Inhaltsverzeichnis

1 Erste Schritte ... 3

1.1 ServiceCenter 3

2 Installation 4

2.1 Nach der Installation 4

3 SecurityCenter 6

3.1 Lizenz 6

3.2 CPU-Last 6

4 Virenschutz 8

5 Virensignaturen 11

6 Webschutz 12

7 E-Mail-Prüfung 13

8 Firewall 14

9 Spamschutz 15

10 Kindersicherung 17

11 Einstellungen 18

11.1 Allgemein 18

11.2 AntiVirus 18

11.3 AntiSpam 18

11.4 Firewall 18

12 Firewall-Bedienung 36

12.1 Status 36

12.2 Netzwerke 36

12.3 Regelsätze 36

12.4 Protokoll 36

13 Kindersicherung-Bedienung 42

13.1 Status 42

13.2 Eigene Filter 42

13.3 Protokolle 42

14 BootScan 46

15 Wissenswertes 48

15.1 G Data Symbol 48

15.2 Virenprüfung 48

15.3 Virenfund 48

15.4 Malware-Feedback 48

15.5 Not-a-virus-Meldung 48

15.6 Quarantäne 48

15.7 Protokolle 48

15.8 Mehrfach-Lizenz 48

15.9 Lizenzverlängerung 48

15.10 Rechnerwechsel 48

15.11 Deinstallation 48

15.12 Copyright 48

1 Erste Schritte ...

Wir freuen uns, dass Sie sich für unser Produkt entschieden haben und hoffen, dass Sie mit Ihrer neuen Software rundherum zufrieden sind. Sollte mal etwas auf Anhieb nicht klappen, hilft Ihnen unsere Hilfe-Dokumentation weiter. Für weitere Fragen stehen Ihnen unsere Experten im **ServiceCenter** zur Verfügung. Diese Schnellanleitung hilft Ihnen dabei, Ihre neue Software zu installieren.

Sie können in der Software jederzeit die ausführliche Programmhilfe aufrufen und erhalten dort vor Ort alle notwendigen Informationen. Drücken Sie dazu einfach im Programm die Taste F1.

1.1 ServiceCenter

Installation und Bedienung der G Data Software sind unkompliziert und selbsterklärend. Sollte sich doch mal ein Problem ergeben, setzen Sie sich doch einfach mit den kompetenten Mitarbeitern unseres ServiceCenters in Verbindung:

www.gdata.de

2 Installation

Damit die Software problemlos funktioniert, sollte Ihr Computer je nach Betriebssystem eine der folgenden **Mindestanforderungen** erfüllen:

- Microsoft Windows 7 / Vista (32/64bit), 1 GB verfügbarer Arbeitsspeicher,
- Microsoft Windows XP (SP2 oder höher, 32bit), 512 MB verfügbarer Arbeitsspeicher.

Wenn Ihr Computer fabrikneu ist oder auch bisher schon von einer Antivirensoftware geschützt wurde, können Sie die Installation mit folgenden Schritten durchführen. Sollten Sie jedoch den begründeten Verdacht haben, dass Ihr Computer schon virenverseucht ist, empfiehlt es sich, vor der Installation der Software einen **BootScan** durchzuführen.

***Achtung**: Sollten Sie bisher Antivirensoftware von einem anderen Hersteller verwendet haben, sollte diese vorher gründlich von Ihrem Computer deinstalliert werden. Da Antivirensoftware sehr tief in die Systemstruktur von Windows eingreift, ist es hierbei ratsam, sich nicht nur auf die normale **Deinstallation** der Software zu verlassen, sondern - wenn möglich - auch die **Bereinigungstools** zu verwenden, die dieser Hersteller in seinem Supportcenter online zur Verfügung stellt.*

Schritt 1

Starten Sie bitte die Installation folgendermaßen:

- **CD/DVD-Installation**: Um mit der Installation zu beginnen, legen Sie die Programm-CD oder DVD ein. Es öffnet sich automatisch ein Installationsfenster.

Schritt 2

Wählen Sie nun bitte aus, in welcher Sprache Sie Ihre neue G Data Software installieren möchten.

Schritt 3

Klicken Sie jetzt bitte auf die Schaltfläche **Installieren**. Ein Assistent begleitet Sie nun bei der Installation der Software auf Ihrem Computer. Hier können Sie auch festlegen, ob Sie die Software als **Vollversion** oder als **Testversion** installieren möchten. Wenn Sie die Software gekauft haben und eine Registriernummer besitzen, sollten Sie hier natürlich den Eintrag **Vollversion** auswählen.

Um die G Data Software einfach mal kostenlos kennenzulernen, können Sie auch einfach unseren zeitlich eingeschränkten Testzugang nutzen. Geben Sie hier bitte eine gültige E-Mail-Adresse und Ihren Namen an und Sie erhalten von uns per E-Mail die Zugangsdaten.

Schritt 4

Während der Installation erfolgt die **Produktaktivierung**. Hier können Sie Ihre Software freischalten.

- **Neue Registriernummer eingeben**: Wenn Sie Ihre G Data Software neu installieren, wählen Sie bitte diese Option aus und geben anschließend die Registriernummer ein, die dem Produkt beiliegt. Sie finden diese je nach Art des Produktes z.B. auf der Rückseite des Bedienungshandbuchs, in der Bestätigungsmail beim Softwaredownload oder auf der CD-Stecktasche.

  Durch die Eingabe der Registriernummer wird Ihr Produkt aktiviert und Sie erhalten außerdem per E-Mail für die spätere Verwendung Ihre Zugangsdaten zugesendet.

  Sollten Sie bei der Eingabe der Registriernummer Probleme haben, überprüfen Sie bitte die Registriernummer auf die korrekte Eingabe. Je nach verwendetem Schriftsatz wird ein großes "I" (wie Ida) oft als die Ziffer "1", bzw. dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und "8", "G" und 6, "O" und "0", "Z" und "2".

- **Zugangsdaten eingeben**: Wenn Sie Ihre G Data Software schon einmal aktiviert hatten, haben Sie Zugangsdaten (**Benutzername** & **Passwort**) erhalten. Um die Software erneut zu installieren oder bei einer Mehrfachlizenz weitere Computer anzumelden, geben Sie hier einfach die Zugangsdaten an.

  Zugangsdaten erhalten Sie ausschließlich per E-Mail. Dem Produkt liegen keine Zugangsdaten bei.

  Sollten Sie Ihre Zugangsdaten verlegt oder vergessen haben, so klicken Sie in der Anmeldung auf den

*Eintrag **Zugangsdaten verlegt?** Es öffnet sich eine Webseite, auf der Sie Ihre Registriernummer erneut eingeben können. Nach Eingabe werden Ihnen die Zugangsdaten an die bei der Registrierung hinterlegte E-Mail-Adresse geschickt. Sollte sich Ihre **E-Mail-Adresse** zwischenzeitlich geändert haben, so wenden Sie sich bitte an unser **ServiceCenter**.*

- **Später aktivieren**: Wenn Sie sich die Software nur einmal anschauen möchten, können Sie sie auch ohne die Angabe von Daten installieren. Da auf diese Weise allerdings vom Programm keine Aktualisierungen aus dem Internet geladen werden, ist kein echter Schutz vor Schadsoftware gegeben. Sie können Ihre Registriernummer oder Ihre Zugangsdaten jederzeit nachträglich eingeben, sobald Sie ein Update durchführen.

Schritt 5

Eventuell müssen Sie nach der Installation Ihren Computer neu starten. Dann steht Ihnen die G Data Software zur Verfügung.

***Falls die Installation nicht starten sollte**: Es kann sein, dass Sie die **Autostart-Funktion** Ihres Computers nicht entsprechend eingestellt haben. Dann kann die Software den Installationsvorgang nach Einlegen der Programm-CD nicht automatisch starten und es öffnet sich kein Fenster, über das Sie die G Data Software installieren können.*

- *Wenn sich statt dessen ein Auswahlfenster für eine automatische Wiedergabe öffnet, klicken Sie bitte auf die Option **AUTOSTRT.EXE ausführen**.*
- *Wenn sich kein Auswahlfenster öffnet, suchen Sie bitte über Ihren Windows-Explorer den Datenträger mit der G Data Software und starten dann die Datei **Setup** bzw. **Setup.exe.***

2.1 Nach der Installation

Securitysymbol: Ihre G Data Software schützt Ihren Rechner permanent vor Schadsoftware und Angriffen. Ein Symbol in der Taskleiste Ihres Rechners weist Sie darauf hin, sobald die Software einen Eingriff von Anwenderseite aus für notwendig erachtet. Durch das Anklicken des Symbols mit der rechten Maustaste, können Sie die G Data Programmoberfläche öffnen.

Schnellprüfung: Mit der Schnellprüfung können Sie Dateien ganz einfach kontrollieren, ohne die Software überhaupt starten zu müssen. Markieren Sie einfach Dateien oder Ordner z.B. im Windows Explorer mit der Maus. Klicken Sie nun die rechte Maustaste und wählen im erscheinenden Dialogfenster **auf Viren prüfen**. Nun wird automatisch eine Virenprüfung der betreffenden Dateien durchgeführt.

G Data Shredder: Sollten Sie den Shredder bei der Installation ausgewählt haben (bei **G Data AntiVirus** nicht integriert), steht Ihnen dieser als Desktop-Symbol zur Verfügung. Daten, die Sie in den Shredder verschieben, werden so entfernt, dass sie auch mit professionellen Datenrettungstools nicht wiederhergestellt werden können.

Ihr Computer startet nach der Installation der Software anders als üblich**: Falls der Computer nach der Installation der Software und einem anschließenden Neustart nicht direkt mit Microsoft Windows startet, dann kann das daran liegen, dass sich die Programm-CD noch im Laufwerk befindet. Entfernen Sie einfach die CD und Ihr Computer startet wieder wie gewohnt. Weitere Informationen finden Sie hierzu in der Online-Hilfe im Kapitel **BootScan.

3 SecurityCenter

Das SecurityCenter brauchen Sie nur dann aufzurufen, wenn Sie auf eine der vielen Zusatzfunktionen der Software aktiv zugreifen möchten. Der eigentliche Schutz Ihres Computers vor Viren und anderen Bedrohnungen findet permanent im Hintergrund statt. In den Fällen, in denen die Software Ihr Eingreifen erfordert, werden Sie automatisch über Informationen in der Taskleiste Ihres Computers daran erinnert. Mit einem Klick können Sie mögliche Gefährdungen Ihres Computers aus dem Weg räumen. Dazu steht Ihnen das **Sicherheitsstatus**-Symbol zur Verfügung.

Solange ein grünes Häkchen neben dem Eintrag **Sicherheitsstatus** leuchtet, ist Ihr System gesichert.

Ein rotes Ausrufezeichen weist darauf hin, dass für Ihr System unmittelbare Gefahr besteht. Sie sollten dann möglichst sofort Maßnahmen einleiten, damit der Schutz Ihrer Daten gewahrt bleibt.

Wenn Sie auf die Schaltfläche **Korrigieren** klicken, schlägt Ihnen die Software vor, welche Aktionen Sie durchführen sollten, um Ihr System wieder optimal zu schützen. Wählen Sie einfach nacheinander die angezeigten Aktionen aus, bis der Sicherheitsstatus wieder grünes Licht zeigt. Die Schaltfläche wechselt dann selbsttätig auf inaktiv und kann erst dann wieder genutzt werden, wenn sich der Sicherheitsstatus verschlechtern sollte. Dann ist Ihre Software auf dem neuesten Stand und Sie können das SecurityCenter wieder schließen. Darüber hinaus gibt es noch folgende Statusmeldungen:

Ein gelbes Symbol weist darauf hin, dass ein baldiges Eingreifen durch den Benutzer erforderlich ist.

Wenn das Platzhaltersymbol angezeigt wird, heißt dies, dass die jeweilige Sicherheitsfunktion von Ihnen nicht aktiviert wurde (z.B. der Spamschutz).

Alle Funktionen und Einstellungen, die Sie unterhalb des Sicherheitsstatus-Symbols sehen (wie z.B. **Virenschutz** oder **Virensignaturen**), können Sie dann nutzen, wenn Sie sich mit der Sicherheit Ihres Systems aktiv beschäftigen möchten - aber Sie müssen es nicht! Entscheiden Sie selbst, wie sehr Sie sich mit dem Thema Virenschutz befassen. In den jeweiligen Unterabschnitten sehen Sie im Einzelnen, welche Bereiche Ihrer Software optimal eingestellt sind und welche vielleicht verbessert werden sollten.

3.1 Lizenz

Unter dem Eintrag **Lizenz** auf der linken Seite der Programmoberfläche sehen Sie, wie lange Ihre Lizenz für Virenupdates noch gültig ist. Bei keiner anderen Software sind ständige Aktualisierungen so wichtig, wie bei Antivirensoftware. Bevor Ihre Lizenz abläuft, erinnert die Software Sie deshalb automatisch daran, Ihre Lizenz zu verlängern. Am besten bequem und unkompliziert per Internet.

Was passiert bei Ablauf meiner Lizenz?

Ein paar Tage bevor Ihre Lizenz abläuft, erscheint ein Informationsfenster in der Taskleiste. Wenn Sie dieses anklicken, öffnet sich ein Dialog, in dem Sie Ihre Lizenz problemlos und in wenigen Schritten direkt verlängern können. Klicken Sie einfach auf die Schaltfläche **Jetzt kaufen**, vervollständigen Sie Ihre Daten und Ihr Virenschutz ist dann sofort wieder gewährleistet. Sie erhalten die Rechnung dann in den nächsten Tagen bequem über den Postweg zugestellt.

Dieser Dialog erscheint nur nach Ablauf des ersten Jahres. Danach verlängert sich Ihre G Data Lizenz jedes Jahr automatisch. Sie können dieses Abo jedoch jederzeit ohne Angabe von Gründen kündigen.

Wie erhalte ich zusätzliche/erweiterte Lizenzen?

Selbstverständlich ist es jederzeit möglich, die Anzahl Ihrer Lizenzen zu erweitern oder ein Upgrade auf Produkte mit erweitertem Funktionsumfang durchführen. Wenn Sie auf den Eintrag **Mehr PCs schützen** im SecurityCenter klicken, werden Sie direkt auf die Webseite unseres Online-Shops geleitet. Über den Eintrag **Funktionsumfang erweitern** erreichen Sie unser Upgrade-Center, in dem Sie zu besonderen Konditionen auch den erweiterten Funktionsumfang unserer anderen Softwareversionen bestellen können.

3.2 CPU-Last

Unter der Beschriftung **G Data** sehen Sie die aktuelle Auslastung Ihres Computers durch die Software. Darunter - unter der Beschriftung **System** - die momentane Gesamtauslastung Ihres Rechners. Bei Überprüfungen kann die Systemauslastung durch die G Data Software sehr hoch sein, im normalen Wächterbetrieb verbraucht Ihre G Data Software dagegen nur sehr wenig Prozessorleistung. Sollte Ihr Computer also einmal langsamer als gewöhnlich reagieren, können Sie hier mit einem Blick feststellen, ob die G Data Software gerade eine intensive Überprüfung durchführt oder Ihr Rechner aus anderen Gründen gebremst wird, die nicht mit einer Überprüfung des Systems im Zusammenhang stehen.

Voreingestellt ist Ihre G Data Software übrigens so eingerichtet, dass Sie Ihren Computer nur dann überprüft, wenn Sie ihn nicht benutzen. Wie ein Bildschirmschoner erfolgt die Virenprüfung also immer nur dann, wenn Sie dadurch nicht gestört werden. Der permanente Virenschutz durch den Virenwächter ist natürlich jederzeit voll aktiv.

- **Virenprüfung**: Die regelmäßige Überprüfung, ob sich Viren oder Schadprogramme auf Ihrem Computer eingenistet haben.
- **Virenwächter**: Der durchgängige Schutz Ihres Computers vor angreifender Schadsoftware.

4 Virenschutz

In diesem Bereich erhalten Sie Informationen darüber, wann Ihr Computer das letzte Mal auf Virenbefall untersucht wurde und ob der Virenwächter ihn momentan aktiv vor Infektionen schützt.

Letzter Leerlauf-Scan

Hier wird Ihnen angezeigt, wann Ihr Computer das letzte Mal komplett auf Virenbefall kontrolliert wurde. Wenn dieser Eintrag rot markiert ist, sollten Sie möglichst bald eine Virenprüfung durchführen. Klicken Sie dazu einfach auf den Eintrag und Sie können den Prüfvorgang starten, indem Sie die Schaltfläche **Rechner prüfen** drücken. Nach der Prüfung ist der Eintrag grün markiert, ein Zeichen dafür, dass die Virenprüfung vor ausreichend kurzer Zeit erfolgte.

> Wie genau eine Virenprüfung abläuft und was Sie tun sollten, wenn Sie tatsächlich einen Virus finden, lesen Sie im Kapitel: **Was geschieht bei einer Virenprüfung?**

Der Leerlauf-Scan startet automatisch in Phasen, in denen Ihr Rechner inaktiv ist und führt so in automatisch festgelegten Abständen eine Prüfung des gesamten Rechners durch. Wenn Sie den Leerlauf-Scan vor dem nächsten automatisch festgelegten Termin starten wollen, wählen Sie bitte **Leerlauf-Scan jetzt starten**. Wenn Sie nicht möchten, dass Ihre G Data Software automatisch bei Arbeitspausen mit dem Leerlauf-Scan beginnen soll, können Sie diese Funktion unter **Leerlauf-Scan ausschalten** auch deaktivieren.

> Achtung: Bitte achten Sie dann bewusst darauf, Ihren Computer regelmäßig auf Virenbefall und andere Infektionen zu überprüfen!

Virenwächter

Der Virenwächter sollte immer aktiv sein. Wenn Sie den Wächter doch mal abschalten möchten oder an den Einstellungen etwas verändern möchten, klicken Sie bitte den Eintrag **Virenwächter ausschalten** an.

> **Virenprüfung & Virenwächter**: Beide Funktionen dienen dazu, Ihren Computer vor Infektionen zu schützen, haben dabei aber unterschiedliche Herangehensweisen.
>
> - Der **Virenwächter** prüft Ihren Computer durchgängig auf Viren, er kontrolliert Schreib- und Lesevorgänge und sobald ein Programm Schadfunktionen ausführen oder schädliche Dateien verbreiten möchte, wird dies vom Wächter verhindert. Der Virenwächter ist Ihr wichtigster Schutz! Er sollte nie ausgeschaltet sein.
> - Die **Virenprüfung** ist ein zusätzlicher Schutz. Sie überprüft, ob sich nicht doch ein Virus auf Ihrem System befindet. Eine Virenprüfung würde auch Viren finden, die auf Ihren Computer kopiert wurden, bevor Sie die G Data Software installiert hatten oder die Sie erhielten, während der Virenwächter mal nicht eingeschaltet war. Eine Virenprüfung sollte in regelmäßigen Abständen erfolgen, am besten automatisch zu Zeiten, in denen Ihr Computer nicht benötigt wird. Dies kann entweder manuell oder zeitgesteuert über die Funktion **Rechner prüfen** erfolgen oder automatisch über den **Leerlauf-Scan**.

Auswahlmenü

Wenn Sie direkt auf die Überschrift **Virenschutz** klicken, erscheint eine Auswahl von Aktionen, die Sie hier direkt durchführen können.

Rechner prüfen: Wenn Sie Ihren Computer unabhängig von der automatischen Prüfung kontrollieren möchten (z.B. weil Sie einen aktuellen Virenverdacht haben), dann klicken Sie einfach diesen Eintrag an. Ihr Computer wird nun direkt auf Virenbefall untersucht. Lesen Sie hierzu bitte auch das Kapitel: **Was geschieht bei einer Virenprüfung**.

Speicher und Autostart prüfen: Hierbei werden für alle laufenden Prozesse die Programmdateien und Programmbibliotheken (DLLs) geprüft. Schadprogramme können so direkt aus dem **Speicher** und **Autostart-Bereich** entfernt werden. Aktive Viren können also direkt entfernt werden, ohne dass die ganze Festplatte durchsucht werden muss. Da diese Überprüfung relativ schnell durchgeführt werden kann, ist es empfehlenswert, sie z.B. im Rahmen einer automatischen Virenprüfung regelmäßig durchzuführen. Diese Funktion ist kein Ersatz für eine regelmäßige Virenkontrolle der gespeicherten Daten, sondern eine Ergänzung.

Verzeichnisse/Dateien prüfen: Hiermit prüfen Sie ausgewählte Laufwerke, Verzeichnisse oder Dateien auf Virenbefall. Wenn Sie diese Aktion anklicken, öffnet sich eine Verzeichnis- und Dateiauswahl. Hier können Sie gezielt einzelne Dateien und auch ganze Verzeichnisse auf Virenbefall überprüfen.

> Im Verzeichnisbaum können Sie durch Anklicken der Plus-Symbole Verzeichnisse öffnen und auswählen, deren Inhalt dann in der Datei-Ansicht angezeigt wird. Jedes Verzeichnis oder jede Datei, die Sie mit einem Häkchen versehen, wird von der Software geprüft. Wenn in einem Verzeichnis nicht alle Dateien geprüft werden, findet sich an diesem Verzeichnis ein graues Häkchen.

Wechselmedien prüfen: Prüfen Sie mit dieser Funktion **CD-ROMs** oder **DVD-ROMs**, **Speicherkarten** oder **USB-Sticks** auf Virenbefall. Wenn Sie diese Aktion anklicken, werden alle Wechselmedien, die mit Ihrem Computer verbunden sind (also auch eingelegte CDs, eingeschobene Speicherkarten oder per USB verbundene Festplatten oder USB-Sticks) überprüft. Bitte beachten Sie, dass die Software natürlich keine Viren auf Medien entfernen kann, die keinen Schreibzugriff erlauben (z.B. gebrannte CD-ROMs). Hier wird der Virenfund dann protokolliert.

Auf RootKits prüfen: **Rootkits** versuchen sich herkömmlichen Virenerkennungsmethoden zu entziehen. Sie können mit dieser Funktion gezielt nach Rootkitviren suchen, ohne eine komplette Überprüfung der Festplatten und gespeicherten Daten vorzunehmen.

Leerlauf-Scan ausschalten: Während der Virenwächter Ihr System permanent vor Infektionen durch Schadsoftware schützt, ist der **Leerlauf-Scan** eine intelligente Virenprüfung, die alle Dateien Ihres Computers immer wieder darauf überprüft, ob sie nicht schon mit einem Virus infiziert sind. Der Leerlauf-Scan arbeitet wie ein Bildschirmschoner immer nur dann, wenn Sie Ihren Computer eine Weile nicht benötigen und hört sofort wieder auf, sobald sie weiterarbeiten, um Ihnen optimale Performance zu gewährleisten.

> Selbstverständlich ist Ihr Computer durch den Virenwächter weiterhin vor Virenattacken geschützt, auch wenn der Leerlauf-Scan ausgeschaltet ist. Dies kann zum Beispiel sinnvoll sein, wenn Sie die Virenprüfung auf Ihrem System lieber manuell starten möchten.

Virenwächter ausschalten: Hiermit können Sie den **Virenwächter** bei Bedarf abschalten und auch wieder einschalten. Dies kann z.B. dann sinnvoll sein, wenn Sie auf Ihrer Festplatte große Dateimengen von einem Ort zum anderen kopieren oder speicherplatzintensive Rechenvorgängen (z.B. DVDs kopieren o.ä.) ablaufen lassen.

> Sie sollten den Virenwächter nur so lange abschalten, wie es unbedingt nötig ist. Achten Sie darauf, dass das System während dieses Zeitraums möglichst nicht mit dem Internet verbunden ist oder auf neue, ungeprüfte Daten (z.B. über CDs, DVDs, Speicherkarten oder USB-Sticks) zugreifen kann.

Quarantäne: Die Quarantäne ist ein geschützter Bereich innerhalb der Software, in dem infizierte Dateien verschlüsselt gespeichert werden und auf diese Weise den Virus nicht mehr an andere Dateien weitergeben können. Lesen Sie hierzu bitte auch das Kapitel: **Wie funktioniert die Quarantäne?**

Einstellungen: Über diese Schaltfläche können Sie bei Bedarf auf grundlegende Einstellungsoptionen zugreifen. Lesen Sie hierzu bitte das Kapitel: **Einstellungen - AntiVirus**

5 Virensignaturen

In diesem Bereich erhalten Sie Informationen zu den Programm-Updates.

Letztes Update

Hier wird Ihnen angezeigt, wann Ihr Computer das letzte Mal aktuelle Virensignaturen aus dem Internet erhalten hat. Wenn dieser Eintrag rot markiert ist, sollten Sie möglichst bald ein Virenupdate durchführen. Klicken Sie dazu einfach auf den Eintrag und wählen Sie dann die Option **Virensignaturen aktualisieren** aus.

Nächstes Update

Unter diesem Eintrag können Sie sehen, wann die nächste Aktualisierung erfolgt.

> **Virensignaturen**: Viren und andere Schadprogramme sind durch charakteristische Merkmale erkennbar. Ihre G Data Software hat Funktionen, Viren auch anhand ihres Verhaltens aufzuspüren. Durch eine Virensignatur, die man sich wie einen Steckbrief vorstellen kann, ist das Auffinden und Bekämpfen des jeweiligen Schadprogrammes jedoch ungleich viel schneller und effektiver. Erst mit einer regelmäßigen Aktualisierung dieser Steckbriefe über die G Data Datenbanken im Internet ist ein Virenschutz wirklich sicher.

Auswahlmenü

Wenn Sie direkt auf die Überschrift **Virensignaturen** klicken, erscheint eine Auswahl von Aktionen, die Sie hier direkt durchführen können.

Virensignaturen aktualisieren: Normalerweise werden die Updates der Virensignaturen automatisch ausgeführt. Wenn Sie eine Aktualisierung sofort durchführen möchten, dann klicken Sie bitte auf diese Schaltfläche.

Automatische Updates deaktivieren: Wenn Sie nicht möchten, dass sich die G Data Software automatisch darum kümmert, die Virensignaturen auf den neuesten Stand zu bringen, dann wählen Sie bitte diese Option aus. Die Abschaltung stellt allerdings ein hohes Sicherheitsrisiko dar und sollte nur in Ausnahmefällen erfolgen.

Einstellungen: Über diese Schaltfläche können Sie bei Bedarf auf grundlegende Einstellungsoptionen zugreifen. Lesen Sie hierzu bitte das Kapitel: **Einstellungen - AntiVirus**

6 Webschutz

In diesem Bereich können Sie den Webschutz aktivieren bzw. deaktivieren. Beim Webschutz handelt es sich um ein Modul, welches beim Surfen im Internet und bei Downloads automatisch Bedrohungen erkennt und gegebenenfalls unschädlich macht. Es dient als sinnvolle Unterstützung zum Virenwächter und blockt schädliche Websites und Downloads schon, bevor sie überhaupt aufgerufen werden können.

Wenn eine Internetseite von der G Data Software als Bedrohung erkannt und gesperrt wird, erhalten Sie statt der Website eine Informationsseite von G Data im Browser angezeigt.

Auswahlmenü

Wenn Sie direkt auf die Überschrift **Webschutz** klicken, erscheint eine Auswahl von Aktionen, die Sie hier direkt durchführen können.

Ausnahmen festlegen: Der Webschutz sorgt dafür, dass Sie im Internet nicht Opfer von infizierten oder betrügerischen Webseiten werden. In seltenen Fällen kann es aber vorkommen, dass eine Internetseite nicht richtig dargestellt wird, obwohl Sie von einem sicheren Anbieter kommt. In einem solchen Fall können Sie diese Internetadresse dann auf die Whitelist setzen, d.h. Sie können sie als Ausnahme definieren und der Webschutz wird diese Seite nicht weiter blockieren. Lesen Sie im Kapitel **Ausnahmen festlegen**, wie dies erfolgt.

Whitelist: Eine Auswahl von Objekten (z.B. Internetseiten), die vom Anwender als unbedenklich eingestuft werden und deshalb nicht gesondert überprüft werden.

Webschutz deaktivieren: Wenn Sie den Webschutz deaktivieren, kann das z.B. bei sehr großen Downloads aus sicherer Quelle einen Zeitvorteil mit sich bringen. Prinzipiell ist Ihr Computer auch ohne Webschutz durch den Virenwächter geschützt. Dennoch sollten Sie nur in Ausnahmefällen auf den Webschutz verzichten.

Einstellungen: Über diese Schaltfläche können Sie bei Bedarf auf grundlegende Einstellungsoptionen zugreifen. Lesen Sie hierzu bitte das Kapitel: **Einstellungen - Webschutz**

7 E-Mail-Prüfung

Mit der E-Mail-Prüfung können Sie ein- und ausgehende E-Mails und deren Datei-Anhang auf Viren überprüfen und mögliche Infektionen direkt an der Quelle ausschalten. Die Software ist in der Lage, bei Virenfund Datei-Anhänge direkt zu löschen oder infizierte Dateien zu reparieren.

In **Microsoft Outlook** wird die E-Mail-Prüfung durch ein **Plug-In** realisiert. Dieses bietet denselben Schutz wie die **POP3**/**IMAP** orientierte Schutzfunktion innerhalb der **AntiVirus** Optionen. Nach der Installation dieses Plug-Ins finden Sie im **Outlook**-Menü **Extras** die Funktion **Ordner auf Viren überprüfen**, mit der Sie Ihre Mailordner einzeln auf Virenbefall checken können.

Auswahlmenü

Wenn Sie direkt auf die Überschrift **E-Mail-Prüfung** klicken, erscheint eine Auswahl von Aktionen, die Sie hier direkt durchführen können.

E-Mail-Prüfung deaktivieren: Wenn Sie nicht möchten, dass Ihre G Data Software E-Mails überprüft, dann wählen Sie bitte diese Option aus. Die Abschaltung stellt allerdings ein hohes Sicherheitsrisiko dar und sollte nur in Ausnahmefällen erfolgen.

Einstellungen: Über diese Schaltfläche können Sie bei Bedarf auf grundlegende Einstellungsoptionen zugreifen. Lesen Sie hierzu bitte das Kapitel: **Einstellungen - E-Mail-Prüfung**

8 Firewall

Eine Firewall schützt Ihren Computer davor, "ausgespäht" zu werden. Sie überprüft, welche Daten und Programme aus dem Internet oder Netzwerk auf Ihren Rechner gelangen und welche Daten von Ihrem Computer gesendet werden. Sobald etwas darauf hindeutet, dass Daten auf Ihrem Rechner unberechtigt aufgespielt oder heruntergeladen werden sollen, schlägt die Firewall Alarm und blockt den unberechtigten Datenaustausch.

Auswahlmenü

Wenn Sie direkt auf die Überschrift **Firewall** klicken, erscheint eine Auswahl von Aktionen, die Sie hier direkt durchführen können.

Firewall öffnen: Über diese Funktion öffnen Sie die G Data Firewall in einem zusätzlichen Fenster und können Sie umfangreich konfigurieren. Dies ist allerdings im Normalfall nicht nötig. Alle Grundeinstellungen sind über die SecurityCenter-Programmoberfläche steuerbar.

Autopilot ausschalten: In der Regel ist es sinnvoll, die Firewall in der Funktion **Autopilot** zu verwenden. Sie läuft dann quasi im Hintergrund und schützt Sie, ohne dass Sie große Einstellungen vornehmen müssen.

Wenn Sie die Firewall ohne den Autopiloten verwenden, erscheint in Zweifelsfällen ein Dialogfenster, in dem Sie die Firewall nach und nach auf Ihre Systemgegebenheiten hin optimieren. Für erfahrene Anwender ist dies ein hilfreiches Feature. Normalerweise ist ein Abschalten des Autopiloten allerdings nicht notwendig.

Firewall ausschalten: Sie können die Firewall bei Bedarf auch abschalten. Ihr Computer ist dann weiterhin mit dem Internet und anderen Netzwerken verbunden, wird von der Firewall aber **nicht** mehr vor Angriffen oder Spionage-Attacken geschützt.

Einstellungen: Über diese Schaltfläche können Sie bei Bedarf auf grundlegende Einstellungsoptionen zugreifen. Lesen Sie hierzu bitte das Kapitel: **Einstellungen - Firewall**

9 Spamschutz

Sonderangebote, Werbung, Newsletter – die Flut an unerwünschten E-Mails steigt immer weiter. Quillt Ihr Posteingang über dank Unmengen an unerwünschter elektronischer Post? Die G Data Software schützt sicher vor Spam-Müll, blockiert Spam-Absender effizient und verhindert Fehlkennungen aufgrund der Kombination modernster Spam-Prüfungskriterien.

Auswahlmenü

Wenn Sie direkt auf die Überschrift **Spamschutz** klicken, erscheint eine Auswahl von Aktionen, die Sie hier direkt durchführen können.

Protokoll: Spam: Hier erhalten Sie eine ausführliche Übersicht über alle E-Mails, die von der G Data Software als Spam eingestuft wurden. Über die Schaltfläche **Aktualisieren** können Sie den aktuellsten Datenstand der Software abrufen, über die Schaltfläche **Löschen** entfernen Sie alle bisher markierten Einträge. Die eigentlichen E-Mails in ihrem E-Mailprogramm werden dabei natürlich nicht gelöscht.

Über die Schaltfläche **Auf Whitelist** können Sie eine markierte E-Mail auf die **Whitelist** setzen und damit die betreffende E-Mail-Adresse generell von einer weiteren Spamprüfung ausschließen. Über die Schaltfläche **Auf Blacklist** können Sie eine markierte E-Mail auf die **Blacklist** setzen und damit die betreffende E-Mail-Adresse besonders auf Spam-Elemente überprüfen.

Protokoll: Kein Spam: Hier erhalten Sie eine ausführliche Übersicht über alle E-Mails, die von der G Data Software nicht als Spam definiert wurden. Über die Schaltfläche **Aktualisieren** können Sie den aktuellsten Datenstand der Software abrufen, über die Schaltfläche **Löschen** entfernen Sie alle bisher markierten Einträge. Die eigentlichen E-Mails in ihrem E-Mailprogramm werden dabei natürlich nicht gelöscht.

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@informationsseite.de) oder Domain (z.B. informationsseite.de) ein, die Sie vom Spamverdacht ausnehmen möchten und die G Data Software behandelt E-Mails von diesem Absender bzw. dieser Absenderdomain nicht als Spam. Über die Schaltfläche **Import** 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 Schaltfläche **Export** 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 die G Data Software behandelt E-Mails von diesem Absender bzw. dieser Absenderdomain generell als E-Mails mit sehr hoher Spamwahrscheinlichkeit. Über die Schaltfläche **Import** 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 Schaltfläche **Export** können Sie eine solche Blacklist auch als Textdatei exportieren.

Spamschutz deaktivieren: Hier können Sie im Bedarfsfall den Spamschutz auf Ihrem Computer deaktivieren, z.B. dann, wenn Sie gar kein E-Mailprogramm auf Ihrem Rechner installiert haben.

Einstellungen: Über diese Schaltfläche können Sie bei Bedarf auf grundlegende Einstellungsoptionen zugreifen. Lesen Sie hierzu bitte das Kapitel: **Einstellungen - AntiSpam**

10 Kindersicherung

Mit der Kindersicherung können Sie das Surfverhalten und die Nutzung des Computers für Ihre Kinder regeln.

Die Kindersicherung wird bei einer Standardinstallation der G Data Software nicht mit installiert. Sie können Sie jedoch jederzeit auch nachträglich installieren.

Auswahlmenü

Wenn Sie direkt auf die Überschrift **Kindersicherung** klicken, erscheint eine Auswahl von Aktionen, die Sie hier direkt durchführen können.

Kindersicherung öffnen: Über diese Funktion öffnen Sie die G Data Kindersicherung in einem zusätzlichen Fenster und können Sie umfangreich konfigurieren.

Aktivieren für: Sie können die Kindersicherung als Administrator für alle anderen Benutzer Ihres Computers hier ein- oder ausschalten. Die Bearbeitung der Sicherheitseinstellungen erfolgt in der eigentlichen Programmoberfläche der Kindersicherung.

Um die Kindersicherung verwenden zu können, muss im Bereich Webschutz der G Data Software das Häkchen bei **Internetinhalte (HTTP) verarbeiten** gesetzt sein, da sonst die Kindersicherung nicht korrekt funktioniert. Sie finden diese Option unter **Einstellungen > Webschutz > Internetinhalte (HTTP)**.

11 Einstellungen

Im Bereich **Einstellungen** können Sie die jeweiligen Programm-Module Ihren Wünschen gemäß konfigurieren. In der Regel ist es gar nicht nötig, hier Veränderungen vorzunehmen, da Ihre G Data Software schon bei der Installation für Ihr System optimal konfiguriert wurde.

11.1 Allgemein

Hier finden Sie allgemeine Einstellungsmöglichkeiten.

Sicherheit/Performance

Hier finden Sie grundlegende Einstellungsmöglichkeiten zum Thema Sicherheit und Performance.

- **Engines benutzen**: Die Software arbeitet mit zwei **Engines** (= engl. für Maschine/Motor), also zwei grundsätzlich voneinander unabhängigen Virenprüfungsprogrammen. Jede Engine für sich alleine würde Sie schon in sehr hohem Maß vor Viren schützen, aber gerade die Kombination beider Engines liefert allerbeste Ergebnisse. Bei älteren und langsamen Rechnern kann man durch die Nutzung einer einzelnen Engine die Virenprüfung beschleunigen, in der Regel sollten Sie jedoch die Einstellung **Beide Engines** beibehalten.

11.2 AntiVirus

Hier finden Sie alle Einstellungsmöglichkeiten zum Thema Virenschutz.

Wächter

In dem Dialog **Optionen** des **Virenwächters** haben Sie folgende Einstellungsmöglichkeiten. Es ist nur in Ausnahmefällen nötig, hier Änderungen vorzunehmen:

- **Wächterstatus**: Legen Sie hier fest, ob der Wächter eingeschaltet oder ausgeschaltet sein soll.
- **Engines benutzen**: Die Software arbeitet mit zwei **Engines** (= engl. für Maschine/Motor), also zwei grundsätzlich voneinander unabhängigen Virenprüfungsprogrammen. Jede Engine für sich alleine würde Sie schon in sehr hohem Maß vor Viren schützen, aber gerade die Kombination beider Engines liefert allerbeste Ergebnisse. Bei älteren und langsamen Rechnern kann man durch die Nutzung einer einzelnen Engine die Virenprüfung beschleunigen, in der Regel sollten Sie jedoch die Einstellung **Beide Engines** beibehalten.
- **Infizierte Dateien**: Bei einem Virenfund werden Sie in der Standard-Einstellung gefragt, wie Sie mit dem Virus und der infizierten Datei verfahren möchten. Wenn Sie immer dieselbe Aktion durchführen möchten, dann können Sie das hier einstellen. Höchste Sicherheit für Ihre Daten bietet hierbei die Einstellung **Desinfizieren (wenn nicht möglich: in Quarantäne)**.
- **Infizierte Archive**: Legen Sie hier fest, ob **Archiv-Dateien** (also z.B. Dateien mit der Endung **RAR**, **ZIP** oder auch **PST**) anders behandelt werden sollen, als normale Dateien. Beachten Sie jedoch, dass das Verschieben eines Archivs in Quarantäne dieses beschädigen kann, sodass es auch nach einer Zurückbewegung nicht mehr benutzt werden kann.
- **Systemschutz**: Wenn die Verhaltensüberwachung aktiviert ist, wird jede Aktivität auf dem System unabhängig vom Virenwächter überwacht. Dadurch werden auch Schädlinge erkannt, für die noch keine Signatur existiert.

Ausnahmen

Über das Anklicken der Schaltfläche **Ausnahmen** können Sie bestimmte Laufwerke, Verzeichnisse und Dateien von der Überprüfung ausschließen und auf diese Weise die Virenerkennung teilweise erheblich beschleunigen. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche **Ausnahmen**.
2. Klicken Sie in dem Fenster **Wächter Ausnahmen** auf **Neu**.

3 Wählen Sie nun aus, ob Sie ein Laufwerk, ein Verzeichnis oder eine Datei bzw. einen Dateityp ausschließen möchten.

4 Wählen Sie nun darunter das Verzeichnis oder das Laufwerk aus, welches Sie schützen möchten. Um Dateien zu schützen, geben Sie den kompletten Dateinamen in das Eingabefeld unter Dateimaske ein. Sie können hier auch mit **Platzhaltern** arbeiten.

Die Funktionsweise von Platzhaltern ist folgendermaßen:

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

Um z.B. sämtliche Dateien mit der Datei-Endung **.sav** schützen zu lassen, geben Sie ***.sav** ein. Um eine spezielle Auswahl an Dateien mit fortlaufenden Dateinamen zu schützen (z.B. text1.doc, text2,doc, text3.doc), geben Sie beispielsweise **text?.doc** ein.

Sie können diesen Vorgang bei Bedarf beliebig oft wiederholen und vorhandene Ausnahmen auch wieder löschen oder modifizieren.

Erweitert

Legen Sie außerdem über das Anklicken die Schaltfläche **Erweitert** fest, welche zusätzlichen Prüfungen vom Virenwächter durchgeführt werden sollen. Im Regelfall brauchen Sie hier keine weiteren Einstellungen vornehmen.

- **Modus**: Hier können Sie festlegen, ob Dateien bei der Ausführung, nur beim Lesen oder beim Schreiben und Lesen überprüft werden sollen. Wenn die Überprüfung beim Schreiben einer Datei erfolgt, dann wird direkt beim Erstellen einer neuen Datei oder Dateiversion überprüft, ob ein unbekannter Prozess diese Datei eventuell infiziert hat. Andernfalls werden Dateien nur überprüft, wenn Sie von Programmen gelesen werden.
- **Netzwerkzugriffe prüfen**: Wenn für Ihren Rechner eine Netzwerkverbindung zu ungeschützten Rechnern besteht (z.B. fremden Notebooks), ist es sinnvoll, auch die Netzwerkzugriffe auf die Übertragung von Schadprogrammen hin zu überprüfen. Wenn Sie Ihren Rechner als Einzelplatzrechner ohne Netzwerkzugang verwenden, muss diese Option nicht aktiviert werden. Wenn Sie auf allen Rechnern im Netzwerk einen Virenschutz installiert haben, empfiehlt es sich ebenfalls, diese Option abzuschalten, da ansonsten manche Dateien doppelt geprüft werden, was sich negativ auf die Geschwindigkeit auswirkt.
- **Heuristik**: In der heuristischen Analyse werden Viren nicht nur anhand der Virenupdates erkannt, die Sie regelmäßig online von uns erhalten, sondern auch auf Basis bestimmter virentypischer Merkmale ermittelt. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch einen Fehlalarm erzeugen.
- **Archive prüfen**: Das Überprüfen gepackter Daten in Archiven (diese erkennt man an Datei-Endungen wie z.B. **ZIP**, **RAR** oder auch **PST**) ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der Virenwächter generell auf dem System aktiv ist. Um die Geschwindigkeit der Virenprüfung zu erhöhen, können Sie die Größe der Archiv-Dateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail-Archive prüfen**: Da die Software schon den Aus- und Eingang von E-Mails auf Virenbefall überprüft, ist es in den meisten Fällen sinnvoll, das regelmäßige Überprüfen der E-Mail-Archive zu unterlassen, da dieser Vorgang je nach Größe des E-Mail-Archives teilweise mehrere Minuten dauern kann.
- **Systembereiche beim Systemstart prüfen**: Systembereiche (z.B. Bootsektoren) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim **Systemstart** überprüfen oder beim **Medium-Wechsel (z.B. neue** CD-ROM). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.

- **Systembereiche beim Medium-Wechsel prüfen**: Systembereiche (z.B. Bootsektoren) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim **Medium-Wechsel** (neue CD-ROM o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit der Software können Sie Ihr System auch auf **Dialer** und andere Schadprogramme (**Spyware**, **Adware**, **Riskware**) überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.
- **Nur neue bzw. veränderte Dateien prüfen**: Wenn Sie diese Funktion aktivieren, werden bei der Prüfung Dateien übersprungen, die sich seit längerer Zeit nicht verändert haben und die zuvor als unschädlich erkannt worden sind. Das bringt einen Performance-Gewinn bei der täglichen Arbeit – ohne Sicherheits-Risiko.

Manuelle Virenprüfung

Hier können Sie grundsätzliche Programmeinstellungen zur **Virenprüfung** vornehmen. Dies ist aber im Normalbetrieb nicht nötig.

- **Engines benutzen**: Die Software arbeitet mit zwei **Engines** (= engl. für Maschine/Motor), also zwei grundsätzlich voneinander unabhängigen Virenprüfungsprogrammen. Jede Engine für sich alleine würde Sie schon in sehr hohem Maß vor Viren schützen, aber gerade die Kombination beider Engines liefert allerbeste Ergebnisse. Bei älteren und langsamen Rechnern kann man durch die Nutzung einer einzelnen Engine die Virenprüfung beschleunigen, in der Regel sollten Sie jedoch die Einstellung **Beide Engines** beibehalten.
- **Infizierte Dateien**: Ihre Software hat einen Virus gefunden? In der Standard-Einstellung fragt die Software nun, was Sie mit dem Virus und der infizierten Datei machen möchten. Wenn Sie immer dieselbe Aktion durchführen möchten, dann können Sie das hier einstellen. Höchste Sicherheit für Ihre Daten bietet hierbei die Einstellung **Desinfizieren (wenn nicht möglich: in Quarantäne)**.
- **Infizierte Archive**: Legen Sie hier fest, ob **Archiv-Dateien** (also z.B. Dateien mit der Endung **RAR**, **ZIP** oder auch **PST**) anders behandelt werden sollen, als normale Dateien. Beachten Sie jedoch, dass das Verschieben eines Archivs in Quarantäne dieses beschädigen kann, sodass es auch nach einer Zurückbewegung nicht mehr benutzt werden kann.
- **Bei Systemlast die Virenprüfung pausieren**: Normalerweise sollte eine Virenprüfung dann erfolgen, wenn der Computer von Ihnen nicht genutzt wird. Sollten Sie den Rechner dann doch verwenden, pausiert die Virenprüfung, damit Ihr Computer für Sie in gewohntem Tempo zur Verfügung steht. Die Virenprüfung findet also während Ihrer Arbeitspausen statt.

Ausnahmen

Über das Anklicken der Schaltfläche **Ausnahmen** können Sie bestimmte Laufwerke, Verzeichnisse und Dateien von der Überprüfung ausschließen und auf diese Weise die Virenerkennung teilweise erheblich beschleunigen. Gehen Sie dazu folgendermaßen vor:

1 Klicken Sie auf die Schaltfläche **Ausnahmen**.

2 Klicken Sie in dem Fenster **Ausnahmen für die manuelle Rechnerprüfung** auf **Neu**.

3 Wählen Sie nun aus, ob Sie ein Laufwerk, ein Verzeichnis oder eine Datei bzw. einen Dateityp ausschließen möchten.

4 Wählen Sie nun darunter das Verzeichnis oder das Laufwerk aus, welches Sie schützen möchten. Sie können hier auch Dateitypen als Ausnahmen definieren.

Um z.B. sämtliche Dateien mit der Datei-Endung **.sav** schützen zu lassen, geben Sie **sav** ein.

Sie können diesen Vorgang bei Bedarf beliebig oft wiederholen und vorhandene Ausnahmen auch wieder löschen oder modifizieren.

> **Ausnahmen auch für den Leerlauf-Scan verwenden**: Während bei der manuellen Virenprüfung gezielt der Computer nach Viren gescannt wird und nicht für andere Aufgaben verwendet werden sollte, ist der **Leerlauf-Scan** eine intelligente Virenprüfung, die alle Dateien Ihres Computers immer wieder darauf überprüft, ob sie nicht schon mit einem Virus infiziert sind. Der Leerlauf-Scan arbeitet wie ein Bildschirmschoner immer nur dann, wenn Sie Ihren Computer eine Weile nicht benötigen und hört sofort wieder auf, sobald sie weiterarbeiten, um Ihnen optimale Performance zu gewährleisten. Hier können Sie festlegen, ob auch für den Leerlauf-Scan Ausnahmedateien oder Ausnahmeverzeichnisse definiert werden sollen.

Erweitert

Mit Anklicken der Schaltfläche **Erweitert** können Sie weiterführende Einstellungen zur Virenprüfung vornehmen. In den meisten Fällen ist es aber vollkommen ausreichend, die vorgegebenen Standardeinstellungen zu verwenden.

- **Dateitypen**: Hier können Sie festlegen, welche Dateitypen von der Software auf Viren untersucht werden sollen. Die Auswahl der Option **nur Programmdateien und Dokumente** bringt Geschwindigkeitsvorteile mit sich.
- **Heuristik**: In der heuristischen Analyse werden Viren nicht nur anhand der Virendatenbanken erkannt, die Sie mit jedem Update der Antivirensoftware erhalten, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch einen Fehlalarm erzeugen.
- **Archive prüfen**: Das Überprüfen gepackter Daten in Archiven (diese erkennt man an Datei-Endungen wie z.B. **ZIP**, **RAR** oder auch **PST**) ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der Virenwächter generell auf dem System aktiv ist. Um die Geschwindigkeit der Virenprüfung zu erhöhen, können Sie die Größe der Archiv-Dateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail-Archive prüfen**: Hier können Sie festlegen, ob auch Ihre Mailarchive auf Infektionen untersucht werden sollen.
- **Systembereiche prüfen**: Systembereiche (z.B. Bootsektoren) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden.
- **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit dieser Funktion können Sie Ihr System auch auf **Dialer** und andere Schadsoftware (**Spyware**, **Adware** und **Riskware**) überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.
- **Auf Rootkits prüfen**: **Rootkits** versuchen sich herkömmlichen Virenerkennungsmethoden zu entziehen. Eine zusätzliche Kontrolle auf diese Schadsoftware ist immer ratsam.
- **Nur neue bzw. veränderte Dateien prüfen**: Wenn Sie diese Funktion aktivieren, werden bei der Prüfung Dateien übersprungen, die sich seit längerer Zeit nicht verändert haben und die zuvor als unschädlich erkannt worden sind. Das bringt einen Performance-Gewinn bei der täglichen Arbeit – ohne Sicherheits-Risiko.
- **Protokoll anfertigen**: Über dieses Häkchenfeld können Sie festlegen, dass die Software über den Virenprüfungsvorgang ein Protokoll anlegt. Dies kann dann im Bereich **Protokolle** eingesehen werden.

Updates

Sollte die Aktualisierung der Software oder der Virensignaturen übers Internet nicht funktionieren, können Sie in diesem Bereich alle notwendigen Angaben machen, um eine automatische Aktualisierung zu ermöglichen. Geben Sie hier in den Optionen die Zugangsdaten (**Benutzername** und **Passwort**) ein, die Sie bei der Online-Anmeldung Ihrer Software per E-Mail erhalten haben. Mit Hilfe dieser Daten werden Sie vom G Data Updateserver erkannt und Aktualisierungen können nun vollautomatisch erfolgen.

Wenn Sie eine neue Lizenz erworben haben und diese aktivieren möchten, wählen Sie **Lizenz aktivieren**. Die Internet-Einstellungen zeigen spezielle Optionen, die nur in wenigen Ausnahmefällen (Proxyserver, andere Region) benötigt werden. Die Versionsprüfung sollten Sie nur temporär deaktivieren, wenn Sie Schwierigkeiten bei der Aktualisierung der Virensignaturen haben.

Virensignaturen automatisch aktualisieren

Wenn Sie nicht möchten, dass sich dich G Data Software automatisch darum kümmert, die Virensignaturen auf den neuesten Stand zu bringen, dann können Sie das Häkchen hier entfernen. Die Abschaltung stellt allerdings ein hohes Sicherheitsrisiko dar und sollte nur in Ausnahmefällen erfolgen. Wenn Ihnen der Abstand zwischen den Aktualisierungen zu klein sein sollte, können Sie diesen individuell anpassen und z.B. festlegen, dass diese nur beim Internetverbindungsaufbau erfolgen. Bei Rechnern die nicht permanent mit dem Internet verbunden sind, ist diese Auswahl z.B. sinnvoll.

Protokoll anfertigen: Wenn Sie hier ein Häkchen setzen, wird jede Aktualisierung der Virensignaturen in das Protokoll aufgenommen, welches Sie bei den Zusatzfunktionen der G Data Software (im **SecurityCenter** unter **Mehr** > **Protokolle**) einsehen können. Neben diesen Einträgen finden Sie im Protokoll z.B. Informationen über Virenfunde und andere Aktionen, die vom Programm durchgeführt werden.

Lizenz aktivieren

Wenn Sie Ihre G Data Software noch nicht registriert haben sollten, können Sie dies jetzt nachholen und Ihre Registriernummer und Kundendaten eingeben. Sie finden die **Registriernummer** je nach Art des Produktes z.B. auf der Rückseite des Bedienungshandbuchs, der Bestätigungsmail beim Softwaredownload oder auf der CD-Stecktasche.

Durch die Eingabe der Registriernummer wird Ihr Produkt aktiviert

Klicken Sie nun auf die Schaltfläche **Anmelden** und Ihre Zugangsdaten werden auf dem Updateserver erzeugt. Wenn die Anmeldung erfolgreich verlief, erscheint ein Info-Bildschirm mit dem Vermerk **Die Anmeldung wurde erfolgreich durchgeführt**, den Sie mit Anklicken der Schließen-Schaltfläche verlassen können.

Achtung: Für Ihre Unterlagen und für etwaige Neuinstallationen der Software erhalten Sie Ihre **Zugangsdaten** auch per E-Mail zugeschickt. Bitte vergewissern Sie sich deshalb, dass Ihre in der Online-Registrierung angegebene E-Mail-Adresse korrekt ist; ansonsten stehen Ihnen die Zugangsdaten nicht zur Verfügung.

Abschließend werden die Zugangsdaten automatisch in die ursprüngliche Eingabemaske übernommen und Sie können von nun an Virensignaturen übers Internet aktualisieren.

Sie können Ihre Lizenz nicht aktivieren? Wenn Sie sich nicht am Server anmelden können, kann dies vielleicht an einem Proxyserver liegen. Klicken Sie bitte auf die Schaltfläche **Internet Einstellungen**. Hier können Sie Einstellungen für Ihre Internetverbindung vornehmen. Generell sollten Sie bei Problemen mit dem Update der Virensignaturen erst einmal überprüfen, ob Sie generell mit einem Internetbrowser (z.B. InternetExplorer) ins Internet kommen. Wenn Sie überhaupt keine Verbindung mit dem Internet aufbauen können, liegt das Problem wahrscheinlich im Bereich der Internetverbindung und nicht bei den Angaben zum Proxyserver.

Internet Einstellungen

Sollten Sie einen Proxyserver nutzen, setzen Sie bitte das Häkchen bei **Proxyserver verwenden**. Sie sollten diese Einstellung nur ändern, wenn das Update der Virensignaturen nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Systemadministrator oder Internetzugangsanbieter. Falls notwendig, können Sie hier außerdem die Zugangsdaten für den Proxyserver eingeben.

> **Proxyserver**: Ein Proxyserver bündelt Anfragen an Netzwerke und verteilt Sie an seine angeschlossenen Rechner. Wenn Sie z.B. Ihren Rechner in einem Firmennetzwerk verwenden, kann es gut sein, dass Sie über einen Proxyserver ins Netz gehen. Generell sollten Sie bei Problemen mit dem Update der Virensignaturen erst einmal überprüfen, ob Sie generell mit einem Internetbrowser ins Netz kommen. Wenn Sie überhaupt keine Verbindung mit dem Internet aufbauen können, liegt das Problem wahrscheinlich im Bereich der Internetverbindung und nicht bei den Angaben zum Proxyserver.

Webschutz

Folgende Einstellungen können Sie hier vornehmen.

- **Internetinhalte (HTTP) verarbeiten**: In den Webschutz-Optionen können Sie bestimmen, dass sämtliche **HTTP-Webinhalte** schon beim Browsen auf Viren überprüft werden. Infizierte Webinhalte werden dann gar nicht erst ausgeführt und die entsprechenden Seiten nicht angezeigt. Setzen Sie hierzu bitte das Häkchen bei **Internetinhalte (HTTP) verarbeiten**.

  > Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift natürlich der **Virenwächter** dann ein, wenn infizierte Dateien gestartet werden. Ihr System ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der Virenwächter aktiviert ist.
  >
  > Sie können bestimmte Webseiten auch als Ausnahmen definieren, wenn Sie diese für unbedenklich halten. Lesen Sie hierzu bitte das Kapitel **Ausnahmen festlegen**. Über die Schaltfläche **Erweitert** können Sie weitere Einstellungen zum Umgang mit Internetinhalten vornehmen.

- **Phishingschutz:** Mit dem sogenannten **Phishing** versuchen Betrüger im Internet, Kunden einer bestimmten Bank oder eines Shops auf eine gefälschte Webseite zu lenken, um dort dann Ihre Daten zu stehlen. Die Aktivierung des Phishingschutzes ist sehr empfehlenswert.
- **Adressen von infizierten Internetseiten einsenden**: Über diese Funktion können Sie - natürlich anonym - automatisch Internetseiten melden, die von der Software als gefährlich beurteilt werden. Damit optimieren Sie die Sicherheit für alle Anwender.
- **Instant-Messaging-Inhalte verarbeiten**: Da auch über Instant Messaging-Tools Viren und andere Schadprogramme verbreitet werden können, kann die Software auch hier die Anzeige und den Download infizierter Daten im Vorfeld unterbinden. Sollten Ihre Instant Messaging-Anwendungen nicht über die Standardportnummern ablaufen, geben Sie bitte unter **Erweitert**, die entsprechenden **Ports** ein.
- **Einbindung in die Messenger-Anwendung**: Sollten Sie den **Microsoft Messenger** oder **Trillian** verwenden, können Sie durch Setzen des Häkchens für das jeweilige Programm ein Kontextmenü definieren, in dem Sie verdächtige Dateien direkt auf Viren überprüfen können.

Ausnahmen festlegen

Um eine Internetseite als Ausnahme in die Whitelist aufzunehmen, gehen Sie bitte folgendermaßen vor:

1. Klicken Sie auf die Schaltfläche **Ausnahmen festlegen**. Nun erscheint das Whitelist-Fenster. Hier werden Ihnen die Webseiten angezeigt, die Sie als sicher eingestuft und hier eingegeben haben.
2. Um eine weitere Internetseite hinzuzufügen, klicken Sie nun bitte auf die Neu-Schaltfläche. Es öffnet sich eine Eingabemaske. Geben Sie hier bitte unter **URL** die Adresse der Webseite an, also z.B. (www.unbedenklicheseite.de) und unter **Bemerkung** gegebenenfalls eine Notiz dazu, wieso Sie diese Webseite aufgenommen haben. Bestätigen Sie die Eingabe mit einem Klick auf OK.
3. Bestätigen Sie nun mit einem Klick auf OK alle Änderungen an der Whitelist.

Um eine Webseite wieder von der Whitelist zu löschen, markieren Sie diese in der Liste mit der Maus und klicken dann einfach auf die Löschen-Schaltfläche.

Erweitert

Hier können Sie festlegen, welche **Serverportnummer** vom Webschutz überwacht werden sollen. In der Regel reicht für eine Überwachung des normalen Browsens hier die Portnummer 80.

- **Zeitüberschreitung im Browser vermeiden**: Da die Software die Internetinhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die Daten zugestellt bekommt, da diese von der Antivirensoftware auf Schadroutinen überprüft werden. Mit Setzen des Häkchens bei **Zeitüberschreitung im Browser vermeiden** wird eine solche Fehlermeldung unterdrückt und sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese dann ganz normal an den Internetbrowser überreicht.
- **Größenbegrenzung für Downloads**: Hiermit können Sie die HTTP-Überprüfung für zu große Webinhalte unterbinden. Die Inhalte werden dann vom Virenwächter überprüft, sobald etwaige Schadroutinen aktiv werden. Der Vorteil bei dieser Größenbegrenzung liegt darin, dass es beim Surfen im Web nicht zu Verzögerungen durch die Virenkontrolle kommt.

E-Mail-Prüfung

Mit der E-Mail-Prüfung können Sie ein- und ausgehende E-Mails und deren Datei-Anhang auf Viren überprüfen und mögliche Infektionen direkt an der Quelle ausschalten. Die Software ist in der Lage, bei Virenfund Datei-Anhänge direkt zu löschen oder infizierte Dateien zu reparieren.

In **Microsoft Outlook** wird die E-Mail-Prüfung durch ein **Plug-In** realisiert. Dieses bietet denselben Schutz wie die **POP3**/**IMAP** orientierte Schutzfunktion innerhalb der **AntiVirus** Optionen. Nach der Installation dieses Plug-Ins finden Sie im **Outlook**-Menü **Extras** die Funktion **Ordner auf Viren überprüfen**, mit der Sie Ihre Mailordner einzeln auf Virenbefall checken können.

Eingehende Mails

- **Im Fall einer Infektion**: Hier können Sie festlegen, was bei Entdeckung einer infizierten Mail geschehen soll. Je nachdem, für welche Zwecke Sie Ihren Computer verwenden, sind hier unterschiedliche Einstellungen sinnvoll. In der Regel ist die Einstellung **Desinfizieren (wenn nicht möglich: Anhang/Text löschen)** empfehlenswert.
- **Empfangene Mails prüfen**: Mit Aktivierung dieser Option werden sämtliche **E-Mails** auf Viren überprüft, die Sie während Ihrer Arbeit am Computer erreichen.

- **Bericht an empfangene, infizierte Mails anhängen**: Wenn Sie die Berichtoption aktiviert haben, erscheint im Fall eines Virenfundes in der Betreffzeile der infizierten Mail die Warnung **VIRUS** und am Anfang des Mailtextes die Mitteilung **Achtung! Diese Mail enthält folgenden Virus** gefolgt vom Namen des Virus und der Angabe, ob der Virus gelöscht oder die infizierte Datei repariert werden konnte.

Ausgehende Mails

- **Mails vor dem Senden prüfen**: Damit Sie nicht versehentlich selber Viren verschicken, bietet die Software auch die Möglichkeit, Ihre Mails vor dem Versenden auf Virenbefall zu überprüfen. Sollten Sie tatsächlich einen Virus (unbeabsichtigt) versenden wollen, erscheint die Meldung **Die Mail [Betreffzeile] enthält folgenden Virus: [Virusname]**. Die Mail kann nicht verschickt werden und die entsprechende E-Mail wird nicht versandt.

Scanoptionen

- **Engines benutzen**: Die Software arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Analyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe.
- **OutbreakShield**: Hiermit aktivieren Sie das OutbreakShield. Die Software erstellt bei aktiviertem OutbreakShield Prüfsummen von Mails, gleicht diese im Internet mit stets aktualisierten Anti-Spam-Blacklists ab und ist dadurch in der Lage, auf ein Massenmailing zu reagieren, bevor entsprechende Virensignaturen zur Verfügung stehen. 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 Virensignaturen besteht. Das OutbreakShield ist in den E-Mail-Virenblocker integriert.

Erweitert

Wenn Sie bei der Nutzung Ihrer E-Mail-Programme nicht die **Standardports** verwenden, können Sie unter **Serverportnummer** auch den **Port** angeben, den Sie für eingehende oder ausgehende Mails verwenden. Mit Anklicken der **Standard**-Schaltfläche können Sie automatisch die Standardportnummern wiederherstellen. Sie können auch mehrere Ports eintragen. Trennen Sie diese jeweils durch ein Komma.

Microsoft Outlook wird durch ein spezielles Plug-In geschützt, mit dem Sie direkt aus **Outlook** heraus Ordner und Mails überprüfen können. Um in Outlook eine E-Mail oder eine Ordner auf Viren zu überprüfen, wählen Sie einfach in der Outlook-Menüleiste den Befehl **Extras > Ordner auf Viren überprüfen**. und der aktuell ausgewählte Mailordner wird auf Viren überprüft.

Da die Software die eingehenden Mails zeitlich vor dem eigentlichen Mailprogramm bearbeitet, kann es bei großen Mail-Mengen oder langsamen Verbindungen vorkommen, dass eine Fehlermeldung beim Mailprogramm erscheint, weil es nicht sofort die Maildaten zugestellt bekommt, da diese ja von der Software auf Viren überprüft werden. Mit Aktivieren des Häkchenfeldes bei **Zeitüberschreitung beim E-Mail-Server vermeiden** wird eine solche Fehlermeldung des Mailprogramms unterdrückt und sobald sämtliche Maildaten auf Viren überprüft wurden, werden diese von der Software dann ganz normal an das Mailprogramm überreicht.

Automatische Virenprüfungen

Hier können Sie den **Leerlauf-Scan** ein- oder ausschalten. Darüber hinaus können Sie stattdessen oder auch zusätzlich regelmäßig Ihren Rechner oder Bereiche Ihres Rechners auf Infektionen hin untersuchen. Zum Beispiel können Sie dann solche Prüfungen zu Zeiten durchführen, in denen Sie Ihren Computer nicht nutzen.

> **Unterschiedliche Virenprüfungen:** In vielen Fällen reicht es, wenn der Computer durch den Leerlauf-Scan untersucht wird. Über die Schaltfläche **Neu** können Sie aber auch verschiedene, voneinander unabhängige automatische Virenprüfungen erstellen. So ist es z.B. vorstellbar, dass Sie den Ordner **Downloads** täglich überprüfen, während Sie z.B. ihre MP3-Sammlung nur einmal im Monat checken.

Allgemein

Legen Sie hier fest, welchen Namen die neu eingerichtete automatische Virenprüfung haben soll. Zur Unterscheidung sind aussagekräftige Namen ratsam wie z.B. **Lokale Festplatten (wöchentliche Überprüfung)** oder **Archive (monatliche Überprüfung)**.

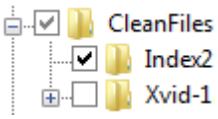
Wenn Sie ein Häkchen bei **Nach Beendigung des Jobs den Rechner ausschalten** setzen, wird der Rechner automatisch heruntergefahren, nachdem die automatische Virenprüfung durchgeführt wurde. Dies macht Sinn, wenn Sie die Virenprüfung z.B. nach der Arbeit im Büro durchführen möchten.

> **Job:** Jeder einzeln aufgeführte automatische Auftrag zur Prüfung des Rechners oder bestimmter Bereiche, wird als Job bezeichnet.

Analyse-Umfang

Legen Sie hier fest, ob die Virenprüfung auf den **Lokalen Festplattenlaufwerken** stattfinden soll, ob **Speicher** und **Autostart-Bereiche** getestet werden sollen oder ob Sie nur bestimmte **Verzeichnisse** und **Dateien** prüfen wollen. Sollte dies der Fall sein, geben Sie bitte über die Schaltfläche **Auswahl** die gewünschten Verzeichnisse an.

> **Verzeichnisse/Dateien auswählen**: Im Verzeichnisbaum können Sie durch Anklicken der Plus-Symbole Verzeichnisse öffnen und auswählen, deren Inhalt dann in der Datei-Ansicht angezeigt wird. Jedes Verzeichnis oder jede Datei, die Sie mit einem Häkchen versehen, wird von von der Software geprüft. Wenn in einem Verzeichnis nicht alle Dateien geprüft werden, findet sich an diesem Verzeichnis ein graues Häkchen.



Zeitplanung

Über diese Karteikarte können Sie festlegen, wann und in welchem Rhythmus der jeweilige Job erfolgen soll. Unter **Ausführen** geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter **Zeitpunkt** näher erläutern. Wenn Sie **Beim Systemstart** auswählen, fallen die Vorgaben der Zeitplanung natürlich fort und die Software führt die Prüfung immer aus, wenn Ihr Rechner neu gestartet wird.

- **Job nachholen, wenn der Rechner zur Startzeit nicht eingeschaltet ist**: Durch Aktivierung dieser Option werden nicht ausgeführte automatische Virenprüfungen automatisch nachgeholt, sobald der Rechner wieder hochfährt.
- **Nicht im Batteriebetrieb ausführen**: Um die Akkulaufzeit nicht unnötig zu verringern, können Sie z.B. für **Notebooks** festlegen, dass automatische Virenprüfungen nur dann erfolgen, wenn der tragbare Computer ans Stromnetz angeschlossen ist.

Scan-Einstellungen

In diesem Bereich können Sie festlegen, mit welchen Einstellungen die automatische Virenprüfung stattfinden soll.

- **Engines benutzen**: Die Software arbeitet mit zwei **Engines**, also zwei grundsätzlich voneinander unabhängigen Virenprüfungsprogrammen. Jede Engine für sich alleine würde Sie schon in sehr hohem Maß vor Viren schützen, aber gerade die Kombination beider Engines liefert allerbeste Ergebnisse. Bei älteren und langsamen Rechnern kann man durch die Nutzung einer einzelnen Engine die Virenprüfung beschleunigen, in der Regel sollten Sie jedoch die Einstellung **Beide Engines** beibehalten.
- **Infizierte Dateien**: Ihre Software hat einen Virus gefunden? In der Standard-Einstellung fragt die Software nun, was Sie mit dem Virus und der infizierten Datei machen möchten. Wenn Sie immer dieselbe Aktion durchführen möchten, dann können Sie das hier einstellen. Höchste Sicherheit für Ihre Daten bietet hierbei die Einstellung **Desinfizieren (wenn nicht möglich: in Quarantäne)**.
- **Infizierte Archive**: Legen Sie hier fest, ob **Archiv-Dateien** (also z.B. Dateien mit der Endung **RAR**, **ZIP** oder auch **PST**) anders behandelt werden sollen, als normale Dateien. Beachten Sie jedoch, dass das Verschieben eines Archivs in Quarantäne dieses beschädigen kann, sodass es auch nach einer Zurückbewegung nicht mehr benutzt werden kann.

Legen Sie über das Anklicken der Schaltfläche **Erweitert** fest, welche zusätzlichen Virenprüfungen durchgeführt oder unterlassen werden sollen.

In den meisten Fällen ist es aber vollkommen ausreichend, die vorgegebenen Standardeinstellungen zu verwenden.

- **Dateitypen**: Hier können Sie festlegen, welche Dateitypen von der Software auf Viren untersucht werden sollen.
- **Heuristik**: In der heuristischen Analyse werden Viren nicht nur anhand der Virendatenbanken erkannt, die Sie mit jedem Update der Software erhalten, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch einen Fehlalarm erzeugen.
- **Archive prüfen**: Das Überprüfen gepackter Daten in Archiven (diese erkennt man an Dateiendungen wie z.B. **ZIP**, **RAR** oder auch **PST**) ist sehr zeitintensiv und kann in der Regel dann unterbleiben, wenn der **Virenwächter** generell auf dem System aktiv ist. Dieser erkennt dann beim Entpacken des Archives einen bis dahin verborgenen Virus und unterbindet automatisch dessen Verbreitung.
- **E-Mail-Archive prüfen**: Hier können Sie festlegen, ob auch Ihre Mailarchive auf Infektionen untersucht werden sollen.
- **Systembereiche prüfen**: Systembereiche (z.B. **Bootsektoren**) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden.
- **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit dieser Funktion können Sie Ihr System auch auf **Dialer** und andere Schadsoftware (**Spyware**, **Adware** und **Riskware**) überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surfverhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit übers Internet an fremde Personen weiterleiten.
- **Auf Rootkits prüfen**: **Rootkits** versuchen sich herkömmlichen Virenerkennungsmethoden zu entziehen. Eine zusätzliche Kontrolle auf diese Schadsoftware ist immer ratsam.
- **Protokoll anfertigen**: Über dieses Häkchenfeld können Sie festlegen, dass die Software über den Virenprüfungsvorgang ein Protokoll anlegt. Dies kann dann im Bereich **Protokolle** eingesehen werden.

Benutzerkonto

Hier kann das Benutzerkonto auf dem Rechner angegeben werden, auf dem die Virenprüfung stattfinden soll. Dieses Konto wird für den Zugriff auf Netzwerklaufwerke benötigt.

11.3 AntiSpam

Hier können Sie grundlegende Einstellungen zum Umgang mit Spam-E-Mails definieren.

Spam-Filter

Über den Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um E-Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der E-Mails, die typisch für Spam sind. Anhand der zutreffenden Merkmale wird ein Wert errechnet, der die Wahrscheinlichkeit für Spam widerspiegelt. Über die Schaltfläche **Spam-Filter verwenden** aktivieren bzw. deaktivieren Sie den Spam-Filter. Um die unterschiedlichen Filter-Arten des Spam-Filters ein- oder auszuschalten, setzen oder entfernen Sie einfach das Häkchen vor dem jeweiligen Eintrag. Um bei den unterschiedlichen Filtern Änderungen vorzunehmen, klicken Sie einfach auf den jeweiligen Eintrag. Dann erscheint ein Dialogfenster, in dem Sie entsprechende Einstellungen variieren können. Folgende Einstellungsmöglichkeiten stehen zur Verfügung:

- **Spam-OutbreakShield**: Mit dem **OutbreakShield** können Schädlinge in Massenmails schon erkannt und bekämpft werden, bevor aktualisierte Virensignaturen dafür verfügbar sind. Das OutbreakShield erfragt dabei über das Internet besondere Häufungen von verdächtigen E-Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht.

  > Falls Sie einen Rechner hinter einem Proxyserver verwenden, klicken Sie zur Einrichtung bitte auf die Schaltfläche **Internet-Einstellungen** und nehmen die entsprechenden Änderungen vor. Sie sollten diese Einstellung nur ändern, wenn das OutbreakShield nicht funktioniert.

- **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@informationsseite.de) oder Domain (z.B. informationsseite.de) ein, die Sie vom Spamverdacht ausnehmen möchten und die G Data Software behandelt E-Mails von diesem Absender bzw. dieser Absender-Domain nicht als Spam. Über die Schaltfläche **Import** 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 Schaltfläche **Export** 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 die G Data Software behandelt E-Mails von diesem Absender bzw. dieser Absender-Domain generell als E-Mails mit sehr hoher Spamwahrscheinlichkeit. Über die Schaltfläche **Import** 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 Schaltfläche **Export** können Sie eine solche Blacklist auch als Textdatei exportieren.

- **Realtime Blacklists verwenden**: Im Internet finden sich Listen, die IP-Adressen von Servern enthalten, über die bekanntermaßen Spam verschickt wird. Die G Data Software ermittelt durch Anfragen an die 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 (Mailtext) verwenden**: Über die Liste der **Schlüsselwörter** können Sie E-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 Schaltfläche **Import** 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 Schaltfläche **Export** können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. Über den Haken vor **Nur vollständige Wörter suchen** können Sie festlegen, dass die G Data Software die Betreffzeile einer E-Mail nur nach ganzen Wörtern durchsucht. So würde z.B. ein Begriff wie **cash** unter Spamverdacht fallen, während der gemeine **Cashew-Kern** weiterhin unbeanstandet bliebe.

- **Schlüsselwörter (Betreff) verwenden**: Über die Liste der Schlüsselwörter können Sie E-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.

- **Inhaltsfilter verwenden**: Beim **Inhaltsfilter** handelt es sich um einen selbst lernenden Filter, 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 E-Mail weiter dazu. Über die Schaltfläche **Tabelleninhalte abfragen** können Sie sich die Wortlisten anzeigen lassen, die der Inhaltsfilter zur Einordnung einer E-Mail als Spam verwendet. Über die Schaltfläche **Tabellen zurücksetzen** löschen Sie alle gelernten Tabelleninhalte und der selbst lernende Inhaltsfilter startet den Lernvorgang erneut von Beginn an.

Reaktion

Hier können Sie bestimmen, wie der Spam-Filter mit E-Mails umgehen soll, die möglicherweise Spam enthalten. Dabei können Sie drei Abstufungen vornehmen, die davon beeinflusst werden, wie hoch die G Data Software die Wahrscheinlichkeit dafür ansetzt, dass es sich bei der betreffenden E-Mail um Spam handelt.

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

Jede dieser drei abgestuften Reaktionen können Sie individuell gestalten. Klicken Sie dazu einfach auf die Schaltfläche **Ändern** und definieren die Reaktion, mit der die G Data Software reagieren soll. So haben Sie über **Mail zurückweisen** die Möglichkeit, die E-Mail gar nicht erst in Ihr Postfach gelangen zu lassen. Über **Spamwarnung in Betreff** und **Text der Mail einfügen** können Sie als Spam identifizierten E-Mails auch als solche auffällig kennzeichnen, um sie z.B. besser aussortieren zu können. Wenn Sie **Microsoft Outlook** verwenden (Achtung: Nicht zu verwechseln mit **Outlook Express** oder **Windows Mail**), haben Sie auch die Möglichkeit, E-Mails mit Spamverdacht in einen frei definierbaren Ordner in Ihrem Postfach zu verschieben (**Mail in Ordner verschieben**). Sie können diesen Ordner direkt über die G Data Software anlegen, in dem Sie unter **Ordnername** den entsprechenden Ordner definieren.

Auch wenn Sie kein **Outlook** verwenden, können Sie die als Spam erkannten E-Mails in einen **Ordner** verschieben lassen. Fügen Sie dazu eine Warnung in die Betreffzeile ein (z.B. "[Spam]") und erstellen Sie in Ihrem E-Mailprogramm eine Regel, die E-Mails mit dem Text in der Betreffzeile in einen anderen Ordner verschiebt.

Profi-Einstellungen

In diesem Bereich können Sie die Spam-Erkennung der G Data Software sehr detailliert verändern und an die Gegebenheiten Ihres E-Mailverkehrs anpassen. Generell empfiehlt es sich hier jedoch, die Standardeinstellungen zu verwenden. In den Profi-Einstellungen sollten Sie nur dann Veränderungen vornehmen, wenn Sie sich mit der Thematik auskennen und genau wissen, was Sie tun.

Weitere Filter

Folgende Filter sind hier standardmäßíg eingestellt, können von Ihnen im Bedarfsfall aber durch Entfernen des Häkchens auch abgeschaltet werden.

- **HTML-Skripte deaktivieren**
- **Gefährliche Anhänge filtern**

Darüber hinaus können Sie über die Schaltfläche **Neu** im neue Filterregeln anlegen oder über die Schaltfläche **Bearbeiten** vorhandene Filter bearbeiten. Die erstellten Filter werden in der Liste angezeigt und können über die Häkchenfelder links vom jeweiligen Eintrag beliebig an- bzw. abgeschaltet werden. Wenn sich ein Häkchen im Häkchenfeld befindet, ist der jeweilige Filter aktiv. Wenn sich kein Häkchen im Häkchenfeld befindet, ist der Filter nicht aktiv. Um einen Filter endgültig zu löschen, markieren Sie diesen bitte mit einem einfachen Mausklick und verwenden dann die Schaltfläche **Löschen**.

> Bei den Filtermöglichkeiten, die Ihnen hier zur Verfügung stehen, handelt es sich um zusätzliche Filter, die den eigentlichen Spam-Filter der G Data Software unterstützen und Ihnen individuelle Einstellungen erleichtern. Über den eigentlichen Spam-Filter haben Sie umfangreiche Einstellungsmöglichkeiten, um E-Mails mit unerwünschten Inhalten oder von unerwünschten Absendern (z.B. Massenmailversendern) wirkungsvoll zu blockieren. Das Programm prüft viele Merkmale der E-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.

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.

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

- **Gefährliche Anhänge filtern**: Beim Filtern von Anhängen haben Sie eine große Auswahl von Möglichkeiten, um E-Mail-Anhänge (= Attachments) und Anlagen zu filtern. Die meisten E-Mail-Viren 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 E-Mail-Anhängen große Vorsicht walten lassen und im Zweifelsfall lieber noch einmal eine Rückfrage beim Absender einer E-Mail durchführen, bevor er eine Datei ausführt, die er nicht ausdrücklich angefordert hat. Unter **Dateierweiterungen** können Sie die Datei-Endungen 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 E-Mailserver darstellen. Selbstverständlich können Sie auch beliebige **Archivdateien** (z.B. ZIP, RAR oder CAB) filtern. Trennen Sie bitte alle Datei-Erweiterungen einer Filtergruppe durch **Semikolon**. Über die Funktion **Auch Anhänge in eingebetteten Mails filtern** sorgen Sie dafür, dass die Filterung der unter **Dateierweiterungen** ausgewählten Anlagentypen auch in E-Mails stattfindet, die selber eine Anlage einer E-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 diese 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 Datei-Endung 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 E-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 **Suchkriterium** einfach die **Schlüsselwörter** und **Ausdrücke** ein, auf die die G Data Software reagieren soll. Dabei können Sie Text auf beliebige Weise mit den logischen Operatoren **UND** und **ODER** verknüpfen. Geben Sie nun unter **Suchbereich** an, in welchen Bereichen einer E-Mail nach diesen Ausdrücken gesucht werden soll. Als **Header** wird der Bereich einer E-Mail bezeichnet, der unter anderem die E-Mail-Adresse des Absenders und des Empfängers, die Betreffzeile und Informationen zu den verwendeten Programmen, Protokollen und Absendedaten enthält. Im Unterschied dazu wird mit **Betreff** nur der Inhalt der Betreffzeile ohne weitere Textinformationen aus dem Header überprüft. Beim **Mailtext** haben Sie zudem die Auswahl, ob sich der Suchbereich nur auf reine **Text-Mails** oder auch auf den Text in **HTML-Mails** (HTML-Text) erstreckt. Über **Eingebettete Mails** können Sie festlegen, ob die Suche des Inhaltsfilters sich auch auf E-Mails erstreckt, die in der empfangenen E-Mail als Anlage vorhanden sind. Unter **Reaktion** können Sie festlegen, wie mit E-Mails verfahren werden soll, die von der G Data Software als Spam erkannt wurden. Über **Mail zurückweisen** wird die betreffende E-Mail von Ihrem E-Mailprogramm erst gar nicht in Empfang genommen, wenn Sie das Häkchen bei **Warnung in Betreff und Text der Mail einfügen** setzen, können Sie dem eigentlichen Text der Betreffzeile eine Warnung voranstellen (**Prefix in Betreffzeile**), z.B. **Spam** oder **Achtung**. Wahlweise können Sie auch einen Text eingeben, der bei Spam-Verdacht dem eigentlichen E-Mailtext vorangestellt wird (**Meldung in Text**). Wenn Sie **Microsoft Outlook** verwenden (Achtung: Nicht zu verwechseln mit **Outlook Express** oder **Outlook Mail**), haben Sie auch die Möglichkeit, E-Mails mit Spamverdacht in einem frei definierbaren Ordner in Ihrem Postfach zu verschieben (**Mail in Ordner verschieben**). Sie können diesen Ordner direkt über die G Data Software anlegen, in dem Sie unter **Ordnername** den entsprechenden Ordner definieren.

  > Der logische Operator **UND** setzt also voraus, dass alle mit UND verknüpften Elemente vorhanden sind, der logische Operator **ODER** setzt lediglich voraus, dass mindestens ein Element vorhanden ist.

- **Absenderfilter**: Über den Absenderfilter können Sie E-Mails, die von bestimmten Absendern kommen, auf bequeme Weise blocken. Geben Sie dazu unter **Absender/Domains** einfach die **E-Mail-Adressen** oder **Domain-Namen** ein, auf die die G Data Software reagieren soll. Mehrere Einträge können Sie durch **Semikolon** voneinander trennen. Unter **Reaktion** können Sie festlegen, wie mit E-Mails verfahren werden soll, die von der G Data Software als Spam erkannt wurden. Über **Mail zurückweisen** wird die betreffende E-Mail von Ihrem E-Mailprogramm erst gar nicht in Empfang genommen, wenn Sie das Häkchen bei **Warnung in Betreff und Text der Mail einfügen** setzen, können Sie dem eigentlichen Text der Betreffzeile eine Warnung voranstellen (**Prefix in Betreffzeile**), z.B. **Spam** oder **Achtung**. Wahlweise können Sie auch einen Text eingeben, der bei Spam-Verdacht dem eigentlichen E-Mailtext vorangestellt wird (**Meldung in Text**). Wenn Sie **Microsoft Outlook** verwenden (Achtung: Nicht zu verwechseln mit **Outlook Express** oder **Windows Mail**), haben Sie auch die Möglichkeit, E-Mails mit Spamverdacht in einem frei definierbaren Ordner in Ihrem Postfach zu verschieben (**Mail in Ordner verschieben**). Sie können diesen Ordner direkt über die G Data Software anlegen, in dem Sie unter **Ordnername** den entsprechenden Ordner definieren.

- **Sprachenfilter**: Mit dem Sprachenfilter können Sie automatisch E-Mails bestimmter Landessprachen als Spam definieren. Wenn Sie also in der Regel z.B. keinen E-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 E-Mails erhalten und die G Data Software erhöht damit die Spameinschätzung für diese E-Mails erheblich. Unter **Reaktion** können Sie festlegen, wie mit E-Mails verfahren werden soll, die von der G Data Software als Spam erkannt wurden. Über **Mail zurückweisen** wird die betreffende E-Mail von Ihrem E-Mailprogramm erst gar nicht in Empfang genommen, wenn Sie das Häkchen bei **Warnung in Betreff und Text der Mail einfügen** setzen, können Sie dem eigentlichen Text der Betreffzeile eine Warnung voranstellen (**Prefix in Betreffzeile**), z.B. **Spam** oder **Achtung**. Wahlweise können Sie auch einen Text eingeben, der bei Spam-Verdacht dem eigentlichen E-Mailtext vorangestellt wird (**Meldung in Text**). Wenn Sie **Microsoft Outlook** verwenden (Achtung: Nicht zu verwechseln mit **Outlook Express** oder **Windows Mail**), haben Sie auch die Möglichkeit, E-Mails mit Spamverdacht in einem frei definierbaren Ordner in Ihrem Postfach zu verschieben (**Mail in Ordner verschieben**). Sie können diesen Ordner direkt über die G Data Software anlegen, in dem Sie unter **Ordnername** den entsprechenden Ordner definieren.

Sonstiges

In diesem Bereich haben Sie die Möglichkeit weitere Einstellungen vorzunehmen.

- **Ungelesene Mails im Posteingang beim Programmstart prüfen**: Nur für **Microsoft Outlook**: Diese Option dient dazu, E-Mails auf Spamverdacht zu kontrollieren. Sobald Sie **Outlook** öffnen, werden deshalb sämtliche ungelesenen E-Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern von der G Data Software kontrolliert.
- **Andere Mailprogramme (Verwendung von POP3)**: Über **POP3** empfangene E-Mails können aus technischen Gründen nicht direkt gelöscht werden. Wenn ein Filter E-Mails zurückweisen soll, wird diese E-Mail dann mit einem Standard-Ersatztext versehen. Der Ersatztext bei zurückgewiesenen E-Mails lautet dabei: **Die Nachricht wurde zurückgewiesen**. Sie können den Text für diese Benachrichtigungsfunktionen aber auch individuell gestalten. Im frei definierbaren Text für den Betreff und den E-Mailtext stehen Ihnen folgende **Platzhalter** (definiert durch ein Prozentzeichen mit einem anschließenden Kleinbuchstaben) zur Verfügung:

  %s Absender
  %u Betreff

  Sie können in Ihrem E-Mailprogramm eine Regel definieren, die E-Mails mit dem hier definierten Ersatztext automatisch löscht.

11.4 Firewall

Neben dem Autopilot-Modus, der für viele Anwender sicherlich die beste Wahl ist, haben Sie darüber hinaus auch umfangreiche Optionen, die G Data-Firewall optimal auf Ihre Bedürfnisse und Anforderungen auszurichten.

> Wenn Sie sich intensiv mit der Firewall-Thematik auseinandersetzen, erhalten Sie im Kapitel **Firewall-Bedienung** weitere Informationen.

Automatik

In den Firewall-Einstellungen gibt es zwei grundlegende Bereiche, die individuell konfiguriert werden können:

Modus

Hier können Sie festlegen, ob die Firewall selbstständig und selbstlernend agiert und den Anwender bei der Entscheidung über das Blocken oder Freigeben von Anfragen aus dem Internet nicht zu Rate zieht oder ob der Anwender bei Zweifelsfällen zu Rate gezogen wird und in das Erstellen von neuen Firewall-Regeln durch Nachfrage eingebunden wird.

- **Autopilot-Modus**: Hier arbeitet die Firewall vollkommen autonom und hält Gefahren automatisch vom heimischen PC ab. Diese Einstellung bietet einen praktischen Rundumschutz und ist in den meisten Fällen empfehlenswert.
- **Manuelle Regelerstellung**: Wenn Sie Ihre Firewall individuell konfigurieren möchten, können Sie über die manuelle Regelerstellung Ihren Firewallschutz ganz auf Ihre Bedürfnisse einrichten.
- **Autopilot-Modus anbieten, wenn eine Vollbild-Anwendung gestartet wird**: Gerade bei **Computerspielen** (und anderen **Vollbildanwendungen**) kann es störend sein, wenn die Firewall mit Nachfragefenstern den Spielfluss oder einfach nur die Darstellung stört. Um einen ungestörten Spielgenuss ohne Sicherheitseinbußen zu gewährleisten, ist der Autopilot eine sinnvolle Einstellung, da er Nachfragen der Firewall unterdrückt. Sollten Sie den Autopiloten nicht als Standardeinstellung verwenden, können Sie über diese Funktion dafür sorgen, dass er immer dann angeboten wird, wenn Sie ein Programm nutzen, welches im **Vollbildmodus** läuft.

Sicherheitseinstellung

Während Sie den Computer für ihre tägliche Arbeit nutzen, lernt die Firewall nach und nach, welche Programme Sie für den Zugang zum Internet nutzen, welche nicht und welche Programme ein Sicherheitsrisiko sind. Der Vorteil bei der Nutzung der vordefinierten Sicherheitsstufen liegt darin, ohne administrativen Aufwand und Fachkenntnisse im Bereich der Netzwerksicherheit die Firewall trotzdem auf individuelle Bedürfnisse anpassen zu können. Stellen Sie einfach mit dem Schieberegler die Sicherheitsstufe ein, die Sie benötigen. Folgende Sicherheitsstufen stehen dabei zur Auswahl:

- **Höchste Sicherheit**: Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (TCP, UDP, Ports etc.). Die Firewall bemerkt kleinste Ungereimtheiten und wird während der Lernphase sehr häufig nachfragen.
- **Hohe Sicherheit**: Die Firewall-Regeln werden mit sehr feinkörnigen Richtlinien erstellt. Dazu sollten Sie sich mit netzwerkspezifischen Fachbegriffen auskennen (TCP, UDP, Ports etc.). Die Firewall wird während der Lernphase unter Umständen häufig nachfragen.
- **Normale Sicherheit**: Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern. Sie werden während der Lernphase möglichst wenig gefragt.
- **Niedrige Sicherheit**: Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern und Sie werden während der Lernphase selten gefragt. Höchst sicherer Schutz vor ankommenden Verbindungsanforderungen besteht auch in dieser Sicherheitsstufe.
- **Firewall deaktiviert**: Sie können die Firewall bei Bedarf auch abschalten. Ihr Computer ist dann weiterhin mit dem Internet und anderen Netzwerken verbunden, wird von der Firewall aber nicht mehr vor Angriffen oder Spionage-Attacken geschützt.

> Wenn Sie die Firewall spezifischer einstellen möchten, setzen Sie bitte das Häkchen bei **Benutzerdefinierte Sicherheit (für erfahrene Anwender)**. Beachten Sie aber, dass für diese Einstellungen zumindest ein Grundwissen zum Thema Netzwerksicherheit nötig ist.

Nachfragen

Hier legen Sie fest, wann, wie und ob die Firewall beim Anwender nachfragen soll, sobald Programme einen Verbindungsaufbau mit dem Internet oder Netzwerk anfragen.

- **Regel erstellen**: Wenn die Firewall eine Verbindungsaufnahme mit dem Netzwerk feststellt, erscheint eine Infobox, in der Sie festlegen, wie mit der jeweiligen Anwendung weiter zu verfahren ist. Hier können Sie festlegen, was genau Sie mit dem Erlauben oder Verbieten eines Netzwerkzugriffs bestimmen möchten:

  Pro Anwendung: Hier wird der Netzwerkzugriff für die aktuell angezeigte Anwendung generell auf jedem Port und mit jedem Übertragungsprotokoll (z.B. **TCP** oder **UDP**) erlaubt oder verweigert.

Pro Protokoll/Port/Anwendung: Die Anwendung, die einen Netzwerkzugriff erfragt, erhält die Erlaubnis nur mit dem erfragten Übertragungsprotokoll und ausschließlich mit dem angefragten Port online zu gehen. Sollte dieselbe Anwendung einen weiteren Netzwerkzugriff auf einem anderen Port oder mit einem anderen Protokoll erfragen, erscheint die Nachfrage erneut und es kann eine weitere Regel diesbezüglich erstellt werden.

Pro Anwendung, wenn mind. __ Nachfragen anstehen: Es gibt Anwendungen (z.B. Microsoft Outlook), die bei einer Netzwerkanfrage gleich mehrere Ports anfragen bzw. gleichzeitig unterschiedliche Protokolle nutzen. Da dieses z.B. in der Einstellung **Pro Protokoll/Port/Anwendung** mehrere Nachfragen mit sich brächte, kann hier auch festgelegt werden, dass Anwendungen eine generelle Freigabe bzw. Absage für die Netzwerknutzung erhalten, sobald Ihnen die Verbindung vom Anwender erlaubt oder untersagt wird.

- **Unbekannte Serveranwendungen**: Anwendungen, die noch nicht über eine Regel in der Firewall verwaltet werden, können unterschiedlich behandelt werden. Der Zeitpunkt der Nachfrage steht dabei in einem gewissen Ermessensspielraum. Wenn die **Serveranwendung** auf Empfang geht, heißt das, dass sie quasi auf Standby eine Verbindungsanforderung erwartet. Andernfalls erfolgt die Nachfrage erst, wenn die eigentliche Verbindungsanforderung gestellt wird.
- **Prüfung auf ungeschützte Netzwerke**: Natürlich kann eine Firewall nur dann problemlos funktionieren, wenn alle Netzwerke, auf die der zu schützende Rechner zugreift, von ihr auch erkannt und überwacht werden. Sie sollten deshalb unbedingt diese Prüfung auf ungeschützte Netzwerke aktiviert lassen.
- **Wiederholte Anwendungsnachfragen**: Sie können erneut wiederkehrende Verbindungsanfragen einer Anwendung bündeln. Auf diese Weise erscheint bei Verbindungsversuchen, die Sie noch nicht über eine Regel spezifiziert haben, nicht ständig eine Nachfrage, sondern z.B. nur in 20-Sekunden-Abständen oder einem anderen von Ihnen definierbaren Zeitraum.

Referenzprüfung

Bei der Referenzprüfung wird für Anwendungen, denen von der Firewall schon der Zugriff auf das Netzwerk erlaubt wurde, eine Prüfsumme auf Basis der Dateigröße und anderer Kriterien ermittelt. Wenn diese Prüfsumme des Programms plötzlich abweicht, kann es daran liegen, dass das Programm durch ein Schadprogramm verändert wurde. In diesem Fall schlägt die Firewall Alarm.

Die **Referenzprüfung für geladene Module** beobachtet auf gleiche Weise die **Module**, die die Anwendungen verwenden (z.B. DLLs). Da diese sich häufig ändern oder auch neue Module nachgeladen werden, kann eine konsequente Prüfung auf modifizierte und unbekannte Referenzen bei Modulen zu einem erheblichen Administrationsaufwand bei der Nutzung der Firewall führen. Jedes geänderte Modul würde dann nämlich eine Sicherheitsabfrage der Firewall nach sich ziehen. Die Modulprüfung sollte deshalb nur bei sehr hohen Ansprüchen an die Sicherheit in dieser Weise genutzt werden.

Sonstiges

Hier stehen Ihnen weitere Einstellungsmöglichkeiten zur Verfügung.

- **Vorgabe für den Regelassistenten**: Hier können Sie festlegen, ob Sie das Erstellen neuer Regeln generell über den **Regelassistenten** oder im **erweiterten Bearbeitungsmodus** durchführen möchten. Für Anwender, die sich in der Materie der Netzwerksicherheit nicht auskennen, empfehlen wir den **Regelassistenten**.
- **Prüfungen bei Programmstart**: Hier können Sie festlegen, ob die Firewall bei jedem Programmstart nach unbekannten **Serveranwendungen** sucht. Diese Suchfunktionen sollten immer eingeschaltet sein, es sei denn, Sie arbeiten in einem geschlossenen Netzwerk.

- **Verbindungsprotokoll speichern**: Hier können Sie festlegen, wie lange die Firewall Verbindungsdaten aufbewahren soll. Sie können die Daten von einer Stunde bis zu 60 Stunden nachhalten und im Firewall-Programmbereich **Protokoll** einsehen.

12 Firewall-Bedienung

In den folgenden Kapiteln erhalten Sie ausführliche Informationen zur Funktionalität der G Data Firewall. Hierbei handelt es sich um Fachinformationen, die für den regulären Betrieb der Firewall nicht notwendigerweise benötigt werden.

12.1 Status

Im Status-Bereich der Firewall erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und der Firewall. Diese finden sich rechts vom jeweiligen Eintrag als Text- oder Zahlenangabe. Darüber hinaus wird der Status der Komponenten auch grafisch dargestellt. 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 Warnsymbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Häkchensymbol.

- **Sicherheit**: Während Sie den Computer für ihre tägliche Arbeit nutzen, lernt die Firewall nach und nach, welche Programme Sie für den Zugang zum Internet nutzen, welche nicht und welche Programme ein Sicherheitsrisiko sind. Abhängig davon, wie sehr sie sich in der Materie der Firewall-Technologie auskennen, können Sie die Firewall so konfigurieren, dass Sie Ihnen entweder einen sehr guten Basis-Schutz bietet, ohne viele Nachfragen zu stellen oder aber einen professionellen Schutz, der sich sehr genau an ihrem Computernutzungsverhalten ausrichtet, aber auch gewisse Kenntnisse von Ihnen als Anwender verlangt.

- **Modus**: Hier werden Sie darüber informiert, mit welcher Grundeinstellung Ihre Firewall gerade betrieben wird. Möglich wären hier entweder die manuelle Regelerstellung oder die Automatik (**Autopilot**).

  Automatik (Autopilot): Hier arbeitet die Firewall vollkommen autonom und hält Gefahren automatisch vom heimischen PC ab. Diese Einstellung bietet einen praktischen Rundumschutz und ist in den meisten Fällen empfehlenswert.

  Manuelle Regelerstellung: Wenn Sie Ihre Firewall individuell konfigurieren möchten oder bestimmte Anwendungen nicht mit dem Autopilot-Modus zusammenarbeiten wollen, können Sie über die manuelle Regelerstellung Ihren Firewallschutz ganz auf Ihre Bedürfnisse einrichten.

- **Netzwerke**: Die Firewall überwacht natürlich sämtliche Netzwerkaktivitäten, wie z.B. ein DFÜ-Netzwerk und eine LAN-Verbindung. Sollten ein oder mehrere Netzwerke nicht geschützt werden, weil sie z.B. manuell von der Firewallüberwachung ausgenommen wurden, weist Sie ein Warnsymbol darauf hin. Ein Doppelklick auf den jeweiligen Eintrag öffnet ein Dialogfenster, über den Sie die Regeln und Einstellungen zum gewählten Netzwerk individuell konfigurieren können. Wählen Sie hier unter Regelsatz einfach aus, ob das jeweilige Netzwerk zu den vertrauenswürdigen Netzwerken, den nicht vertrauenswürdigen Netzwerken oder den zu blockierenden Netzwerken gehören soll.

  Die Einstellung **direkte Verbindung mit dem Internet** orientiert sich weitestgehend an den Einstellungen, die auch für **vertrauenswürdige Netzwerke** gelten.

  Jedem **Netzwerk** kann ein spezieller **Regelsatz** zugeordnet werden. Während Sie im Bereich **Netzwerke** sehen, welche Netzwerke auf Ihrem Computer vorhanden sind, sehen Sie im Bereich **Regelsätze**, welche automatischen oder selbst erstellten Regelsätze Ihnen in der Firewall zur Verfügung stehen.

- **Registrierte Angriffe**: Sobald die Firewall einen Angriff auf Ihren Computer registriert, wird dieser verhindert und hier protokolliert. Sie können durch Anklicken des Menüpunktes weitergehende Informationen erhalten.
- **Anwendungs-Radar**: Der Anwendungs-Radar zeigt Ihnen, welche Programme momentan von der Firewall blockiert werden. Sollten Sie eine der blockierten Anwendungen doch die Erlaubnis für die Nutzung des Netzwerkes erteilen wollen, wählen Sie diese hier einfach aus und klicken dann die Schaltfläche **Erlauben** an.

12.2 Netzwerke

Im Netzwerke-Bereich werden die Netzwerke (z.B. LAN, DFÜ etc.) aufgelistet, mit denen ihr Rechner verbunden ist. Hier wird auch aufgezeigt, nach welchem Regelsatz (siehe Kapitel **Regelsätze**) das jeweilige Netzwerk geschützt wird. Wenn Sie das Häkchen vor dem jeweiligen Netzwerk entfernen, wird dieses vom Firewall-Schutz ausgenommen. Sie sollten den Schutz allerdings nur in begründeten Einzelfällen abschalten. Wenn Sie ein Netzwerk mit der Maus markieren und die Bearbeiten-Schaltfläche anklicken, können Sie die Firewall-Einstellungen für dieses Netzwerk einsehen bzw. verändern.

Netzwerk bearbeiten

Beim Bearbeiten von Netzwerk-Einstellungen haben Sie die Auswahl, den Regelassistenten oder den erweiterten Bearbeitungsmodus zu verwenden. Generell ist der Regelassistent zu empfehlen, da er den Anwender beim Erstellen von Regeln und Einstellungen unterstützt.

- **Netzwerk-Info**: Hier erhalten Sie Informationen zum Netzwerk, als - soweit vorhanden - Angaben zu IP-Adresse, Subnetzmaske, Standardgateway, DNS- und WINS-Server.
- **Firewall aktiv, auf diesem Netzwerk**: Sie können die Firewall für das Netzwerk hier deaktivieren, sollten dies allerdings nur in begründeten Einzelfällen tun.
- **Gemeinsame Nutzung der Internet-Verbindung**: Bei direkten Verbindungen mit dem Internet können Sie festlegen, ob alle Rechner im Netzwerk über einen mit dem Internet verbundenen Rechner Zugriff auf das Internet erhalten sollen oder nicht. Diese Internetverbindungsfreigabe (ICS) kann für ein Heimnetzwerk in der Regel aktiviert werden.
- **Automatische Konfiguration (DHCP) zulassen**: Bei der Verbindung Ihres Computers mit dem Netzwerk wird eine dynamische IP-Adresse (über das DHCP = Dynamic Host Configuration Protocol) vergeben. Wenn Sie über diese Standardkonfiguration mit dem Netzwerk verbunden sind, sollten Sie das Häkchen hier gesetzt lassen.
- **Regelsatz**: Sie können hier sehr schnell zwischen vorstrukturierten Regelsätzen wählen und auf diese Weise festlegen, ob es sich bezüglich der Überwachungskriterien der Firewall z.B. um ein vertrauenswürdiges, nicht vertrauenswürdiges oder zu blockierendes Netzwerk handelt. Mit der Schaltfläche **Regelsatz bearbeiten** haben Sie auch die Möglichkeit, die Regelsätze individuell zu konfigurieren. Lesen Sie hierzu bitte auch das Kapitel **Regelsätze**.

12.3 Regelsätze

In diesem Bereich können Sie für verschiedene Netzwerke spezielle Regeln erstellen. Diese Regeln werden dann jeweils zu einem Regelsatz zusammengefasst. Voreingestellt sind Regelsätze für direkte Verbindung mit dem Internet, nicht vertrauenswürdige Netzwerke, vertrauenswürdige Netzwerke und zu blockierende Netzwerke. In der Übersicht wird der jeweilige Regelsatz mit Namen angezeigt. Mit Hilfe der Schaltflächen **Neu**, **Löschen** und **Bearbeiten** können Sie bestehende Regelsätze verändern, bzw. weitere Regelsätze hinzufügen.

> Die vorgegebenen Regelsätze für direkte Verbindung mit dem Internet, vertrauenswürdige Netzwerke, nicht vertrauenswürdige Netzwerke und zu blockierende Netzwerke können nicht gelöscht werden. Zusätzliche Regelsätze, die Sie selber erstellt haben, können Sie natürlich jederzeit löschen.

Regelsätze erstellen

Sie können jedem Netzwerk einen eigenen **Regelsatz** (also eine Sammlung speziell darauf abgestimmter Regeln) zuweisen. Auf diese Weise können Sie Netzwerke mit unterschiedlichen Gefährdungsstufen unterschiedlich mit der Firewall absichern. So benötigt ein privates Heimnetzwerk sicherlich weniger Schutz (und damit auch Administrationsaufwand), als ein DFÜ-Netzwerk, das im direkten Kontakt mit dem Internet steht.

Die Firewall beinhaltet drei voreingestellte Regelsätze für folgende Netzwerktypen:

- **Regelsatz für ein nicht vertrauenswürdiges Netzwerk**: Hierunter fallen in der Regel offene Netzwerke, wie z.B. DFÜ-Netzwerke, die auf das Internet Zugriff haben.

- **Regelsatz für ein vertrauenswürdiges Netzwerk**: Vertrauenswürdig sind in der Regel Heim- und Firmennetzwerke.
- **Regelsatz für ein zu blockierendes Netzwerk**: Wenn zeitweise oder dauerhaft der Kontakt des Rechners zu einem Netzwerk blockiert werden soll, kann diese Einstellung verwendet werden. Dies macht z.B. Sinn bei der Verbindung mit fremden Netzwerken, über deren Sicherheitsstandard man sich nicht ganz im Klaren ist (z.B. auf LAN-Partys, fremden Firmennetzwerken, öffentlichen Arbeitsplätzen für Notebooks etc.)

Sie können neu etablierten Netzwerken auf Ihrem Computer einen entsprechend ausgewählten Regelsatz zuordnen. Darüber hinaus können Sie über die Neu-Schaltfläche auch eigene Regelsätze für Netzwerke erstellen. Klicken Sie dazu im Regelsätze-Bereich auf die Neu-Schaltfläche und legen in dem erscheinenden Dialogfenster folgendes fest:

- **Regelsatzname**: Geben Sie hier einen aussagekräftigen Namen für den Regelsatz ein.
- **Einen leeren Regelsatz erzeugen**: Hier können Sie einen vollkommen leeren Regelsatz erzeugen und diesen ausschließlich mit selbstdefinierten Regeln bestücken.
- **Einen Regelsatz erzeugen, der einige sinnvolle Regeln enthält**: Bei dieser Auswahl können Sie entscheiden, ob beim neuen Regelsatz grundlegende Regeln für nichtvertrauenswürdige, vertrauenswürdige oder zu blockierende Netzwerke vordefiniert werden sollen. Auf Basis dieser Voreinstellungen können Sie dann individuelle Änderungen vornehmen.

Der neue Regelsatz erscheint nun im Regelsätze-Bereich unter dem jeweiligen Regelsatznamen (z.B. Neuer Regelsatz) in der Liste. Wenn Sie nun auf **Bearbeiten** klicken, öffnet sich - je nach Einstellung, die Sie unter **Sonstiges** (siehe gleichnamiges Kapitel) getroffen haben - der **Regelassistent** oder der **erweiterten Bearbeitungsmodus** zum Bearbeiten der einzelnen Regeln dieses Regelsatzes. Wie Sie in den Regelsätzen neue Regeln vergeben, lesen Sie in den Kapiteln **Regelassistent verwenden** bzw. **erweiterten Bearbeitungsmodus verwenden**.

> Neben der direkten Eingabe von Regeln haben Sie natürlich noch die Möglichkeit über die Info-Box des Firewall-Alarms Regeln zu erstellen. Dieser Lernprozess der Firewall wird Ihnen im Kapitel **Firewall-Alarm** erläutert.

Regel Assistenten verwenden

Mit dem Regelassistenten können Sie bestimmte zusätzliche Regeln für den jeweiligen Regelsatz definieren oder bestehende Regeln ändern. Gerade für Anwender, die sich nicht gut mit der Firewalltechnologie auskennen, ist der Regelassistent dem erweiterten Bearbeitungsmodus vorzuziehen.

> Mit dem Regelassistenten verändern Sie eine oder mehrere Regeln in dem jeweils ausgewählten Regelsatz. Sie erstellen also immer eine Regel innerhalb eines Regelsatzes, der verschiedene Regeln beinhaltet.
>
> Abhängig davon, welchen Regelsatz Sie für das jeweilige Netzwerk definiert haben, kann eine Anwendung in dem einen Regelsatz (z.B. für nicht vertrauenswürdige Netze) gesperrt sein, in dem anderen Regelsatz (z.B. für vertrauenswürdige Netze) vollen Netzzugriff haben. So könnten Sie z.B. einen Browser mit entsprechend unterschiedlichen Regeln so beschränken, dass er wohl auf Seiten zugreifen kann, die in ihrem Heimnetzwerk bereitstehen, aber keine Möglichkeit hat, auf Inhalte aus dem DFÜ-Netzwerk zuzugreifen.

Der Regelassistent stellt Ihnen folgende Basisregeln zur Verfügung:

- **Einer bestimmten Anwendung den Zugriff erlauben oder verweigern**: Hiermit können Sie gezielt eine Anwendung (ein Programm) auf Ihrer Festplatte auswählen und ihm explizit den Zugriff auf das über den Regelsatz definierte Netzwerk erlauben oder verbieten. Wählen Sie im Assistenten dazu einfach das gewünschte Programm aus (**Programmpfad**) und geben Sie dann unter **Verbindungsrichtung** an, ob das Programm für eingehende Verbindungen, ausgehende Verbindungen oder sowohl ein-, als auch ausgehende Verbindungen gesperrt werden soll. Auf diese Weise können Sie z.B. ihre MP3-Playersoftware ggf. daran hindern, Daten über Ihre Hörgewohnheiten weiterzugeben (ausgehende Verbindungen) oder dafür sorgen, dass nicht automatisch Programmupdates aufgespielt werden (eingehende Verbindungen).

- **Einen bestimmten Internet-Dienst (Port) öffnen oder sperren**: Als **Port** werden spezielle Adressbereiche bezeichnet, die über ein Netzwerk übermittelte Daten automatisch an ein bestimmtes Protokoll und darüber an bestimmte Software weiterleiten. So wird z.B. die Übermittlung von regulären Webseiten über den Port 80 abgewickelt, E-Mail-Versand über den Port 25, E-Mail-Abholung über Port 110 usw. Ohne Firewall stehen an Ihrem Computer generell alle Ports offen, obwohl die meisten von normalen Anwendern gar nicht benötigt werden. Über das Sperren eines oder mehrerer Ports können deshalb schnell Lücken geschlossen werden, die sonst von Hackern für Angriffe genutzt werden könnten. Im Assistenten haben Sie die Möglichkeit Ports komplett zu sperren oder aber auch nur für eine bestimme Anwendung (z.B. Ihre MP3-Abspielsoftware).
- **Datei- und Druckerfreigabe (NetBIOS) erlauben oder verweigern**: Das **NetBIOS** ist eine spezielle Schnittstelle in Netzwerken und kann dazu genutzt werden z.B. Datei- oder Druckerfreigaben direkt von Rechner zu Rechner durchzuführen, ohne dabei z.B. das TCP/IP-Protokoll zu nutzen. Da dies in Heimnetzwerken meistens unnötig ist und das NetBIOS von Hackern dazu genutzt werden kann, einen Rechner zu beeinflussen, ist es in vielen Fällen ratsam, diese Freigabe für nicht vertrauenswürdige Netze zu verweigern.
- **Domänen-Dienste erlauben oder verweigern**: Eine **Domäne** ist eine Art Gliederungsverzeichnis für Computer in einem Netzwerk und ermöglicht damit eine zentralisierte Verwaltung der im Netzwerk eingebunden Rechner. Freigaben für Domänen-Dienste in nicht vertrauenswürdigen Netzen sollten in der Regel verweigert werden.
- **Gemeinsame Nutzung der Internet-Verbindung erlauben**: Bei direkten Verbindungen mit dem Internet können Sie festlegen, ob alle Rechner im Netzwerk über einen mit dem Internet verbundenen Rechner Zugriff auf das Internet erhalten sollen oder nicht. Diese Internetverbindungsfreigabe (ICS) kann für ein Heimnetzwerk in der Regel aktiviert werden.
- **In den erweiterten Bearbeitungsmodus wechseln**: Hiermit können Sie vom Regelassistenten zum erweiterten Bearbeitungsmodus wechseln. Informationen zum erweiterten Bearbeitungsmodus erhalten Sie im Kapitel **erweiterten Bearbeitungsmodus verwenden**.

> Wenn Sie das Häkchen bei **Auch in Zukunft den Regelassistenten starten** entfernen, öffnet die Firewall für neue Regeln automatisch den erweiterten Bearbeitungsmodus.

Erweiterten Bearbeitungsmodus verwenden

Im erweiterten Bearbeitungsmodus können Sie - gewisse Kenntnisse in Netzwerksicherheit vorausgesetzt - sehr individuelle Regeln für das jeweilige Netzwerk definieren. Dabei können natürlich sämtliche Regeln erzeugt werden, die Sie auch über den Regelassistenten erzeugen können, aber auch darüber hinaus weitergehende Einstellungen vorgenommen werden. Folgende Einstellungsmöglichkeiten stehen Ihnen hier zur Verfügung:

- **Name**: Hier können Sie den Namen für den aktuellen Regelsatz gegebenenfalls verändern. Unter diesem Namen wird der Regelsatz dann in der Liste im **Regelsätze**-Bereich angezeigt und kann mit den dort von der Firewall identifizierten Netzwerken kombiniert werden.
- **Stealth-Modus**: Mit dem Stealth-Modus (engl.: verborgen, heimlich) werden Anfragen an den Computer, die dazu dienen, die Erreichbarkeit der jeweiligen Ports zu überprüfen nicht beantwortet. Dies erschwert Hackern, auf diese Weise Informationen über das System zu erhalten.
- **Aktion, falls keine Regel zutrifft**: Hier können Sie festlegen, ob der Zugriff im Netzwerk generell erlaubt, verweigert oder auf Nachfrage geregelt werden soll. Sollten durch die Lernfunktion der Firewall für einzelne Programme Sonderregeln definiert sein, werden diese natürlich berücksichtigt.
- **Adaptiv-Modus**: Der Adaptiv-Modus unterstützt Sie bei Anwendungen, die die sogenannte Rückkanal-Technik verwenden (z.B. FTP und viele Online-Spiele). Solche Anwendungen verbinden sich mit einem entfernten Rechner und handeln mit ihm einen Rückkanal aus auf dem sich der entfernten Rechner mit Ihrer Anwendung "zurückverbindet". Ist der Adaptiv-Modus aktiv, so erkennt die Firewall diesen Rückkanal und lässt ihn zu ohne gesondert nachzufragen.

Regeln

In der Liste der Regeln finden Sie sämtliche Regeln, die als Ausnahmetatbestände für diesen Regelsatz definiert wurden. So können hier z.B. ausgewählten Programmen umfangreiche Netzzugriffe gestattet werden, obgleich das Netzwerk an sich als nicht vertrauenswürdig definiert wird. Die Regeln, die hier einfließen, können auf verschiedene Weise erzeugt worden sein:

- Über den **Regelassistenten**
- Direkt über den **erweiterten Bearbeitungsmodus** über die Neu-Schaltfläche
- Über den Dialog in der Info-Box, die bei einem Firewall-Alarm erscheint.

Jeder Regelsatz hat natürlich eine eigene Liste mit Regeln.

> Da die Firewall-Regeln teilweise hierarchisch verschachtelt sind, ist es in manchen Fällen wichtig, die Rangfolge bei den Regeln zu beachten. So kann es sein, dass eine Freigabe für einen Port durch die Verweigerung eines Protokollzugriffs wieder blockiert werden kann. Sie können den Rang einer Regel in der Abfolge ändern, indem Sie diese mit der Maus markieren und dann über die Pfeiltasten unter **Rang** in der Liste hinauf- oder hinab bewegen.

Wenn Sie eine neue Regel über den erweiterten Bearbeitungsmodus erstellen oder eine bestehende Regel über den Bearbeiten-Dialog verändern, erscheint der **Regel bearbeiten** Dialog mit folgenden Einstellungsmöglichkeiten:

- **Name**: Hier findet sich bei voreingestellten und automatisch generierten Regeln der Programmname für den die jeweilige Regel zutrifft. Sie können den Namen über die Schaltfläche **Bearbeiten** auch jederzeit verändern oder um zusätzliche Informationen ergänzen.
- **Regel aktiv**: Sie können eine Regel durch Entfernen des Häkchens inaktiv setzen, ohne sie gleich zu löschen.
- **Kommentar**: Hier erfahren Sie, auf welche Weise die Regel erzeugt wurde. Bei für den Regelsatz voreingestellten Regeln steht **Voreingestellte Regel**, bei Regeln, die sich aus dem Dialog aus dem **Firewall-Alarm** ergeben steht **per Nachfrage generiert** und für Regeln, die Sie selber über den erweiterten Bearbeitungsmodus generieren, können Sie einen eigenen Kommentar einfügen.
- **Verbindungs-Richtung**: Mit der **Richtung** wird definiert, ob es sich bei dieser Regel um eine Regel für eingehende, ausgehende oder ein- und ausgehende Verbindungen handelt.
- **Zugriff**: Hier wird eingestellt, ob für das jeweilige Programm innerhalb dieses Regelsatzes der Zugriff erlaubt oder verweigert werden soll.
- **Protokoll**: Hier können Sie auswählen, welchen Verbindungsprotokollen Sie einen Zugriff erlauben oder verwehren wollen. Dabei haben Sie die Möglichkeit, Protokolle generell zu sperren oder freizugeben oder die Verwendung des Protokolls mit der Nutzung einer bestimmten Anwendung oder mehrerer Anwendungen zu koppeln (Anwendungen zuordnen). Genauso können Sie die unerwünschten bzw. erwünschten Ports über die Schaltfläche **Internet-Dienst zuordnen** genau definieren.
- **Zeitfenster**: Sie können den Zugriff auf Netzwerkressourcen auch zeitabhängig gestalten und so z.B. dafür sorgen, dass ein Zugriff nur zu Ihren Arbeitszeiten und nicht außerhalb dieser Zeiten erfolgt.
- **IP-Adressraum**: Gerade für Netzwerke mit fest vergebenen IP-Adressen macht es Sinn, deren Nutzung über eine Beschränkung des IP-Adressraumes zu reglementieren. Ein klar definierter IP-Adressraum verringert die Gefahr eines Hackerangriffs deutlich.

Firewall-Alarm

Generell fragt die Firewall im Modus **manuelle Regelerstellung** bei unbekannten Programmen und Prozessen, die mit dem Netzwerk in Verbindung treten wollen, nach, ob dies erlaubt oder verweigert werden soll. Dazu öffnet sich eine Info-Box, in der Ihnen Details zur jeweiligen Anwendung geliefert werden. Hier haben Sie auch die Möglichkeit, der Anwendung einen Zugriff auf das Netzwerk einmal oder auch dauerhaft zu erlauben oder zu verweigern. Sobald Sie einem Programm den Zugriff dauerhaft erlauben oder verweigern, wird dies als **Regel** in den **Regelsatz** des jeweiligen Netzwerkes aufgenommen und von nun an nicht mehr nachgefragt.

Hier stehen Ihnen folgende Schaltflächen zur Verfügung:

- **Immer erlauben**: Über diese Schaltfläche erstellen Sie für die oben aufgeführte Anwendung (z.B. Opera.exe oder Explorer.exe oder iTunes.exe) eine Regel, die in dem genannten Netzwerk der Anwendung einen dauerhaften Zugriff aufs Netzwerk bzw. Internet erlaubt. Diese Regel finden Sie dann auch als auf Nachfrage erzeugte Regel im Bereich **Regelsätze**.
- **Temporär erlauben**: Über diese Schaltfläche erlauben Sie der jeweiligen Anwendung nur ein einziges Mal Zugriff aufs Netzwerk. Beim nächsten Versuch eines Netzwerkzugriffs durch dieses Programm fragt die Firewall erneut nach.
- **Immer verweigern**: Über diese Schaltfläche erstellen Sie für die oben aufgeführte Anwendung (z.B. dialer.exe oder spam.exe oder trojan.exe) eine Regel, die in dem genannten Netzwerk der Anwendung einen dauerhaften Zugriff aufs Netzwerk bzw. Internet verweigert. Diese Regel finden Sie dann auch als auf Nachfrage erzeugte Regel im Bereich **Regelsätze**.
- **Temporär verweigern**: Über diese Schaltfläche verbieten Sie der jeweiligen Anwendung nur ein einziges Mal den Zugriff aufs Netzwerk. Beim nächsten Versuch eines Netzwerkzugriffs durch dieses Programm fragt die Firewall erneut nach.

Des Weiteren erhalten Sie Informationen zu **Protokoll**, **Port** und **IP-Adresse** mit der die jeweilige Anwendung interagieren möchte.

12.4 Protokoll

Im Protokoll-Bereich werden alle von der Firewall erlaubten und blockierten Verbindungen mit Netzwerk und Internet protokolliert. Sie können diese Liste durch Anklicken der jeweiligen Spaltenüberschriften beliebig sortieren und mit Anklicken der Details-Schaltfläche zu einzelnen Verbindungen weitergehende Informationen erhalten.

13 Kindersicherung-Bedienung

Mit der Kindersicherung können Sie das Surfverhalten und die Nutzung des Computers für Ihre Kinder regeln. Die Bedienung der Kindersicherung ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Karteikarten, die Sie über die links angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen Programmbereich und können dort Aktionen durchführen, Voreinstellungen vornehmen oder Vorgänge überprüfen.

> Die Kindersicherung wird bei einer Standardinstallation der G Data Software nicht mit installiert. Sie können Sie jedoch jederzeit über ein angepasstes Setup (siehe Kapitel **Installation**) auch nachträglich installieren.

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

Testen: Hier können Sie als Administrator überprüfen, ob Ihre Einschränkungen für bestimmte Benutzer den gewünschten Effekt haben. Im **Test-Modus** können Sie probeweise mit Ihrem Internetbrowser Seiten anwählen, die gesperrt sein müssten und sich so von der Korrektheit der Einstellungen überzeugen.

Einstellungen: Hier können Sie grundlegende Einstellungen zum Betrieb der Kindersicherung verändern und an individuelle Bedürfnisse anpassen.

13.1 Status

Im Status-Bereich können Sie als Administrator unter **Benutzer** den Benutzer auswählen, für den Sie Änderungen und Einstellungen vornehmen möchten, außerdem können Sie hier neue Benutzer anlegen.

> Benutzer, für die auf Ihrem Computer ein **Windows-Benutzerprofil** besteht, können Sie unter **Benutzer** direkt auswählen. Um hier Einstellungen zu verändern, wählen Sie einfach den gewünschten Benutzer aus und klicken dann auf die Bearbeiten-Schaltfläche.

Neuen Benutzer anlegen

Klicken Sie auf die Schaltfläche **Neuer Benutzer**. Es öffnet sich eine Dialogbox, in der Sie den Benutzernamen und das Passwort für diesen Benutzer eingeben können.

Ein **Passwort** sollte im Hinblick auf Sicherheitsaspekte mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben, sowie Zahlen enthalten.

Nun erscheint unter **Benutzer** der neu angelegte Benutzername, gleichzeitig wird ein **Windows-Benutzerkonto** für diesen Benutzer angelegt. Das bedeutet, dass die Kindersicherung automatisch für die Person mit den jeweiligen Einstellungen aktiv ist, die sich mit ihrem Benutzernamen beim Start von Windows anmeldet. Führen Sie jetzt einen Doppelklick mit der Maus auf den Einstellungsbereich aus, der für diesen Benutzer eingestellt werden soll, also z.B. die Unterbindung **Verbotener Inhalte** oder die ausschließliche Bereitstellung **Erlaubter Inhalte** oder legen Sie fest, ob für diesen Benutzer die **Internetnutzungszeit** oder **Computernutzungszeit** überwacht werden soll.

Verbotene Inhalte

In diesem Bereich wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet blockieren können. Wählen Sie dazu die gewünschten Kategorien, die geblockt werden sollen durch Setzen eines Häkchens aus. Klicken Sie nun auf OK und die Internetseiten, die den **Blockierkriterien** entsprechen sind damit gesperrt.

> Wenn Sie die Neu-Schaltfläche anklicken, öffnet sich ein Dialogfenster, in dem Sie eigene **Blockierkriterien** (auch **Blacklists** genannt) definieren können. Definieren Sie dazu erst den Namen und ggf. einen Informationstext zum individuell erzeugten Filter.

Wenn Sie nun auf OK klicken, öffnet sich ein weiteres Fenster, indem Sie Inhalte zusammenfassen können, die durch diesen Filter unterdrückt werden sollen. Geben Sie dazu unter **Filter** einen Begriff ein, der blockiert werden soll und unter **Ort der Suche** den Bereich einer Webseite, in dem danach gesucht werden soll.

Hier haben Sie folgende Auswahlmöglichkeiten:

- **URL**: Wenn Sie das Häkchen hier setzen, wird der zu blockierende Text in der **Webadresse** gesucht. Wenn Sie z.B. Seiten unterbinden wollen, die z.B. www.chatcity.no; www.crazychat.co.uk o.ä. lauten, reicht es, wenn Sie als Filter chat eingeben, das Häkchen bei **URL** setzen und dann auf die **Hinzufügen**-Schaltfläche klicken. Es werden nun alle Seiten blockiert, die im **Domain-Namen**, also der **Internetadresse** irgendwie die Buchstabenfolge chat verwenden.
- **Titel**: Wenn Sie das Häkchen hier setzen, wird der zu blockierende Text im Titel der Webseite gesucht. Dies ist der Bereich, den Sie z.B. sehen, wenn Sie eine Seite in Ihrer **Favoritenliste** als **Lesezeichen bookmarken** möchten. Wenn Sie Seiten unterbinden wollen, die z.B. Chat City Detroit; Teenage Chat 2005 o.ä. lauten, reicht es, wenn Sie als Filter chat eingeben, das Häkchen bei **Titel** setzen und dann auf die **Hinzufügen**-Schaltfläche klicken. Es werden nun alle Seiten blockiert, die im Titel irgendwie die Buchstabenfolge chat verwenden.
- **Meta**: Die sogenannten **Metatags** sind verborgene Texteinträge auf Webseiten, die dazu dienen, diese in **Suchmaschinen** sinnvoller oder einfach auch nur häufiger zu listen. Suchbegriffe wie sex oder chat werden hier gerne verwendet, um die Seitenzugriffe zu erhöhen. Wenn Sie Seiten unterbinden wollen, die im Metatag irgendwo chat stehen haben, reicht es, wenn Sie als Filter chat eingeben, das Häkchen bei **Meta** setzen und dann auf die **Hinzufügen**-Schaltfläche klicken. Es werden nun alle Seiten blockiert, die in den Metatags irgendwie die Buchstabenfolge chat verwenden.
- **Im gesamten Text**: Wenn Sie den lesbaren Inhalt einer Seite direkt auf zu blockierende Inhalte überprüfen möchten, geben Sie einfach den zu blockierenden Begriff - z.B. ***chat*** - ein, setzen das Häkchen bei Im gesamten Text und dann auf die Schaltfläche **Hinzufügen** klicken. Es werden nun alle Seiten blockiert, die im angezeigten Seitentext irgendwie die Buchstabenfolge ***chat*** enthalten.

Natürlich kann es passieren, dass durch zu allgemein gehaltene **Filterbegriffe** auch Seiten blockiert werden, die an sich harmlos sind. So würde z.B. ein gesperrter Begriff wie cash auch dazu führen, dass Einträge über Cashew-Kerne gesperrt wären.

> Sie können spezielle Seiten, die aus Versehen in den Filterbereich fallen, aber durch die **Ausnahmen**-Funktion explizit wieder freischalten. Klicken Sie dazu einfach auf die **Ausnahme**-Schaltfläche und geben in dem dortigen Filter z.B. cashew als Ausnahme an.
>
> Selbst erstellte Filter können Sie im Bereich **Eigene Filter** beliebig bearbeiten und ggf. auch löschen. Lesen Sie hierzu das Kapitel **Eigene Filter**.

Erlaubte Inhalte

Über diesen Bereich wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet erlauben können. Wählen Sie dazu die gewünschten Kategorien, die erlaubt werden sollen durch Setzen eines Häkchens aus. Klicken Sie nun auf OK und die Internetseiten, die den gewünschten Kriterien entsprechen sind damit erlaubt.

> Wenn Sie die Neu-Schaltfläche anklicken, öffnet sich ein Dialogfenster, in dem Sie eigene zu erlaubende Inhalte (auch **Whitelists** genannt) definieren können. Definieren Sie dazu erst den Namen und ggf. einen Informationstext zum individuell erzeugten Filter.

Klicken Sie nun auf **OK**. Es öffnet sich ein Dialog, in dem Sie die Whitelist mit Webseiten füllen können, die z.B. kindgerecht sind. Geben Sie dazu unter **Filter** ein, welche **Domain-Namensbestandteile** erlaubt sein sollen. Wenn Sie z.B. eine Webseite mit kinderfreundlichen Inhalten freigeben wollen, können Sie hier z.B. www.elefanti.de eingeben und erlauben damit den Zugriff auf diese Webseite. Geben Sie nun unter **Beschreibung** ein, was auf dieser Webseite zu finden ist, z.B. eben Elefanti - Kinderfreundliche Webseite und geben Sie unter **Link zum Angebot** die genaue Web-Adresse des Seite an. Die Beschreibung und der Link zum Angebot werden dann wichtig, wenn Ihr Kind z.B. tatsächlich mal eine Seite aufruft, die Sie nicht erlaubt haben. Statt einer Fehlermeldung erscheint dann nämlich eine HTML-Seite im Browser, die alle hier in der Whitelist eingegebenen Webseiten inklusive Beschreibung auflistet. So kann Ihr Kind direkt wieder auf die Seiten zugreifen, die ihm erlaubt sind. Wenn alle Eingaben erfolgt sind, klicken Sie auf **Hinzufügen** und die Whitelist wird um diese Angaben ergänzt.

> Der **Filter** sucht Segmente im Domain-Namen. Je nach Angabe im Filter können sich die Ergebnisse also voneinander unterscheiden. Weitere oder engere Einschränkungen sind hier je nach Webseite hilfreich.

Internetnutzungszeit überwachen

Hier können Sie festlegen, wie lange und zu welchen Zeiten der gewählte Benutzer Internetzugriff hat. Setzen Sie dazu das Häkchen bei **Internetnutzungszeit überwachen**. Nun können Sie festlegen, wie lange der Benutzer im Monat insgesamt ins Internet darf, wie lange pro Woche und wie viele Stunden zu bestimmten Wochentagen. So können z.B. die Wochenenden für schulpflichtige Kinder anders gehandhabt werden, als die Werktage. Sie können die entsprechenden Zeiträume dazu einfach unter **Tage/hh:mm** eingeben, wobei z.B. die Angabe **04/20:05** eine Internetnutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten ergäbe.

> Im Zusammenspiel der Angaben zur Internetnutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, beschränkt die Software die Internetnutzung für den Benutzer automatisch auf vier Tage.

Wenn der jeweilige Benutzer versucht, über das erlaubte Zeitkontingent hinaus auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er sein Zeitkontingent überschritten hat.

Zeiten sperren

Über die Schaltfläche **Zeiten sperren** können Sie ein Dialogfeld aufrufen, in dem Sie - zusätzlich zur mengenmäßigen Eingrenzung der Internetnutzung - spezielle Zeiträume in der Woche kategorisch sperren können. Gesperrte Zeiträume sind dabei rot dargestellt, freigegebene Zeiträume in grün. Um einen Zeitraum freizugeben oder zu sperren, markieren Sie diesen einfach mit der Maus. Dann erscheint neben dem Mauszeiger ein Kontextmenü, in dem Sie zwei Möglichkeiten haben: **Zeit freigeben** und **Zeit sperren**. Wenn der jeweilige Benutzer versucht, während der gesperrten Zeiten auf das Internet zuzugreifen, erscheint im Browser ein Info-Bildschirm, der ihn darüber informiert, dass er zu diesem Zeitpunkt keinen Zugriff auf das Internet hat.

Computernutzungszeit überwachen

Hier können Sie festlegen, wie lange und zu welchen Zeiten der gewählte Benutzer den Computer verwenden darf. Setzen Sie dazu das Häkchen bei **Computernutzungszeit überwachen**. Nun können Sie festlegen, wie lange der Benutzer im Monat insgesamt den Computer nutzen darf, wie lange pro Woche und wie viele Stunden zu bestimmten Wochentagen. So können z.B. die Wochenenden für schulpflichtige Kinder anders gehandhabt werden, als die Werktage. Sie können die entsprechenden Zeiträume dazu einfach unter **Tage/hh:mm** eingeben, wobei z.B. die Angabe **04/20:05** eine Computernutzungszeit von 4 Tagen, 20 Stunden und 5 Minuten ergäbe. Über die Schaltfläche **Warnmeldung vor Ablaufen der Zeit anzeigen** können Sie einen Benutzer kurz bevor der Computer automatisch heruntergefahren wird, informieren, damit dieser noch seine Daten sichern kann. Wird der Computer ohne Warnmeldung heruntergefahren, kann es sonst zu Datenverlusten führen.

Im Zusammenspiel der Angaben zur Computernutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, deckelt die Software die Computernutzung für den Benutzer automatisch auf vier Tage.

13.2 Eigene Filter

In diesem Bereich können Sie Ihre selbst erstellten Whitelists (also erlaubte Inhalte) und Blacklists (also verbotene Inhalte) verändern und auch komplett neue Listen manuell anlegen.

Die folgenden Listentypen unterscheiden sich grundlegend voneinander:

- **Whitelist**: Wenn Sie für einen der oben ausgewählten Benutzer eine Whitelist auswählen, kann dieser ausschließlich Webseiten ansehen, die sich auf dieser Whitelist befinden. Im Bereich **Stammdaten** können Sie als Administrator diese Whitelist nach eigenen Wünschen gestalten oder aus vorgegebenen Whitelists die passende Liste für einen Benutzer auswählen. Eine Whitelist eignet sich besonders dafür, jüngeren Kindern einen sehr begrenzten Zugriff aufs Internet zu erlauben, ihnen also die Möglichkeit zu geben, Webseiten mit pädagogisch empfehlenswerten Inhalten zu nutzen, aber nichts darüber hinaus.
- **Blacklist**: Mit einer Blacklist können Sie ausgewählte Webseiten für einen Benutzer sperren. Ansonsten besteht für den Benutzer freier Zugang zum Internet. Beachten Sie, dass Sie über diese Funktion zwar spezielle Seiten sperren können, gleichartige Inhalte aber auch auf anderen Webseiten zur Verfügung stehen können. Eine Blacklist von Internet-Adressen ist in dieser Hinsicht nie ein vollkommener Schutz vor unerwünschten Inhalten.

Sie können nicht gleichzeitig eine Whitelist zusammen mit einer Blacklist betreiben, da eine Whitelist an sich schon größtmögliche Zugangsbeschränkungen ermöglicht.

Folgende Schaltflächen ermöglichen Ihnen die Bearbeitung der Ausschlusslisten:

- Löschen: Über die Funktion **Löschen** können Sie mit der Maus ausgewählte Listen einfach löschen.
- Neu: Hiermit können Sie eine komplett neue Blacklist oder Whitelist anlegen. Die Vorgehensweise ist dabei dieselbe, wie Sie in den Kapitel Verbotene Inhalte und Erlaubte Inhalte beschrieben wird.
- Bearbeiten: Hiermit können Sie eine bestehende Liste inhaltlich verändern.

13.3 Protokolle

Im Protokoll-Bereich haben Sie als Administrator eine Übersicht über sämtliche Versuche von anderen Benutzern, geblockte Inhalte aufzurufen. Oben können Sie dazu aus der Liste den Benutzer auswählen, dessen Protokoll Sie sich anzeigen lassen möchten.

Sie können diese Protokolle über die Schaltfläche **Protokolle löschen** natürlich auch löschen.

Einstellungen: Über diese Schaltfläche können Sie grundlegende Einstellungen für die Informationen im Protokoll-Bereich verändern. So können Sie festlegen, ob Verstöße gegen erlaubte und/oder verbotene Inhalte protokolliert werden sollen oder nicht. Wenn die Inhalte protokolliert werden, können Sie die Protokolle der unterschiedlichen Benutzer im Protokoll-Bereich einsehen.

Da Protokolldateien bei regelmäßiger Nutzung sehr groß werden, können Sie sich von der Kindersicherung unter **Meldung anzeigen wenn Datei ____ KB erreicht** daran erinnern lassen, dass die Protokolldatei eine gewisse Größe überschritten hat und diese dann im Protokoll-Bereich unter **Protokolle löschen** von Hand löschen.

14 BootScan

Der **BootScan** hilft Ihnen dabei, Viren zu bekämpfen, die sich vor der Installation der Antivirensoftware auf Ihrem Rechner eingenistet haben und möglicherweise die Installation der G Data Software unterbinden möchten. Dazu gibt es eine spezielle Programmversion der Software, die schon vor dem Start von Windows ausgeführt werden kann.

Was versteht man unter Bootvorgang? Wenn Sie ihren Computer anschalten, startet normalerweise automatisch Ihr Windows-Betriebssystem. Dieser Vorgang nennt sich **Booten**. Es gibt aber auch die Möglichkeit, andere Programme anstelle Ihres Windows-Betriebssystems automatisch zu starten. Um Ihren Rechner schon vor dem Start von Windows auf Viren zu überprüfen, stellt G Data Ihnen zusätzlich zu der Windows-Version noch eine bootfähige Spezialversion zur Verfügung.

Wie breche ich einen BootScan ab? Wenn Ihr Rechner nach einem Neustart einmal nicht die gewohnte Windows-Umgebung anzeigen sollte, sondern eine spezielle Oberfläche der G Data Software, dann ist das kein Grund zur Sorge. Sollten Sie keinen BootScan geplant haben, wählen Sie einfach mit den Pfeiltasten den Eintrag **Microsoft Windows** aus und klicken dann auf **Return**. Nun startet Ihr Windows ganz normal ohne vorherigen BootScan.

Wenn Sie einen **BootScan** durchführen möchten, gehen Sie bitte folgendermaßen vor:

1a **BootScan mit der Programm-CD**: Legen Sie die G Data **CD** in das Laufwerk. Klicken Sie auf dem sich öffnenden Startfenster auf **Abbrechen** und schalten Sie den Computer aus.

1b **BootScan mit G Data Software, die Sie aus dem Internet heruntergeladen haben**: Sie brennen sich über den Eintrag **G Data BootCD erstellen** in der **G Data Programmgruppe** eine eigene BootCD. Legen Sie Ihre selbstgebrannte BootCD in das Laufwerk. Klicken Sie auf dem sich öffnenden Startfenster auf **Abbrechen** und schalten Sie den Computer aus.

Wenn Sie **Windows XP** verwenden, kann es passieren, dass Sie beim Versuch, eine BootCD zu erstellen, eine Meldung erhalten, dass **IMAPI 2.x** nicht installiert ist. Hierbei handelt es sich um ein Update von Microsoft für ältere Betriebssysteme, das zum Brennen von Datenträgern notwendig ist. Sie können das notwendige Update direkt auf der Microsoft-Homepage herunterladen und installieren.

Nach dem ersten Schritt verläuft der BootScan für alle Varianten identisch:

2 Starten Sie den Computer neu. Es erscheint das Startmenü des G Data **BootScans**.

3 Wählen Sie mit den Pfeiltasten die Option G Data **BootCD** und bestätigen die Auswahl mit **Enter**. Es wird nun ein Linux-Betriebssystem von der CD gestartet und es erscheint eine G Data **Spezialversion** für BootScans.

Falls Sie Probleme mit der Ansicht der Programmoberfläche haben, starten Sie den Rechner erneut und wählen bitte die Option G Data **BootCD – Alternativ** aus.

4 Das Programm schlägt nun vor, die Virensignaturen zu aktualisieren.

Wenn Sie eine G Data Software-Version verwenden, die Backup-Funktionen unterstützt, haben Sie hier zusätzlich die Möglichkeit, hier direkt das Zurückspielen von Backups Ihrer gesicherten Daten zu starten.

5 Klicken Sie hier auf **Ja**. Um das Update durchführen zu können, müssen Sie entweder Ihre bereits erhaltenen Zugangsdaten oder Ihre Registriernummer eingeben. Danach können Sie das Update durchführen. Sobald die Daten über das Internet aktualisiert wurden, erscheint die Meldung **Update erledigt**. Verlassen Sie nun den Update-Bildschirm mit Anklicken der **Schließen**-Schaltfläche.

Das automatische **Internet Update** steht Ihnen dann zur Verfügung, wenn Sie einen **Router** verwenden, der IP-Adressen automatisch vergibt (**DHCP**). Sollte das Internet Update nicht möglich sein, können Sie den **BootScan** auch mit alten Virensignaturen durchführen. Dann sollten Sie allerdings nach der Installation der G Data Software möglichst bald einen neuen BootScan mit aktualisierten Daten durchführen.

6 Nun sehen Sie die Programmoberfläche. Klicken Sie auf den Eintrag **Überprüfe Computer** und Ihr Computer wird nun auf Viren und Schadsoftware untersucht. Dieser Vorgang kann je nach Rechnertyp und Festplattengröße eine Stunde oder länger dauern.

7 Sollte die G Data Software Viren finden, entfernen Sie die bitte mit Hilfe der im Programm vorgeschlagenen Option. Nach einer erfolgreichen Entfernung des Virus steht Ihnen die Originaldatei weiter zur Verfügung.

8 Nach Abschluss der Virenüberprüfung verlassen Sie nun bitte das System, in dem Sie auf das kleine x (oben rechts im Fenster) klicken.

9 Entfernen Sie die G Data Software **CD** aus dem Laufwerk, sobald sich die Lade Ihres Laufwerks öffnet.

10 Schalten Sie ihren Computer wieder aus und starten Sie ihn erneut. Nun startet Ihr Computer wieder mit Ihrem Standard-Windows-Betriebssystem und es ist gewährleistet, dass Sie die reguläre G Data Software auf einem virenfreien System installieren können.

Sollte Ihr Computer nicht von CD/DVD-ROM booten, kann es sein, dass Sie diese Option erst einstellen müssen. Führen Sie hierzu bitte folgende Schritte durch:

1. Schalten Sie Ihren Computer aus.
2. Starten Sie Ihren Computer wieder. Üblicherweise gelangen Sie zum BIOS-Setup, indem Sie beim Hochfahren (= Booten) des Rechners die **Entf**-Taste (manchmal auch die Taste **F2** oder **F10**) drücken.
3. Wie Sie die Einstellungen in Ihrem BIOS-Setup im Einzelnen ändern, ist von Computer zu Computer unterschiedlich. Lesen Sie bitte in der Dokumentation Ihres Computers. Im Ergebnis sollte die Bootreihenfolge **CD/DVD-ROM:, C:** lauten, d.h. das CD/DVD-ROM-Laufwerk wird zum **1st Boot Device** und die Festplatten-Partition mit Ihrem Windows-Betriebssystem zum **2nd Boot Device**.
4. Speichern Sie die Änderungen und starten Sie Ihren Computer neu. Jetzt ist Ihr Computer bereit für einen BootScan.

15 Wissenswertes

Hier erhalten Sie Informationen zu wichtigen Programmfunktionen der Software.

15.1 G Data Symbol

Ihre G Data Software schützt Ihren Rechner permanent vor Viren und Schadsoftware. Damit Sie sehen, dass der Schutz aktiv ist, wird in der Taskleiste unten neben der Uhr ein Symbol eingeblendet.

Dieses G Data Symbol zeigt Ihnen an, dass alles in Ordnung ist und der Schutz auf Ihrem Computer aktiv ist.

Falls der Wächter abgeschaltet wurde oder andere Probleme vorliegen, zeigt das G Data Symbol einen Warnhinweis. Sie sollten dann möglichst bald die G Data Software starten und die Einstellungen überprüfen.

Wenn die G Data Software einen Download von Daten aus dem Internet durchführt, zeigt Sie dieses auch durch ein spezielles Symbol an.

Wenn Sie das Symbol mit der rechten Maustaste anklicken, erscheint ein Kontextmenü, mit dem Sie grundlegende Sicherheitsaspekte der Software steuern können.

Folgende Funktionen stehen Ihnen hier zur Verfügung:

- **G Data Software starten**: Hiermit rufen Sie das **SecurityCenter** auf und können dort z.B. die Einstellungen für den Virenwächter vornehmen. Was Sie im SecurityCenter tun können, lesen Sie im Kapitel: **SecurityCenter**
- **Wächter ausschalten**: Hiermit können Sie den **Virenwächter** bei Bedarf abschalten und auch wieder einschalten. Dies kann z.B. dann sinnvoll sein, wenn Sie auf Ihrer Festplatte große Dateimengen von einem Ort zum anderen kopieren oder speicherplatzintensive Rechenvorgängen (z.B. DVDs kopieren o.ä.) ablaufen lassen. Sie sollten den Virenwächter nur so lange abschalten, wie es unbedingt nötig ist und darauf achten, dass das System während dieses Zeitraums möglichst nicht mit dem Internet verbunden ist oder auf neue ungeprüfte Daten (z.B. über CDs, DVDs, Speicherkarten oder USB-Sticks) zugreifen kann.
- **Firewall ausschalten**: Sollten Sie eine Version der G Data Software mit integrierter Firewall verwenden, können Sie die **Firewall** über das Kontextmenü bei Bedarf auch abschalten. Ihr Computer ist dann weiterhin mit dem Internet und anderen Netzwerken verbunden, wird von der Firewall aber nicht mehr vor Angriffen oder Spionage-Attacken geschützt.
- **Autopilot ausschalten**: Der **Autopilot** ist ein Teil der **Firewall** und entscheidet ganz selbstständig, welche Anfragen und Kontakte Ihr Rechner übers Netzwerk oder Internet annehmen soll oder nicht. Für eine normale Nutzung ist der Autopilot optimal und sie sollten Ihn immer eingeschaltet lassen. Wie die Firewall steht der Autopilot in ausgewählten Versionen der G Data Software zur Verfügung.
- **Viren-Update**: Eine Antivirensoftware sollte immer auf dem neuesten Stand sein. Die Aktualisierung der Daten können Sie von der Software natürlich automatisch durchführen lassen. Sollten Sie jedoch unverzüglich eine Aktualisierung benötigen, können Sie diese über die Schaltfläche **Virenupdate** starten. Wozu ein Virenupdate nötig ist, lesen Sie im Kapitel: **Updates**
- **Statistik**: Hier können Sie sich eine Statistik über die Prüfvorgänge des Virenwächters anzeigen lassen, aber auch Informationen zu Leerlauf-Scans, Meldungen des Webfilters und weiteren Parametern erhalten.

15.2 Virenprüfung

Mit der Virenprüfung überprüfen Sie Ihren Computer auf den Befall mit schädlicher Software. Wenn Sie die Virenprüfung starten, kontrolliert diese jede Datei auf Ihrem Rechner darauf, ob sie andere Dateien infizieren kann oder selbst schon infiziert ist. Sollten bei einer Virenprüfung Viren oder andere Schadsoftware gefunden werden, dann gibt es unterschiedliche Möglichkeiten, wie der Virus entfernt oder unschädlich gemacht werden kann.

1 Starten Sie die Virenprüfung. Wie das geht, lesen Sie im Kapitel: **Virenschutz**

2 Nun erfolgt eine Überprüfung Ihres Rechners auf Virenbefall. Dazu öffnet sich ein Fenster, in dem Sie Informationen zum Status der Überprüfung erhalten.

Ein Fortschrittsbalken im oberen Bereich des Fensters zeigt Ihnen, wie weit die Überprüfung Ihres System schon vorangekommen ist. Schon während der Virenprüfung haben Sie unterschiedliche Möglichkeiten, Einfluss auf den Verlauf der Virenprüfung zu nehmen:

- **Bei Systemlast die Virenprüfung pausieren**: Über dieses Auswahlfeld können Sie festlegen, dass die Software so lange mit der Virenprüfung wartet, bis Sie andere Tätigkeiten am Computer abgeschlossen haben.
- **Rechner nach der Virenprüfung ausschalten**: Wenn Sie die Virenprüfung über Nacht oder nach Dienstschluss laufen lassen möchten, ist diese Funktion sehr praktisch. Sobald die Virenprüfung von der G Data Software beendet wurde, wird Ihr Computer heruntergefahren.
- **Passwortgeschützte Archive**: Solange ein Archiv passwortgeschützt ist, kann die G Data Software die Dateien dieses Archives nicht überprüfen. Wenn Sie das Häkchen hier setzen, informiert die Antivirensoftware Sie darüber, welche passwortgeschützten Archive sie nicht überprüfen konnte. Solange diese Archive nicht entpackt werden, stellt ein darin enthaltener Virus auch kein Sicherheitsrisiko für Ihr System dar.
- **Zugriff verweigert**: Generell gibt es unter Windows Dateien, die von Anwendungen exklusiv verwendet werden und deshalb nicht überprüft werden können, solange diese Anwendungen laufen. Am besten sollten Sie deshalb während einer Virenprüfung keine anderen Programme auf Ihrem System laufen lassen. Wenn Sie hier ein Häkchen setzen, werden Ihnen die nicht überprüften Daten angezeigt.

3a Falls Ihr System virenfrei ist, können Sie nach Abschluss der Überprüfung das Assistentenfenster über die Schaltfläche **Schließen** verlassen.

Ihr System wurde nun auf Viren überprüft und ist virenfrei.

3b Für den Fall, dass Viren und andere Schadprogramme gefunden wurden, haben Sie nun die Möglichkeit zu entscheiden, wie Sie mit den Virenfunden verfahren wollen. Im Regelfall reicht es nun, auf die Schaltfläche **Aktionen ausführen** zu klicken.

Die G Data Software verwendet nun eine Standardeinstellung (*sofern Sie dies in den Einstellungen unter **AntiVirus > Manuelle Virenprüfung für infizierte Dateien und Archive** nicht anders konfiguriert haben*) und desinfiziert die befallenen Dateien, d.h. sie repariert diese, so dass diese ohne Einschränkungen wieder benutzt werden können und nicht mehr gefährlich für Ihren Computer sind.

Sollte eine Desinfektion nicht möglich sein, wird die Datei unter Quarantäne gestellt, d.h. sie wird verschlüsselt in einen extra gesicherten Ordner verschoben, in dem sie keinen Schaden mehr anrichten kann.

Sollten Sie diese infizierte Datei noch benötigen, können Sie sie im Ausnahmefall auch wieder aus dem Quarantäne-Bereich herausholen und verwenden.

Ihr System wurde nun auf Viren überprüft und ist virenfrei.

3c Wenn Ihnen die infizierten Dateien/Objekte bekannt sind und Sie unterscheiden können, welche davon vielleicht nicht mehr benötigt werden, haben Sie auch die Möglichkeit, sehr individuell auf jeden einzelnen Virenfund zu reagieren.

In der Auflistung der Virenfunde können Sie nämlich in der Spalte **Aktion** für jede infizierte Datei einzeln definieren, was mit ihr geschehen soll.

- **Nur protokollieren**: In der **Protokolle**-Ansicht wird die Infektion aufgelistet. Eine Reparatur oder Löschung der betroffenen Dateien findet jedoch nicht statt. **Achtung: Wenn ein Virus nur protokolliert wird, ist er weiterhin aktiv und gefährlich.**
- **Desinfizieren (wenn nicht möglich: nur protokollieren)**: Hier wird versucht, den Virus aus einer befallenen Datei zu entfernen, falls das nicht möglich ist, ohne die Datei zu beschädigen, wird der Virus protokolliert und Sie können sich später über den Protokolleintrag damit beschäftigen. **Achtung: Wenn ein Virus nur protokolliert wird, ist er weiterhin aktiv und gefährlich.**
- **Desinfizieren (wenn nicht möglich: in Quarantäne)**: Dies ist die Standardeinstellung. Hier wird versucht, den Virus aus einer befallenen Datei zu entfernen, falls das nicht möglich ist, ohne die Datei zu beschädigen, wird die Datei in die **Quarantäne** verschoben. Lesen Sie hierzu bitte auch das Kapitel: **Wie funktioniert die Quarantäne?**
- **Desinfizieren (wenn nicht möglich: Datei löschen)**: Hier wird versucht, den Virus aus einer befallenen Datei zu entfernen, falls das nicht möglich ist, wird die Datei gelöscht. Diese Funktion sollten Sie nur dann verwenden, wenn sich auf Ihrem Rechner keine wichtigen Daten befinden. Eine konsequente Löschung infizierter Dateien kann im schlimmsten Fall dazu führen, dass Ihr Windows nicht mehr funktioniert und eine Neuinstallation nötig ist.
- **Datei in die Quarantäne verschieben**: Infizierte Dateien werden direkt in die **Quarantäne** verschoben. In der Quarantäne sind Dateien verschlüsselt gespeichert. Der Virus kann hier also keinen Schaden anrichten und die infizierte Datei ist für eventuelle Reparaturversuche weiterhin existent. Lesen Sie hierzu bitte auch das Kapitel: **Wie funktioniert die Quarantäne?**

- **Datei löschen**: Diese Funktion sollten Sie nur dann verwenden, wenn sich auf Ihrem Rechner keine wichtigen Daten befinden. Eine konsequente Löschung infizierter Dateien kann im schlimmsten Fall dazu führen, dass Ihr Windows nicht mehr funktioniert und eine Neuinstallation nötig ist.

Wenn Sie nun auf die Schaltfläche **Aktionen ausführen** klicken, verfährt die G Data Software mit jedem einzelnen Virenfund so, wie Sie es definiert haben.

Ihr System wurde nun auf Viren überprüft. Falls Sie jedoch eine Einstellung mit der Option Protokollieren verwendet haben, kann es sein, dass Ihr Rechner nicht virenfrei ist.

15.3 Virenfund

Wenn die G Data Software auf Ihrem Rechner einen Virus oder ein anderes Schadprogramm findet, haben Sie folgende Möglichkeiten, mit der infizierten Datei umzugehen.

- **Nur protokollieren**: In der **Protokolle**-Ansicht wird die Infektion aufgelistet, Eine Reparatur oder Löschung der betroffenen Dateien findet jedoch nicht statt. Allerdings können Sie über das Protokoll die gefundenen Viren einzeln überprüfen und gezielt entfernen. **Achtung: Wenn ein Virus nur protokolliert wird, ist er weiterhin aktiv und gefährlich.**
- **Desinfizieren (wenn nicht möglich: in Quarantäne verschieben)**: Hier wird versucht, den Virus aus einer befallenen Datei zu entfernen, falls das nicht möglich ist, ohne die Datei zu beschädigen, wird die Datei in die **Quarantäne** verschoben. Lesen Sie hierzu bitte auch das Kapitel: **Wie funktioniert die Quarantäne?**
- **Datei in die Quarantäne verschieben**: Infizierte Dateien werden direkt in die **Quarantäne** verschoben. In der Quarantäne sind Dateien verschlüsselt gespeichert. Der Virus kann hier also keinen Schaden anrichten und die infizierte Datei ist für eventuelle Reparaturversuche weiterhin existent. Lesen Sie hierzu bitte auch das Kapitel: **Wie funktioniert die Quarantäne?**
- **Infizierte Datei löschen**: Diese Funktion sollten Sie nur dann verwenden, wenn sich auf Ihrem Rechner keine wichtigen Daten befinden. Eine konsequente Löschung infizierter Dateien kann im schlimmsten Fall dazu führen, dass Ihr Windows nicht mehr funktioniert und eine Neuinstallation nötig ist.

> **Quarantäne und Mail-Postfächer**: Es gibt Dateien, bei denen es nicht ratsam ist, diese in die Quarantäne zu verschieben, z.B. die Archivdateien für Mail-Postfächer. Wenn ein Mail-Postfach in die Quarantäne verschoben wird, kann ihr Mailprogramm nicht mehr darauf zugreifen und funktioniert möglicherweise nicht mehr. Gerade bei Dateien mit der Endung **PST** sollten Sie deshalb vorsichtig sein, da diese in der Regel Daten Ihres **Outlook-Mail-Postfaches** enthalten.

15.4 Malware-Feedback

Die G Data Security Labs erforschen ständig Verfahren, um G Data Kunden vor Malware zu schützen. Je mehr Informationen dazu vorliegen, desto effektiver können Schutzmechanismen entwickelt werden. Viele Informationen sind aber nur auf attackierten oder infizierten Systemen vorhanden. Um auch solche Informationen in die Analyse einschließen zu können, wurde die G Data Malware Information Initiative gegründet. In diesem Rahmen werden Malware-bezogene Informationen an die G Data Security Labs geschickt. Durch Ihre Teilnahme tragen Sie dazu bei, dass alle G Data Kunden das Internet sicherer nutzen können.

> **Malware**: Ein Sammelbegriff für alle Dateien, Programme und Codes, die darauf programmiert sind, einen Computer ohne Wissen des Anwender zu infizieren, auszuspionieren oder zu kontrollieren. Darunter fallen z.B. Viren, Würmer, Rootkitviren, Trojaner, Keylogger und vieles mehr.

Während der Installation der G Data Software können Sie entscheiden, ob Sie den G Data Security Labs Informationen zur Verfügung stellen möchten oder nicht.

15.5 Not-a-virus-Meldung

Bei als **not-a-virus** gemeldeten Dateien handelt es sich um potentiell gefährliche Anwendungen. Solche Programme verfügen nicht direkt über schädliche Funktionen, könnten allerdings unter bestimmten Umständen von Angreifern gegen Sie verwendet werden. Zu dieser Kategorie zählen beispielsweise bestimmte Dienstprogramme zur entfernten Administration, Programme zum automatischen Umschalten der Tastaturbelegung, IRC-Clients, FTP-Server oder unterschiedliche Dienstprogramme zum Erstellen oder Verstecken von Prozessen.

15.6 Quarantäne

Während der Virenprüfung haben Sie die Möglichkeit, mit **Virenfunden** auf unterschiedliche Weise umzugehen. Eine Option ist es, die infizierte Datei in die Quarantäne zu verschieben. Die Quarantäne ist ein geschützter Bereich innerhalb der Software, in dem infizierte Dateien verschlüsselt gespeichert werden und auf diese Weise den Virus nicht mehr an andere Dateien weitergeben können.

Die Dateien in der Quarantäne bleiben dabei in dem Zustand erhalten, in dem sie die G Data Software vorgefunden hat und Sie können entscheiden, wie Sie weiterverfahren möchten.

- **Aktualisieren**: Sollten Sie das Dialogfenster für die Quarantäne längere Zeit offen haben und zwischendurch ein Virus gefunden und in die Quarantäne verschoben werden (z.B. automatisch über den Virenwächter), können Sie über diese Schaltfläche die Ansicht aktualisieren.
- **Einsenden**: In bestimmten Fällen können Sie eine infizierte Datei, die Sie nicht desinfizieren können, über das Internet an G Data übermitteln. Der Inhalt dieser Datei wird selbstverständlich vertraulich behandelt. Die Ergebnisse der Untersuchung fließen in die Verbesserung und Aktualisierung der Virensignaturen und der Software ein. Lesen Sie hierzu auch das Kapitel: **Malware-Feedback**
- **Desinfizieren**: In vielen Fällen können infizierte Dateien noch gerettet werden. Die Software entfernt dann die Virenbestandteile in der infizierten Datei und rekonstruiert auf diese Weise die nicht infizierte Originaldatei. Wenn eine Desinfektion erfolgreich ist, wird die Datei automatisch an den Ort zurückbewegt, an dem sie vor der Virenprüfung gespeichert war und steht Ihnen dort wieder uneingeschränkt zur Verfügung.
- **Zurückbewegen**: Manchmal kann es nötig sein, eine infizierte Datei, die sich nicht desinfizieren lässt, aus der Quarantäne an ihren ursprünglichen Speicherort zurückzubewegen. Dies kann z.B. aus Gründen der Datenrettung erfolgen. Sie sollten diese Funktion nur im Ausnahmefall und unter strengen Sicherheitsmaßnahmen (z.B. Rechner vom Netzwerk/Internet trennen, vorheriges Backup nicht infizierter Daten etc.) durchführen.
- **Löschen**: Wenn Sie die infizierte Datei nicht mehr benötigen, können Sie diese auch einfach aus der Quarantäne löschen.

15.7 Protokolle

Im Protokolle-Bereich sind durch die Software angefertigte Protokolle aufgelistet. In dem Sie auf die Spaltenüberschriften **Startzeit**, **Art**, **Titel** oder **Status** klicken, können Sie die vorhandenen Protokolle entsprechend sortieren. Mit den Schaltflächen **Speichern unter** und **Drucken** können Protokolldaten auch als Textdatei gespeichert oder direkt ausgedruckt werden. Um ein Protokoll zu löschen, markieren Sie den Tabelleneintrag mit der Maus und klicken dann bitte auf die **Entf**-Taste oder betätigen die **Löschen**-Schaltfläche.

15.8 Mehrfach-Lizenz

Mit einer Mehrfachlizenz können Sie die G Data Software auf der lizenzierten Anzahl von Computern betreiben. Nach der Installation auf dem ersten Rechner und dem Internet Update erhalten Sie online Zugangsdaten übermittelt. Wenn Sie Ihre Software nun auf dem nächsten Rechner installieren, geben Sie einfach den Benutzernamen und das Passwort ein, welche Sie bei der Registrierung auf dem G Data UpdateServer erhalten haben. Wiederholen Sie den Vorgang bei jedem weiteren Rechner.

Bitte verwenden Sie auf allen PCs Ihre **Zugangsdaten** (Benutzername und Passwort) für das Internet Update, die Ihnen nach Ihrer Erstregistrierung zugewiesen worden sind. Hierfür gehen Sie bitte wie folgt vor:

1. Starten Sie die G Data Software.

2. Klicken Sie im SecurityCenter auf **Virensignaturen > Virensignaturen aktualisieren**.

3. Tragen Sie in dem nun erscheinenden Fenster bitte die Zugangsdaten ein, die Sie zuvor per E-Mail erhalten haben. Wenn Sie nun auf OK klicken, wird Ihr Rechner lizenziert.

15.9 Lizenzverlängerung

Ein paar Tage bevor Ihre Lizenz abläuft, erscheint ein Informationsfenster in der Taskleiste. Wenn Sie diese anklicken, öffnet sich ein Dialog, in dem Sie Ihre Lizenz problemlos und in wenigen Schritten direkt verlängern können. Klicken Sie einfach auf die Schaltfläche **Jetzt kaufen**, vervollständigen Sie Ihre Daten und Ihr Virenschutz ist dann sofort wieder gewährleistet. Sie erhalten die Rechnung in den nächsten Tagen dann bequem über den Postweg zugestellt.

> Dieser Dialog erscheint nur nach Ablauf des ersten Jahres. Danach verlängert sich Ihre G Data Lizenz jedes Jahr automatisch. Sie können dieses Abo jedoch jederzeit ohne Angabe von Gründen kündigen.

15.10 Rechnerwechsel

Sie können mit Ihren vorhandenen Zugangsdaten auf einem neuen oder anderen Computer Ihr G Data-Produkt nutzen. Installieren Sie einfach die Software und geben Sie die Zugangsdaten ein. Der Updateserver richtet in dem Fall die Verbindung zu dem neuen Computer ein. Sollte sich auf Ihrem alten Rechner noch die G Data Software befinden, muss die Lizenz von dem alten auf den neuen Rechner übertragen werden. Die Anzahl der Lizenzübertragungen ist begrenzt - bei Erreichen des Grenzwertes wird die Lizenz vollständig gesperrt, sodass dann keinerlei Updates mehr geladen werden können.

15.11 Deinstallation

Wenn Sie die G Data Software irgendwann wieder von Ihrem Rechner entfernen möchten, können Sie dies am einfachsten durchführen, indem Sie in der G Data **Programmgruppe** auf die **Deinstallieren**-Schaltfläche klicken. Die Deinstallation erfolgt dann vollautomatisch. Alternativ können Sie auch über die Windows-Systemsteuerung eine Deinstallation durchführen.

- **Windows Vista**, **Windows 7**: Klicken Sie in der Windows-Taskleiste auf das Startsymbol (normalerweise unten links auf Ihrem Bildschirm) und wählen Sie den Ordner **Systemsteuerung** aus. Dort finden Sie den Punkt **Programme > Programm deinstallieren**. Wählen Sie hier die G Data Software aus der Liste aus und klicken dann auf die **Deinstallieren**-Schaltfläche, um die Deinstallation durchzuführen.

- **Windows XP**: Klicken Sie in der Windows-Taskleiste auf **Start** und wählen Sie den Ordner **Einstellungen > Systemsteuerung > Software**. Dort finden Sie auf der Karteikarte **Installieren/ Deinstallieren** die Möglichkeit, die G Data Software mit der Maus zu markieren. Klicken Sie dann auf die **Hinzufügen/Entfernen**-Schaltfläche, um die Deinstallation durchzuführen.

Sollten Sie während der Deinstallation noch Dateien im **Quarantäne**-Bereich der G Data Software liegen haben, erfolgt eine Abfrage, ob diese Dateien gelöscht werden sollen oder nicht. Wenn Sie die Dateien nicht löschen, befinden diese sich weiterhin in einem speziellen G Data **Ordner** verschlüsselt auf Ihrem Computer und können auf diese Weise keinen Schaden anrichten. Diese Dateien stehen Ihnen erst wieder zur Verfügung, wenn Sie die G Data Software erneut auf Ihrem Computer installieren. Während der Deinstallation werden Sie gefragt, ob Sie **Einstellungen und Protokolle** löschen möchten. Wenn Sie diese Dateien nicht löschen, stehen Ihnen die Protokolle und Einstellungen bei einer erneuten Installation der Software wieder zur Verfügung. Schließen Sie die Deinstallation mit Anklicken der Beenden-Schaltfläche ab. Die Software ist nun vollständig von Ihrem System deinstalliert.

15.12 Copyright

Copyright © 2012 G Data Software AG
Engine A: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2012 BitDefender SRL.
Engine B: © 2012 Alwil Software
OutbreakShield: © 2012 Commtouch Software Ltd.
[G Data - 26.09.2012, 14:12]

Index

A

Absenderfilter 30

Adaptiv-Modus 39

Adressen von infizierten Internetseiten einsenden 23

Adware 18

Aktion, falls keine Regel zutrifft 39

Allgemein 18, 26

Analyse-Umfang 26

Andere Mailprogramme (Verwendung von POP3) 32

Anmelden 22

Anwendungs-Radar 36

Archiv-Dateien 18, 20, 27

Archive prüfen 18, 27

Attachments 30

Auf Dialer / Spyware / Adware / Riskware prüfen 18, 27

Auf Rootkits prüfen 8, 27

Ausgehende Mails 24

Ausnahmen 18

Ausnahmen auch für den Hintergrundscan verwenden 20

Ausnahmen festlegen 12, 24

Auswahlmenü 8, 11

Automatik 32

Automatik (Autopilot) 36

Automatische Konfiguration (DHCP) zulassen 37

Automatische Updates deaktivieren 11

Automatische Virenprüfungen 25

Autopilot 14, 36

Autopilot ausschalten 14

Autopilot-Modus 32

Autopilot-Modus anbieten, wenn eine Vollbild-Anwendung gestartet wird 32

Autostart-Bereich 8

B

Bei Systemlast die Virenprüfung pausieren 20, 49

Beim Systemstart 26

Benutzer 42

Benutzerdefinierte Sicherheit (für erfahrene Anwender) 32

Benutzerkonto 27

Benutzername 4, 22

Bereinigungstools 4

Bericht an empfangene, infizierte Mails anhängen 24

Blacklist 15, 28, 45

Blacklists 45

BootCD 6

BootScan 4, 46

BootScan vor der Installation 46

Bootsektoren 27

C

CD-ROMs 8

Computernutzungszeit überwachen 44

Computerspielen 32

CPU-Last 7

D

Datei in die Quarantäne verschieben 49

Datei löschen 49

Datei- und Druckerfreigabe (NetBIOS) erlauben oder verweigern 38

Dateitypen 27

Deinstallation 4, 53

Deinstallationshinweise 53

Desinfizieren (wenn nicht möglich: Anhang/Text löschen) 24

Desinfizieren (wenn nicht möglich: Datei löschen) 49

Desinfizieren (wenn nicht möglich: in Quarantäne) 18, 20, 49

Desinfizieren (wenn nicht möglich: nur protokollieren) 49

Desktop-Symbol 5

Dialer 18

Die Anmeldung wurde erfolgreich durchgeführt 22

Domäne 38

Domänen-Dienste erlauben oder verweigern 38

DVD-ROMs 8

E

Eigene Filter 45

Einbindung in die Messenger-Anwendung 23

Einen bestimmten Internet-Dienst (Port) öffnen oder sperren 38

Einen leeren Regelsatz erzeugen 37

Einen Regelsatz erzeugen, der einige sinnvolle Regeln enthält 37

Einer bestimmten Anwendung den Zugriff erlauben oder verweigern 38

Eingehende Mails 24

Einstellungen 15, 18, 32

E-Mail-Archive prüfen 18, 27

E-Mail-Prüfung 13, 24

E-Mails 24

Empfangene Mails prüfen 24

Engines 18, 20, 27

Engines benutzen 18, 20, 24, 27

Erlaubte Inhalte 43

Erweitert 18, 20, 24, 27

Extras 24

F

Firefox 23

Firewall 14, 28, 32

Firewall aktiv, auf diesem Netzwerk 37

Firewall ausschalten 14

Firewall deaktiviert 32

Firewall öffnen 14

Firewall-Alarm 40

Firewall-Bedienung 36

Fragezeichen-Symbol 18

Full-Screen Anwendungen 32

G

Gefährliche Anhänge filtern 30
Gemeinsame Nutzung der Internet-Verbindung 37
Gemeinsame Nutzung der Internet-Verbindung erlauben 38
Größenbegrenzung für Downloads 24

H

Heuristik 18, 27
Hilfe anzeigen 6
Hintergrundscan 8
Höchste Sicherheit 32
Hohe Sicherheit 32
HOSTS-Datei 18
HTML-Skripte deaktivieren 30
HTTP-Webinhalte 23

I

Im Fall einer Infektion 24
IMAP 24
Immer erlauben 40
Immer verweigern 40
In den erweiterten Bearbeitungsmodus wechseln 38
Infizierte Archive 18, 20, 27
Infizierte Dateien 18, 20, 27
Info 6
Inhaltsfilter 28, 30
Inhaltsfilter verwenden 28
Installation 4
Installationsnachbereitung 5
Instant-Messaging-Inhalte verarbeiten 23
Internet Einstellungen 22, 23
Internet Explorer 23
Internet Update 23
Internet-Dienst zuordnen 40
Internetinhalte (HTTP) verarbeiten 17, 23
Internetnutzungszeit überwachen 44
IP-Adresse 40
IP-Adressraum 40

J

Job nachholen, wenn der Rechner zur Startzeit nicht eingeschaltet ist 26

K

Kindersicherung 17
Kindersicherung-Bedienung 42
Kommentar 40
Kundendaten 22

L

Leerlauf-Scan 8, 25
Leerlauf-Scan ausschalten 8
Leerlauf-Scan jetzt starten 8
Letzte Virenprüfung 8
Letzter Leerlauf-Scan 8
Letztes Update 11
Letztes Virenupdate 11
Lizenz 6
Lizenz aktivieren 22
Lizenzablauf 53
Lizenzverlängerung 53

M

Mail-Anhänge 30
Mails vor dem Senden prüfen 24
Malware Infomation Initiative 51
Manuelle Regelerstellung 32, 36
Manuelle Virenprüfung 20
Medium-Wechsel 18
Mehr PCs schützen 6
Mehrfach-Lizenz 52
Microsoft Messenger 23
Microsoft Outlook 13, 24, 32
Mindestanforderungen 4
Module 34
Modus 18, 32

N

Nach Beendigung des Jobs den Rechner ausschalten 26
Nachfragen 33
Nächstes Update 11
Name 39, 40
NetBIOS 38
Netzwerk bearbeiten 37
Netzwerke 36, 37
Netzwerken 34
Netzwerk-Info 37
Netzwerkzugriffe prüfen 18
Neuen Benutzer anlegen 42
Neuinstallation 53
Nicht im Batteriebetrieb ausführen 26
Niedrige Sicherheit 32
Normale Sicherheit 32
not-a-virus 52
not-a-virus-Meldung 52
Notebooks 26
Nur neue bzw. veränderte Dateien prüfen 18
Nur protokollieren 49

O

Ordner auf Viren überprüfen 24
OutbreakShield 24, 28
Outlook 13, 24, 32

P

Passwort 4, 22
Passwortgeschützte Archive 49
Phishing 23
Phishingschutz 23
Platzhalter 32
Platzhaltern 18
Plug-In 24
POP3 24, 32
Port 24, 40

pro Anwendung 33
pro Protokoll/Port/Anwendung 33
Produktaktivierung 4
Profi-Dialog verwenden 39
Profi-Einstellungen 30
Programm aktualisieren 6
Programmversion 6
Protokoll 40, 41
Protokoll anfertigen 22, 27
Protokoll: Kein Spam 15
Protokoll: Spam 15
Protokolle 6, 45, 52
Proxyserver 23
Proxyserver verwenden 23
Prüfung auf ungeschützte Netzwerke 33
PST 18, 20

Q

Quarantäne 8, 52

R

Rang 40
RAR 18, 20
Reaktion 29
Realtime Blacklists verwenden 28
Rechner nach der Virenprüfung ausschalten 49
Rechner prüfen 8
Rechnerwechsel 53
Referenzprüfung 34
Referenzprüfung für geladene Module 34
Regel aktiv 40
Regel Assistenten verwenden 38
Regel bearbeiten 40
Regel erstellen 33
Regelassistenten 34
Regeln 40
Regelsatz 36, 37
Regelsatz bearbeiten 37
Regelsatz für ein nicht vertrauenswürdiges Netzwerk 37
Regelsatz für ein vertrauenswürdiges Netzwerk 37
Regelsatz für ein zu blockierendes Netzwerk 37
Regelsätze 37
Regelsätze erstellen 37
Regelsatzname 37
Registriernummer 3, 22
Registriernummer eingeben 4
Registrierte Angriffe 36
Richtung 40
Riskware 18
Rootkits 8, 27

S

Scan-Einstellungen 27
Scanoptionen 24
Schlüsselwörter (Betreff) verwenden 28
Schlüsselwörter (Mailtext) verwenden 28
Schnellprüfung 5
SecurityCenter 6
Security-Symbol 5
Serveranwendung 33
Serveranwendungen 34
Serverportnummer 24
ServiceCenter 3
Shredder 5
Sicherheit 36
Sicherheit/Performance 18
Sicherheitseinstellung 32
Skripte 30
Sonstiges 34
Spam-Filter 28
Spam-OutbreakShield 28
Spamschutz 15
Spamschutz deaktivieren 15
Speicher 8
Speicher und Autostart prüfen 8
Speicherkarten 8
Sprachenfilter 30
Spyware 18
Standardports 24
Status 36, 42
Stealth-Modus 39
Sternchen-Symbol 18
Symbol 48
Systembereiche beim Medium-Wechsel prüfen 18
Systembereiche beim Systemstart prüfen 18
Systembereiche prüfen 27
Systemschutz 18
Systemstart 18

T

Temporär erlauben 40
Temporär verweigern 40
Testen 42
Testversion 4
Trillian 23

U

Unbekannte Serveranwendungen 33
Ungelesene Mails im Posteingang bei Programmstart prüfen 32
Updates 22
USB-Sticks 8

V

VB-Skripte 30
Verbindungsprotokoll speichern 34
Verbindungs-Richtung 40
Verbotene Inhalte 42
Verhaltensüberwachung 18
Versionsprüfung 22
Verzeichnisse/Dateien prüfen 8
Virenfund 51
Virenprüfung 7, 8, 48, 49
Virenprüfungsverlauf 49

Virenschutz 8
Virensignaturen 11
Virensignaturen aktualisieren 11
Virensignaturen automatisch aktualisieren (empfohlen) 22
Virenwächter 7, 8
Virenwächter ausschalten 8
Vollbildmodus 32
Vollversion 4
Vorgabe für den Regelassistenten 34

W

Wächter 18
Wächterstatus 18
Was passiert bei Ablauf meiner Lizenz? 6
Webschutz 12, 23
Wechselmedien prüfen 8
Weitere Filter 30
Whitelist 12, 15, 28, 45
Whitelists 45
Wie erhalte ich zusätzliche oder erweiterte Lizenzen? 6
Wiederholte Anwendungsnachfragen 33
Windows-Benutzerprofil 42
Wissenswertes 48
Wollen sie das erlauben? 40

Z

Zeiten sperren 44
Zeitfenster 40
Zeitplanung 26
Zeitüberschreitung beim E-Mail-Server vermeiden 24
Zeitüberschreitung im Browser vermeiden 24
ZIP 18, 20
Zugangsdaten 3
Zugangsdaten eingeben 4
Zugangsdaten für die Internetverbindung 23
Zugriff 40
Zugriff verweigert 49