
Inhaltsverzeichnis

Allgemeines	3
Supportrahmen	3
Vor der Installation	8
Installation des MailGateways auf dem Mail-Server (SMTP)	8
Installation des MailGateways auf separatem Rechner (SMTP)	8
Systemvoraussetzungen	8
Installation	12
G Data MailSecurity MailGateway	14
G Data MailSecurity Administrator	16
Erster Programmstart (Kennwortvergabe)	16
Weitere Programmstarts (Zugangskennwort)	16
Programmbereiche des Administrators	18
Status	18
Filter	18
Warteschlangen	18
Aktivität	18
Virenfunde	18
Menüleiste des Administrators	29
Optionen	29
Update	29
Spam-Filter	29
Anhang	46
Problemlösungen (FAQ)	46

Welche Bedrohungen gibt es? 47

Wie schütze ich mich vor Computerschädlingen? 54

Notizen 56

Allgemeines

Der sichere Viren- und Spamschutz für Ihre Mail-Korrespondenz. *G Data MailSecurity* arbeitet als **Gateway** unabhängig von Ihrem **Mail-Server**, ist daher mit beliebiger Mail-Server-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 ein erfolgreiches Arbeiten mit *G Data MailSecurity*!

Ihr *G Data-Team*

Supportrahmen

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

G Data PremiumHotline

Die **PremiumHotline** für Ihre *G Data Software* steht allen registrierten Business-Kunden jederzeit zur Verfügung. .

Telefon: 0180 11 55 190

(3,9 Cent/Minute a. d. deutschen Festnetz. Aus dem Mobilfunknetz können ggf. abweichende Preise gelten)

Telefax: 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)** zur *G Data Software* 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 ManagementServers (diese finden Sie im **Hilfe**-Menü der *G Data Software*)
- die **Registrierungsnummer** oder den **Benutzernamen** für das **Internet Update**. Die Registriernummer befindet sich auf der Rückseite des Benutzerhandbuchs. Der Benutzername wird Ihnen bei der **Online-Registrierung** übermittelt.
- genaue Windows-Version (Client/Server)
- zusätzlich installierte Hard- und Softwarekomponenten (Client/Server)

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.

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 befristet oder unbefristet abgeschlossen oder verlängert werden. Kontaktieren Sie uns einfach unter

Telefon: 0234 / 9762-170 (Mo. bis Fr. von 9 bis 18 Uhr)

Telefax: 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*.

Lizenzvereinbarungen

Nachfolgend sind die Vertragsbedingungen für die Benutzung der *Software G Data MailSecurity* durch den Endverbraucher (im Folgenden auch: Lizenznehmer), aufgeführt.

1. Gegenstand des Vertrages: Gegenstand des Vertrages ist die auf einem Datenträger aufgezeichnete oder aus dem Internet geladene *G Data Software* 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, Software 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 einer vertraglich vereinbarten Anzahl von Computern zu benutzen. Die Nutzung der Software kann sowohl in Form einer Installation auf einer physikalischen Einheit (CPU), einer virtuellen / emulierten Maschine (wie z.B. VMWare) oder einer Instanz einer Terminal Session erfolgen. 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 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. Diese Laufzeit umfasst nicht den Bezug von Updates. 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 Software der eventuell vorhandene Datenträger (CD-ROM), auf dem die Software aufgezeichnet ist, unter normalen Betriebsbedingungen und bei normaler Instandhaltung in Materialausführung fehlerfrei ist.
- b) Sollte der Datenträger oder der Download aus dem Internet fehlerhaft sein, so kann der Erwerber Ersatzlieferung während der Gewährleistungszeit von 6 Monaten ab Lieferung verlangen. Er muss dazu den Erwerb der Software belegen.
- c) Aus 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 der Firmensitz von *G Data*.
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.



Copyright ©2009 G Data Software AG

Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2009 BitDefender SRL.

Engine B: ©2009 Alwil Software

OutbreakShield: © 2009 Commtouch Software Ltd.

[G Data MailSecurity - 01.04.2009, 16:22]

Vor der Installation

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 Mail-Server und ist daher mit beliebiger Mail-Server-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 MailGateways 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 gleichzeitig 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-Mail-Server einen neue Port-Nummer (z.B. 7100 oder höher). Das *MailGateway* verwendet dann weiterhin **Port 25** zur Verarbeitung eingehender 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 **winntsystem32\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

? 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 Vista oder Windows Server 2003, 32 MB RAM
- Voraussetzungen für das *G Data MailSecurity Mail Gateway*: Pentium PC mit Betriebssystem Windows XP, 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 die Schaltfläche **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.



? Über den Installationsabschnitt **E-Mail-Statistik** können Sie eine statistische Auswertung des E-Mail-Verkehrs auf dem Mailserver mitinstallieren. Wenn Sie diese Option verwenden, finden Sie im **Optionen**-Menü des Administrators eine zusätzliche Registerkarte namens **Datenbank**.

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 die Schaltfläche **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 Virenschanner 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: JMUENTEST

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 die **OK**-Schaltfläche. Es öffnet sich ein Kennworteingabefenster, in dem Sie unter **Neues Kennwort** ein neues Kennwort für den *G Data MailSecurity Administrator* vergeben können.

Kennwort ändern

Altes Kennwort: []

Neues Kennwort: []

Neues Kennwort bestätigen: []

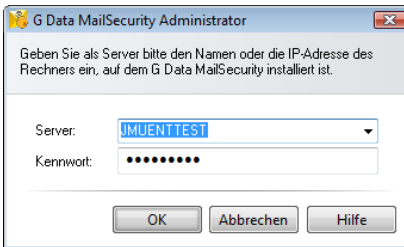
OK Abbrechen

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 die Schaltfläche **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.

Programmbereiche des Administrators

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](#)



[Filter](#)



[Warteschlangen](#)



[Aktivität](#)



[Virenfunde](#)

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



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



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.



Update: 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: Über diese Schaltfläche 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: Hier rufen Sie die Online-Hilfe zum Produkt auf.



Info: Hier erhalten Sie Informationen zur Programmversion.

Status

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 der **Bearbeiten**-Schaltfläche) 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.

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.

? Wenn Sie bei der Installation die Option **E-Mail-Statistik** aktiviert haben, können Sie hier Zugriff auf die statistische Auswertung Ihres Mailverkehrs bzw. Spamaufkommens nehmen. Das Konfigurieren der Statistik erfolgt dabei im **Optionen**-Menü des Administrators auf der Registerkarte namens **Datenbank**.

Filter

Im Filter-Bereich können Sie auf komfortable Weise Filter nutzen, die ein- und ausgehende Mails blocken oder automatisch möglicherweise gefährlichen Inhalte aus Mails entfernen.

Die jeweiligen 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.

- **Import**: Sie können einzelne Filter mit ihren speziellen Einstellungen auch als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen.
- **Export**: Sie können einzelne Filter mit ihren speziellen Einstellungen auch als XML-Datei speichern und ggf. erneut oder auf anderen Rechnern nutzen. Um mehrere Filter zu exportieren, wählen Sie diese bitte mit der Maus aus und halten dabei die **Strg-Taste** gedrückt.
- **Neu**: Über die **Neu**-Schaltfläche können Sie neue Filterregeln anlegen. 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.
- **Bearbeiten**: Über die **Bearbeiten**-Schaltfläche können Sie vorhandene Filter bearbeiten.
- **Löschen**: Um einen Filter endgültig zu löschen, markieren Sie diesen

bitte mit einem einfachen Mausklick und verwenden dann die **Löschen**-Schaltfläche.

- **Statistik:** Zu jedem Filter können Sie statistische Informationen aufrufen.
- **Protokoll:** Für den **Spam-Filter** gibt es ein Protokoll mit einer Liste, in der die als Spam eingestuftten Mails aufgelistet sind. Dem Protokoll kann man auch entnehmen, welche Kriterien für die Einstufung als Spam verantwortlich waren (Spam-Index-Werte). 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.

? 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 Skripten zu bewahren und potentielle Virenherde schon vor der eigentlichen Virenerkennung durch *G Data MailSecurity* zu minimieren.

? **Allgemeine Filterfunktionen**

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.

? **Reaktion**

Im Abschnitt **Reaktion** können Sie festlegen, wie mit Mails verfahren werden soll, sobald Sie die Filterkriterien erfüllen, also als Spam-Mails definiert wurden.

Sie können dabei den Text für die Funktionen **Absender benachrichtigen** und **Meldung an folgende Personen senden** individuell gestalten.

Klicken Sie dazu einfach auf die **•••**-Schaltfläche rechts von der

jeweiligen Reaktion. 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:

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

Die unterschiedlichen Filtertypen werden in den folgenden Abschnitten ausführlich erläutert:

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 weiterzubreiten, 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 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 VB-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 Mail-Server 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*.

Geben Sie unter **Modus** an, ob Sie die unter **Dateierweiterungen** aufgelisteten Dateiendungen erlauben möchten (**Nur angegebene Anhänge erlauben**) oder verbieten (**Angegebene Anhänge filtern**).

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 Skripte 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 Dateieindung 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.

Über die **Neu**-Schaltfläche 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. *Alkohol UND Drogen* eingeben, würde der Filter bei einer Mail, die z.B. die Begriffe *Alkohol* und *Drogen* enthält, aktiviert werden, nicht aber bei einer Mail, die nur den Begriff *Alkohol* oder nur den Begriff *Drogen* 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:

<u>ODER</u>	entspricht dem Trennstrich	(AltGr + <)	
<u>UND</u>	entspricht dem Kaufmanns-Und	(Shift + 6)	&

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.

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.

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 Spam-Filters werden im Kapitel [Spam-Filter](#) 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.

Unter **Modus** können Sie dabei festlegen, ob der IP-Filter im Whitelist-Modus nur bestimmte IP-Adressräume erlauben soll oder im Blacklist-Modus nur bestimmte IP-Adressräume sperren soll.

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

Sprachenfilter

Mit dem Sprachenfilter können Sie automatisch Mails bestimmter Landessprachen als Spam definieren. Wenn Sie also in der Regel z.B. keinen Mailkontakt zu englischsprachigen Personen haben, können Sie über die Definierung von *Englisch* als Spam-Sprache sehr viele Spams ausfiltern. Wählen Sie hier einfach die Sprachen aus, bei denen Sie davon ausgehen, dass Sie in eben diesen Sprachen keine regulären Mails erhalten und *G Data MailSecurity* erhöht damit die Spameinschätzung für diese Mails erheblich.

Warteschlangen

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 die Schaltfläche **Eingehend/Ausgehend** wechseln Sie von der **Listenansicht für eingehende Mails** zur **Listenansicht für ausgehende Mails**. Über die Schaltfläche **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 der **Löschen**-Schaltfläche entfernen Sie eine nicht zustellbare Mail endgültig aus der Queue.

Aktivität

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 die **Zurücksetzen**-Schaltfläche löschen Sie das bis dahin erzeugte Protokoll und *G Data MailSecurity* beginnt die Aufzeichnung der Aktivitäten erneut. Mit der Funktion **Bildlauf deaktivieren** wird die Liste wohl weiterhin aktualisiert, aber die neuesten Aktivitäten werden nicht direkt an erster Stelle eingeblendet. Sie können dann konzentrierter in der Liste scrollen.

? 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

Im Virenfunde-Bereich werden sie detailliert darüber informiert, wann *G Data MailSecurity* eine infizierte Mail ermittelt hat, welche Maßnahmen dahingehend erfolgten, um welche Art von Virus es sich handelt und wer die eigentlichen Sender und Empfänger dieser betreffenden Mail sind.

Über die **Vireninformation**-Schaltfläche 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.

Menüleiste des Administrators

Hier finden Sie übergeordnete Funktionen der Administrationssoftware.

Optionen

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.

Eingehend (SMTP)

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

Empfang

Hier können Sie festlegen, ob **eingehende Mails** verarbeitet werden sollen. Generell ist hier **Port 25** voreingestellt. Sollte auf Grund besonderer Umstände dieser **Standardport** nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Port-Einstellungen und Protokoll-Einstellungen für eingehende Mails definieren.

Weiterleitung

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. Sollten mehrere Netzwerkkarten zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

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.

? **ActiveDirectory** ist eine in Microsoft Windows (XP, 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

Über das Häkchenfeld **Ausgehende Mail verarbeiten** legen Sie grundlegend fest, ob Sie ausgehende SMTP-Mails auf Virenbefall kontrollieren möchten oder nicht. Unter **IP-Adressen/Subnetze der Rechner, 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. Generell ist der **Port 25** für den Empfang ausgehender Mails voreingestellt. Sollte auf Grund besonderer Umstände dieser Standardport nicht verwendet werden, können Sie über die Schaltfläche **Konfigurieren** auch andere Port-Einstellungen und Protokoll-Einstellungen für eingehende Mails definieren.

Weiterleitung

Aktivieren Sie den Eintrag **DNS zum Versenden der Mails verwenden**, damit die Mails direkt an den für die Zieldomäne zuständigen Mail-Server geschickt werden. 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. Sollten mehrere **Netzwerkarten** zur Verfügung stehen, können Sie über die Auswahl unter **Absende-IP** festlegen, welche dieser Karten Sie verwenden möchten.

Eingehend (POP3)

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

Anfragen

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 gegebenenfalls den **Port** angeben, den Ihr Mailprogramm für POP3-Anfragen verwendet (in der Regel **Port 110**). 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.

Abholung

Unter Mails von diesem POP3-Server abholen müssen Sie gegebenenfalls den POP3-Server angeben, von dem Sie die Mails abholen (z.B. *pop3.maieldienstanbieter.de*).

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. 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 Falle 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. 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 die **•••-Schaltfläche** 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. 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.

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **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 der **☐**-Schaltfläche können Sie dann eine Dialogbox öffnen, in der Sie die gewünschten Dateitypen ins obere Eingabefeld eintragen und dann über die **Hinzufügen**-Schaltfläche 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 Dateiendung **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 die Schaltfläche **Einstellungen** an, ob Sie einen Proxyserver verwenden und gegebenenfalls - um OutbreakShield einen jederzeitigen Zugang zum Internet zu ermöglichen - die **Zugangsdaten für die 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 Mail-Server weitergeleitet werden können.

Mails können sich dabei aus verschiedenen Gründen in der Warteschlange befinden. So kann z.B. der Mail-Server, an den Sie nach der Virenprüfung weitergeleitet werden sollen, überlastet oder ausgefallen sein.

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

Nichtzustellbare 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 die Schaltfläche **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.

Rechnername

Hier können Sie ggf. den Rechnernamen (**FQDN = Full Qualified Domain Name**) des Mailservers ändern.

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.

Einstellungen

Über die Schaltflächen **Import** und **Export** können Sie die Einstellungen der Programm-Optionen auch als **XML-Datei** speichern und so ggf. erneut einspielen, wenn der Bedarf gegeben ist.

Kennwortändern

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 der **OK**-Schaltfläche wird die Kennwortänderung durchgeführt.

Datenbank

Im **Datenbank**-Bereich können Sie den Mailverkehr auf Ihrem Server statistisch auswerten. Die Ergebnisse dieser Statistikfunktion können Sie im Statistik-Bereich der Programmoberfläche aufrufen, den Sie durch Anklicken der Schaltfläche **Statistik** im Programmbereich **Status** finden.

Update

Im Update-Bereich können Sie umfangreiche Einstellungen vornehmen, um *G Data MailSecurity* optimal auf die Gegebenheiten anzupassen, die in Ihrem Netzwerk existieren. Hier können Sie die Virensignaturen und Programmdateien von *G Data MailSecurity* manuell oder automatisiert auf den neuesten Stand bringen.

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 die Schaltfläche **Einstellungen und Zeitplanung** gelangen Sie in einen Bereich, in dem Sie sämtliche notwendigen Einstellungen für manuelle und automatische Internet Updates eingeben können.

Zugangsdaten

Geben Sie unter **Zugangsdaten** den Benutzernamen und das Passwort ein, das Sie bei der Anmeldung von *G Data MailSecurity* erhalten haben. Klicken Sie auf die Schaltfläche **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 Anmelde Nummer 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.

Zeitplanung Viren-Update

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** 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, dass 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.

Internet-Einstellungen

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 Internet Einstellungen (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.

Benutzerkonto

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 Schaltflächen **Viren-Update** und **Status aktualisieren** können Sie auch unabhängig von den Vorgaben, die Sie unter Zeitplanung vorgenommen

haben, ein aktuelles Virensignaturupdate starten.

Programmdateien

Über die Schaltfläche **Programm-Update** können Sie auch die Programmdateien von *G Data MailSecurity* aktualisieren, sobald sich hier Änderungen und Verbesserungen ergeben.

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. 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.

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 Sammelmailables, 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.

? 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.

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 die **Import**-Schaltfläche 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 die **Export**-Schaltfläche 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 die **Import**-Schaltfläche 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 die **Export**-Schaltfläche 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 Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern. Über die **Import**-Schaltfläche 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 die **Export**-Schaltfläche 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 Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** beliebig verändern.

Über die **Import**-Schaltfläche 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 die **Export**-Schaltfläche 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 die Schaltfläche **Tabelleninhalte abfragen** können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer Mail als Spam verwendet. Über die Schaltfläche **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 Mail-Servers 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.

Anhang

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](#).

Welche Bedrohungen gibt es?

Wenn von **Viren**, **Wurmern** und **Trojanischen Pferden** gesprochen wird, ist damit im Allgemeinen ein schädlicher Aspekt von Software verbunden. Als Oberbegriff dafür hat sich der Begriff **Malware** (Eine Kombination der Worte *malicious* = *boshaft*, *schädlich* und *Software*) durchgesetzt. Unter **Malware** werden Programme zusammengefasst, die in böser Absicht elektronische Daten zugänglich machen, verändern oder löschen. **Malware** besitzt immer eine Schadensfunktion (engl. **Payload**) und verursacht unterschiedliche Effekte. Dies kann von eher harmlosen Bekundungen des eigenen Vorhandenseins über ausspionieren von persönlichen Daten bis hin zur Löschung der Festplatte reichen. Malware kann man in die drei Gruppen **Trojanische Pferde**, **Würmer** und **Viren** untergliedern. In einem erweiterten Sinn fallen auch **Spysware** und **Dialer** darunter.

- **Trojaner:** Trojaner unterscheiden sich von Würmern und Viren dadurch, dass sie sich nicht selbsttätig reproduzieren. Der Name **Trojanisches Pferd** ist angelehnt an das geschichtliche Vorbild und beschreibt ein Programm, das dem Anwender vorgibt, eine bestimmte und gewollte Funktion zu besitzen. Zusätzlich dazu beinhalten Trojaner jedoch noch einen versteckten Programmteil, der gleichsam eine Hintertür zum befallenen Rechner öffnet und so nahezu vollen Zugriff auf das betroffene System gewähren kann, ohne dass der Benutzer dies bemerkt. Die Methoden von Trojanern, sich zu verstecken sind dabei schier unbegrenzt. Sie können sich in Kommandozeilenbefehlen verstecken (sog. **Rootkits**) oder als **Remote Access Trojans** (sog. **RATs**, auch **Backdoor** genannt) daherkommen. Diese heimtückischen Programme werden aber auch als Bildschirmschoner oder Spiele per E-Mail verschickt.
- **Gemeinsamkeiten von Viren und Wurmern:** **Viren** und **Würmer** sind aus folgenden Teilen aufgebaut:

Reproduktionsteil: Mit diesem Programmteil wird die Vermehrung des Virus durchgeführt. Dieser Teil ist obligatorisch für alle Viren. Die Infektion kann über Disketten, USB-Sticks (und andere wechselbare Datenträger), freigegebene Ordner, Netzwerkscans, Peer-to-Peer Netzwerke oder E-Mail erfolgen. Dabei nutzen die Schädlinge viele verschiedene Angriffspunkte, die teilweise nur auf bestimmten Kombinationen von Hardware, Software und Betriebssystem funktionieren.

Erkennungsteil: Im Erkennungsteil wird geprüft, ob schon eine Infektion mit diesem Virus vorliegt. Jedes Wirtsprogramm wird nur einmal infiziert, um die Verbreitung zu beschleunigen und die Tarnung aufrecht zu erhalten.

Schadensteil: Die Schadensfunktionen (engl. **Payload**) kann man in folgende Gruppen einordnen:

- Mit **Backdoor**-Programmen verschafft sich der Hacker Zugang zum Rechner und den Daten und kann so Daten manipulieren oder **Denial of Service Attacken** starten.
- Es können **Datenmanipulationen** vorgenommen werden. Das reicht von (mehr oder weniger lustigen) Meldungen, Anzeigen und Geräuschen bis hin zum Löschen von Dateien und Laufwerken.
- Es können auch **Informationen** ausgespäht und versendet werden. Ziel dieser Attacken sind **Passwörter**, **Kreditkartennummern**, **Loginnamen** und andere persönliche Daten.
- Oft werden verseuchte Rechner für **Denial of Service (DoS)** Attacken missbraucht. Diese zielen darauf ab, z.B. eine Webseite durch häufige Anfragen zu überlasten. Wenn die Attacke nur von einer Quelle kommt, lassen sich solche Attacken sehr leicht abwehren. In **Distributed Denial of Service (DDoS)** Attacken werden daher infizierte Rechner missbraucht, um die Attacken zu unterstützen. **DoS** und **DDoS** Attacken können darauf zielen, das Zielsystem herunterzufahren, die Bandbreite und Speicherauslastung zu überladen oder den Dienst im Netzwerk nicht mehr auffindbar zu machen.

Bedingungsteil: Sowohl die Verbreitung als auch die Schadensfunktion können von Bedingungen abhängig programmiert sein.

- Im einfachsten Fall startet der schädliche Code automatisch, ohne dass das Opfer etwas davon bemerkt.
- in einigen Fällen muss die Payload vom Opfer selbst gestartet werden. Das kann der Aufruf eines verseuchten Programms sein, das Öffnen eines E-Mail-Anhangs bis hin zum **Phishing** von persönlichen Daten.
- der Start des schädlichen Codes kann auch an Bedingungen geknüpft sein. Z.B. tritt bei einigen Viren der Schaden an einem bestimmten Datum oder bei einer bestimmten Anzahl von Aufrufen ein.

Tarnungsteil: Würmer, Trojaner und Viren versuchen sich vor der Entdeckung durch Benutzer und Virenerkennern zu schützen. Dazu verwenden Sie eine Reihe von Mechanismen.

- Sie erkennen z.B. wenn Debugger laufen oder schützen sich durch überflüssige und verwirrende (Assembler-) Codezeilen.
 - Sie verbergen die Spuren einer Infektion. Dazu wird u.a. die Ausgabe von Statusmeldungen oder Log-Einträge gefälscht. Z.B. kann ein speicherresidenter Virus dem System vorgaukeln, dass der Speicher den er belegt immer noch von dem zuvor entfernten Programm stammt.
 - Um der Entdeckung zu entgehen verschlüsseln manche Viren sich selbst und/oder Ihren Schadenscode. Bei der Entschlüsselung können immer die gleichen Schlüssel verwendet werden, die Schlüssel können aus einer Liste entnommen sein (**oligomorph**) oder die Schlüssel können unbegrenzt neu erzeugt werden (**polymorph**).
- **Würmer:** Ein **Wurm** hängt sich im Gegensatz zu einem Virus nicht an ausführbare Dateien an. Er verbreitet sich dadurch, dass er sich automatisch über Netzwerke oder Mailverbindungen auf andere Rechner überträgt.

Netzwerk-Würmer: In Netzwerken werden auf zufällig ausgewählten Rechnern einige Ports gescannt und wenn eine Attacke möglich ist, werden die Schwachstellen in Protokollen (z.B. IIS) oder deren Implementierung zur Verbreitung ausgenutzt. Bekannte Vertreter dieser Art sind **Lovsan/Blaster** und **CodeRed**. **Sasser** nutzt einen **Buffer Overflow-Fehler** in der **Local Security Authority Subsystem Service (LSASS)** und infiziert Rechner während einer Verbindung zum Internet.

E-Mail-Würmer: Bei der Verbreitung per E-Mail kann ein Wurm vorhandene E-Mail Programme (z.B. Outlook, Outlook Express) verwenden oder eine eigene SMTP-Mailengine mitbringen. Abgesehen vom entstehenden Netzwerktraffic und den erhöhten Systemressourcen können Würmer noch weitere Schadensfunktionen beinhalten. Prominente Mitglieder dieser Gruppe sind **Beagle** und **Sober**.

- **Viren:** Auch Viren zielen auf ihre eigene Reproduktion und Verbreitung auf andere Computer ab. Dazu hängen sie sich an andere Dateien an oder nisten sich im Bootsektor von Datenträgern ein. Sie werden oft unbemerkt von austauschbaren Datenträgern (wie z.B. Disketten), über Netzwerke (auch Peer-to-Peer), per E-Mail oder aus dem Internet auf den PC eingeschleust. Viren können an vielen unterschiedlichen Stellen im Betriebssystem ansetzen, über unterschiedlichste Kanäle wirken. Man unterscheidet folgende Gruppen:

Bootsektorviren: Bootsektor- oder **MBR-Viren** (= Master Boot Record-Viren) setzen sich vor den eigentlichen Bootsektor eines Datenträgers und sorgen so dafür, dass bei einem Bootvorgang über diesen Datenträger erst der Viruscode gelesen wird und danach der Original-Bootsektor. Auf diese Weise kann sich der Virus unbemerkt in das System einnisten und wird von da ab auch beim Booten von der Harddisk mit ausgeführt. Oft bleibt der Virencode nach der Infektion im Speicher bestehen. Solche Viren nennt man **speicherresident**. Beim Formatieren von Disketten wird der Virus dann weitergegeben und kann sich so auch auf andere Rechner ausbreiten. Aber nicht nur bei Formatier-Vorgängen kann der Bootbereichvirus aktiv werden. So kann durch den DOS-Befehl **DIR** die Übertragung des Virus von einer infizierten Diskette in Gang gesetzt werden. Je nach Schadensroutine können Bootbereichviren hochgradig gefährlich oder einfach nur störend sein. Der älteste und verbreitetste Virus dieser Art trägt den Namen **Form**.

Datei-Viren: Viele Viren nutzen die Möglichkeit, ausführbare Dateien als Versteck zu nutzen. Dazu kann die Wirtsdatei entweder gelöscht/ überschrieben werden oder der Virus hängt sich an die Datei an. In letzterem Fall bleibt der ausführbare Code der Datei weiterhin funktionsfähig. Wenn die ausführbare Datei aufgerufen wird, wird zunächst der meist in Assembler geschriebene Virencode ausgeführt und danach das ursprüngliche Programm gestartet (sofern nicht gelöscht).

Multipartite Viren: Diese Virengruppe ist besonders gefährlich, da ihre Vertreter sowohl den Bootsektor (bzw. Partitionstabellen) infizieren als auch ausführbare Dateien befallen.

Companion Viren: Unter DOS werden COM Dateien vor gleichnamigen **EXE** Dateien ausgeführt. Zu den Zeiten als Rechner nur oder häufig über Kommandozeilenbefehle bedient wurden war dies ein wirkungsvoller Mechanismus um unbemerkt schädlichen Code auf einem Rechner auszuführen.

Makroviren: Auch Makroviren hängen sich an Dateien an. Diese sind aber nicht selbst ausführbar. Die Makroviren sind auch nicht in Assembler, sondern in einer Makrosprache wie etwa **Visual Basic** geschrieben. Um die Viren auszuführen bedarf es eines Interpreters für eine Makrosprache wie sie in Word, Excel, Access und PowerPoint integriert sind. Ansonsten können die Makroviren die gleichen Mechanismen wirken wie bei Datei-Viren. Auch sie können sich tarnen, zusätzlich den Bootsektor verseuchen oder Companion-Viren erstellen.

Stealth-Viren: Stealth-Viren oder **Tarnkappen-Viren** besitzen spezielle Schutzmechanismen, um sich einer Entdeckung durch Virensuchprogramme zu entziehen. Dazu übernehmen sie die Kontrolle über verschiedene Systemfunktionen. Ist dieser Zustand erst einmal hergestellt, so können diese Viren beim normalen Zugriff auf Dateien oder Systembereiche nicht mehr festgestellt werden. Sie täuschen dem Virensuchprogramm einen nicht infizierten Zustand einer infizierten Datei vor. Die Tarnmechanismen von Stealth-Viren wirken erst, nachdem der Virus im Arbeitsspeicher resident geworden ist.

Polymorphe Viren: Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern. Dazu werden Teile des Virus verschlüsselt. Die im Virus integrierte Verschlüsselungsroutine generiert dabei für jede Kopie einen neuen Schlüssel und teilweise sogar neue Verschlüsselungsroutinen. Zusätzlich können Befehlssequenzen ausgetauscht oder zufällig eingestreut werden, die nicht für das Funktionieren des Virus erforderlich sind. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensteckbriefe (auch *Signatures* genannt) häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.

Intended Virus: Als **Intended Virus** wird ein teilweise defekter Virus bezeichnet, der zwar eine Erstinfektion einer Datei vollbringt, sich von dort aus aber nicht mehr reproduzieren kann.

E-Mail-Viren: E-Mail-Viren gehören zur Gruppe der sog. **Blended threats** (= vermischte Bedrohung). Solche Malware kombiniert die Eigenschaften von Trojanern, Würmern und Viren. Im Rahmen des **Bubbleboy-Virus** wurde bekannt, dass es möglich ist, schon über

die Voransicht einer HTML-Mail einen Virus auf den PC einzuschleusen. Der gefährliche Virencode versteckt sich in HTML-Mails und nutzt eine Sicherheitslücke des Microsoft Internet Explorers. Die Gefahr dieser Kombi-Viren nicht zu unterschätzen.

- **Malware im weiteren Sinn:** Der Vollständigkeit halber sollen hier noch einige andere lästige und teilweise auch schädliche Kategorien erwähnt werden, die wir nicht zur Gruppe der Malware zählen.

Hoaxes: Hoaxes sind angebliche Viren-Warnungen, die oft per E-Mail verbreitet werden. Empfänger werden aufgefordert die E-Mail-Warnung an Freunde und Bekannte weiterzuleiten. Meistens handelt es sich bei diesen Hinweisen allerdings nur um Panikmache.

Backdoor-Programme: Viele Systemadministratoren verwenden Fernwartungsprogramme, um Rechner quasi fernzusteuern. Insbesondere bei großen Unternehmen ist dies sehr nützlich. Üblicherweise erfolgt der Eingriff des Systemadministrators dabei mit dem Wissen und Einverständnis des PC-Users. Erst wenn diese Backdoor-Funktionen ohne Wissen des PC-Users eingesetzt werden und schädliche Aktionen ausgeführt werden wird ein Backdoorprogramm zur Malware.

Spyware: Spyware zeichnet die Aktivitäten und Prozesse auf einem Rechner auf und machen sie Fremden zugänglich. Oft werden sie verwendet um das Surfverhalten zu analysieren, um passende Werbebanner einzublenden. Spyware lässt sich in der Regeldurch entsprechende AntiSpyware-Programme entfernen..

Dialer: Ähnlich wie Viren, Würmer und Trojaner werden Dialer oft unbemerkt auf dem Rechner installiert. Sofern die DFÜ-Verbindung über ein Modem hergestellt wird, wird dann beim nächsten Verbindungsaufbau eine teure Service-Telefonnummer verwendet. Eine lästige Plage, die mitunter zu hohen finanziellen Schäden führen kann. Mit Anti-Dialer-Programmen wie **Dialer Control** kann man sich vor unerwünschten Dialern schützen.

Spam: Eine ebenfalls teure und lästige Plage ist das Versenden unerwünschter Werbe-E-Mail oder Propagandamail. Moderne Anti-Spam Programme kombinieren statische (Textanalyse, Mailserverlisten) und automatische (basierend auf Bayes Theorem) Verfahren um die unerwünschte Post zu filtern.

Phishing: Unter **Phishing** versteht man den Versuch persönliche Daten wie Loginnamen, Passwörter, Kreditkartennummern, Bankzugangsdaten etc. durch gefälschte Webseiten oder E-Mails zu erhalten. Oft wird man dazu auf gefälschte Webseiten geleitet. In den letzten Jahren hat dieses Phänomen stark zugenommen. Mehr dazu erfährt man auf www.antiphishing.org.

Wie schütze ich mich vor Computerschädlingen?

Obwohl die **G Data Software** nicht nur bekannte Viren entdeckt und beseitigt, sondern mit Hilfe der heuristischen Analyse auch bis dato unbekannte Schadprogramme erkennt, ist es fraglos besser, einen Virenbefall von vornherein auszuschließen. Dazu sollten einige Sicherheitsvorkehrungen getroffen werden, die nicht viel Mühe kosten, die Sicherheit Ihres Systems und Ihrer Daten jedoch merklich erhöhen.

- **Benutzerkonten verwenden:** Sie sollten auf Ihrem Computer zwei Benutzerkonten verwenden. Ein **Administrator-Konto**, das Sie immer dann verwenden, wenn Sie Software installieren oder grundlegende Einstellungen an Ihrem Computer vornehmen und ein **Benutzerkonto** mit eingeschränkten Rechten. Das Benutzerkonto sollte z.B. nicht in der Lage sein Programme zu installieren oder Veränderungen im Windows-Betriebssystem vorzunehmen. Mit diesem Konto können Sie dann relativ gefahrlos z.B. im Internet surfen, Daten von Fremdrechnern übernehmen usw. Wie Sie unterschiedliche Benutzerkonten anlegen, wird Ihnen in der Hilfe-Dokumentation Ihres Windows-Betriebssystems erläutert.
- **Spam-Mails ignorieren:** Auf Kettenbriefe und Spam-Mail sollte grundsätzlich nicht geantwortet werden. Selbst wenn solche E-Mails keinen Virus enthalten sollten, belastet Ihre unerwünschte Weiterleitung den Datenfluss im Internet erheblich.
- **Virenverdacht überprüfen:** Sollten Sie einen begründeten Virenverdacht haben, z.B. weil eine neu installierte Software nicht das tut, was erwartet wurde oder eine Fehlermeldung erscheint, dann überprüfen Sie das entsprechende Programm am besten noch vor dem Neustart des Rechners auf Virenbefall. Dies ist sinnvoll, da z.B. einige Trojanische Pferde Löschbefehle erst beim nächsten Neustart des Rechners ausführen und auf diese Weise vorher einfacher zu entdecken und bekämpfen sind.
- **Regelmäßige Windows-Updates:** Es sollte es zur regelmäßigen Routine werden, die aktuellen Patches von Microsoft einzuspielen, da diese neu entdeckte Sicherheitslücken von Windows oftmals schon schließen, bevor ein Virenprogrammierer überhaupt auf die Idee kommt, diese für neue Schadroutinen auszunutzen. Das Windows-Update lässt sich auch automatisieren.

- **Original-Software verwenden:** Auch wenn in sehr seltenen Fällen auch die Datenträger von Original-Software virenverseucht sein können, ist die Wahrscheinlichkeit einer Vireninfiltration durch Raubkopien oder Kopien auf wiederbeschreibbaren Datenträgern erheblich höher. Benutzen Sie deshalb nur Original-Software.
- **Software aus dem Internet mit Vorsicht behandeln:** Seien Sie beim Download von Software aus dem Internet äußerst kritisch und verwenden Sie nur Software die Sie auch wirklich benötigen und deren Herkunft Ihnen vertrauenswürdig erscheint. Öffnen Sie niemals Dateien, die Ihnen per E-Mail von Unbekannten zugeschickt wurden oder die überraschend von Freunden, Kollegen oder Bekannten kommen. Vergewissern Sie sich vorher lieber durch eine Nachfrage an betreffender Stelle, ob Sie die jeweilige Anwendung gefahrlos starten können oder nicht.

? Wenn Sie sich eingehend mit der Virenproblematik beschäftigen möchten, finden Sie viele interessante Artikel und Informationen online im **G Data Virenlexikon**: www.antiviruslab.com

Notizen

Index

A

- Abholung 32
- Absende-IP 29, 31
- Absender 21, 32, 33, 34
- Absender benachrichtigen 21
- Absender der infizierten Mail benachrichtigen 34
- Absender der Nachricht benachrichtigen 42
- Absender von Nachrichten in der Warteschlangen alle x Stunden benachrichtigen 37
- Absenderfilter 26
- Absender-IP 21, 32, 33, 34
- ActiveDirectory 30
- ActiveDirectory-Anbindung 30
- Administrator 8, 14, 16
- Administrator-Konto 54
- Administrator-Passwort 39
- AdministratorTool 16
- Administrator-Tool 14
- Adressen/Domains 26, 43
- Aktionsbeschreibung 28
- Aktivität 18, 28
- Allgemeine Filterfunktionen 21
- Allgemeines 3
- Altes Kennwort 39
- Am Server anmelden 40
- An folgende Personen weiterleiten 42
- Anfragen 31
- Angegebene Anhänge filtern 24
- Anhang 46
- Anhänge filtern 24
- Anhänge nur umbenennen 24
- Anmeldung am Server 40
- AntiVirusLab 28
- AntiVirusLab-Virenlexikon 18
- Anzahl von SMTP Client-Verbindungen begrenzen 38
- Archivdateien 24
- Archive prüfen 35
- Attachments 24
- Auch Anhänge in eingebetteten Mails filtern 24
- Auf Standardwerte zurücksetzen 37
- Ausführen 12, 40
- Ausgehend 34
- Ausgehend (SMTP) 30
- Ausgehende Mail verarbeiten 30
- ausgehende Mails 21
- Ausgehende Mails auf Viren prüfen 34
- automatische Einwahl 41
- Automatische Updates 19
- Autostart-Funktion Ihres CD-ROM-Laufwerks 12

B

- Backdoor 47
- Backdoor-Programme 47
- Beagle 47
- Bedingungsteil 47
- Begrenzung 38
- Bemerkung 21, 27, 42
- Benachrichtigungsoptionen 33, 34
- benutzerdefiniert 35
- Benutzerkonten verwenden 54
- Benutzerkonto 41
- Benutzernamen 3
- Bericht an ausgehende (nicht infizierte) Mails anhängen 34
- Betreff 21, 32, 33, 34
- Betreffzeile 44
- Bildlauf deaktivieren 28

- Blacklist 43
- Blacklist 1, 2 und 3 44
- Blacklists 44
- Blended threats 47
- Bootsektorviren 47
- Bubbleboy-Virus 47
- Buffer Overflow-Fehler 47
- Business-Vertrieb 4

- C**
- Cc 21, 32, 33, 34
- CD-ROM 12
- CodeRed 47
- Companion Viren 47

- D**
- Dateierweiterungen 24
- Dateitypen 35
- Datei-Viren 47
- Datenbank 39
- Datenmanipulationen 47
- Datum 21, 32, 33, 34
- Datum der Virensignaturen 19
- DDoS 47
- Denial of Service 47
- Denial of Service Attacken 47
- Denial of Service-Attacken 38
- Desinfizieren (wenn nicht möglich: löschen) 33
- Desinfizieren (wenn nicht möglich: nur protokollieren) 33
- Desinfizieren (wenn nicht möglich: umbenennen) 33
- Dialer 47
- Dialer Control 47
- Die Nachricht wurde vom Systemadministrator zurückgewiesen 32
- Distributed Denial of Service 47
- DNS zum Versenden der Mails verwenden 29, 31
- DNS-Eintrag 10
- DoS 47
- Durchsuchen 12

- E**
- Eingehend 33
- Eingehend (POP3) 31
- Eingehend (SMTP) 29
- Eingehend/Ausgehend 27
- Eingehend/Ausgehend (SMTP, POP3) 38
- eingehende Mails 21, 29
- Eingehende Mails auf Viren prüfen 33
- Eingehende Mails nur für folgende Domains akzeptieren 30
- Einstellungen 35, 39, 40
- Einstellungen und Zeitplanung 40
- E-Mails 14
- E-Mail-Viren 47
- E-Mail-Würmer 47
- Empfang 29, 30
- Empfänger 21, 32, 33, 34
- Empfängerfilter 26
- Engines benutzen 35
- Erkennungsteil 47
- Ersatztext 35
- Ersatztext bei zurückgewiesenen Mails 32
- Erster Programmstart (Kennwortvergabe) 16
- Erweitert 16, 38
- Export 21, 39, 43, 44, 45
- Externe Referenzen deaktivieren 23

F

- False Positive 21
- Fehlerwartezeit 37
- Filter 18, 21, 32, 42
- Firewall 8, 10, 41
- Firewall-Konfigurationen 8
- Form 47
- FQDN 38
- Full Qualified Domain Name 38

G

- G Data AntiVirus 35, 40
- G Data AntiVirus Business 35
- G Data AntiVirus Business- oder G Data AntiVirus Enterprise-Lösung 35
- G Data AntiVirus Business-Lösung 40
- G Data AntiVirus Enterprise 4
- G DATA MailSecurity Administrator 16
- G DATA MailSecurity MailGateway 14
- G Data PremiumHotline 3
- Gateway 3
- Gemeinsamkeiten von Viren und Würmern 47
- gepackter Dateien 35
- Größenbegrenzung 38

H

- Header 21, 32, 33, 34
- Heuristik 35
- Hilfe 3, 18
- Hinzufügen 35
- Hoaxes 47
- Hohe Spamwahrscheinlichkeit 42
- Hotline 3
- HTML-Mailformat 23
- HTML-Skripte deaktivieren 23
- Hyperlink 23

I

- Ich verwende AVM Ken! und möchte G Data MailSecurity auf dem gleichen Rechner wie den Ken!-Server installieren 46
- Ich verwende einen Exchange-Server 2000 und möchte G Data MailSecurity auf dem gleichen Rechner wie den Exchange-Server installieren. 46
- ID 28
- Im Falle einer Infektion 33, 35
- Import 21, 39, 43, 44, 45
- Infizierte Anhänge löschen 33
- Infizierte Anhänge umbenennen 33
- Infizierte Nachricht nicht versenden 34
- Info 18
- Informationen 47
- Inhaltsfilter 25, 45
- Installation 12
- Installation des MailGateways auf dem Mail-Server (SMTP) 9
- Installation des MailGateways auf separatem Rechner (SMTP) 10
- Installieren 12
- Intended Virus 47
- Internet Update 3, 19
- Internet Update der Virensignaturen selbst durchführen 40
- Internet-Einstellungen 41
- IP-Adresse 10
- IP-Adressen/Subnetze der Rechner, die ausgehende Mails senden 30
- IP-Filter 27

J

- Jetzt wiederholen 27

K

- Kaufmanns-Und 25

Kennwort 16
Kennwort ändern 16, 39
Konfiguration MailGateway (Ausgehend (SMTP)) 9, 10
Konfiguration MailGateway (Eingehend (SMTP)) 10
Konfiguration MailGateway (Eingehended (SMTP)) 9
Konfiguration Mail-Server 9, 10
Konfigurieren 29, 30
Kreditkartennummern 47

L

Lesebestätigung filtern 23
Listenansicht für ausgehende Mails 27
Listenansicht für eingehende Mails 27
Lizenzvereinbarungen 5
Local Security Authority Subsystem Service 47
Loginnamen 47
Lowsan/Blaster 47
LSASS 47

M

Mail zurückweisen 42
Mail-Anhänge 24
MailGateway 8, 10
Mails an diesen SMTP-Server weiterleiten 29, 31
Mails mit sehr hoher Spamwahrscheinlichkeit 43
Mails von diesem POP3-Server abholen 32
Mail-Server 3
Mailtext 21, 33, 34, 45
Makroviren 47
Malware 47
Malware im weiteren Sinn 47
manuell konfiguriert 31

MBR-Viren 47
Meldung an folgende Personen senden 21
Meldung im Text der Mail einfügen 24
Menüleiste des Administrators 29
Microsoft Exchange 5.5 9
Mindest-Systemvoraussetzungen 12
Modus 24, 27
Multipartite Viren 47
MX-Record 10

N

Nachricht löschen 33, 35
Name 21, 27, 42
Net-Framework 1.1 30
Netzwerkkarten 31
Netzwerk-Würmer 47
Neues Kennwort 16, 39
Neues Kennwort bestätigen 16, 39
Nicht zustellbare Nachrichten 37
Notizen 56
Nur angegebene Anhänge erlauben 24
Nur protokollieren 33
Nur vollständige Wörter suchen 44, 45

O

oligomorph 47
Online-Datenbank für häufig gestellte Fragen (FAQ) 3
Online-Registrierung 3
Online-Registrierungsformular 3
Optionen 16, 18, 29
Original-Software verwenden 54
OutbreakShield 19, 35

P

Passwörter 47

Payload 47
Phishing 47
Platzhalter 21, 32, 34, 35
polymorph 47
Polymorphe Viren 47
POP3 8, 14
POP3-Anfragen verarbeiten 31
POP3-Mails 14, 31, 32
POP3-Sammelkonto 14
Port 29, 31
Port 110 31
Port 25 9, 29, 30
Postfach 14
PremiumHotline 3
PremiumSupport 4
PremiumSupport-Verlängerungen 4
Problemlösungen (FAQ) 46
Profi-Einstellungen 45
Programmbereiche des Administrators 18
Programmdateien 42
Programm-Update 42
Protokoll 21
Protokollieren 33
Proxyserver 41
Prüfung ausgehender Mails (SMTP) 14
Prüfung eingehender Mails (POP3) 14
Prüfung eingehender Mails (SMTP) 14

R

RATs 47
RBLs 44
Reaktion 21, 42
Realtime Blacklists 44
Rechnername 38
Regelmäßige Windows-Updates 54
Registriernummer 3

Registrierungsnummer 3
Regulärer Ausdruck 25
Relay 31
Relay-Schutz 30
Remote Access Trojans 47
Reproduktionsteil 47
Richtung 21
Rootkits 47

S

Sasser 47
Scanparameter 35
Schadensteil 47
Schlüsselwörter (Betreff) 44
Schlüsselwörter (Mailtext) 45
Schutz vor Relaying 30
Sehr hohe Spamwahrscheinlichkeit 42
Senden 40
Server 16, 17
ServiceCenter 4
Setup 9
SMTP 8, 14
SMTP-Mails 29, 30
SMTP-Server 9, 14
Sober 47
Software aus dem Internet mit Vorsicht behandeln 54
Spam 42, 47
Spam filtern 26
Spam-Filter 18, 19, 21, 26, 42
Spam-Mails ignorieren 54
Spam-OutbreakShield 19
Spamverdacht 42
Spamwarnung in Betreff und Text der infizierten Mail einfügen 42
speicherresident 47
Sprachenfilter 27

- Spyware 47
- Standardport 29
- Start-Menü 12
- Statistik 21, 39
- Status 18, 19
- Status aktualisieren 41
- Status-Bereich 14
- Stealth-Viren 47
- Suchbegriffe 25
- Suchbereich 25
- Suffix 24
- Supportrahmen 3
- Support-Team 46
- Systemnachrichten 38
- Systemvoraussetzungen 11
- Systemwarnung 38

- T**
- Tabellen zurücksetzen 45
- Tabelleninhalte abfragen 45
- Täglich 40
- Tarnkappen-Viren 47
- Tarnungsteil 47
- TimeOut-Fehler 31
- Trennstrich 25
- Trojaner 47
- Trojanische Pferde 47

- U**
- Uhrzeit 28
- Update 18, 39
- Updates 19

- V**
- Verarbeitung ausgehender Mails 19
- Verarbeitung eingehender Mails 19
- Versionsnummern 3
- Viren 47
- Virenfunde 18, 28
- Virenfunde an G Data AntiVirus Business melden 35
- Virenfunden 33
- Vireninformation 28
- Virenlexikon 18
- Virenmeldung an folgende Personen senden 34
- Virenprüfung 33, 35
- Virenprüfung ausgehender Mails 19
- Virenprüfung eingehender Mails 19
- Virensignaturen 19, 41
- Virensignaturen vom G Data AntiVirus Client verwenden 40
- Viren-Update 41
- Virenverdacht überprüfen 54
- Virus 32, 33, 34
- Visual Basic 47
- Von folgenden IP-Adressen keine Mails annehmen 27
- Vor der Installation 8
- Vorschauansicht einer Mail 23

- W**
- Warteschlangen 18
- Warteschlange 37
- Warteschlangen 27
- Weitere Programmstarts (Zugangskennwort) 17
- Weiterleitung 29, 31, 42
- Welche Bedrohungen gibt es? 47
- Whitelist 43
- Wie kann ich im Exchange-Server die Ports für eingehende und ausgehende Mails umstellen? 46
- Wie schütze ich mich vor Computerschädlingen? 54
- Wiederholungsintervall 37
- Wochentage 40

Würmer 47

Wurmern 47

Wurm 47

X

XML-Datei 39

Z

Zeitplanung Viren-Update 40

Zeitpunkt 40

Zeitüberschreitung beim Mail-Programm
vermeiden 31

Zugangsdaten 40, 41

Zugangsdaten für die
Internetverbindung 35