGateway 13, 17
- G DATA MailSecurity Mailgateway 11
- G DATA PremiumHotline 6
- gepackter Dateien in Archiven 54
- gesang 31
- GIF 30
- globale Einstellungen 58
- Größe der Warteschlange 57
- Größenbegrenzung 57
- Grundlegende Vorgehensweise 11

H

- Häkchen bei Anhänge nur umbenennen 30
- Häkchenfelder 26
- Header 45, 47, 49
- Heuristik 54
- Heuristik-Analyse 54
- HighTech für höchste Sicherheit 5
- Hilfe 6
- Hilfe-Bereich 21
- Hintergrund 17
- Hinzufügen 37, 66, 67
- Hinzufügen-Button 53
- Hohe Spamwahrscheinlichkeit 60
- HTML-Scripte deaktivieren 26
- HTML-Skripte deaktivieren 29
- HTML-Teil einer Mail 29
- Hyperlink 29

I

- Ich verwende AVM Ken! und möchte G DATA MailSecurity auf dem gleichen Rechner wie den Ken!-Server installieren 73
- Ich verwende einen Exchange-Server 2000 und möchte G DATA MailSecurity auf dem gleichen Rechner wie den Exchange-Server installieren. Wie kann ich im Exchange-Server die Ports für eingehende und ausgehende Mails umstellen? 73
- ID 38, 39
- Im Falle einer Infektion 54
- im Fall einer Infektion 47
- Import-Button 63, 64, 66, 67
- importieren 37
- Infizierte Anhänge löschen 47

- Infizierte Anhänge umbenennen 47
- Infizierte Nachricht nicht versenden 49
- Info 6
- Info-Bereich 21
- Inhaltsfilter 26, 31, 34, 35, 68
- Installation 15
- Installation des MailGateways auf dem Mail-Server (SMTP) 12
- Installation des MailGateways auf separatem Rechner (SMTP) 13
- Installieren: 15
- Internet-Update 6
- Internet-Updates 6
- Internet Update 23
- Internet Update-Bereich 21, 70
- Internet Update der Virensignaturen selbst durchführen 70
- Internetverbindung 70
- IP-Adresse 11, 13, 19, 20
- IP-Adressen 37, 65
- IP-Adressen der Server, die ausgehende Mails senden 43
- IP-Adressen der Server, die ausgehende Mails senden können 12, 13
- IP-Filter 26, 37

J

- Jetzt wiederholen 38
- JPEG 30
- JPG 30

K

- Kapiteln 17
- Karteikarten 41
- Karteireiters 41
- Kennwort 19, 20
- Kennwort ändern 19, 59
- Kennworteingabefenster 19
- Konfiguration G DATA MailSecurity MailGateway (Ausgehend (SMTP)) 12, 13
- Konfiguration G DATA MailSecurity MailGateway (Eingehend (SMTP)) 13
- Konfiguration G DATA MailSecurity MailGateway (Eingehended (SMTP)) 12
- Konfiguration Mail-Server 12, 13
- Kundendaten 70

L

Laufwerksbuchstaben 15
leerem Empfängerfeld 35
Lernvorgang 68
Lesebestätigung filtern 26, 29
Links 29
Linux 5
Liste 63, 66
Listenansicht für ausgehende Mails 38
Listenansicht für eingehende Mails 38
Lizenzvereinbarungen 8
logischen Operatoren UND und ODER 31
Löschen 38, 40, 66, 67
Löschen-Button 26, 38

M

Mail-Anhänge (= Attachments) 30
Mail-Server 11, 13
Mail-Server-Rechner 15
Mailempfänger 54
MailGateway 11, 13, 15, 17, 19, 20
Mailgateway 11
MailGateway-Rechner 15
MailGateway-Software 17
MailGateways 6, 11, 17, 19, 20, 23, 51
Mails an diesen SMTP-Server weiterleiten 12, 13, 42, 43
Mailserver 5, 6
Mailserver-Software 5
Mails mit sehr hoher Spamwahrscheinlichkeit 64
Mails von diesem POP3-Server abholen 45
Mailtext 31, 45, 47, 49
Mail zurückweisen 31, 34, 35, 60
Mailzustellung 38
Makros 30
ManagementServer-Software 7
manuelle Konfiguration 45
Massenmails 23, 54
Massenmailversendern 36
Mehrfach- und Netzwerkklizenzen 6
Meldung an folgende Personen senden 31, 34, 35
Meldung im Text der Mail einfügen 30
Meldung über den Virenfund 47
Microsoft Exchange 5.5 12
Microsoft Windows 42
Mindest-Systemvoraussetzungen 15
MP3 30

MPEG 30
MX-Record 13

N

Nachrichtenübermittlung 12, 13
Nachricht löschen 47, 54
Name 26, 37, 60
Net-Framework 1.1 42
Netzwerk 41
Netzwerk-Firewall 11
Neu-Button 26, 31
Neues Kennwort 19, 59
Neues Kennwort bestätigen 19, 59
Newsletter-Mails 60
Nicht zustellbare Nachrichten 57
Notepad 66, 67
Nur protokollieren 47
Nur vollständige Wörter suchen 66, 67

O

ODER 31
OK 15, 19
OK-Button 41
Online-Datenbank 6
Online-Hilfe 21
Online-Lexikon 21
Online-Registrierung 6, 7
Online-Registrierung\; Internet-Update 7
Online-Registrierungsformular 6
Optionen-Bereich 21, 38, 41
Optionen > Ausgehend (SMTP) 23
Optionen > Eingehend (SMTP) 23
Optionen > Virenprüfung 23
Optionen > Warteschlange 38
OutbreakShield 23, 54
OutbreakShield-Server 26
OutbreakShield: 23

P

Passwort 70
Performance 52
Platzhalter 31, 34, 35, 45, 47
Platzhaltern 53
POP3 5
POP3 (= Post Office Protokoll 3) 17
POP3-Anfragen verarbeiten 45

- POP3-basierte Mailprogramme 45
- POP3-Mails 17, 45
- POP3-Sammelkonto 17
- POP3-Server:127.0.0.1/Benutzername:mail.xxx.de:
 - Erika Musterfrau 45
- POP3-Server:mail.xxx.de/Benutzername:Erika Musterfrau 45
- POP3-Variante 17
- POP3: 11
- Port 11, 12, 13, 42, 45
- Port, auf dem die Mails eingehen 12, 13, 42, 43
- Port-Nummer 12
- Port für eingehende Mails 12, 13
- PremiumHotline 6
- PremiumSupport 7
- PremiumSupport-Verlängerungen 7
- Problemlösungen (FAQ) 73
- Profi-Einstellungen 69
- Programm-Update 72
- Programmaufbau G DATA MailSecurity Administrator 21
- Programmbereich 21
- Programmbereiche 21
- Programmdateien 72
- Programmversion 21
- Protokoll 26
- Protokollieren 47
- Proxy-Adresse 70
- Proxyserver 54, 70
- Prüfung ausgehender Mails (SMTP) 17
- Prüfung eingehender Mails (POP3) 17
- Prüfung eingehender Mails (SMTP) 17
- Prüfung eingehender Mails (SMTP)\; Status-Bereich 17

Q

- Queue 38

R

- RBLs (Realtime Blacklists) 65
- Reaktion 31, 34, 35, 60
- Realtime Blacklists 65
- Registriernummer 6
- registrierten Kunden 6
- Registrierungsnummer 6
- Regulärer Ausdruck 31
- Relay 43
- Relay-Schutz 42

- Richtung 26
- rock'n'roll 31
- Rückantwortmail 29

S

- Sammelmailings 60
- Scanparameter 52
- Schadroutinen 29
- Schlüsselwörter 31
- Schlüsselwörter (Betreff) 66
- Schlüsselwörter (Mailtext) 67
- Schlüsselwörtern 66, 67
- Schutz vor Relaying 42
- schwarze Listen 65
- Scripte 30
- Scrollbar 38, 39
- Sehr hohe Spamwahrscheinlichkeit 60
- selbstlernenden Filter 68
- Semikolon 30
- Senden 70
- Server 19, 20
- Server Ihres MailGateways 45
- Servern 37
- ServiceCenter 7
- Setup 17
- sex 31
- SMTP 5
- SMTP (= Simple Mail Transfer Protokoll) 17
- SMTP-Eintrag 12
- SMTP-Mails 42
- SMTP-Protokoll 17
- SMTP-Server 12, 17, 42
- SMTP/POP3-Datenstrom 11
- SMTP: 11
- Spam-Filter 23, 26, 60
- Spam-Filter: 23
- Spam-Index-Werte 26
- Spam-OutbreakShield 23
- Spam-OutbreakShield: 23
- Spamfilter-Bereich 21, 36, 60
- Spam filtern 26, 36
- Spamverdacht 60, 63, 66
- Spamwahrscheinlichkeit 67, 68
- Spamwarnung in Betreff und Text der infizierten Mail einfügen 60
- Standardeinstellungen 57, 69
- Start-Menü 15

- Start > (Alle) Programme > G DATA MailSecurity 19, 20
- Start > Programme > G DATA MailSecurity > G DATA MailSecurity 17
- Status-Bereich 17, 21, 23
- Status aktualisieren 72
- Sternchen-Symbol 53
- Steuerungssoftware 11
- Suchbegriffe 31
- Suchbereich 31
- Suffix 30
- Support-Team 73
- Supportleistungen 6
- Systemnachrichten 58
- Systemverwalter 49
- Systemvoraussetzungen 14
- Systemwarnungen 58

T

- Tabelleninhalte abfragen 68
- Tabellen zurücksetzen 68
- Täglich 70
- technische Fragen 7
- Tel. 6, 7
- Text 47
- Text für die Benachrichtigungsfunktionen 47
- Text für diese Benachrichtigungsfunktionen 45
- TimeOut-Fehler 45
- txt-Datei 66

U

- Übernehmen-Button 41
- Uhrzeit 39
- Umleitung 13
- UND 31
- Update der Virensignaturen 70
- Updates 23
- Upgrades 7

V

- VBS-Skripte 30
- Verarbeitung ausgehender Mails: 23
- Verarbeitung eingehender Mails: 23
- Versendeversuch 57
- Versionsnummer der Virensignatur 49
- Versionsnummern 6
- verzögert 38

- Verzögerungen 38
- Viren-Update 72
- Virenanalyseeinheiten 53
- Virenenerkennungsleistung von G DATA MailSecurity optimieren 52
- Virenfunde-Bereich 21, 38, 40
- Virenfunde an G DATA AntiVirus Business melden 51
- Virenfunden 47, 49
- Vireninformation-Button 38, 40
- Virenlexikon-Bereich 21
- Virenmeldung an folgende Personen senden 49
- Virenprophylaxe 53
- Virenprüfung 46, 54
- Virenprüfung ausgehender Mails: 23
- Virenprüfung eingehender Mails: 23
- Virensignaturen 23, 72
- Virensignaturen vom G DATA AntiVirus Client verwenden 70
- Virenüberprüfung 56
- Virenwarnung 47
- Virenwarnungen 7
- Virus 45, 47, 49
- Von folgenden IP-Adressen keine Mails annehmen 37
- Voraussetzungen für das G DATA MailSecurity Mail Gateway 14
- Voraussetzungen für die Nutzung des G DATA MailSecurity Administrators 14
- Vor der Installation 11
- Vorschauansicht 29

W

- Warteschlangen-Bereich 21
- Warteschlange 56, 57
- Warteschlangen-Bereich 38
- weib 31
- wein 31
- Weitere Programmstarts (Zugangskennwort) 20
- Weiterleitung 42
- Weiterleitung der eingehenden Mails an Ihren Mail-Server 42
- Whitelist 63
- Wiederholungsintervall 57
- Windows 5
- Windows-Version 6
- Windows 2000 14
- Windows Vista 14
- Windows Vista\; Server 2003 14

Windows XP 14
Wochentage 70
www.antiviruslab.com 21
www.gdata.de 6

Z

Zeitplanung Viren-Update 70
Zeitpunkt 70
Zeitüberschreitung beim Mail-Programm vermeiden 45
Zeitvorgaben 38
Zieldomäne 43
ZIP, RAR 30
Zugangsdaten 70
Zugangsdaten (Benutzername und Passwort) 70
Zugangsdaten für Ihre Internetverbindung 54
Zurücksetzen-Button 38, 39
Zusatzprogramme 6
zustellbar 38
Zustellung 38