G DATA

# Security Software

# Inhaltsverzeichnis

# Erste Schritte

Wir freuen uns, dass Sie sich für unser Produkt entschieden haben und hoffen, dass Sie mit Ihrer neuen G DATA 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.


**Hinweis**: Sie können in der Software jederzeit die ausführliche Programmhilfe aufrufen und erhalten dort vor Ort alle notwendigen Informationen. Klicken Sie dazu einfach im Programm auf das dort abgebildete Hilfe-Symbol.

# 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:

| | |
|---|---|
| G DATA Austria | www.gdata.at |
| G DATA Germany | www.gdata.de |
| G DATA Switzerland | www.gdata.ch |

# Installation

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 - Installationsbeginn

Starten Sie bitte die Installation folgendermaßen:

- **CD/DVD-Installation**: Um mit der Installation zu beginnen, legen Sie die Programm-CD oder DVD ein.
- **Software-Download**: Um mit der Installation einer aus dem Internet heruntergeladenen Version der Software zu beginnen, klicken Sie einfach auf die heruntergeladene Datei.

Nun öffnet sich automatisch ein Installationsfenster.

**Hinweis**: 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.

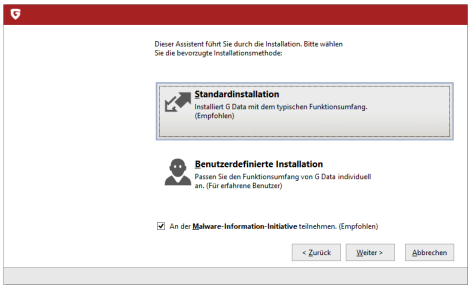
- Wenn sich stattdessen ein Auswahlfenster für eine automatische Wiedergabe öffnet, klicken Sie bitte auf die Option **AUTOSTRT.EXE ausführen**.
- Wenn sich kein Auswahlfenster öffnet, suchen Sie bitte über Ihren Windows-Explorer den Datenträger mit der G DATA Software und starten dann die Datei **Setup**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

## Schritt 2 - Sprachauswahl

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


## Schritt 3 - Installationsmethode

Ein Assistent begleitet Sie nun bei der Installation der Software auf Ihrem Computer. Wählen Sie nun bitte aus, ob Sie die Standardinstallation oder eine benutzerdefinierte Installation durchführen möchten. Wir empfehlen hier die Standardinstallation.




**Malware-Information-Initiative**: Die G DATA SecurityLabs erforschen ständig Verfahren, um G DATA Kunden vor Malware (Viren, Würmern und Schadprogrammen) 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 SecurityLabs geschickt. Durch Ihre Teilnahme tragen Sie dazu bei, dass alle G DATA Kunden das Internet sicherer nutzen können. Während der Installation der G DATA Software können Sie entscheiden, ob Sie den G DATA SecurityLabs Informationen zur Verfügung stellen möchten oder nicht.

**Hinweis**: Bei der benutzerdefinierten Installation können Sie den Speicherort für die Programmdaten individuell auswählen und Module der Software (z. B. den Spamschutz) bei der Installation zu- oder abwählen.

## Schritt 4 - Lizenzvereinbarung

Lesen Sie sich nun bitte die Lizenzvereinbarung durch und geben Sie Ihre Zustimmung.


## Schritt 5 - Benutzerdefinierte Installation (optional)

Wenn Sie die benutzerdefinierte Installation ausgewählt haben, erscheinen nun zwei Assistentenfenster, in denen Sie das Installationsverzeichnis für die Software und den Umfang der installierten Module bestimmen können. Sollten Sie die

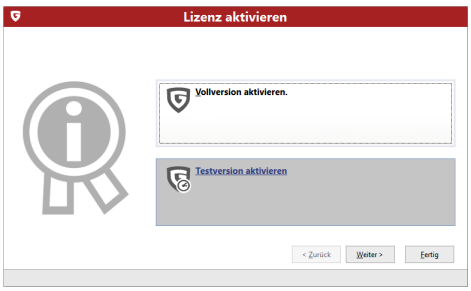
Standardinstallation gewählt haben, können Sie diesen Schritt überspringen.

- **Benutzerdefiniert**: Hier bestimmen Sie den Installationsumfang durch Setzen der Häkchen bei den unterschiedlichen Softwaremodulen (z. B. AntiSpam usw.).
- **Vollständig**: Alle Softwaremodule Ihrer Software-Version werden installiert.
- **Minimal**: Es wird mit dem Modul AntiVirus nur der Basis-Virenschutz Ihrer G DATA Software installiert.

  **Aktualisierungen**: Über das Setup können Sie jederzeit Softwaremodule nachinstallieren oder Ihre Software aktualisieren. Starten Sie dazu einfach das Setup erneut und wählen **Installation anpassen** aus, um Ihre Software um Module zu erweitern oder reduzieren. Wenn Sie eine neue Programmversion besitzen und Ihre Programmversion aktualisieren möchten, können Sie über die Auswahl **Benutzerdefinierte Aktualisierung** bestimmen, welche weiteren Module zu- oder abgewählt werden sollen.

## Schritt 6 - Software-Version

Nun können Sie 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 kostenlos kennenzulernen, können Sie auch einfach unseren zeitlich eingeschränkten Testzugang nutzen.




## Schritt 7 - Produktaktivierung

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

- **Eine 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 Software-Download oder auf der Produktverpackung.

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

- **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.

  **Hinweis**: 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 8 - Installationsabschluss

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


# Nach der Installation

Nach der Installation können Sie über das Programmsymbol auf der Taskleiste Ihre neu installierte G DATA Software starten. Darüber hinaus stehen Ihnen nun auch noch weitere Security-Funktionen auf Ihrem Rechner zur Verfügung:

**Security-Symbol**: 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. Lesen Sie hierzu bitte auch das Kapitel **Security-Symbol**.

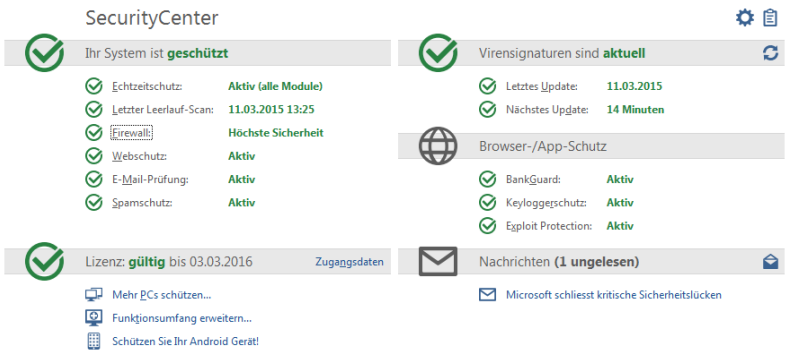
**Shredder**: Sollten Sie den Shredder bei der Installation ausgewählt haben (in der Programmversion G DATA Antivirus nicht integriert), steht Ihnen dieser als Desktop-Symbol zur Verfügung. Daten, die Sie in den Shredder verschieben, werden so entfernt, dass sie auch mit professionellen Datenrettungstools nicht wiederhergestellt werden können. Dabei werden die Daten mit einer frei definierbaren Anzahl von Durchgängen überschrieben. In die Einstellungen gelangen Sie, wenn Sie mit einem Rechtsklick auf das Shredder-Symbol klicken und die Eigenschaften aufrufen.

**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.

**Ihr Computer startet nach der Installation der Software anders als üblich**: Das kann daran liegen, dass sich die Programm-CD noch im Laufwerk befindet. Entfernen Sie einfach die CD und Ihr Computer startet wieder wie gewohnt.

# 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 Bedrohungen 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.




## Sicherheitsstatus

Solange überall ein grünes Häkchen steht, ist Ihr System geschützt.

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

Das gelbe Symbol weist darauf hin, dass ein baldiges Eingreifen des Benutzers erforderlich ist. Dies ist z. B. der Fall wenn ein Programm-Update der Software vorliegt.

Alle anderen Funktionen und Programmbereiche der Software (wie z. B. **Virenschutz** oder **Einstellungen**), 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 und Datensicherung befassen. Eine ausführliche Programmhilfe steht Ihnen in der Software zur Verfügung.

## Übergreifende Funktionen

Folgende Symbole weisen Sie auf den Sicherheitsstatus des jeweiligen Bereiches hin.

**Einstellungen:** Über diese Schaltfläche oben rechts können Sie auf alle Einstellungsdialoge der verschiedenen Bereiche der Software zugreifen. Im jeweiligen Bereich selber haben Sie ebenfalls die Möglichkeit, direkt den passenden Einstellungsdialog auszuwählen.

**Protokolle**: Die Software listet hier aktuelle Protokolle zu allen durchgeführten Aktionen (Virenprüfung, Update, Virenfund etc.) auf.

Oben rechts in der Kopfzeile der Software finden Sie darüber hinaus noch folgende Funktionen:

**Hilfe anzeigen**: Sie können in der Software jederzeit die ausführliche Programmhilfe aufrufen. Drücken Sie dazu einfach im Programm auf die dort abgebildete Hilfe-Schaltfläche.

**Programm aktualisieren**: Wenn neue Programmversionen der Software vorliegen, können Sie diese wie die Vireninformationen ganz bequem per Mausklick aktualisieren. Sollten Sie also hier die Information erhalten, dass ein Update verfügbar ist, klicken Sie einfach auf den Eintrag Programm aktualisieren. Ausführliche Informationen finden Sie im Kapitel: **Updates**

**Info**: Hier erhalten Sie Informationen zur Programmversion. Die Versionsnummer kann z. B. bei Gesprächen mit dem ServiceCenter hilfreich sein.

# Statusanzeigen

Folgende Statusanzeigen informieren Sie über den Sicherheitszustand Ihres Systems. Wenn Sie auf diese Einträge klicken, können Sie sofort Aktionen einleiten, um den Sicherheitsstatus zu optimieren:

## Echtzeitschutz

Der Echtzeitschutz des Virenwächters 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!

- **Virenwächter ausschalten**: Sollten Sie den Virenwächter trotzdem mal ausschalten wollen, können Sie dies hier durchführen. Wenn Sie durch das Abschalten des Wächters die Performance Ihres Rechners optimieren möchten, prüfen Sie bitte unbedingt, ob Sie nicht vielleicht auch mit einer anderen Einstellung des Virenwächters das gewünschte Ergebnis erhalten. Zu diesem Zweck haben Sie beim Ausschalten des Virenwächters die Option, auf die entsprechenden Änderungen der Einstellungen zuzugreifen. Klicken Sie dazu bitte auf **Sicherheit / Performance ändern** und folgen Sie den Hinweisen im gleichnamigen Hilfe-Kapitel. Alternativ können Sie den Virenwächter natürlich trotzdem auch komplett ausschalten.

- **Verhaltensüberwachung ausschalten**: Bei der Verhaltensüberwachung handelt es sich um eine intelligente Erkennung unbekannter Schadsoftware, die unabhängig von Virensignaturen einen zusätzlichen Schutz bietet. Die Verhaltensüberwachung sollte generell eingeschaltet sein.

- **Weitere Einstellungen**: Infos hierzu erhalten Sie im Kapitel **Einstellungen | AntiVirus | Echtzeitschutz**.

## Letzer 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.

- **Rechner prüfen**: Wenn Sie Zeit dazu haben und den Computer in den nächsten Stunden nicht zum Arbeiten nutzen möchten, können Sie hier direkt eine Komplettprüfung des Rechners starten. Sie können den Computer in dieser Zeit weiterhin nutzen, aber da die Virenprüfung bei dieser Einstellung mit maximaler Performance durchgeführt wird, kann es sein, dass andere Anwendungen langsamer reagieren. Weitere Informationen erhalten Sie hierzu im Kapitel **Virenprüfung**.

- **Leerlauf-Scan jetzt starten**: 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 (nicht empfohlen).

## 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. Dieses Software-Modul steht Ihnen in den Programmversionen G DATA Internet Security und G DATA Total Security zur Verfügung.

- **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 (nicht empfohlen).

- **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 empfohlen.

- **Weitere Einstellungen**: Infos hierzu erhalten Sie im Kapitel **Einstellungen | Firewall | Automatik**.

## 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.

- **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.

- **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.

- **Weitere Einstellungen**: Infos hierzu erhalten Sie im Kapitel **Einstellungen | AntiVirus | Webschutz**.

## 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.

- **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.

- **Weitere Einstellungen**: Infos hierzu erhalten Sie im Kapitel **Einstellungen | AntiVirus | E-Mail-Prüfung**.

**Microsoft Outlook**: Hier 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.

## 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. Dieses Software-Modul steht Ihnen in den Programmversionen G DATA Internet Security und G DATA Total Security zur Verfügung.

- **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. 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.

- **Whitelist bearbeiten**: Über die Whitelist können Sie bestimmte Absender-Adressen oder Domains explizit vom Spamverdacht ausnehmen. Klicken Sie dazu auf die Schaltfläche **Neu** und geben Sie dann einfach in das Feld **Absender/Absender-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 bearbeiten**: Über die Blacklist können Sie bestimmte Absender-Adressen oder Domains explizit unter Spamverdacht setzen. Klicken Sie dazu auf die Schaltfläche **Neu** und geben Sie dann einfach in das Feld **Absender/Absender-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.
- **Weitere Einstellungen**: Infos hierzu erhalten Sie im Kapitel **Einstellungen | AntiSpam | Spam-Filter**.

## 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.

- **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 ausschalten**: 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.
- **Weitere Einstellungen**: Infos hierzu erhalten Sie im Kapitel **Einstellungen | AntiVirus | Updates**.

## Nächstes Update

Unter diesem Eintrag können Sie sehen, wann die nächste Aktualisierung erfolgt. Wenn Sie sofort ein Update durchführen möchten, dann klicken Sie dazu einfach auf den Eintrag und wählen Sie die Option **Virensignaturen aktualisieren** aus.

- **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 ausschalten**: 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.
- **Weitere Einstellungen**: Infos hierzu erhalten Sie im Kapitel **Einstellungen | AntiVirus | Updates**.

## BankGuard

Banking-Trojaner werden zu einer immer größeren Bedrohung. Im Stundentakt entwickeln Online-Kriminelle neue Malware-Varianten (z. B. ZeuS, SpyEye), um damit Ihr Geld zu stehlen. Banken sichern den Datenverkehr im Internet, jedoch werden die Daten im Browser entschlüsselt und dort greifen Banking-Trojaner an. Die wegweisende Technologie von G DATA BankGuard sichert Ihre Bankgeschäfte jedoch von Anfang an und schützt sofort dort, wo der Angriff stattfindet. Durch eine Prüfung der Echtheit der benutzten Netzwerkbibliotheken stellt G DATA BankGuard sicher, dass Ihr Internet-Browser nicht von einem Banking-Trojaner manipuliert wurde. Es wird empfohlen, den G DATA BankGuard Schutz eingeschaltet zu lassen.

## Keyloggerschutz

Der Keyloggerschutz überwacht auch unabhängig von Virensignaturen, ob auf Ihrem System Tastatureingaben ausgespäht werden. Damit wird Angreifern die Möglichkeit genommen, Ihre Passworteingaben mitzuprotokollieren. Diese Funktion sollte immer angeschaltet bleiben.

## Exploit Protection

Ein sogenannter Exploit nutzt die Schwachstellen gängiger Anwendersoftware aus und kann über diese Schwachstelle im schlimmsten Fall die Kontrolle über Ihren Rechner übernehmen. Exploits können selbst dann greifen, wenn Anwendungen (wie z. B. PDF-Viewer, Browser usf.) regelmäßig aktualisiert werden. Die Exploit Protection schützt vor solchen Zugriffen, auch proaktiv gegen bisher unbekannte Angriffe.

# 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.

## Zugangsdaten

Wenn Sie im Bereich Lizenz auf **Zugangsdaten** klicken, erscheint ein Dialogfeld, in dem Sie Ihre Zugangsdaten einsehen können. Infos hierzu erhalten Sie im Kapitel **Einstellungen | AntiVirus | Updates**. Sollten Sie mal Fragen zu Ihrer Lizenz haben, können wir Ihnen im **G DATA ServiceCenter** mit diesen Informationen gezielter helfen. Sollten Sie mal Ihr Passwort vergessen haben, können Sie über dieses Dialogfeld auch schnell und unkompliziert ein neues Passwort generieren.

## Mehr PCs schützen / Funktionsumfang erweitern

Selbstverständlich ist es jederzeit möglich, die Anzahl Ihrer Lizenzen zu erweitern oder ein Upgrade auf Produkte mit erweitertem Funktionsumfang durchzuführen. 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.

## Was passiert bei Ablauf?

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 per E-Mail als PDF.

> **Hinweis**: Dieser Dialog erscheint nur nach Ablauf des ersten Jahres. Danach verlängert sich Ihre Lizenz jedes Jahr automatisch. Sie können diesen Verlängerungsservice jederzeit ohne Angabe von Gründen kündigen.

# Software-Module

Folgende Software-Module stehen Ihnen – je nach installierter Software-Version – zur Verfügung:

**SecurityCenter**: Ihr persönliches Sicherheitscenter. Hier erhalten Sie alle Informationen, die zum Schutz Ihres Computers vor Schadsoftware nötig sind und können gezielt auf Bedrohungen reagieren.

**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, außerdem können Sie den Rechner oder Datenträger direkt auf Schadsoftware überprüfen, infizierte Dateien in der Quarantäne bearbeiten und ein Bootmedium erstellen.

**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. Dieses Software-Modul steht Ihnen in den Programmversionen G DATA Internet Security und G DATA Total Security zur Verfügung.

**Backup**: Mit fortschreitender Digitalisierung des täglichen Lebens, der Nutzung von Online-Musikdiensten, Digitalkameras und E-Mail-Korrespondenz wird die Sicherung Ihrer persönlichen Daten immer wichtiger. Sei es durch Hardware-Fehler, ein Versehen oder eine Beschädigung durch Viren oder Hacker-Angriffe: Ihre privaten Dokumente sollten regelmäßig gesichert werden. Das Backup-Modul übernimmt diese Aufgabe für Sie und schützt so Ihre wichtigen Unterlagen und Dateien, ohne dass Sie sich ständig Gedanken darum machen müssen. Dieses Software-Modul steht Ihnen in der Programmversion G DATA Total Security zur Verfügung.

**Passwort Manager**: Über den Passwort Manager können Sie bequem Passwörter verwalten und bequem als Plug-In in Ihrem Browser nutzen. Dieses Software-Modul steht Ihnen in der Programmversion G DATA Total Security zur Verfügung.

**Tuner**: Von der automatischen Erinnerung an Windows Updates über eine regelmäßige zeitgesteuerte Defragmentierung bis hin zur regelmäßigen Entfernung von überflüssigen Registry-Einträgen und temporären Dateien haben Sie mit dem Tuner ein Tool

an der Hand, welches Ihr Windows-System deutlich schneller und übersichtlicher macht. Dieses Software-Modul steht Ihnen in der Programmversion G DATA Total Security zur Verfügung.

**Kindersicherung**: Mit der Kindersicherung können Sie das Surfverhalten und die Nutzung des Computers für Ihre Kinder regeln. Dieses Software-Modul steht Ihnen in den Programmversionen G DATA Internet Security und G DATA Total Security zur Verfügung.

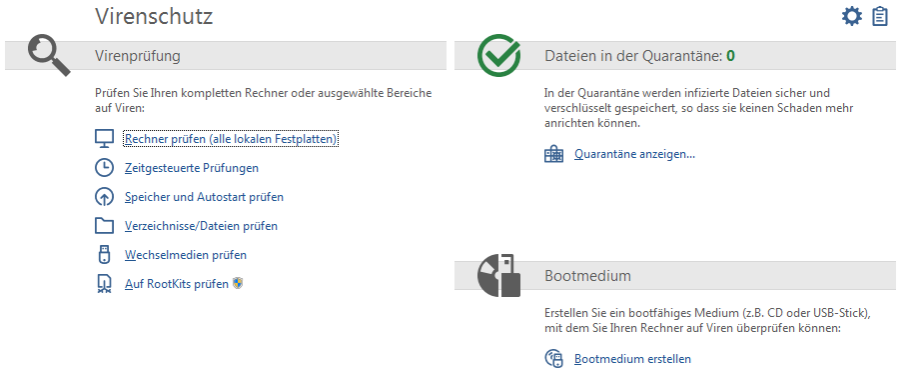
**Verschlüsselung**: Das Verschlüsselungsmodul dient wie ein Banktresor zur Absicherung von sensiblen Daten. Ein Tresor kann z. B. als Extra-Laufwerk wie eine weitere Festplattenpartition benutzt werden und ist sehr leicht zu bedienen. Dieses Software-Modul steht Ihnen in der Programmversion G DATA Total Security zur Verfügung.

**Autostart Manager**: Mit dem Autostart Manager ist es möglich, Programme zu verwalten, die automatisch beim Start von Windows mit gestartet werden. Normalerweise werden diese Programme direkt beim Systemstart hoch geladen. Wenn sie vom Autostart Manager verwaltet werden können sie jedoch auch zeitverzögert oder in Abhängigkeit von der Auslastung des Systems oder der Festplatte gestartet werden. Dieses ermöglicht einen schnelleren Systemstart und damit eine verbesserte Performance Ihres Computers.

**Gerätekontrolle**: Über diese Funktion können Sie für bestimmte Nutzer Ihres Computers die Nutzung von Geräten wie Wechseldatenträgern, CD-/DVD- und Diskettenlaufwerken beschränken. Auf diese Weise können Sie z. B. unerwünschten Export oder Import von Daten oder Installationen von Software unterbinden. Jetzt auch mit USB KeyboardGuard. Weitere Infos hierzu im Kapitel Gerätekontrolle.

# Virenschutz

Über dieses Modul können Sie Ihren Rechner oder ausgewählte Datenträger gezielt auf Infektionen durch Schadsoftware überprüfen. Dies empfiehlt sich, wenn Sie z.B. selbstgebrannte CDs oder USB-Sticks von Freunden, Verwandten oder Arbeitskollegen erhalten. Auch bei der Installation neuer Software und bei Downloads aus dem Internet empfiehlt sich eine Virenprüfung.




**Achtung**: Das Überprüfen des Rechners oder ausgewählter Datenträger dient als zusätzlicher Schutz. Grundsätzlich sind Sie mit dem G DATA Leerlauf-Scan und dem G DATA Virenwächter, welcher ständig im Hintergrund aktiv ist, optimal vor Bedrohungen durch Schadsoftware geschützt. 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.

# Virenprüfung

Wählen Sie hier aus, welchen Bereich Ihres Rechners oder welchen Datenträger Sie gezielt überprüfen möchten:

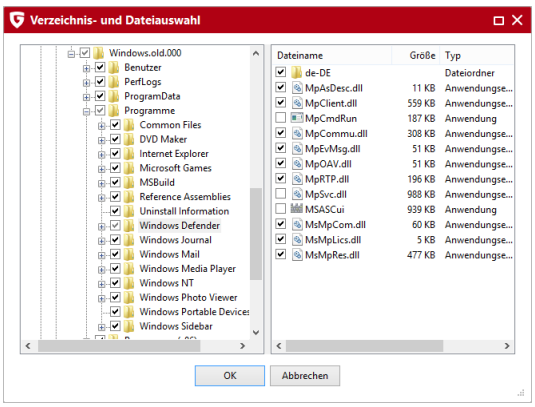
**Rechner prüfen (alle lokalen Festplatten)**: Wenn Sie Ihren Computer unabhängig von der automatischen Prüfung durch den Leerlauf-Scan kontrollieren möchten (z.B. weil Sie einen aktuellen Virenverdacht haben), dann klicken Sie einfach diesen Eintrag an. Ihr Computer wird nun direkt auf Virenbefall untersucht. Lesen Sie hierzu bitte auch folgendes Kapitel: **Virenprüfung durchführen**

**Zeitgesteuerte Prüfungen**: Hiermit planen Sie automatische Virenprüfungen ein. Lesen Sie hierzu bitte folgendes Kapitel: **Automatische Virenprüfungen**.

**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. Diese Funktion ist allerdings 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.



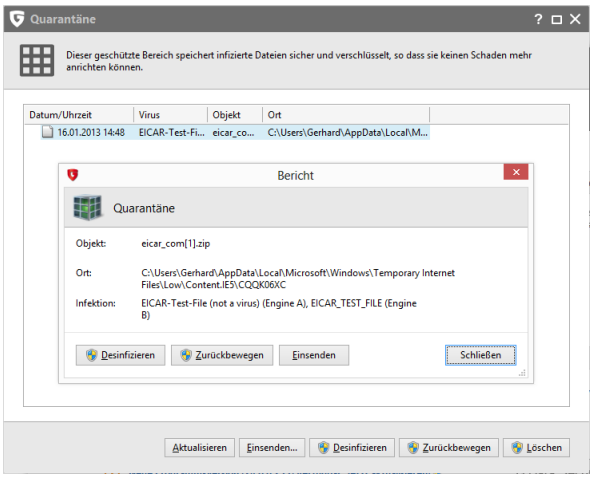
**Wechselmedien prüfen**: Prüfen Sie mit dieser Funktion CD-ROMs oder DVD-ROMs, Speicherkarten oder USB-Sticks auf Virenbefall. Wenn Sie diese Aktion anklicken, werden alle Wechselmedien, die mit Ihrem Computer verbunden sind (also auch eingelegte CDs, eingeschobene Speicherkarten oder per USB verbundene 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.

# Dateien in der 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.

**Quarantäne anzeigen**: Wenn Sie auf diese Schaltfläche klicken, öffnet sich der Quarantäne-Bereich.



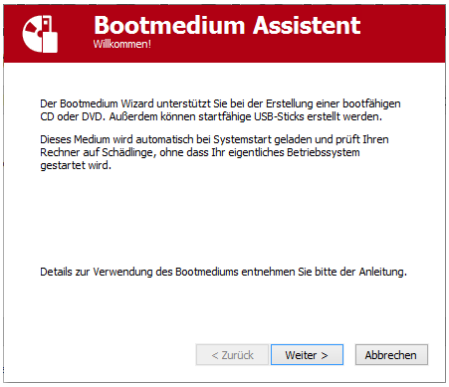

Die Dateien in der Quarantäne bleiben dabei in dem Zustand erhalten, in dem sie die G DATA Software vorgefunden hat und Sie können entscheiden, wie Sie weiter verfahren möchten.

- **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.
- **Zukünftig erlauben**: Sollte die Verhaltensüberwachung eine Datei fälschlicherweise in die Quarantäne verschoben haben, können Sie sie über diese Funktion zur Whitelist hinzufügen, damit die Verhaltensüberwachung sie zukünftig nicht mehr in die Quarantäne verschiebt.
- **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.

# Bootmedium

Das Bootmedium ist ein hilfreiches Werkzeug, um Rechner, die bereits verseucht sind, von Viren zu befreien. Gerade bei Computern, die vor der Installation der G DATA Software keinen Virenschutz hatten, empfiehlt sich die Nutzung eines Bootmediums. Wie Sie ein **Bootmedium** verwenden, lesen Sie im Kapitel **BootScan**.

Um ein Bootmedium zu erstellen, klicken Sie einfach auf die Schaltfläche **Bootmedium erstellen** und folgen den Anweisungen des Installationsassistenten. Hier haben Sie die Möglichkeit, aktuelle Virensignaturen herunterzuladen, um Ihr Bootmedium auf den neuesten Stand zu bringen, außerdem können Sie auswählen, ob Sie als Bootmedium eine CD/DVD brennen oder einen USB-Stick als Bootmedium verwenden möchten.




Wenn Sie die Programmversion G DATA Total Security nutzen, können Sie mit einem Bootmedium ein Laufwerks-Backup auch auf dem Volume wiederherstellen, auf dem sich aktuell das System befindet. Auch die Wiederherstellung eines Laufwerk- oder Datei-Backups auf andere Ziele ist hier möglich. Legen Sie dazu das Bootmedium ein und wählen die Funktion **Wiederherstellung starten**.

# 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.

Im Firewall-Modul stehen Ihnen drei Bereiche zur Verfügung:

- **Status**: Im Status-Bereich der Firewall erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und der Firewall.
- **Netzwerke**: Im Netzwerke-Bereich werden die Netzwerke (z.B. LAN, DFÜ etc.) aufgelistet, mit denen ihr Rechner verbunden ist.
- **Regelsätze**: In diesem Bereich können Sie für verschiedene Netzwerke spezielle Regeln erstellen und damit das Verhalten Ihrer Firewall optimieren.

Sobald etwas darauf hindeutet, dass Daten auf Ihrem Rechner unberechtigt aufgespielt oder heruntergeladen werden sollen, schlägt die Firewall Alarm und blockt den unberechtigten Datenaustausch.

**Einstellungen:** Über diese Schaltfläche oben rechts können Sie auf weitere Einstellungsdialoge der Firewall zugreifen.

# 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 können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln.

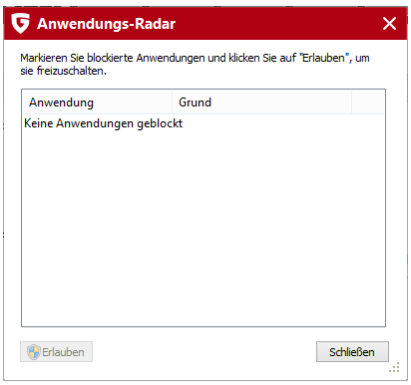

Sobald Sie die Einstellungen einer Komponente mit Warnsymbol optimiert haben, wechselt das Symbol im Status-Bereich wieder auf das grüne Häkchen-Symbol.

- **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. Den Sicherheitsstatus können Sie hier einstellen: **Einstellungen | Firewall | Automatik**.
- **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).

  **Autopilot**: Hier arbeitet die Firewall vollkommen autonom und hält Gefahren automatisch vom heimischen PC ab. Diese Einstellung bietet einen praktischen Rundum-Schutz und ist in den meisten Fällen empfehlenswert. Der Autopilot sollte standardmäßig eingeschaltet sein.

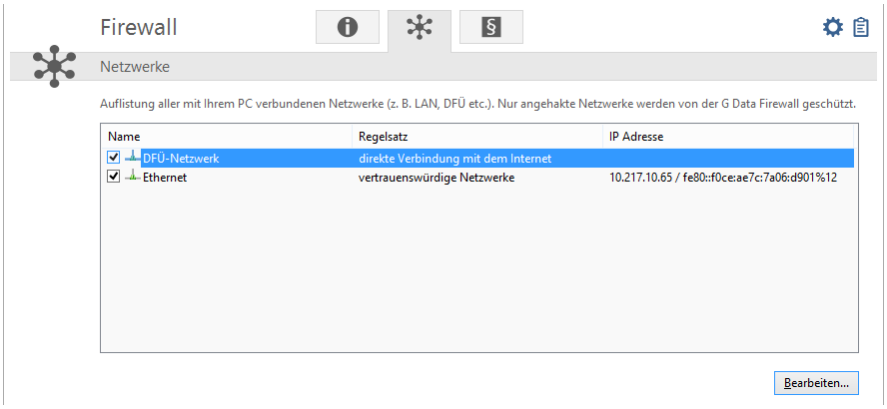
  **Weitere Einstellungen**: Wenn Sie Ihre Firewall individuell konfigurieren möchten oder bestimmte Anwendungen nicht mit dem Autopilot-Modus zusammenarbeiten wollen, können Sie über die manuelle Regelerstellung Ihren Firewall Schutz ganz auf Ihre Bedürfnisse einrichten. Weitere Informationen erhalten Sie in folgendem Kapitel: **Einstellungen | Firewall | Automatik**.
- **Netzwerke**: Hier können Sie sich die Netzwerke anzeigen lassen, in denen sich Ihr Computer befindet. Weitere Informationen erhalten Sie in folgendem Kapitel: **Firewall | Netzwerke**.
- **Abgewehrte 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**: Dieses Dialogfeld 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.



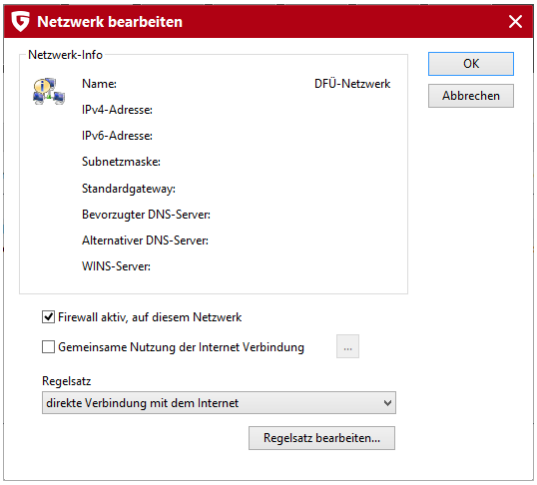

# Netzwerke

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

Folgende Informationen und Einstellungsmöglichkeiten zum ausgewählten Netzwerk werden Ihnen in dieser Übersicht angezeigt:




- **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

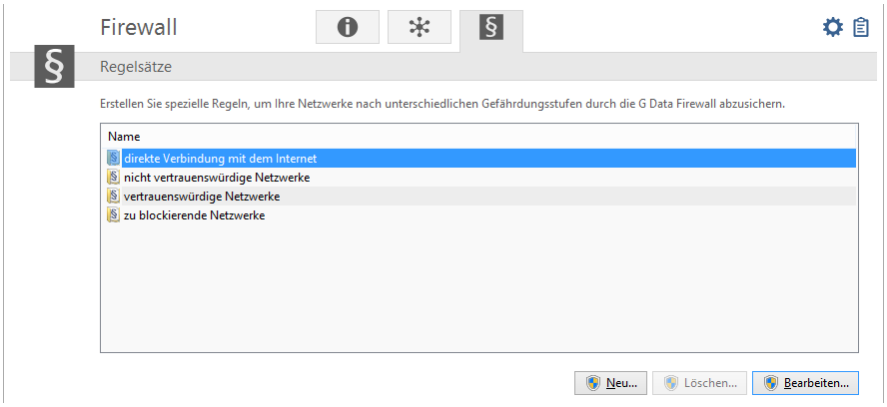
Internetverbindungsfreigabe (ICS) kann für ein Heimnetzwerk in der Regel aktiviert werden.

- **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 erstellen**.

# Regelsätze

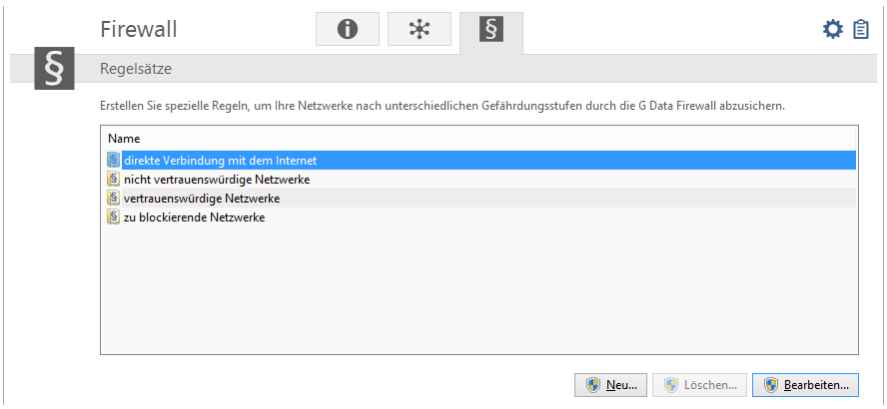
In diesem Bereich können Sie für verschiedene Netzwerke spezielle Regeln erstellen. Diese Regeln werden dann jeweils zu einem Regelsatz zusammengefasst. Voreingestellt sind Regelsätze für direkte Verbindung mit dem Internet, nicht vertrauenswürdige Netzwerke, vertrauenswürdige Netzwerke und zu blockierende 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.



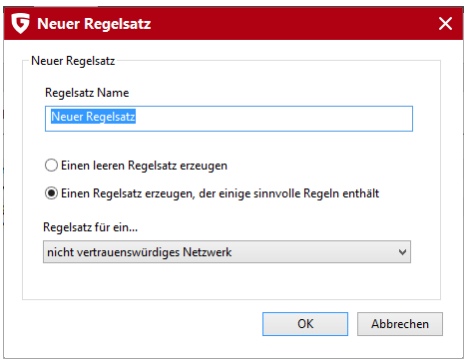

Die vorgegebenen Regelsätze für **direkte Verbindung mit dem Internet**, **vertrauenswürdige Netzwerke**, **nicht vertrauenswürdige Netzwerke** und **zu blockierende Netzwerke** können nicht gelöscht werden. Zusätzliche Regelsätze, die Sie selber erstellt haben, können Sie natürlich jederzeit löschen.

# 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 möglicherweise weniger Schutz (und damit auch Administrationsaufwand), als ein DFÜ-Netzwerk, das im direkten Kontakt mit dem Internet steht.




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:




- **Regelsatz Name**: 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 selbst definierten Regeln bestücken.
- **Einen Regelsatz erzeugen, der einige sinnvolle Regeln enthält**: Bei dieser Auswahl können Sie entscheiden, ob beim neuen Regelsatz grundlegende Regeln für nicht vertrauenswürdige, vertrauenswürdige oder zu blockierende Netzwerke vordefiniert werden sollen. Auf Basis dieser Voreinstellungen können Sie dann individuelle Änderungen vornehmen.

Die Firewall beinhaltet voreingestellte Regelsätze für folgende Netzwerktypen:

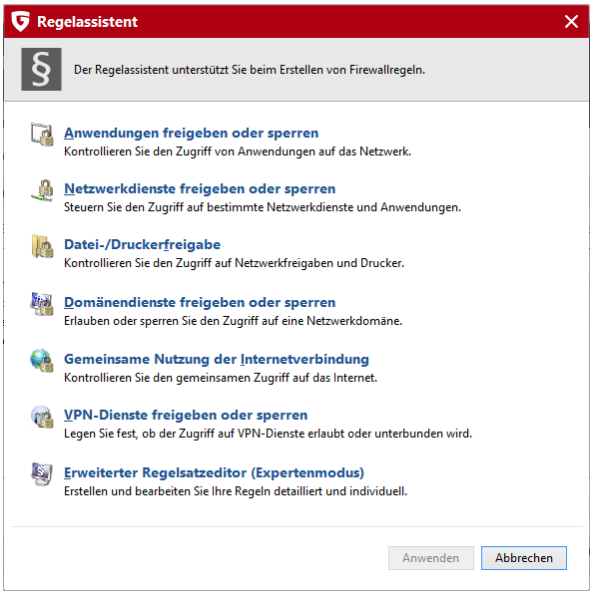
- **direkte Verbindung mit dem Internet**: Hierunter fallen Regeln, die den direkten Internetzugriff behandeln.
- **nicht vertrauenswürdige Netzwerke**: Hierunter fallen in der Regel offene Netzwerke, wie z.B. DFÜ-Netzwerke, die auf das Internet Zugriff haben.
- **vertrauenswürdige Netzwerke**: Vertrauenswürdig sind in der Regel Heim- und Firmennetzwerke.
- **zu blockierende Netzwerke**: 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.)

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 **Einstellungen | 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.

# Regelassistenten 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 Firewall-Technologie 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:

- **Anwendungen freigeben oder sperren**: 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 **Richtung** 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-Player-Software daran hindern, Daten über Ihre Hörgewohnheiten weiterzugeben (ausgehende Verbindungen) oder dafür sorgen, dass nicht automatisch Programmupdates aufgespielt werden (eingehende Verbindungen).

- **Netzwerkdienste freigeben 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-/Druckerfreigabe**: Wenn Sie den Zugriff erlauben, erhalten Sie die Möglichkeit, freigegebene Ordner und Drucker im Netzwerk zu nutzen. Gleichzeitig können auch andere Computer und Benutzer im Netzwerk auf Ihre Freigaben (sofern eingerichtet) zugreifen.

- **Domänendienste freigeben oder sperren**: 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 Internetverbindung**: 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 kann für ein Heimnetzwerk in der Regel aktiviert werden.

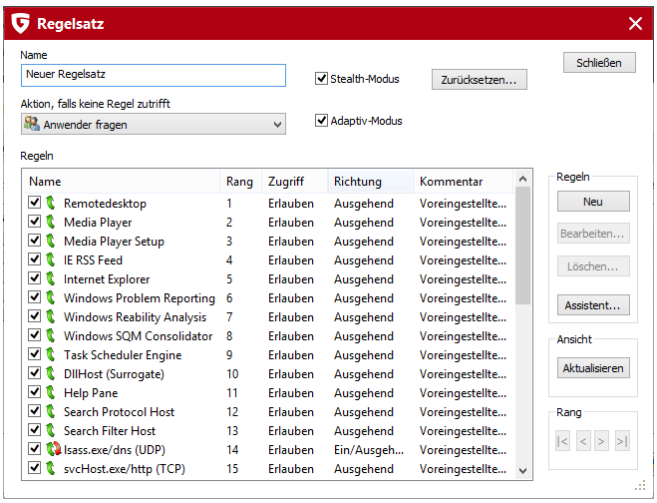
- **VPN-Dienste freigeben oder sperren**: VPN ist die Abkürzung für Virtual-Private-Networks und bezeichnet die Möglichkeit Rechner exklusiv miteinander zu koppeln und quasi eine Direktverbindung zwischen diesen herzustellen. Damit VPN-Dienste funktionieren

können, müssen Sie von der Firewall freigegeben werden.

- **Erweiterter Regelsatzeditor (Expertenmodus)**: Hiermit können Sie vom Regelassistenten zum erweiterten Bearbeitungsmodus wechseln. Informationen zum erweiterten Bearbeitungsmodus erhalten Sie im Kapitel **Erweiterten Bearbeitungsmodus verwenden**.

# 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 entfernte 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 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:

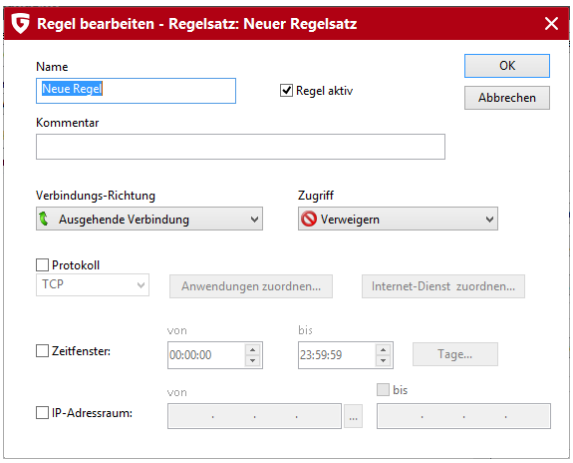
- Über den **Regelassistenten**

- 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:

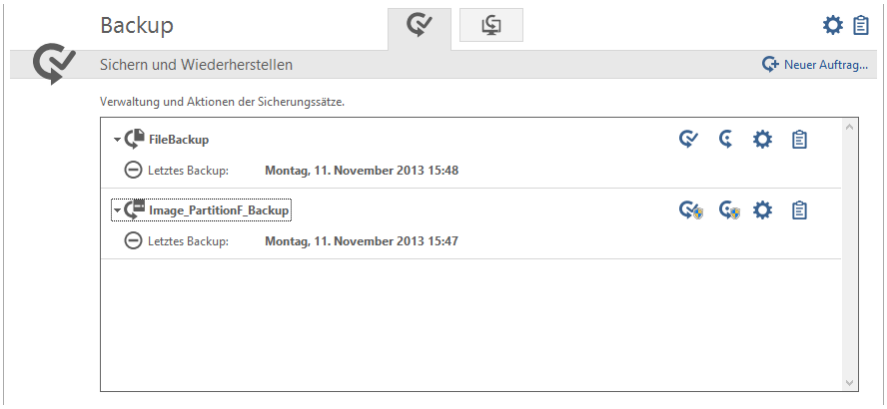
- **Name**: Hier findet sich bei voreingestellten und automatisch generierten Regeln der Programm-Name für den die jeweilige Regel zutrifft.
- **Regel aktiv**: Sie können eine Regel durch Entfernen des Häkchens inaktiv setzen, ohne sie gleich zu löschen.
- **Kommentar**: Hier erfahren Sie, auf welche 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.

# Backup

Mit fortschreitender Digitalisierung des täglichen Lebens, der Nutzung von Online-Musikdiensten, Digitalkameras und E-Mail-Korrespondenz wird die Sicherung Ihrer persönlichen Daten immer wichtiger. Sei es durch Hardware-Fehler, ein Versehen oder eine Beschädigung durch Viren oder Hacker-Angriffe: Ihre privaten Dokumente sollten regelmäßig gesichert werden. Die G DATA Software übernimmt diese Aufgabe für Sie und schützt so Ihre wichtigen Unterlagen und Dateien, ohne dass Sie sich ständig Gedanken darum machen müssen.

## Sichern und Wiederherstellen

Sobald ein Backup-Auftrag über die Funktion **Neuer Auftrag** angelegt ist, können Sie ihn über folgende Symbole direkt bearbeiten und steuern:




**Wiederherstellung**: Hiermit spielen Sie die im Backup archivierten Daten wieder zurück auf Ihr System. Wie die Wiederherstellung abläuft, wird Ihnen im Kapitel **Backup wiederherstellen** erläutert.

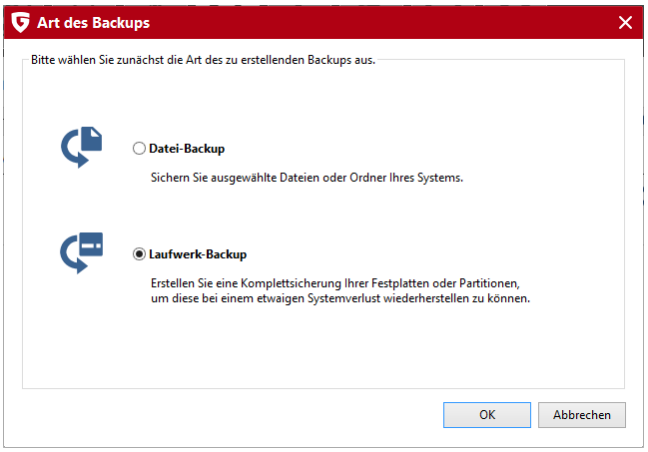
**Backup**: Hiermit starten Sie den Backup-Vorgang für den definierten Backup-Auftrag sofort und außer der Reihe, unabhängig von einem vordefinierten Zeitplan für dieses Backup.

**Einstellungen**: Hiermit können Sie für den jeweiligen Backup-Auftrag die Einstellungen verändern, die Sie beim erstmaligen Erstellen dieses Backup-Auftrags unter **Neuer Backup-Auftrag** vergeben haben.

**Protokolle**: Hier erhalten Sie eine Übersicht über alle Vorgänge, die über diesen Backup-Auftrag erfolgten. Sie finden hier Einträge über erfolgte manuelle oder zeitgesteuerte Backup-Vorgänge, Infos zu eventuellen Wiederherstellungen und gegebenenfalls Fehlermeldungen, z.B. wenn das Zielverzeichnis nicht mehr genügend Speicherplatz für das durchzuführende Backup hatte.

## Neuer Backup-Auftrag

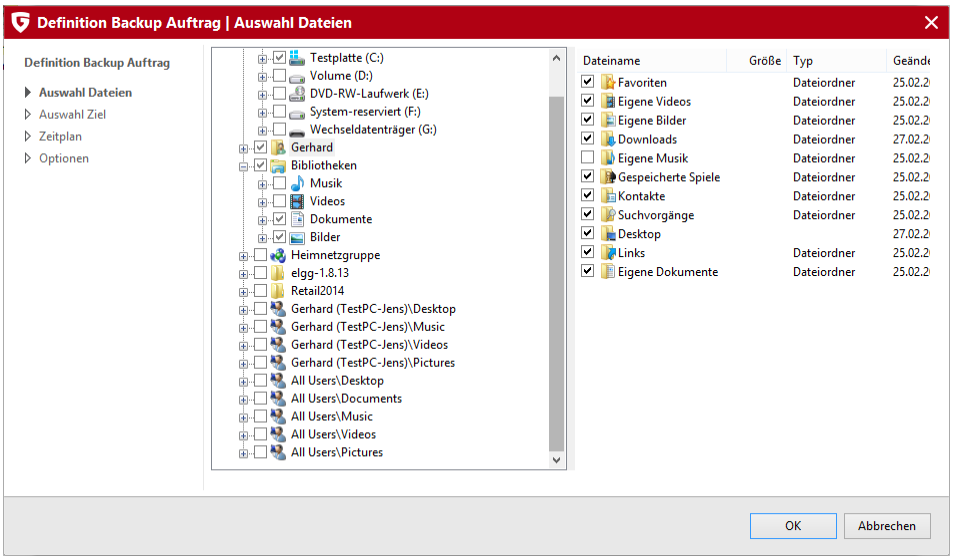
Um einen neuen Backup-Auftrag zu vergeben, klicken Sie bitte auf die Schaltfläche **Neuer Auftrag**.



# Auswahl Dateien / Festplatten / Partitionen

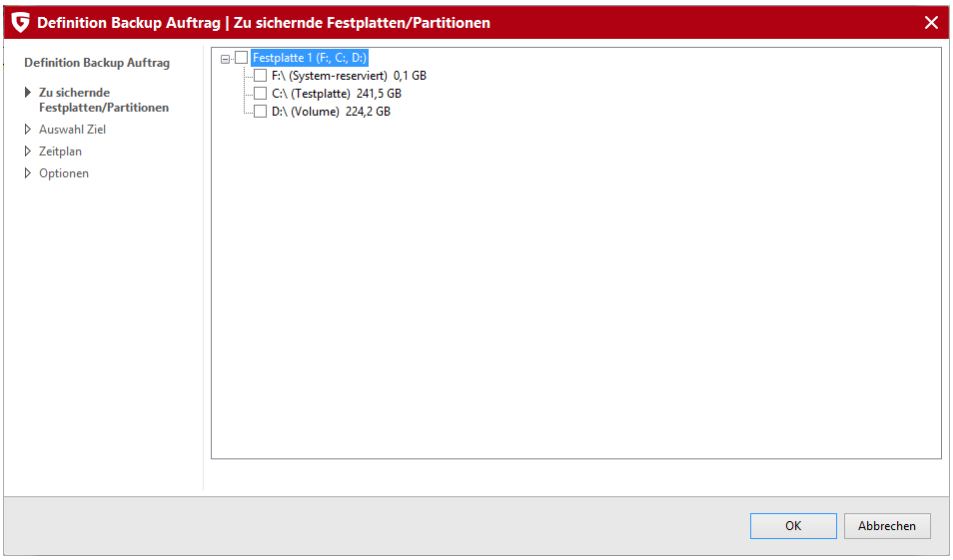
Nun werden Sie vom Backup-Assistenten gefragt, welche Art von Backup Sie durchführen möchten.

**Datei-Backup**: Hierbei handelt es sich um eine Sicherung bestimmter von Ihnen ausgewählter Dateien und Ordner in einer Archiv-Datei.



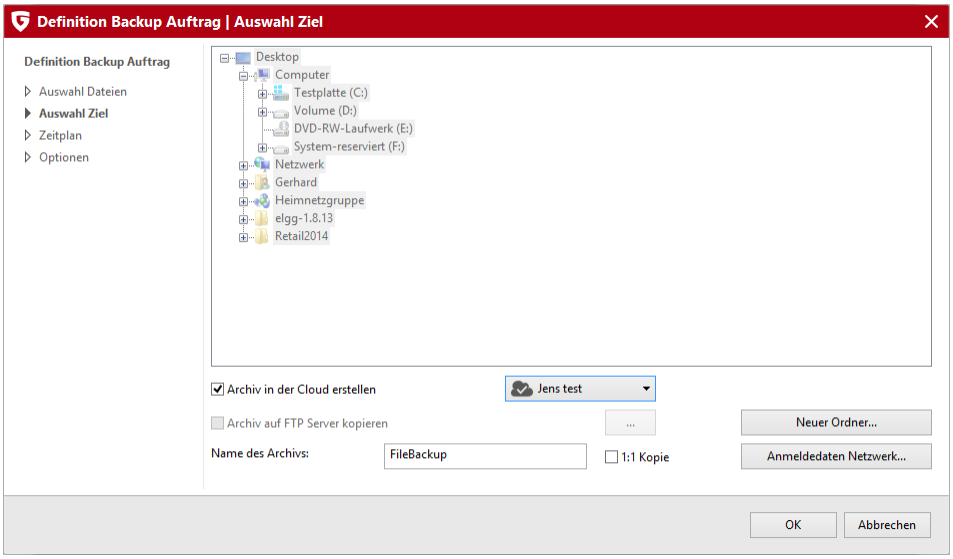

Wählen Sie in der Verzeichnisansicht einfach aus, welche Dateien und Ordner Sie speichern möchten. In der Regel empfiehlt es sich, beim Datei-Backup persönliche Dateien zu speichern und kein Backup installierter Programmdateien durchzuführen. Im Verzeichnisbaum können Sie durch Anklicken der Plus-Symbole 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 fürs Backup verwendet. Wenn in einem Verzeichnis nicht alle Dateien und Ordner fürs Backup verwendet werden, findet sich an diesem Verzeichnis ein graues Häkchen.

**Laufwerk-Backup**: Hierbei handelt es sich um eine Komplettsicherung von Festplatten oder Partitionen in einer Archiv-Datei.



# Auswahl Ziel

Hier können Sie das Ziel, also den Ort bestimmen, an dem die G DATA Software die Sicherungskopie der Dateien und Ordner oder Festplatten und Partitionen erstellen soll. Dies kann ein CD- oder DVD-ROM-Laufwerk sein, eine andere Festplatte, ein USB-Stick, andere Wechselmedien oder ein Verzeichnis im Netzwerk.




**Name des Archivs**: Hier können Sie für die zu erstellende Archivdatei einen aussagekräftigen Namen vergeben, z.B. *Wochen-Backup Eigene Dateien, MP3-Backup* o.ä.

**Neuer Ordner**: Wenn Sie für das Backup einen neuen Ordner anlegen möchten, wählen Sie in der Verzeichnisansicht den gewünschten Speicherort und klicken dann auf die Schaltfläche **Neuer Ordner**.

> **Hinweis**: Bitte achten Sie darauf, dass das Backup nicht auf der gleichen Festplatte erfolgen sollte, auf der sich auch die Originaldaten befinden. Sollte diese Platte nämlich einen Defekt haben, sind Original- und Backup-Daten verloren. Am besten ist es, ein Backup an einem Ort aufzubewahren, der räumlich getrennt von den Originaldateien ist, also z.B. in einem anderen Zimmer auf einer USB-Festplatte oder gebrannt auf CD/DVD-ROM.

**Archiv in der Cloud erstellen**: Nutzen Sie einfach gängige Cloud-Dienste wie z.B. Dropbox, Microsoft OneDrive*, TeamDrive** oder Google Drive, um Ihr Backup dort zu sichern. Melden Sie sich dazu einfach mit den Zugangsdaten für Ihren Cloud-Dienst an und schon wird Ihr Backup-Archiv mit Ihrer Cloud verknüpft.

> **Hinweis**: Sie sollten gerade beim Backup in der Cloud darauf achten, dass Ihre Backupdaten verschlüsselt sind. Im Bereich **Optionen** unter **Neuer Backup-Auftrag** können Sie die Verschlüsselung der Daten ein- bzw. ausschalten.
>
> **(*) Hinweis zu OneDrive**: OneDrive können Sie dann nutzen, wenn Sie diesen Dienst als virtuelles Laufwerk im Windows Explorer integriert haben. Das Archiv wird dann aber ganz normal über das Dateiverzeichnis erstellt und nicht über die Funktion **Archiv in der Cloud erstellen**.
>
> **(**) Hinweis zu TeamDrive**: TeamDrive können Sie dann nutzen, wenn Sie in der auf Ihrem Rechner installierten TeamDrive-Software ein TeamDrive-Space angelegt und ausgewählt haben.

# Zeitplan

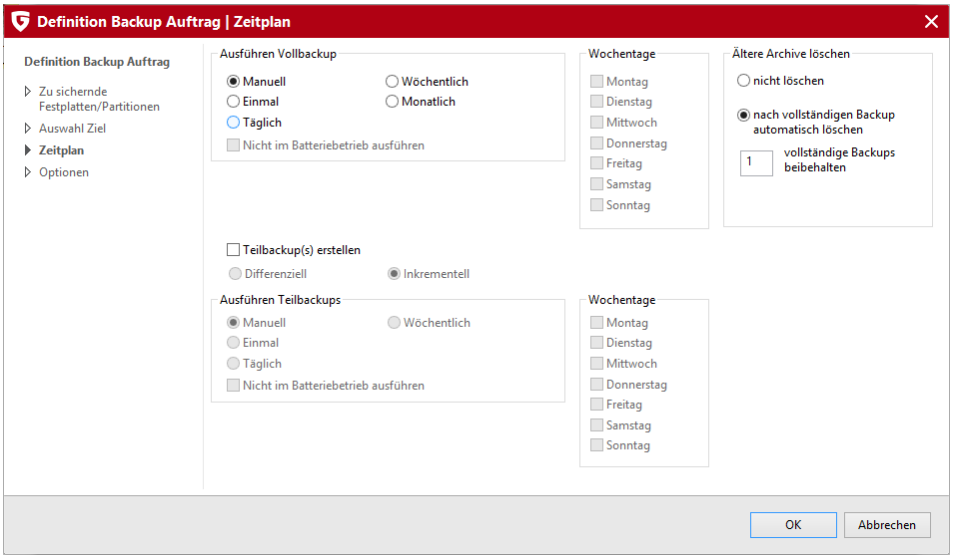
Hier können Sie einerseits festlegen, in welchem Rhythmus Ihre ausgewählten Daten durch ein Backup gesichert werden sollen, andererseits können Sie festlegen, was für eine Art von Backup durchgeführt werden soll. Hier gibt es grundlegend das Vollbackup, in dem alle ausgewählten Daten komplett gesichert werden, wahlweise aber auch die Möglichkeit, über Teilbackups nur die Veränderungen seit dem letzten Backup zu speichern.

Wenn Sie **Manuell** auswählen, wird das Backup nicht automatisch ausgeführt, sondern muss gezielt über die Programmoberfläche von Ihnen gestartet werden. Unter **Täglich** können Sie mit Hilfe der Angaben unter Wochentage z.B. bestimmen, dass Ihr Rechner nur an Werktagen das Tuning durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Darüber hinaus können Sie wöchentliche und monatliche Backups definieren.

**Nicht im Batteriebetrieb ausführen**: Damit ein Backup-Vorgang bei Notebooks nicht plötzlich dadurch unterbrochen wird, dass der Notebook-Akku leer ist, können Sie festlegen, dass Backups nur dann erfolgen, wenn das Notebook ans Stromnetz angeschlossen ist.

## Ausführen Vollbackup

Geben Sie unter **Ausführen Vollbackup** einfach an, wie oft, an welchen Tagen und zu welcher Zeit der jeweilige Backup-Auftrag stattfinden soll. Nun wird in dem angegebenen Turnus automatisch ein Backup aller Daten erstellt, die Sie unter **Auswahl Dateien / Festplatten / Partitionen** dafür ausgewählt haben.




**Achtung**: Das zeitplangesteuerte Backup funktioniert nicht mit CD-ROM oder DVD-ROM, da hier gegebenenfalls beim Wechsel des Rohlings ein Eingreifen des Benutzers erforderlich ist.

Im Abschnitt **Ältere Archive löschen** können Sie bestimmen, wie die G DATA Software mit schon vorhandenen Backups verfährt. Die G DATA Software archiviert Ihre Daten jeweils in einer einzigen Datei mit der Datei-Endung ARC. Bestehende Backups, die nicht überschrieben werden, erhöhen natürlich zusätzlich die Sicherheit Ihrer Daten, da dann selbst in dem Fall, dass das aktuelle Archiv beschädigt sein sollte, ein älteres Archiv zur Verfügung steht, also nicht alle Dateien verloren sind. Generell benötigen Archive allerdings viel Platz auf Datenträgern und so sollten Sie darauf achten, dass sich nicht zu viele Archivdateien ansammeln. Sinnvoll ist es, unter **vollständige Backups beibehalten** eine Maximalanzahl von Backups anzugeben, die auf Ihrem Sicherungsmedium gespeichert werden. Das jeweils älteste Archiv wird dann durch das aktuelle Archiv ersetzt.

Wenn Sie das Häkchen bei **Teilbackup(s) erstellen** setzen, führt die Software nach einem ersten Vollbackup bei folgenden Sicherungen nur noch Teilbackups durch, die erheblich schneller beim Backup-Vorgang sind, ggf. aber länger dauern, wenn aus Ihnen ein Gesamtbackup wiederhergestellt werden muss. Ein weiterer Nachteil des Teilbackups ist ein vergleichsweise hoher Speicherplatzbedarf, da nicht mehr benötigte Daten im Vollbackup ja nicht direkt gelöscht werden. Nach dem nächsten Vollbackup werden die Datenbestände von Voll- und Teilbackup aber wieder zusammengeführt und die Datenmenge ist wieder so, wie bei einem Vollbackup.

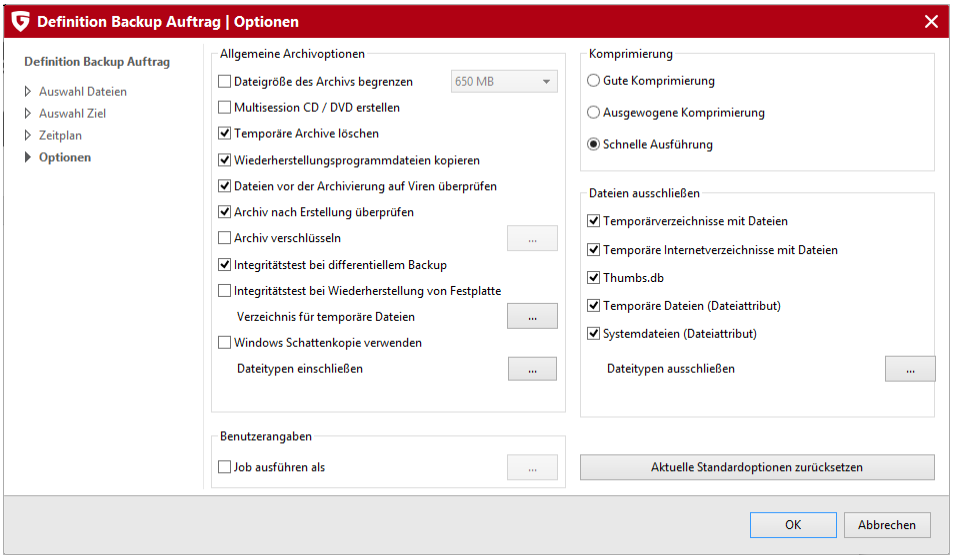
## Ausführen Teilbackups

Teilbackups dienen dazu, eine Datensicherung schneller zu machen. Statt alle Daten für ein Backup zu verwenden, baut das Teilbackup auf ein bestehendes Vollbackup auf und sichert nur die Daten, die sich seit dem letzten Vollbackup verändert haben oder neu erstellt wurden. Auf diese Weise steht Ihnen auch eine komplette Sicherung Ihres Datenbestandes zur Verfügung, wobei der Backup-Vorgang selbst deutlich schneller vonstatten geht.

**Differenziell / Inkrementell**: Bei der differenziellen Sicherung werden alle Daten, die seit der letzten Komplettsicherung geändert wurden oder neu hinzugekommen sind, gespeichert. Es wird also immer wieder auf der letzten Komplettsicherung aufgesetzt. Man spart gegenüber einer neuen Vollsicherung Zeit und Speicherplatz. Die inkrementelle Sicherung geht noch eine Stufe weiter und sichert zwischen zwei Teilbackups die Dateien, die sich von Teilbackup zu Teilbackup geändert haben. Nachteil hierbei ist, dass bei einer Wiederherstellung der Daten mehrere Archive benötigt werden.

# Optionen

Im Optionen-Bereich können Sie allgemeine Backup-Optionen verändern. Im Regelfall müssen Sie hier keine Veränderungen vornehmen, da die G DATA Standardoptionen die meisten Anwendungsfälle abdecken.




## Allgemeine Archivoptionen

In den allgemeinen Archivoptionen haben Sie folgende Einstellungsmöglichkeiten:

- **Dateigröße des Archivs begrenzen**: Wenn Sie Archive auf CD-, DVD-ROM oder anderen beschreibbaren Rohlingen speichern, ist es wichtig, dass die G DATA Software die Größe der Archivdateien begrenzt. Hier haben Sie eine Auswahl von Standardgrößen, die Ihnen das nachträgliche Speichern der Archivdaten auf CD, DVD oder Blu-ray-Discs ermöglicht. Das Archiv wird beim Erreichen der hier angegebenen Maximalgröße gesplittet und die Backup-Informationen werden auf zwei oder mehrere Archivdateien verteilt.

- **Multisession CD / DVD erstellen**: Wenn Sie diese Option wählen, erstellen Sie Backup-CDs oder Backup-DVDs, die mehrfach beschreibbar sind. Dabei wird der vorher gespeicherte Inhalt allerdings nicht gelöscht, sondern nur um den neuen Inhalt ergänzt.

- **Temporäre Archive löschen**: Diese Option sollte generell angeschaltet bleiben. Temporäre Archive benötigen nach einer gewissen Anzahl von Backup-Vorgängen sehr viel Platz auf Ihrer Festplatte und werden nach Ihrer temporären Nutzung eigentlich nicht mehr benötigt.

- **Wiederherstellungsprogrammdateien kopieren**: Wenn Sie diese Funktion aktivieren, wird zusätzlich zu den Archivdaten am Speicherort Ihrer Datensicherung ein Programm aufgespielt, mit dem Sie Ihre Daten auch ohne installierte G DATA Software wiederherstellen können. Starten Sie hierzu von der CD/DVD-ROM das Programm *AVKBackup* bzw. *AVKBackup.exe*.

  Das Wiederherstellungsprogramm wird nur auf CD/DVD-ROM mit kopiert. Bei Sicherheitskopien auf Wechselmedien (USB-Stick, externe Festplatte) ist dies nicht der Fall.

  Wenn Sie die G DATA Software auf dem Rechner installiert haben, auf dem die Wiederherstellung stattfinden soll, führen Sie die Wiederherstellung bitte nicht mit dem Wiederherstellungsprogramm auf der CD/DVD-ROM aus, sondern über die Funktion **Archive importieren**.

- **Dateien vor der Archivierung auf Viren überprüfen**: Wenn das Antiviren-Modul installiert ist, können Sie ihre Daten auf Viren überprüfen, bevor diese im Backup-Archiv gespeichert werden.

- **Archiv nach Erstellung überprüfen**: Diese Funktion dient dazu, das Archiv nach der Erstellung noch mal auf Vollständigkeit und Fehlerlosigkeit zu überprüfen.

- **Archiv verschlüsseln**: Wenn Sie Ihre archivierten Dateien vor Fremdzugriff schützen möchten, können Sie diese mit einem Passwort versehen. Eine Wiederherstellung der Daten kann dann auch nur mit diesem Passwort erfolgen. Sie sollten sich das Passwort gut merken oder an sicherer Stelle notieren. Ohne Passwort sind Ihre Archivdaten nicht wiederherstellbar.

- **Integritätstest bei differentiellem Backup**: Diese Funktion dient dazu, ein Teilbackup nach der Erstellung noch mal auf Vollständigkeit und Fehlerlosigkeit zu überprüfen.

- **Integritätstest bei Wiederherstellung von Festplatte**: Diese Funktion dient dazu, nach einer Wiederherstellung noch einmal das korrekte Rückspielen der Daten zu überprüfen. Beim **Verzeichnis für temporäre Dateien** handelt es sich um den Speicherort für Daten, die die G DATA Software nur zeitweise auf Ihre Festplatte schreibt. Sollte kein ausreichender Platz auf Ihrer

Standardpartition zur Verfügung stehen, können Sie hier die Partition und den temporären Speicherort für diese Dateien wechseln.

- **Windows Schattenkopie verwenden**: Ist diese Option deaktiviert, so kann im laufenden Betrieb kein Image der Systempartition erstellt werden.

## Benutzerangaben

Um überhaupt zeitgesteuerte Backups ausführen zu können, müssen Sie hier das Häkchen beim Eintrag **Job ausführen als** setzen und dort die Zugangsdaten für Ihr Windows Benutzerkonto angeben. Diese Angaben sind nötig, damit das Backup auch dann zeitgesteuert durchgeführt werden kann, wenn Sie nicht als Benutzer angemeldet sind.

## Komprimierung

Im Bereich Komprimierung können Sie festlegen, ob Ihre Archive stark oder schwach komprimiert werden.

- **Gute Komprimierung**: Die Daten werden für das Backup stark komprimiert. Dadurch sparen Sie beim Backup Speicherplatz, aber das Backup selbst dauert länger.
- **Ausgewogene Komprimierung**: Das Backup wird nicht so stark komprimiert, wird dafür aber schneller ausgeführt.
- **Schnelle Ausführung**: Es erfolgt keine Komprimierung der Daten, dafür läuft das Backup aber schnell ab.

## Dateien ausschließen

Generell sichert die G DATA Software Dateien auf Basis ihres Dateiformates. Auf Ihrem Computersystem finden sich entsprechende Dateiformate aber auch in Bereichen, die automatisch verwaltet werden und nicht für ein Backup relevant sind, da die jeweiligen Dateien nur temporär gespeichert wurden (z.B. zur Beschleunigung der Seitendarstellung aus dem Internet). Damit die G DATA Software dies Dateien nicht unnötig mit archiviert, können Sie diese über das Setzen der jeweiligen Häkchen ausschließen.

- **Temporärverzeichnis mit Dateien**: Wenn diese Option gewählt ist, werden die temporären Ordner sowie die dort befindlichen Unterordner und Dateien nicht in die Datensicherung aufgenommen.
- **Temporäre Internetverzeichnisse mit Dateien**: Wenn diese Option gewählt ist, werden die Ordner für die Speicherung von Internetseiten sowie die dort befindlichen Unterordner und Dateien nicht in die Datensicherung aufgenommen.
- **Thumbs.db**: Wenn diese Option gewählt ist, werden die vom Windows Explorer automatisch erstellten Dateien thumbs.db nicht in die Datensicherung aufgenommen. Diese Dateien dienen z.B. dazu die Miniaturansichten für Slideshows zu verwalten und werden aus den Originalbildern automatisch erzeugt.
- **Temporäre Dateien (Dateiattribut)**: Wenn diese Option gewählt ist, werden Dateien mit dem vom System vergebenen Dateiattribut temporär nicht in die Datensicherung übernommen.
- **Systemdateien (Dateiattribut)**: Wenn diese Option gewählt ist, werden Dateien mit dem vom System vergebenen Dateiattribut Systemdatei nicht in die Datensicherung übernommen.
- **Dateitypen ausschließen**: Mit dieser Funktion können Sie selber Datei-Endungen definieren, die nicht in Ihrem Backup berücksichtigt werden. Verfahren Sie dazu folgendermaßen: Geben Sie unter **Dateityp** (z.B. *.txt) die Datei-Endung oder den Dateinamen ein, den Sie ausschließen wollen. Klicken Sie nun auf **OK**. Wiederholen Sie den Vorgang für alle anderen Dateitypen und Dateinamen, die Sie ausschließen möchten, z.B. picasa.ini, *.ini, *bak etc. Das Sternchen-Symbol und das Fragezeichen können Sie hierbei als Platzhalter einsetzen. 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 exe prüfen zu lassen, geben Sie also *.exe ein. Um z.B. Dateien unterschiedlicher Tabellenkalkulationsformate zu überprüfen (z.B. *.xlr, *.xls), geben Sie einfach *.xl? ein. Um Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu prüfen, geben Sie beispielsweise text*.* ein.

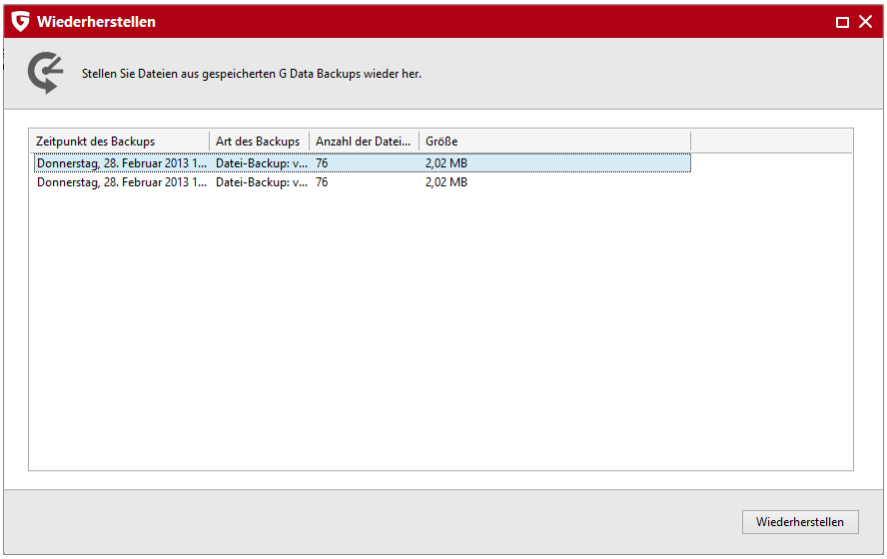
## Aktuelle Standardoptionen zurücksetzen

Mit Anklicken dieser Schaltflächen übernehmen Sie die Optionen, die für die G DATA Software als Standardoptionen definiert wurden. Sollten Sie also beim Erstellen von Backups aus Versehen falsche Optionsvorgaben eingestellt haben und nicht wissen, wie diese zu reparieren sind, klicken Sie die Schaltfläche **Aktuelle Standardoptionen zurücksetzen**.

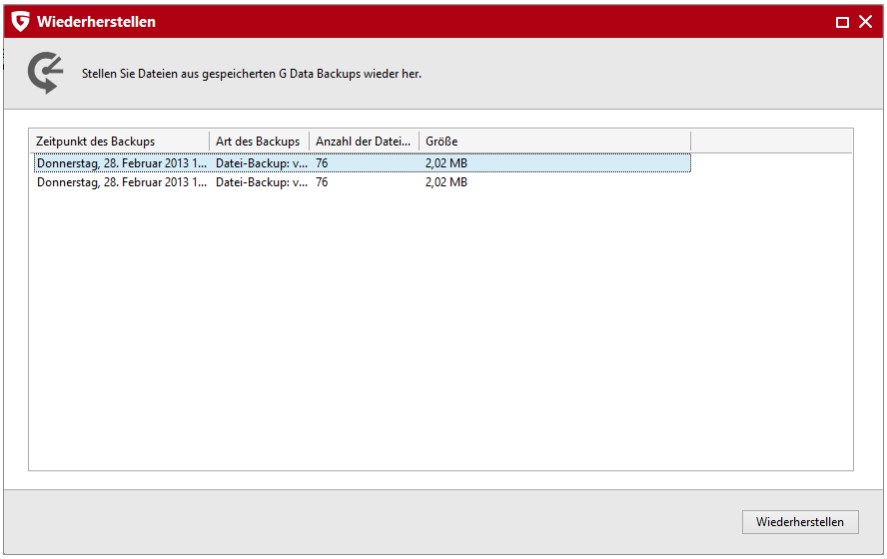
# Backup wiederherstellen

Hier können Sie auf Basis der gesicherten Backup-Daten Ihre Originaldateien nach einem Datenverlust wiederherstellen. Klicken Sie dazu einfach auf die Schaltfläche **Wiederherstellen**.

Nun erscheint ein Dialogfenster, in dem alle gespeicherten Backup-Vorgänge für den jeweiligen Backup-Auftrag aufgeführt sind.

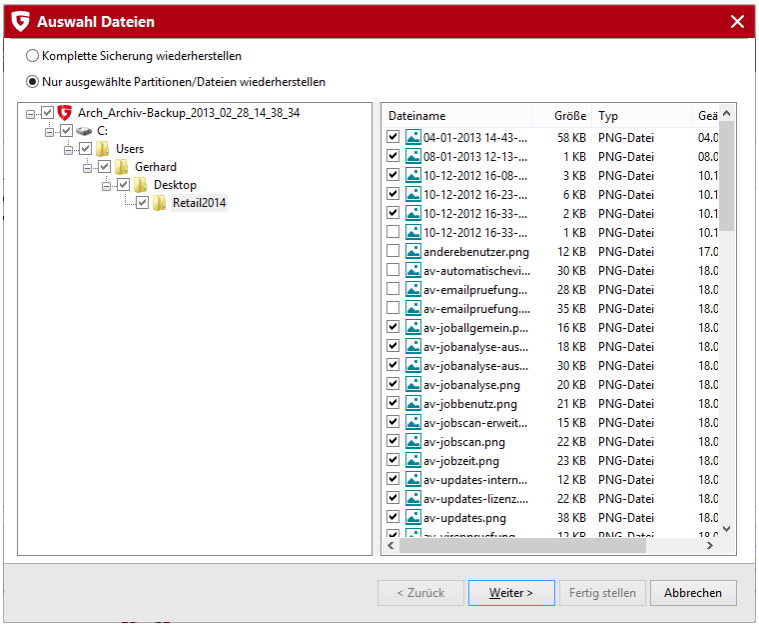



Wählen Sie hier das gewünschte Backup aus (z. B. das zuletzt durchgeführte Backup, falls Sie kurz zuvor versehentlich gelöschte Dokumente wiederherstellen möchten) und tippen dann auf die Schaltfläche **Wiederherstellen**.

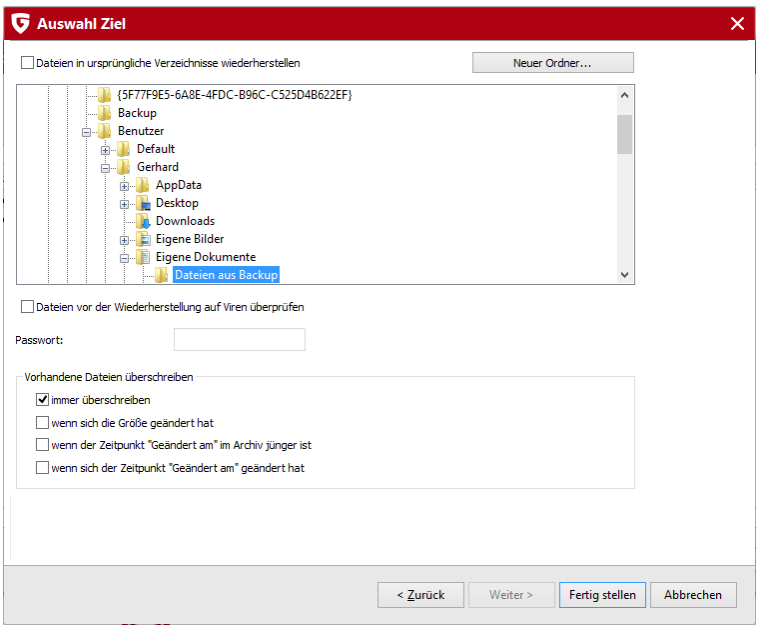



Nun haben Sie die Möglichkeit, festzulegen, welche Form der Wiederherstellung Sie wünschen:

- **Komplette Sicherung wiederherstellen**: Alle Dateien und Ordner, die über dieses Backup gesichert haben, werden wiederhergestellt.
- **Nur ausgewählte Partitionen/Dateien wiederherstellen**: Hier erscheint eine Verzeichnisansicht ihres Backups, in dem Sie gezielt auswählen können, welche Dateien, Ordner oder Partitionen Sie wiederherstellen möchten und welche nicht. 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 aus dem Backup heraus wiederhergestellt. Wenn in einem Verzeichnis nicht alle Dateien geprüft werden, findet sich an diesem Verzeichnis ein graues Häkchen.




Abschließend können Sie festlegen, ob die Dateien in ihren ursprünglichen Verzeichnissen wiederhergestellt werden sollen oder nicht. Sollen die Dateien an anderer Stelle gespeichert werden, können Sie gegebenenfalls unter **Neuer Ordner** einen Ordner auswählen, in dem diese abgelegt werden sollen. Geben Sie unter **Passwort** das Zugangspasswort ein, falls Sie Ihr Backup beim Sichern passwortgeschützt komprimiert haben.



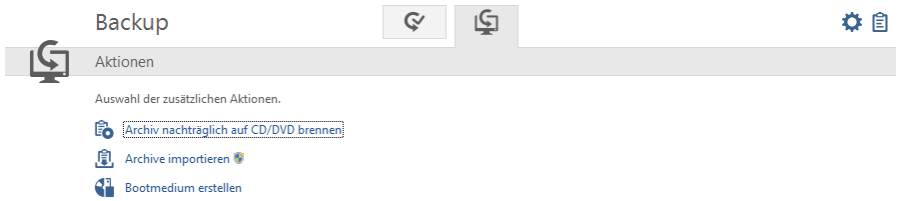

Wenn Sie Dateien in den ursprünglichen Verzeichnissen wiederherstellen, haben Sie folgende Optionen, um gezielt nur geänderte Dateien zurück zu überspielen:

- **immer überschreiben**: In dieser Einstellung werden die Dateien aus der Datensicherung immer wichtiger als die Daten gesehen, die sich im Ursprungsverzeichnis befinden. Sollten Sie hier ein Häkchen setzen, werden eventuell noch vorhandene Daten komplett von den Daten, die sich im Archiv befinden, überschrieben.
- **wenn sich die Größe geändert hat**: Mit dieser Einstellung werden bestehende Daten im Ursprungsverzeichnis nur dann überschrieben, wenn die Ursprungsdatei verändert wurde. Von der Größe her unveränderte Dateien werden übersprungen. Auf diese Weise geht die Wiederherstellung der Daten möglicherweise schneller voran.
- **wenn der Zeitpunkt "Geändert am" im Archiv jünger ist**: Hier werden Dateien immer dann im Ursprungsverzeichnis durch die Kopien aus dem Archiv ersetzt, wenn sie neuer sind, als die Daten des Archivs. Auch hier kann eine Wiederherstellung der Daten schneller vorangehen, da so möglicherweise nicht alle Dateien wiederhergestellt werden müssen, sondern nur geänderte Daten.
- **wenn sich der Zeitpunkt "Geändert am" geändert hat**: Hier werden Daten im Ursprungsverzeichnis immer dann ersetzt, wenn sich am Änderungsdatum im Vergleich zu den archivierten Dateien etwas geändert hat.

Klicken Sie nun abschließend auf die Schaltfläche **Fertig stellen**, um die Wiederherstellung gemäß Ihrer Vorgaben durchzuführen.

# Aktionen

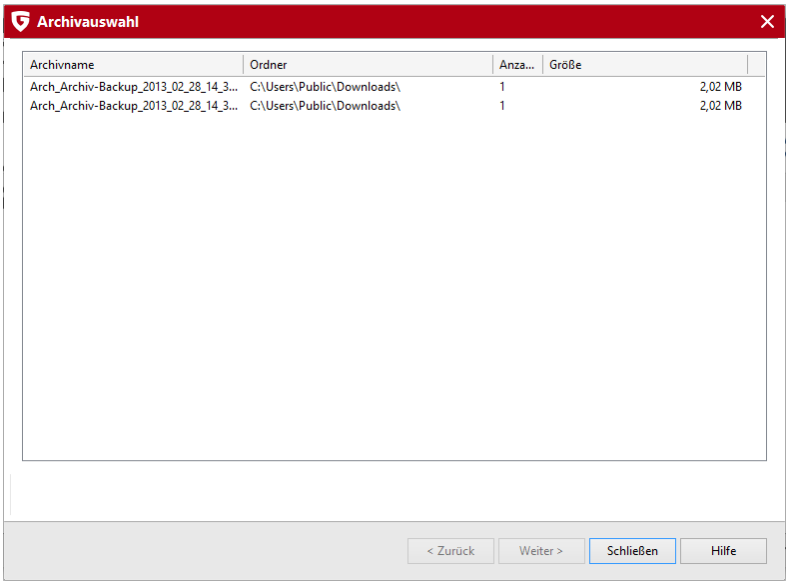
In diesem Bereich können Sie unter anderem Aktionen zur Pflege und Wartung Ihrer Datenbackups vornehmen.



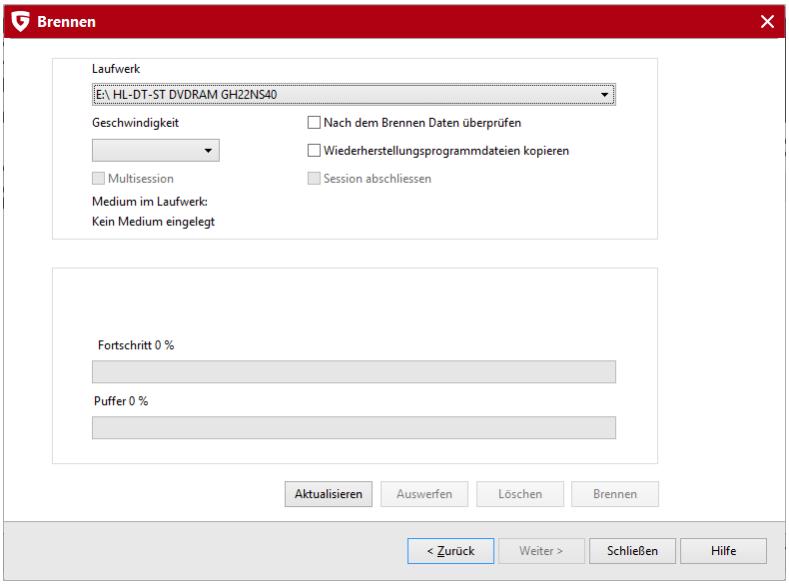

Folgende Dienstprogramme stehen Ihnen hierzu zur Verfügung:

## Archiv nachträglich auf CD/DVD brennen

Sie können Backup-Dateien auch nachträglich auf CD oder DVD brennen. Suchen Sie dazu einfach im erscheinenden Dialogfenster ein Projekt aus, welches Sie brennen möchten und klicken dann auf die **Weiter**-Schaltfläche.




Wählen Sie nun aus, auf welchem Laufwerk Sie das Datenbackup brennen möchten.



Folgende Optionen stehen Ihnen hier zur Verfügung:

- **Nach dem Brennen Daten überprüfen**: Wenn Sie hier ein Häkchen setzen, werden die gebrannten Daten nach dem Brennvorgang noch einmal überprüft. Das dauert etwas länger, als ein Brennvorgang ohne Überprüfung, ist aber generell empfehlenswert.

- **Wiederherstellungsprogrammdateien kopieren**: Wenn Sie diese Funktion aktivieren, wird zusätzlich zu den Archivdaten am Speicherort Ihrer Datensicherung ein Programm aufgespielt, mit dem Sie Ihre Daten auch ohne installierte G DATA Software wiederherstellen können. Starten Sie hierzu von der CD/DVD-ROM das Programm *AVKBackup* bzw. *AVKBackup.exe*.

Klicken Sie auf die Schaltfläche **Brennen**, um den Brennvorgang zu starten. Nach dem Brennvorgang wird die Backup CD/DVD automatisch ausgeworfen.

> **Hinweis**: Natürlich werden die Backup-Daten nach dem Brennvorgang nicht vom Originaldatenträger gelöscht. Das nachträgliche Brennen auf CD/DVD ist eine zusätzliche Sicherung.

# Archive importieren

Um Archive und Datensicherungen wiederherzustellen, die sich nicht auf einem von der G DATA Software verwalteten Laufwerk befinden, verwenden Sie bitte die Funktion **Archive importieren**. Hier öffnet sich dann ein Dialogfenster, in dem Sie die gewünschten Archivdateien mit der Endung *ARC* z.B. auf einer CD, DVD oder im Netzwerk suchen können. Wenn Sie das gewünschte Archiv gefunden haben, markieren Sie es bitte durch ein Häkchen und klicken dann auf die **OK**-Schaltfläche. Ein Info-Fenster weist Sie nun darauf hin, dass das Archiv erfolgreich importiert wurde. Wenn Sie dieses Archiv nun für eine Wiederherstellung von Daten nutzen möchten, begeben Sie sich einfach in den Bereich **Wiederherstellen** der G DATA Software, wählen das gewünschte Backup aus und starten dann die Wiederherstellung.

> **Hinweis**: Von der G DATA Software erstellte Archivdateien haben die Datei-Endung ARC.

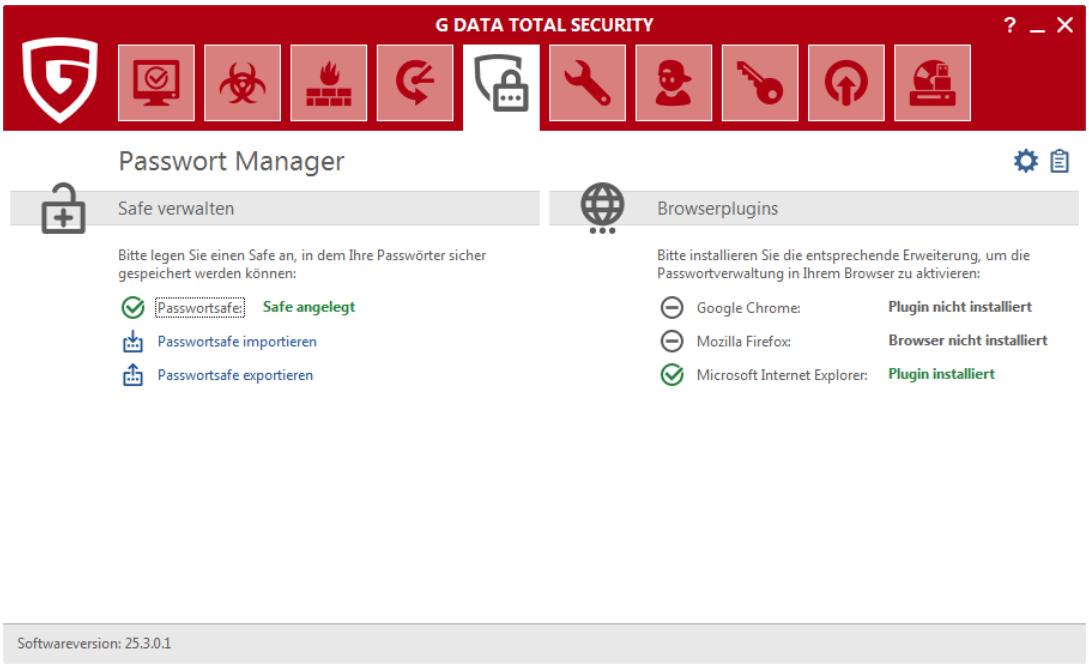
# Bootmedium erstellen

Um Backups auch ohne installierte G DATA Software wiederherstellen zu können, können Sie eine CD/DVD oder einen USB-Stick erstellen, der eine spezielle Software enthält, mit der Sie die Wiederherstellung von Daten durchführen können. Um auf diese Weise Backups wiederherzustellen, starten Sie das Bootmedium und wählen dort das Programm *AVKBackup* bzw. *AVKBackup.exe* aus. Nun können Sie die gewünschten Backups auswählen und die Wiederherstellung starten.

> **Hinweis**: Wie Sie ein Bootmedium erstellen, wird im Kapitel **Bootmedium** erläutert. Das Bootmedium erfüllt bei der G DATA Software eine doppelte Aufgabe. Sie können damit Backup-Wiederherstellungen durchführen und mit dem BootScan Ihren Computer vor dem Start von Windows auf Viren überprüfen.

# Passwort Manager

Über den Passwort Manager können Sie bequem Passwörter verwalten und bequem als Plug-In in Ihrem Browser nutzen.




Der Passwort Manager unterstützt dabei folgende Browser in der jeweils neuesten Generation:

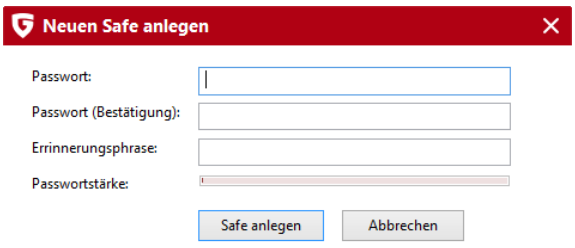
- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

**Hinweis**: Bitte beachten Sie, dass je nach Einstellungen Ihrer Browser (z. B. Datenschutzeinstellungen) die Funktionalität des Passwort Managers eingeschränkt sein kann.

Legen Sie bitte zuerst einen Passwortsafe an und installieren Sie dann das Plug-In für den Browser Ihrer Wahl. Selbstverständlich können Sie auch auf allen kompatiblen Browsern den Passwortsafe installieren.

## Neuen Safe anlegen und Plug-In installieren

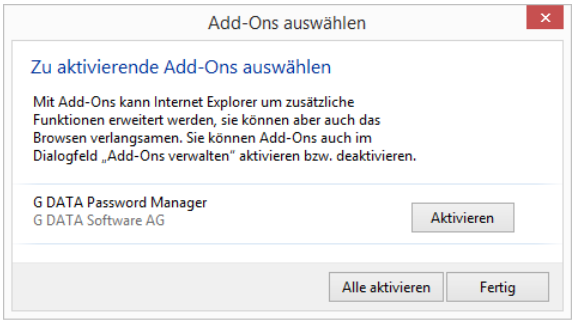
Klicken Sie auf den Eintrag **Passwortsafe**. Nun öffnet sich ein Dialog, in dem Sie über die Auswahl von **Neuen Safe erstellen** einen neuen Safe anlegen können.




Geben Sie hierzu ein Passwort an, bestätigen Sie es, klicken auf **Safe anlegen** und der Safe wird angelegt. Die Erinnerungsphrase kann Ihnen dabei helfen, sich wieder an ein vergessenes Passwort zu erinnern.

Nun ist der Safe angelegt und Sie können auf der rechten Seite des Programmfensters auswählen, in welchen Browsern Sie das Passwort Manager Plug-In installieren möchten. Klicken Sie dazu einfach auf den jeweiligen Browsernamen und das Plug-In wird installiert.

Wenn Sie nun den Browser das nächste Mal öffnen, kann es sein, dass Sie gefragt werden, ob Sie das neue Plug-In verwenden möchten. Bitte bestätigen Sie dieses für den G DATA Password Manager




Nun finden Sie folgendes Symbol in der Taskleiste des Browsers. Durch einen Klick auf das Symbol können Sie den Passwort Manager nutzen.


Geben Sie hierzu bitte Ihr Passwort im erscheinenden Dialog ein und klicken Sie auf **Entriegeln**. Die Verwendung des Browser Plug-Ins wird im folgenden **Kapitel** erläutert.

# Verwendung des Browser Plug-Ins

Durch Anklicken des folgenden Symbols in der Taskleiste des Browsers können Sie den Passwort Manager nutzen.

**Hinweis**: Bitte beachten Sie, dass je nach Einstellung der Privatsphäre (z. B. Speichern des Verlaufs) die Nutzung des Plug-Ins nicht möglich ist. Bei Problemen mit dem Plug-In prüfen Sie daher bitte zunächst die Einstellungen Ihres Browsers.


Geben Sie hierzu bitte Ihr Passwort im erscheinenden Dialog ein und klicken Sie auf **Entriegeln**. Nun stehen Ihnen folgende Bereiche zur Verfügung:

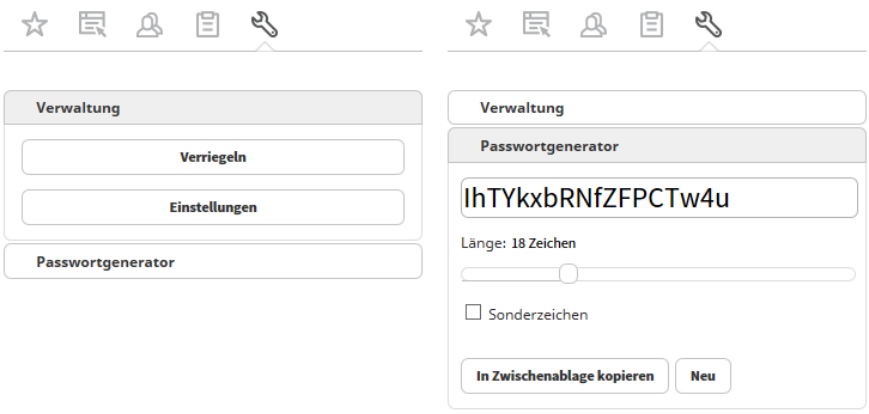
**Favoriten**: Über diese Funktion können Sie schnell die passwortgeschützten Webseiten aufrufen, die Sie regelmäßig nutzen.

**Logins**: Hier verwalten Sie die Logins für passwortgeschützte Webseiten.

**Kontakte**: Mithilfe der hier eingetragenen Kontaktdaten können Formulare, wie z. B. Lieferanschriften automatisch ausgefüllt werden.

**Notizen**: Hier können Sie zusätzliche Notizen passwortgeschützt speichern.

**Einstellungen**: Um den Passwort Manager wieder zu schließen, klicken Sie bitte hier auf **Verriegeln**. Wenn Sie auf Einstellungen klicken, können Sie Favoriten, Logins, Kontakte und Notizen bequem in Dialogfeldern verwalten. Über den Passwortgenerator können Sie sich automatisch ein sicheres Passwort erzeugen lassen und über die Zwischenablage direkt weiterverwenden.

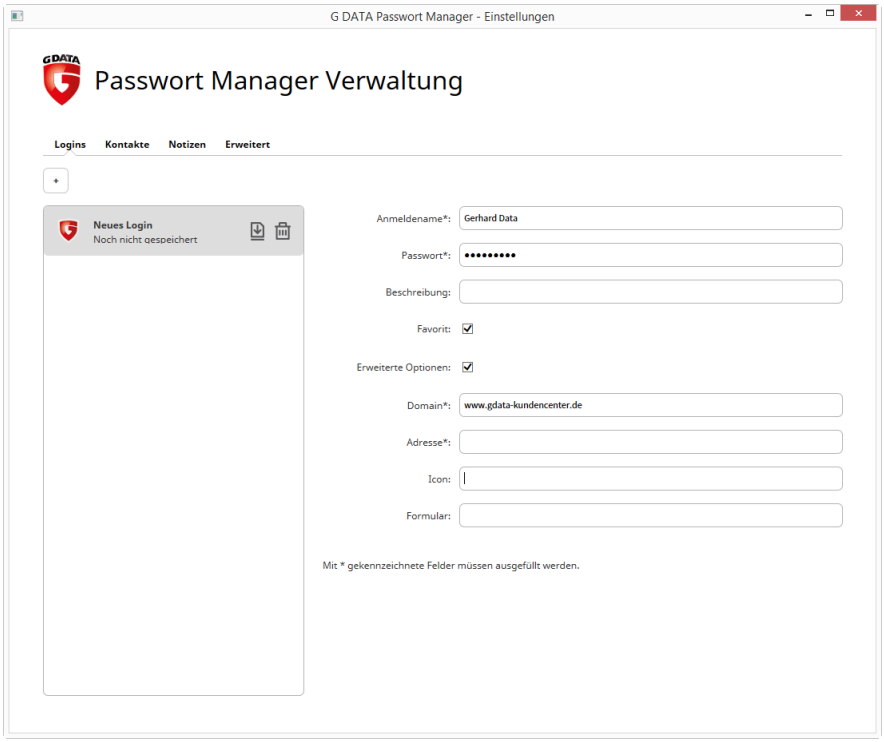



In der Passwort Manager Verwaltung können Sie folgendermaßen neue Einträge hinzufügen, editieren und löschen.

Neuer Eintrag: Durch Anklicken dieses Buttons können Sie einen neuen Eintrag verfassen und alle notwendigen Daten in die jeweiligen Dialogfelder für Logins, Kontakte oder Notizen eintragen.

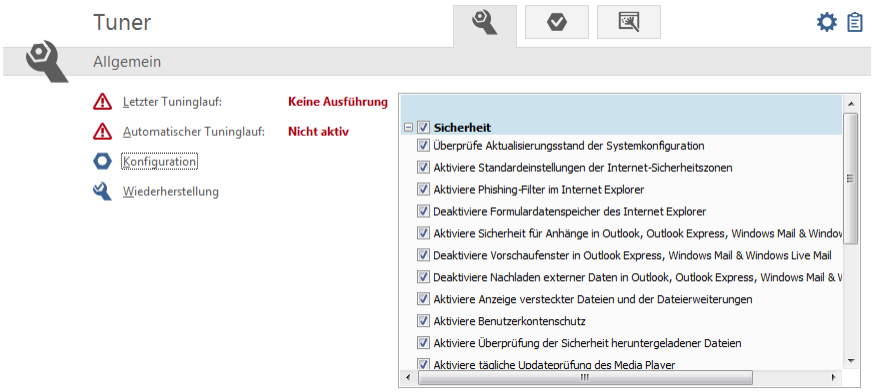
Eintrag speichern: Durch Anklicken dieses Buttons wird der Eintrag gespeichert und taucht dann auch in der Schnellauswahl des Browser Plug-Ins auf.

Eintrag löschen: Hiermit löschen Sie Einträge, die Sie nicht mehr benötigen.


G DATA Passwort Manager - Einstellungen
Passwort Manager Verwaltung
Logins
Kontakte
Notizen
Erweitert
Neues Login
Noch nicht gespeichert
Anmeldename*:
Gerhard Data
Passwort*:
Beschreibung:
Favorit:
Erweiterte Optionen:
Domain*:
www.gdata-kundencenter.de
Adresse*:
Icon:
Formular:
Mit * gekennzeichnete Felder müssen ausgefüllt werden.

# Tuner

Von der automatischen Erinnerung an Windows Updates über eine regelmäßige zeitgesteuerte Defragmentierung bis hin zur regelmäßigen Entfernung von überflüssigen Registry-Einträgen und temporären Dateien haben Sie mit dem Tuner ein Tool an der Hand, welches Ihr Windows-System deutlich schneller und übersichtlicher macht.




Sie können Ihren Computer entweder manuell auf Knopfdruck tunen oder zeitgesteuert regelmäßige Tuning-Aufträge durchführen lassen.

**Letzter Tuninglauf**: Hier wird Ihnen angezeigt, wann das letzte Mal ein Tuning Ihres Computers durchgeführt wurde. Um ein neues Tuning zu starten, wählen Sie hier bitte durch Anklicken des Eintrags **Tuninglauf jetzt durchführen** an. Sobald Sie den Tuninglauf starten, zeigt Ihnen ein Fortschrittsbalken den aktuellen Status des Tunings an.

**Automatischer Tuninglauf**: Wenn Sie das Tuning Ihres Rechners automatisieren wollen, können Sie hier über Anklicken des Eintrags **Automatischen Tuninglauf aktivieren** einen entsprechenden zeitgesteuerten Auftrag erzeugen. Um den automatischen Tuninglauf einzustellen, wählen Sie bitte die Option **Weitere Einstellungen** aus.

**Konfiguration**: Im diesem **Bereich** können Sie alle Module auswählen, die der Tuner für einen Tuning-Vorgang verwenden soll. Ausgewählte Module werden dabei dann entweder über eine automatische zeitgesteuerte Aktion gestartet (siehe Kapitel **Zeitplanung**) oder manuell. Um ein Modul zu aktivieren, führen Sie einfach einen Doppelklick mit der Maus darauf aus. Folgende großen Tuning-Bereiche können Sie hier individuell optimieren:

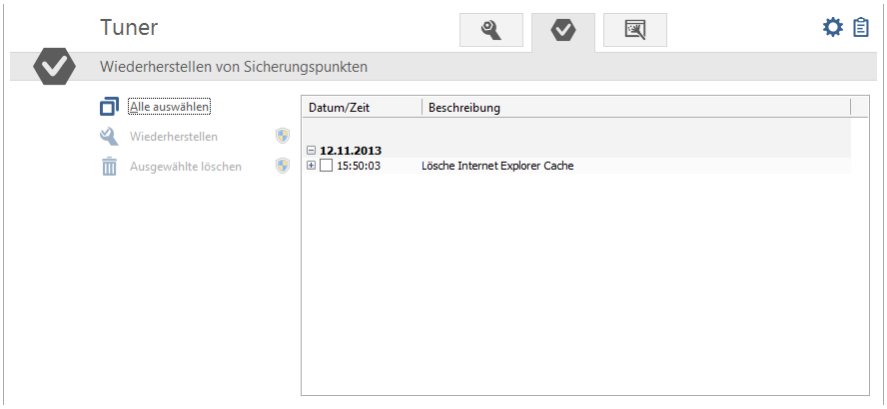
- *Sicherheit*: Diverse Funktionen, die automatisch Daten aus dem Internet nachladen, haben lediglich für den Anbieter und nicht für Sie sinnvolle Aspekte. Oftmals wird über solche Funktionen auch Schadsoftware Tür und Tor geöffnet. Mit diesen Modulen schützen Sie Ihr System und halten es auf dem neuesten Stand.
- *Leistung*: Temporäre Dateien, z. B. nicht mehr benötigte Sicherheitskopien, Protokolldateien oder Installationsdaten, die nach der Installation nur noch Festplattenplatz belegen, bremsen Ihre Festplatte aus und belegen wertvollen Speicherplatz. Darüber hinaus verlangsamen nicht mehr benötigte Prozesse und Dateiverknüpfungen Ihr System merklich. Mit den hier aufgelisteten Modulen können Sie Ihren Rechner von diesem überflüssigen Ballast befreien und beschleunigen.
- *Datenschutz*: Hier sind die Module zusammengefasst, die sich mit dem Schutz Ihrer Daten befassen. Spuren, die beim Surfen oder der allgemeinen Computernutzung unfreiwillig entstehen und viel über Ihr Nutzerverhalten oder sogar wichtige Daten und Passwörter verraten, werden hier gelöscht.

**Wiederherstellung**: Die Software setzt bei jeder durchgeführten Änderung einen Wiederherstellungspunkt. Sollte eine der durchgeführten Tuning-Aktionen zu unerwünschten Ergebnissen geführt haben, können Sie diese so rückgängig machen und den Zustand des Systems vor der jeweiligen Änderung wiederherstellen. Lesen Sie hierzu auch das Kapitel **Wiederherstellung**.

**Browser Cleaner**: Der G DATA Browser Cleaner ist in der Lage, unerwünschte Programmkomponenten und Zusatzprogramme zu blockieren oder zu entfernen. Diese Programme werden oft mit kostenloser Software mitinstalliert und können Browser-Einstellungen verändern oder sogar Daten ausspionieren. Lesen Sie hierzu auch das Kapitel **Browser Cleaner**.

# Wiederherstellung

Die Software setzt bei jeder durchgeführten Änderung einen Wiederherstellungspunkt. Sollte eine der durchgeführten Tuning-Aktionen zu unerwünschten Ergebnissen geführt haben, können Sie diese so rückgängig machen und den Zustand des Systems vor der jeweiligen Änderung wiederherstellen.



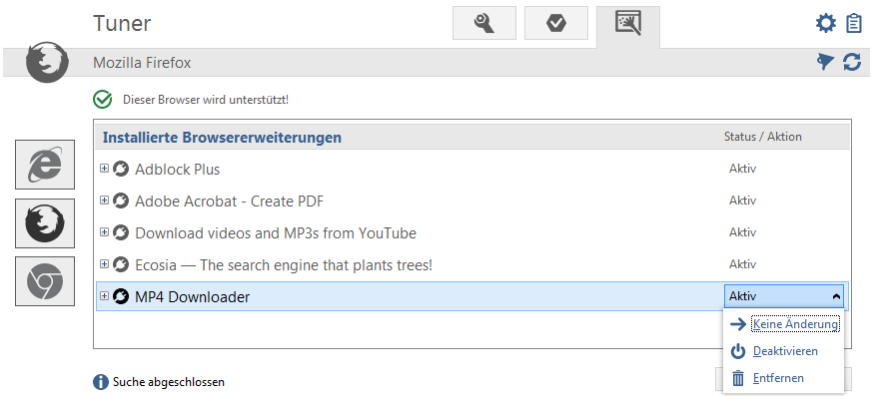

**Alle auswählen**: Wenn Sie alle Änderungen, die durch das Tuning erfolgten, verwerfen möchten, dann wählen Sie hiermit alle Wiederherstellungspunkte aus und klicken danach auf die Schaltfläche **Wiederherstellen**.

**Wiederherstellen**: Wenn Sie nur gezielt Änderungen, die durch das Tuning erfolgten, verwerfen möchten, dann wählen Sie hier einfach den gewünschten Wiederherstellungspunkt aus und klicken danach auf die Schaltfläche **Wiederherstellen**.

**Ausgewählte Löschen**: Wiederherstellungspunkte, die Sie nicht mehr benötigen, können Sie über diese Schaltfläche entfernen.

# Browser Cleaner

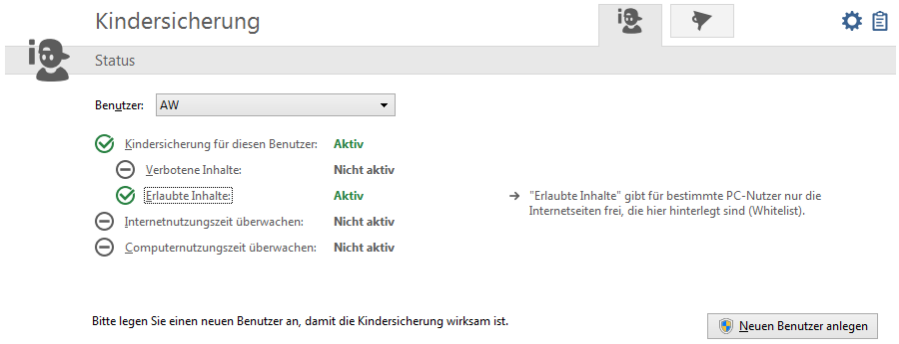
Der G DATA Browser Cleaner ist in der Lage, unerwünschte Programmkomponenten und Zusatzprogramme zu blockieren oder zu entfernen. Diese Programme werden oft mit kostenloser Software mitinstalliert und können Browser-Einstellungen verändern oder sogar Daten ausspionieren. Mit dem Browser Cleaner können Sie sich diese unerwünschten Programme ("PUP" = Potentially Unwanted Programs) bei den Browsern Internet Explorer, Firefox und Google Chrome anzeigen lassen und selbst bestimmen, ob diese nur deaktiviert oder vollständig entfernt werden sollen. Das Deaktivieren der Erweiterungen kann jederzeit wieder rückgängig gemacht werden.




**Hinweis:** Der G DATA Browser Cleaner arbeitet mit Microsoft Internet Explorer, Mozilla Firefox und Google Chrome zusammen und ermöglicht eine spielend leichte Verwaltung aller installierten Browser-Erweiterungen. Mit einem Mausklick lassen sich alle Plug-Ins in der Liste deaktivieren oder entfernen, um den Browser von unerwünschten Erweiterungen zu befreien. Das Tool zeigt per Option alle als sicher eingestuften Plug-Ins an, um sie schnell und leicht von unsicheren oder unerwünschten Erweiterungen unterscheiden zu können. Der G DATA Browser Cleaner ist in der umfassenden Sicherheitslösung G DATA Total Security enthalten und steht dessen Nutzern immer zur Verfügung.

# Kindersicherung

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



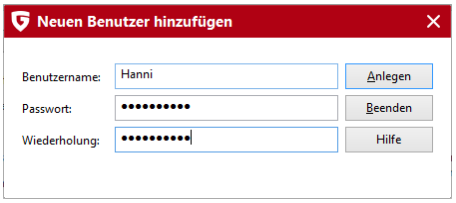

Wählen Sie unter **Benutzer** einen auf Ihrem Rechner angemeldeten Benutzer aus und stellen dann darunter die entsprechenden Beschränkungen für diesen ein. Über die Schaltfläche **Neuen Benutzer anlegen** können Sie auch direkt neue Konten auf Ihrem Rechner einrichten (z.B. für ihre Kinder).

- **Kindersicherung für diesen Benutzer**: Hier können Sie die Kindersicherung für den oben ausgewählten Benutzer ein- oder ausschalten.
- **Verbotene Inhalte**: In diesem Bereich wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet blockieren können. Klicken Sie auf **Bearbeiten**, um die verbotenen Inhalte für den jeweiligen Benutzer zu bestimmen.
- **Erlaubte Inhalte**: Über diesen Bereich wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet erlauben können. Klicken Sie auf **Bearbeiten**, um die erlaubten Inhalte für den jeweiligen Benutzer zu bestimmen.
- **Internetnutzungszeit überwachen**: Hier können Sie festlegen, wie lange und zu welchen Zeiten der gewählte Benutzer Internetzugriff hat. Klicken Sie auf **Bearbeiten**, um die Nutzungszeiten für den jeweiligen Benutzer zu bestimmen.
- **Computernutzungszeit überwachen**: Hier können Sie festlegen, wie lange und zu welchen Zeiten der gewählte Benutzer den Computer verwenden darf. Klicken Sie auf **Bearbeiten**, um die Nutzungszeiten für den jeweiligen Benutzer zu bestimmen.

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

# Neuen Benutzer anlegen

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

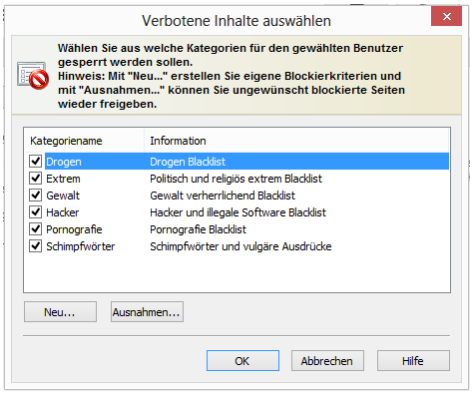



**Hinweis**: Ein Passwort sollte im Hinblick auf Sicherheitsaspekte mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben, sowie Zahlen enthalten.

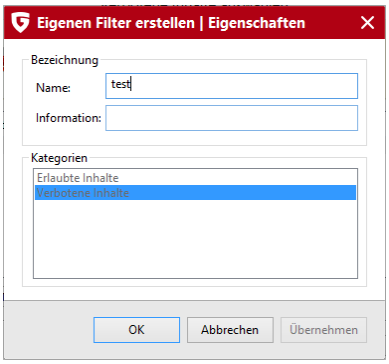
Nun erscheint unter **Benutzer** der neu angelegte Benutzername, gleichzeitig wird ein Windows-Benutzerkonto für diesen Benutzer angelegt. Das bedeutet, dass die Kindersicherung automatisch für die Person mit den jeweiligen Einstellungen aktiv ist, die sich mit ihrem Benutzernamen beim Start von Windows 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

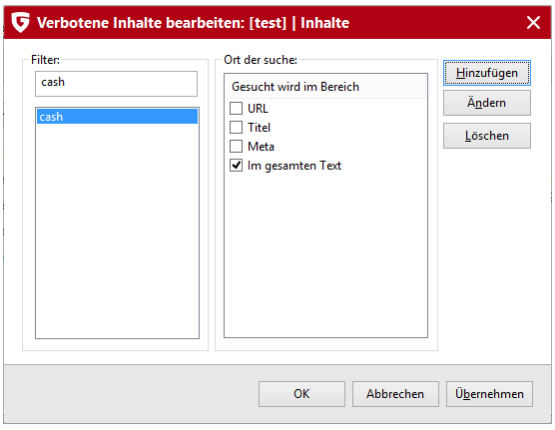
In diesem Bereich wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet blockieren können. Wählen Sie dazu die gewünschten Kategorien, die geblockt werden sollen durch Setzen eines Häkchens aus. Klicken Sie nun auf **OK** und die Internetseiten,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




Wenn Sie die **Neu**-Schaltfläche anklicken, öffnet sich ein Dialogfenster, in dem Sie eigene Blockier-Kriterien (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.

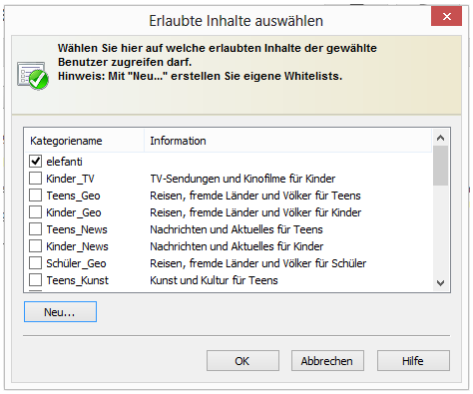
- **Im gesamten Text**: Wenn Sie den lesbaren Inhalt einer Seite direkt auf zu blockierende Inhalte überprüfen möchten, geben Sie einfach den zu blockierenden Begriff - z.B. *chat* - ein, setzen das Häkchen bei **Im gesamten Text** und dann auf die Schaltfläche **Hinzufügen** klicken. Es werden nun alle Seiten blockiert, die im angezeigten Seitentext irgendwie die Buchstabenfolge *chat* enthalten.

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 **Ausnahmen**-Schaltfläche und geben dort die entsprechende Seite ein.

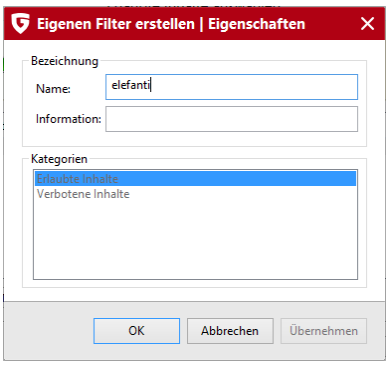
> **Hinweis**: Selbst erstellte Filter können Sie im Bereich **Eigene Filter** beliebig bearbeiten und ggf. auch löschen. Lesen Sie hierzu das Kapitel **Eigene Filter**.

# Erlaubte Inhalte

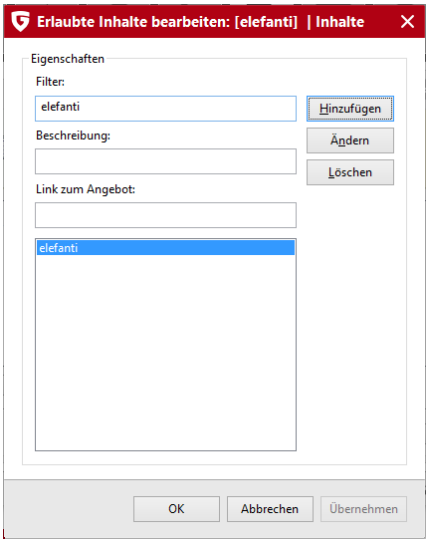
Über diesen Bereich wird ein Dialogfenster geöffnet, in dem Sie für den aktuell angezeigten Benutzer spezielle Inhalte im Internet erlauben können. Wählen Sie dazu die gewünschten Kategorien, die erlaubt werden sollen durch Setzen eines Häkchens aus. Klicken Sie nun auf **OK** und die Internetseiten,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

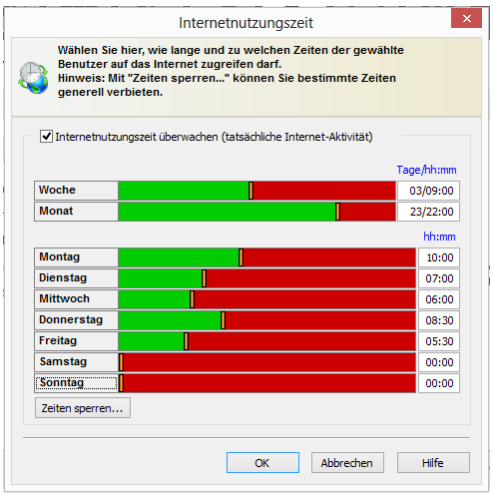



Geben Sie dazu unter **Filter** ein, welche Domain-Namensbestandteile erlaubt sein sollen. Wenn Sie z.B. eine Webseite mit kinderfreundlichen Inhalten freigeben wollen, können Sie hier z.B. *www.fragfinn.de* eingeben und erlauben damit den Zugriff auf diese Webseite. Geben Sie nun unter **Beschreibung** ein, was auf dieser Webseite zu finden ist, z.B. *fragFINN - Das Netz für Kids* 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.

> **Hinweis**: 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.

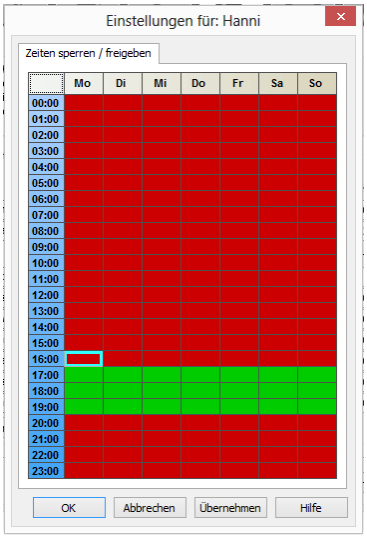



> **Hinweis**: Im Zusammenspiel der Angaben zur Internetnutzung zählt immer der jeweils kleinste Wert. Wenn Sie also für den Monat eine zeitliche Beschränkung von vier Tagen festlegen, in der Woche aber z.B. fünf Tage erlauben, beschränkt die Software die Internetnutzung für den Benutzer automatisch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

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

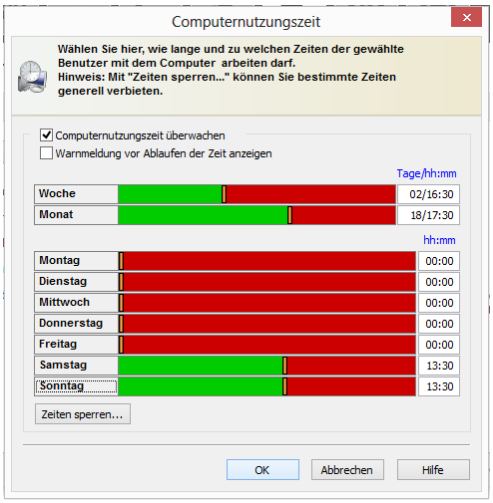
# Zeiten sperren

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

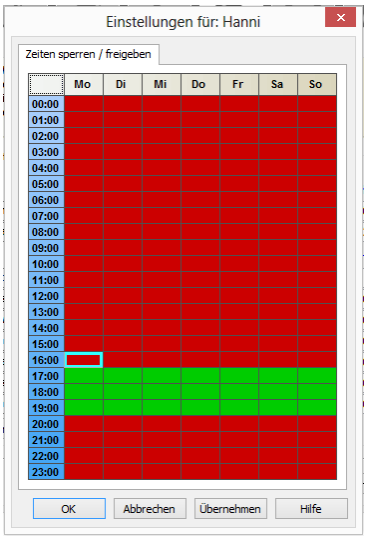
Hier können Sie festlegen, wie lange und zu welchen Zeiten der gewählte Benutzer den Computer verwenden darf. Setzen Sie dazu das Häkchen bei **Computernutzungszeit überwachen**. Nun können Sie festlegen, wie lange der Benutzer im Monat insgesamt den Computer nutzen darf, wie lange pro Woche und wie 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.




**Hinweis**: 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.

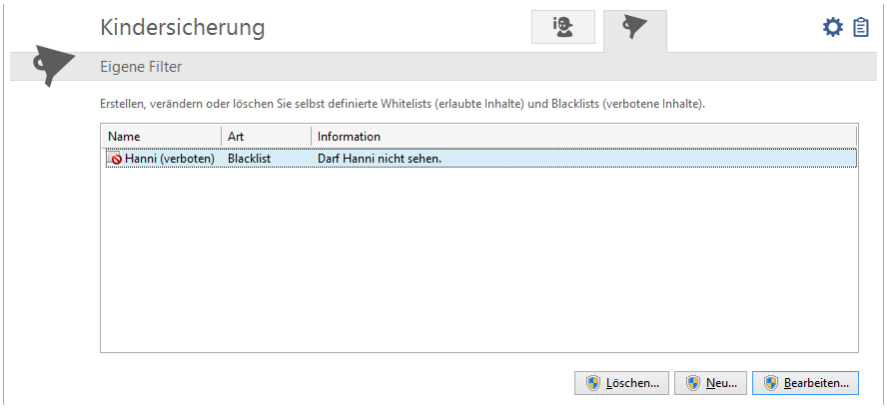
# Zeiten sperren

Über die Schaltfläche **Zeiten sperren** können Sie ein Dialogfeld aufrufen, in dem Sie - zusätzlich zur mengenmäßigen Eingrenzung der Computernutzung - 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**.




# 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:

- **Erlaubte Inhalte**: Wenn Sie für einen der oben ausgewählten Benutzer eine Whitelist auswählen, kann dieser ausschließlich Webseiten ansehen, die sich auf dieser Whitelist befinden. Sie als Administrator können 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.

- **Verbotene Inhalte**: 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.

Folgende Schaltflächen ermöglichen Ihnen die Bearbeitung der Ausschlusslisten:

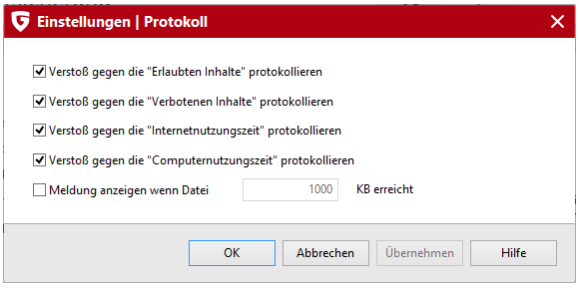
- **Löschen**: Über die Funktion **Löschen** können Sie mit der Maus ausgewählte Listen einfach löschen.

- **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.

# Einstellungen: Protokoll

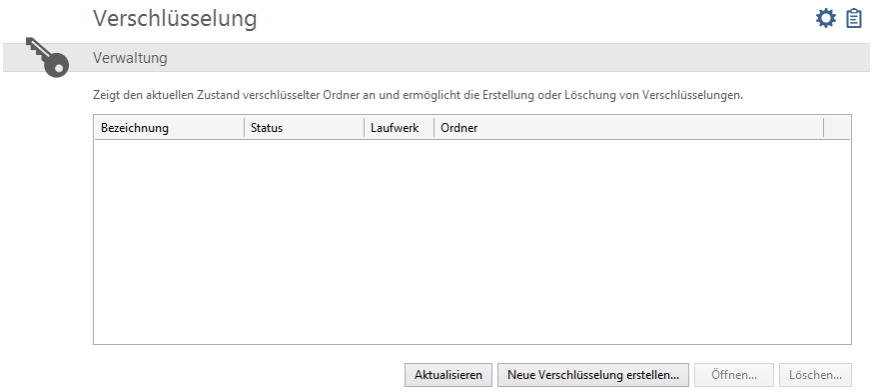
Über diesen Bereich können Sie grundlegende Einstellungen für die Informationen im Protokoll-Bereich verändern. So können Sie festlegen, ob Verstöße gegen erlaubte und/oder verbotene Inhalte protokolliert werden sollen oder nicht. Wenn die Inhalte protokolliert werden, können Sie die Protokolle der unterschiedlichen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

# Verschlüsselung

Das Verschlüsselungsmodul dient wie ein Banktresor zur Absicherung von sensiblen Daten. Ein Safe kann z.B. als Extra-Laufwerk wie eine weitere Festplattenpartition benutzt werden und ist sehr leicht zu bedienen.




Um Safes zu erstellen und zu verwalten haben Sie folgende Auswahlmöglichkeiten:

- **Aktualisieren**: Wenn Sie außerhalb des Verschlüsselungsmoduls zwischenzeitlich Safes geöffnet oder geschlossen haben, empfiehlt es sich, auf **Aktualisieren** zu klicken, um die Statusansicht für die vom Verschlüsselungsmodul verwalteten Safes auf den neuesten Stand zu bringen.
- **Öffnen / Schließen**: Hier können Sie Ihre Safes, die sich auf Ihrem Computer und den angeschlossenen Speichermedien befinden, öffnen oder schließen. Bitte beachten Sie, dass Sie zum Öffnen des Safes das Passwort benötigen, dass Sie für den Safe bei der Erstellung vergeben haben. Safes können hier ohne Passwort geschlossen werden.
- **Neue Verschlüsselung erstellen**: Über diese Funktion können Sie einen neuen Safe anlegen. Dazu öffnet sich ein Assistent, der Ihnen beim Anlegen dieses Safes hilft. Lesen Sie hierzu das Kapitel **Neuen Safe erstellen**.
- **Portablen Safe erstellen**: Sobald Sie einen Safe erstellt haben, können Sie ihn auch zu einem portablen Safe machen, d.h. Sie können ihn so konfigurieren, dass Sie ihn auf einem USB-Stick verwenden oder sogar per Mail verschicken können. Lesen Sie hierzu das Kapitel **Portablen Safe erstellen**.
- **Löschen**: In der Safe-Verwaltung haben Sie eine Übersicht über alle Safes, die sich auf Ihrem Computer und den angeschlossenen Speichermedien befinden. Hier können Sie nicht mehr benötigte Safes auch löschen. Bitte beachten Sie, dass Sie Safes hier auch löschen können, ohne ihr Passwort zu kennen. Sie sollten deshalb Sorge tragen, dass sie den Inhalt des zu löschenden Safes wirklich nicht mehr benötigen.

# Neuen Safe erstellen

Wenn Sie einen neuen Safe erstellen möchten, werden Sie dabei von einem interaktiven Dialog unterstützt. Klicken Sie auf die Schaltfläche **Weiter**, um fortzufahren.

# Speicherort und Größe des Safes

Geben Sie nun bitte an, wo der Safe gespeichert werden soll und welche Größe der Safe haben soll.

> **Hinweis**: Der Safe ist eigentlich eine geschützte Datei, die allerdings wie eine Festplattenpartition wirkt, wenn sie geöffnet ist. D.h. Sie erzeugen über den Speicherort eine Safe-Datei an einem von ihnen gewünschten Ort auf Ihrer Festplatte. Hier werden ihre Daten verschlüsselt gespeichert. Wenn Sie den Safe geöffnet haben und damit arbeiten, können Sie aber Dateien und Verzeichnisse darin bearbeiten, löschen, kopieren und verschieben, wie auf einer normalen Festplatte bzw. Festplattenpartition.

## Speicherort

Wählen Sie hier bitte aus, auf welchem Datenträger (z.b. Lokaler Datenträger (C:)) der Safe erstellt werden soll.

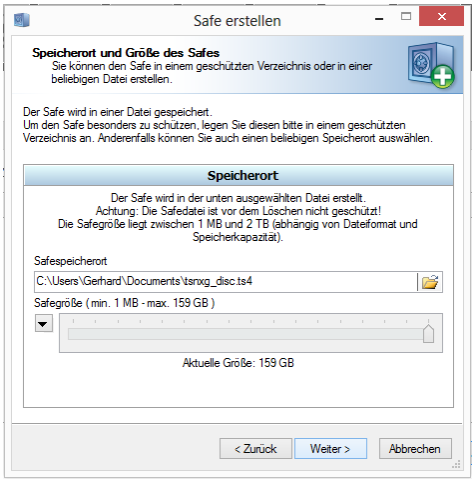
> **Hinweis**: Safes, die in einem geschützten Verzeichnis erstellt werden, sind nur dann auf Ihrem Computer zu sehen, wenn die G DATA Software auf Ihrem Rechner installiert wird. Sollten Sie die Software deinstallieren, sind die so erzeugten Datensafes nicht mehr sichtbar.

## Safegröße

Wählen Sie anschließend eine Safegröße aus, indem Sie den Schieberegler entsprechend positionieren. Sie haben dabei so viel Platz, wie am ausgesuchten Speicherort noch vorhanden ist. Generell sollten Sie aber mindestens 2 GB unter der Maximalgröße bleiben, damit Ihr Computersystem auf Grund von Speicherplatzmangel in anderen Bereichen nicht ausgebremst wird.

> **Hinweis**: Die Schaltfläche links vom Schieberegler für die Safegröße gibt Ihnen die Möglichkeit einer Schnellauswahl. So können Sie dort z.B. den Safe ganz genau von der Größe her definieren oder ihn z.B. gleich so groß machen, dass er gegebenenfalls auf eine CD, DVD oder BluRay gebrannt werden kann.

Klicken Sie nun auf die Schaltfläche **Weiter**.

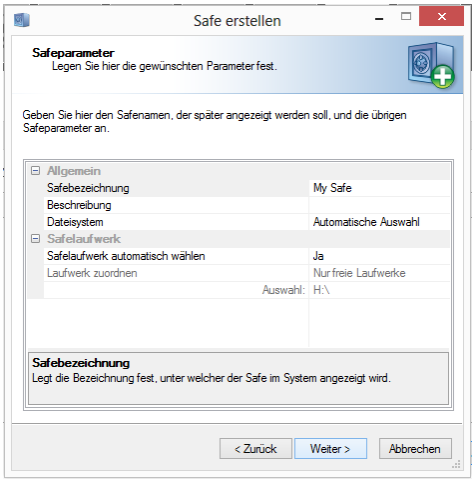



# Safeparameter

In diesem Dialogfenster können Sie folgende Angaben und Einstellungen zum Safe durchführen:

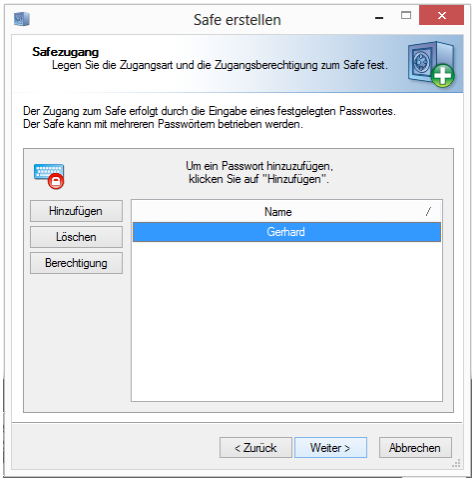
- **Safebezeichnung**: Der Name, unter dem der Safe von der G DATA Software verwaltet wird.
- **Beschreibung**: Eine zusätzliche Kurzbeschreibung, die z.B. Informationen zum Safe-Inhalt enthält.
- **Dateisystem**: Hier können Sie festlegen, ob das virtuelle Laufwerk, welches der Safe erzeugt, das Dateisystem FAT oder NTFS nutzt. In der Regel sollten Sie hier den Eintrag **Automatische Auswahl** stehen lassen.
- **Safelaufwerk automatisch wählen**: Der Safe erscheint auf Ihrem Computer wie ein Festplattenlaufwerk. Sie können hier entweder einen festen Laufwerksbuchstaben für den Safe vergeben oder das System automatisch einen auswählen lassen. In der Regel ist hier die automatische Auswahl empfehlenswert.
- **Laufwerk zuordnen**: Diese Auswahl steht Ihnen nur dann zur Verfügung, wenn Sie das Safelaufwerk nicht automatisch von der Software wählen lassen.

Klicken Sie nun auf die Schaltfläche **Weiter**.

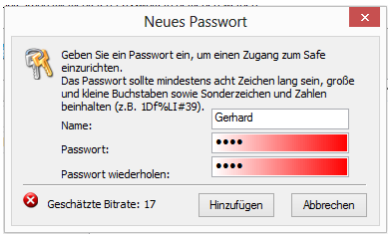



# Safezugang

Hier können Sie ein Passwort für einen Safe vergeben. Klicken Sie dazu auf die Schaltfläche **Hinzufügen**.




Geben Sie nun in dem erscheinenden Dialogfeld unter **Passwort** und **Passwort wiederholen** das gewünschte Passwort ein. Das Passwort wird erst akzeptiert, wenn beide Passworteingaben identisch sind. Dies soll Sie z.B. davor schützen, durch einen Tippfehler ein Passwort zu vergeben, dass Sie selber nicht mehr wiederherstellen können.




Klicken Sie auf **Hinzufügen**, um das Passwort zu aktivieren und danach auf **Weiter**, um die Konfiguration des Safes abzuschließen.

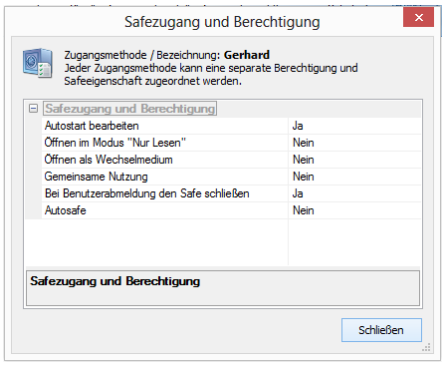
> **Hinweis**: Sie können beim Erstellen eines Safes auch mehrere unterschiedliche Passwörter vergeben und damit unterschiedliche Berechtigungen definieren. So können Sie z.B. einen Safe für sich erstellen, in dem Sie Dateien lesen und verändern können, anderen Leuten mit einem anderen Passwort aber auch die Möglichkeit eröffnen, den Inhalt dieses Safes zu lesen, aber nicht zu verändern.

Wenn Sie nach der Erstellung des Safes diesen anwählen und auf die Schaltfläche **Berechtigung** klicken, haben Sie folgende Einstellungsmöglichkeiten:

- **Autostart bearbeiten**: In jedem Safe befindet sich ein Verzeichnis mit dem Namen Autostart. Wenn diese Option auf Ja eingestellt bleibt, werden beim Öffnen des Safes alle dort befindlichen ausführbaren Dateien automatisch gestartet.
- **Öffne im Modus "Nur lesen"**: Ein Benutzer, der sich mit der Zugangsmethode nur lesen einloggt, wird die im Safe befindlichen Dateien weder speichern noch verändern können. Er kann sie lediglich lesen.
- **Öffnen als Wechselmedium**: Die G DATA Software öffnet Datensafes im Explorer als lokale Festplatten. Wenn Sie möchten, dass der

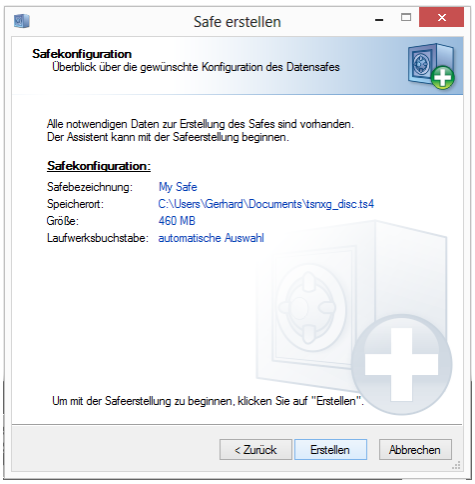
Safe als Wechseldatenträger im System sichtbar wird, markieren Sie bitte diese Option.

- **Gemeinsame Nutzung**: Das Markieren dieser Option ermöglicht die gemeinsame Nutzung des Safeverzeichnisses für andere Computer im Netzwerk. Warnung: Der Safezugang ist bei dieser Einstellung ohne die Notwendigkeit der Passworteingabe möglich. Wir empfehlen an dieser Stelle eine vorsichtige und bewusste Wahl der gemeinsamen Nutzung des Safes. Die gemeinsame Nutzung des Safes für alle Netzwerkteilnehmer ist an dieser Stelle sinnlos, da in diesem Fall die Daten jedem zugänglich sind.
- **Nach Benutzerabmeldung Safe schließen**: Diese Option sollte in der Regel aktiviert sein, denn wenn der Safe auch nach der Benutzerabmeldung offen bleibt, können andere Benutzer den Inhalt des Safes einsehen.
- **Autosafe**: Alle Safes mit dieser Eigenschaft können mit einem einzigen Befehl geöffnet werden.

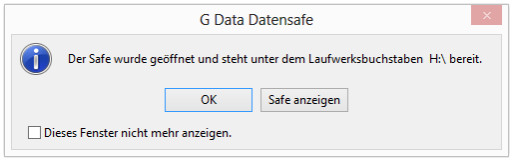



# Safekonfiguration

Der Safeaufbauassistent informiert Sie im letzten Schritt über die Einstellungsparameter. Wenn Sie diese Einstellungen ändern möchten, klicken Sie bitte auf die Schaltfläche **Zurück**. Wenn Sie mit den Einstellungen zufrieden sind, klicken Sie bitte **Erstellen**.




Der virtuelle und verschlüsselte Datensafe wird auf der Festplatte Ihres Computers erstellt. Mit einem letzten Anklicken der Schaltfläche **Fertig stellen** wird der Safe nun erstellt und auf Wunsch direkt geöffnet.



# Portablen Safe erstellen

Sobald Sie einen Safe erstellt haben, können Sie ihn auch zu einem portablen Safe machen, d.h. Sie können ihn so konfigurieren, dass Sie ihn auf einem USB-Stick verwenden oder sogar per Mail verschicken können.

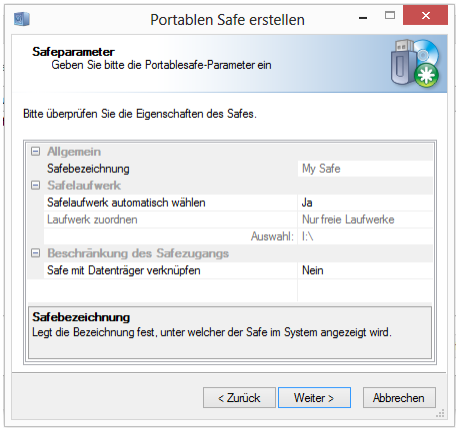
Wählen Sie in der Datensafe-Übersicht einen erstellten Safe aus und klicken Sie dann auf die Schaltfläche **Portablen Safe erstellen**. Nun öffnet sich ein Dialog, der Ihnen bei der Erstellung eines portablen Safes hilft. Klicken Sie auf **Weiter**, um diesen zu starten.


# Safeparameter

Wie bei der Vergabe der Safeparameter für Standard-Safes haben Sie hier die Möglichkeit, Parameter zu verändern. Dabei gibt es für portable Safes allerdings nur eingeschränkte Einstellungsmöglichkeiten:

- **Safelaufwerk automatisch wählen**: Der Safe erscheint, während er geöffnet ist, wie ein Festplattenlaufwerk. Sie können hier entweder einen festen Laufwerksbuchstaben für den Safe vergeben oder das System automatisch einen auswählen lassen. In der Regel ist hier die automatische Auswahl empfehlenswert.

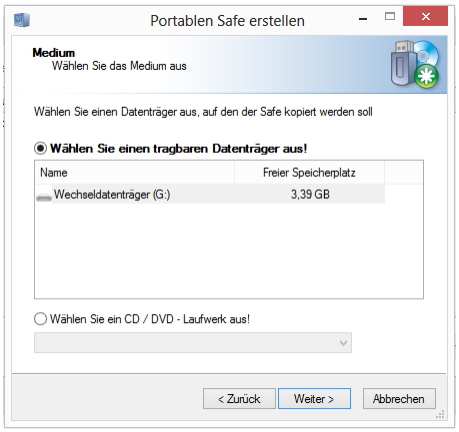
- **Safe mit Datenträger verknüpfen**: Hier können Sie festlegen, dass Sie den portablen Safe z.B. ausschließlich mit dem USB-Stick oder Festplattenlaufwerk verwenden, auf dem Sie ihn erstellen. Wenn Sie den Safe nicht mit dem Datenträger verknüpfen, können Sie die Safedatei (erkennbar an der Dateiendung **tsnxg**) z.B. auch als Mailanhang verschicken oder auf andere Datenträger verschieben/kopieren.



# Medium

Legen Sie hier fest, auf welchem Medium Sie den portablen Safe speichern möchten. Es kann sich hier z.B. um einen USB-Stick, eine externe Festplatte oder aber eine CD/DVD handeln.

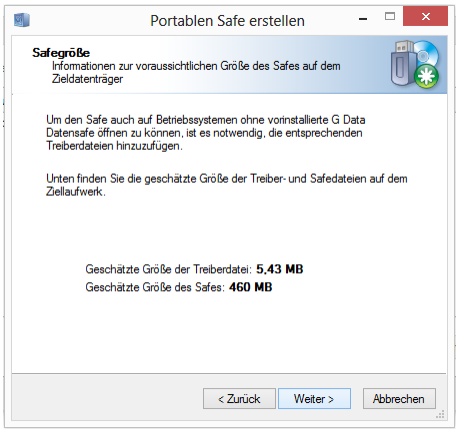
> **Hinweis**: Wenn Sie einen Safe auf CD oder DVD speichern, kann dieser natürlich nur geöffnet und gelesen werden. Ein Ändern von Dateien und Verzeichnissen im Safe ist auf dieser Art Datenträger nicht möglich.




# Safegröße

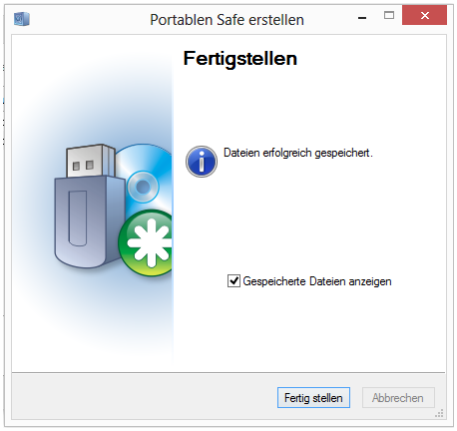
Hier erhalten Sie Informationen dazu, wie viel Speicherplatz der Safe auf dem Zieldatenträger benötigt. Sollte der Speicherplatz zu groß sein, können Sie hier die Erstellung des portablen Safes abbrechen.

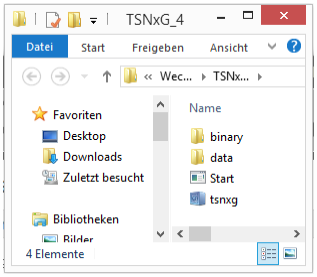
> **Hinweis**: Zusätzlich zu der eigentlichen Safegröße kommen etwa 6 MB zusätzlicher Treiberdaten dazu, damit Sie den Safe auch auf einem Windows-System öffnen können, auf dem die G DATA Software nicht installiert ist.




# Fertigstellen

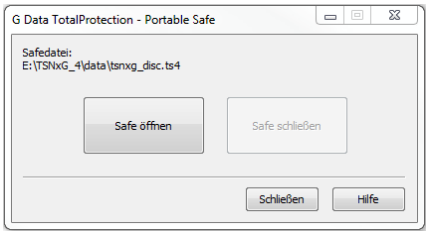
Schließen Sie nun die Erstellung des portablen Safes durch Anklicken der Schaltfläche **Fertig stellen** ab. Wenn Sie es wünschen wird Ihnen nun im Dateibrowser die Datei angezeigt, in der sich der portable Safe auf dem gewünschten Speichermedium befindet.



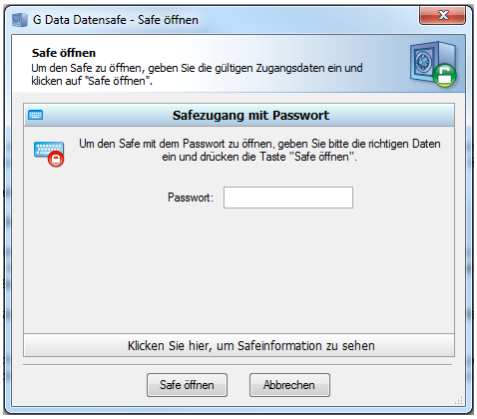



# Portablen Safe öffnen

Wenn Sie einen portablen Safe auf einem Windows-Computer öffnen möchten, der das G DATA Datensafe-Modul nicht enthält, gelangen Sie einfach an die Daten, indem Sie auf dem USB-Stick, der mobilen Festplatte oder CD/DVD die Programmdatei **start.exe** bzw. **start** aus dem Ordner **TSNxG_4** auswählen. Wenn Sie diese anklicken, erscheint ein Dialog, über den Sie den Safe öffnen bzw. (wenn er schon geöffnet ist) schließen können.




**Achtung**: Wenn der G DATA Datensafe das erste Mal auf einem Rechner genutzt wird, werden nun die entsprechenden Treiberdaten und Programmelemente geladen. Danach ist ein Rechnerneustart notwendig. Nach dem Neustart des Rechners wählen Sie bitte nochmals den Eintrag **Start** bzw. **Start.exe** aus.




Geben Sie nun Ihr Passwort ein oder nutzen Sie eine der anderen Safezugangsmethoden.

Der Safe wird nun geöffnet und der Inhalt des Safes kann genutzt werden.

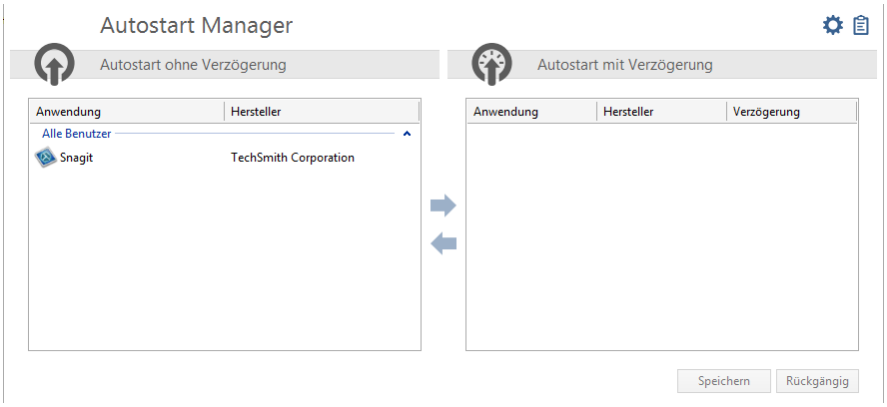
Nach dem erfolgten Einloggen in den Safe erscheint im Windows Explorer neben den lokalen Laufwerken das Symbol des Safes als zusätzliches Laufwerk mit einem entsprechenden Laufwerksbuchstaben. Jeder mobile Safebenutzer kann Daten vom Safe auf dem Computer überspielen. Bei Benutzung eines mobilen Safes auf einem USB Datenträger oder Flash Memory Datenträger kann der entsprechend berechtigte Benutzer die Safedaten von dem Computer in den Safe kopieren.

Das Schließen des mobilen Safes verläuft analog zum Öffnen. Klicken Sie bitte doppelt den Laufwerksbuchstaben des Safes oder wählen einen entsprechenden Befehl mit der rechten Maustaste im Kontextmenü.

**Achtung**: Es wird empfohlen, den Safe nach erfolgter Arbeit noch vor dem Herausziehen des tragbaren Datenträgers zu schließen. Gehen Sie dazu auf den tragbaren Datenträger, öffnen das Verzeichnis von G DATA und klicken auf Start.exe. Es erscheint dann ein Dialogfenster, in welchem das Schließen des Safes möglich ist.

# Autostart Manager

Mit dem Autostart Manager ist es möglich, Programme zu verwalten, die automatisch beim Start von Windows mit gestartet werden. Normalerweise werden diese Programme direkt beim Systemstart geladen. Wenn sie vom Autostart Manager verwaltet werden können sie jedoch auch zeitverzögert oder in Abhängigkeit von der Auslastung des Systems oder der Festplatte gestartet werden. Dieses ermöglicht einen schnelleren Systemstart und damit eine verbesserte Performance Ihres Computers.



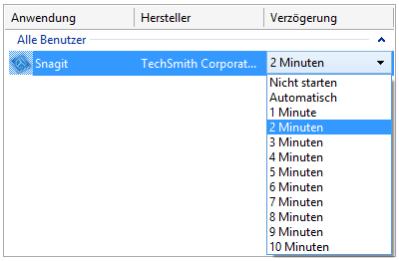

Wenn Sie den Autostart Manager öffnen, sehen Sie auf der linken Seite eine Auflistung aller Autostart-Programme, die auf Ihrem Computer installiert sind. Diese starten normalerweise ohne Verzögerung, also direkt mit dem Start von Windows und können so dazu führen, dass der Start Ihres Computers sehr langsam verläuft.

Wählen Sie einfach mit dem Pfeilsymbol die Autostartprogramme aus, die Sie zeitversetzt starten lassen möchten und entzerren Sie auf diese Weise den Windows-Startvorgang. Ihr Windows-Betriebssystem wird auf diese Weise deutlich schneller hochfahren und betriebsbereit sein.

Wenn Sie ein Autostartprogramm doch wieder ohne Verzögerung starten lassen möchten, bewegen Sie es einfach wieder zurück vom Ordner **Autostart mit Verzögerung** in den Ordner **Autostart ohne Verzögerung**.

## Verzögerung einstellen

Wenn Sie ein Programm im Ordner Autostart mit Verzögerung haben, können Sie ganz einfach bestimmen, um wie viele Minuten sich der Start dieser Software verzögern soll. Klicken Sie dazu einfach auf das Programm und wählen in der Spalte Verzögerung die gewünschte Zeitspanne aus.

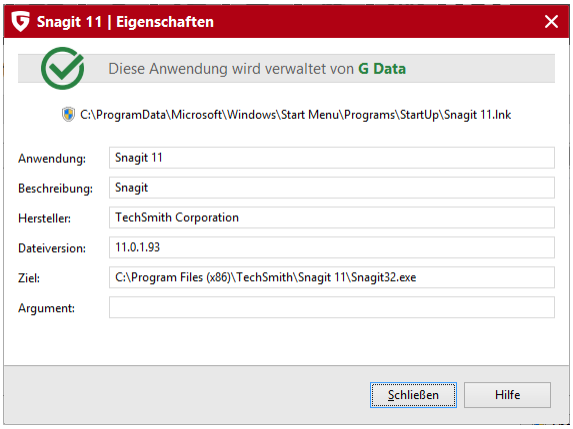



Folgende Einträge stehen Ihnen hier zur Verfügung:

- **Nicht starten**: Die Anwendung wird vom Autostart Manager verwaltet, aber bei den nächsten Neustarts des Systems nicht mitgestartet. Sie bleibt inaktiv.
- **1 - 10 Minuten**: Die Anwendung startet um die hier ausgewählte Anzahl von Minuten später.
- **Automatischer Start**: Die Anwendung wird in Abhängigkeit von der CPU-/Festplattenlast automatisch gestartet. Das bedeutet, dass eine weitere Autostart-Anwendung erst dann gestartet wird, wenn die Systemlast, die durch das Starten anderer Autostartanwendungen oder anderer Prozesse wieder zurückgegangen ist.

# Eigenschaften

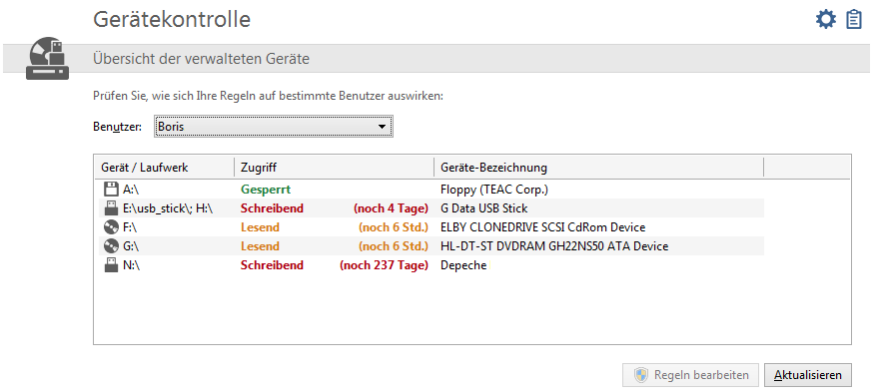
Wenn Sie einen Doppelklick auf den Eintrag eines Programmes in den Listen des Autostart Managers durchführen, erhalten Sie umfangreiche Informationen zur verwalteten Software.



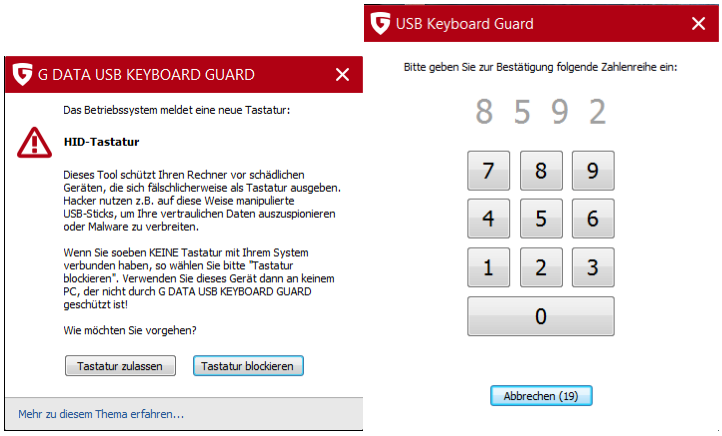
# Gerätekontrolle

Über die Gerätekontrolle können Sie für Ihren Computer festlegen, welche Speichermedien zum Lesen und/oder Schreiben von Daten zugelassen sind. So können Sie z.B. unterbinden, dass private Daten auf einen USB-Stick gezogen oder auf einer CD gebrannt werden. Darüber hinaus können Sie bei Wechseldatenträgern wie USB-Sticks oder externen USB-Festplatten genau festlegen mit welchem Wechseldatenträger Sie Daten herunterladen können. So können Sie z.B. Ihre eigene USB-Festplatte zum Datenbackup nutzen, aber andere Festplatten haben keinen Zugriff.

In dieser Übersicht sehen Sie, welche Auswirkungen die Einstellungen der Gerätekontrolle für den jeweiligen Benutzer haben. Über die Schaltfläche "Regeln bearbeiten" können Sie die Einstellungen für das Gerät und für den Nutzer Ihren Wünschen gemäß anpassen.




**USB Keyboard Guard:** Unsere Software schützt Sie ab jetzt auch gegen eine neue Bedrohung: Infizierte USB-Sticks, die sich als Tastatur gegenüber Ihrem Betriebssystem augeben, und so Schadsoftware einschleusen können. Die Software setzt Sie davon in Kenntnis, wenn Ihr System beim Einstecken eines USB-Geräts davon ausgeht, dass es sich um eine neue Tastatur handelt und Sie können über die Eingabe eines PINs bestätigen, dass es so ist oder nicht. Selbstverständlich merkt sich die Software alle bereits genehmigten Tastaturen und fragt nicht erneut nach.



# 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. Folgende übergreifende Funktionen stehen Ihnen für die Einstellungen zur Verfügung:

**Einstellungen speichern**: Sie können die durchgeführten Einstellungen in einer GDataSettings-Datei speichern. Wenn Sie Ihre G DATA Software auf mehreren Rechnern nutzen, können Sie auf diese Weise auf einem Rechner die Einstellungen vornehmen, abspeichern und die Settings-Datei auf den anderen Rechnern laden.

**Einstellungen laden**: Hiermit können Sie eine auf diesem oder jedem anderen Rechner erstellte GDataSettings-Datei laden.

**Einstellungen zurücksetzen**: Sollten Sie sich bei den Einstellungen Ihrer G DATA Software mal vertan haben, können Sie über diese Schaltfläche alle Einstellungen des Programms wieder auf Werkszustand zurücksetzen. Dabei können Sie bestimmen, ob Sie alle oder nur bestimmte Einstellungsbereiche zurücksetzen möchten. Wählen Sie dazu einfach per Häkchen die Bereiche aus, die Sie zurücksetzen möchten.

# Allgemein

## Sicherheit/Performance

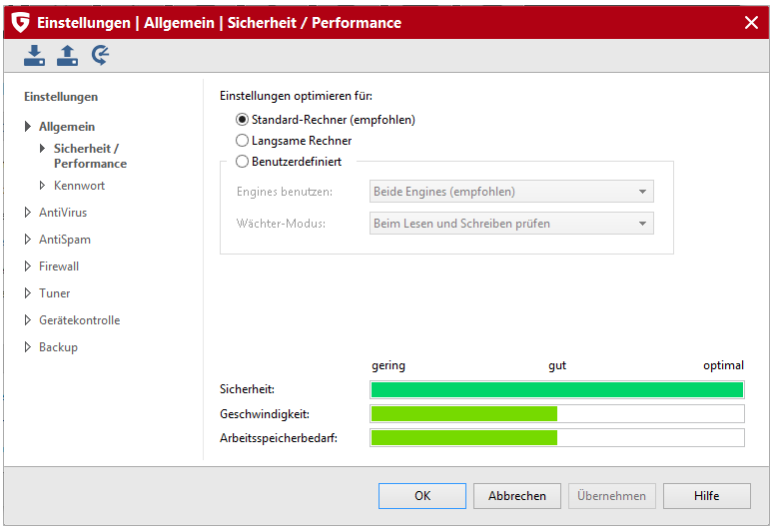
Wenn Sie Ihren Virenschutz auf einem langsamen Rechner nutzen möchten, gibt es die Möglichkeit, den Sicherheitslevel zu Gunsten der Performance, also der Arbeitsgeschwindigkeit des Rechners zu verbessern. In der Diagrammdarstellung sehen Sie dabei, welche Effekte eine Optimierung der Einstellungen mit sich bringt.

- **Standard-Rechner (empfohlen)**: Hier steht Ihnen der optimale Schutz der G DATA Software zur Verfügung. Beide Antiviren-Engines des Programms arbeiten dabei Hand in Hand. Darüber hinaus werden alle Lese- und Schreibzugriffe Ihres Rechners auf Schadcode überprüft.

  **Engine**: Ihre G DATA Software arbeitet mit zwei Antiviren-Engines. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe.

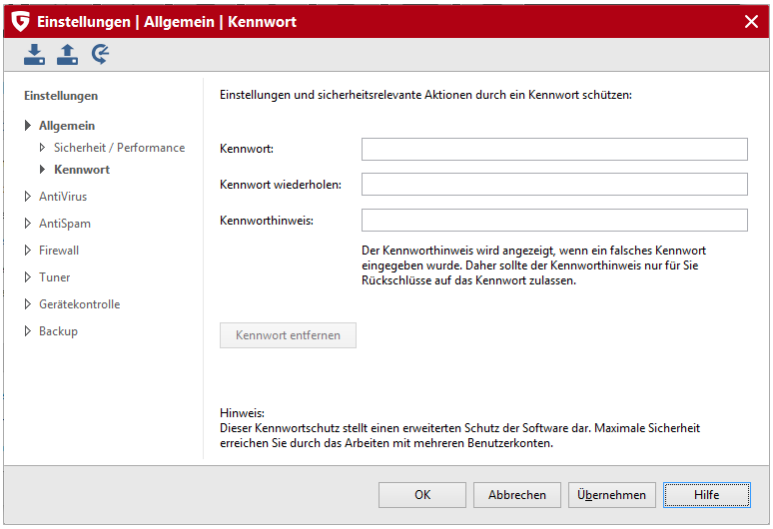
- **Langsame Rechner**: Um bei langsamen Rechnern die Arbeitsgeschwindigkeit nicht zu beeinträchtigen, kann Ihre G DATA Software auch nur mit einer Engine arbeiten. Dieser Schutz steht Ihnen bei vielen Antivirenprogrammen auf dem Markt ausschließlich zur Verfügung, die von vornherein nur mit einer Engine arbeiten. Der Schutz ist auf diese Weise immer noch gut. Darüber hinaus können Sie festlegen, dass im Wächter-Modus nur dann geprüft wird, wenn Schreibvorgänge ausgeführt werden. Auf diese Weise werden nur neu gespeicherte Daten geprüft, was die Performance weiter verbessert.

- **Benutzerdefiniert**: Hier können Sie individuell auswählen, ob Sie beide oder nur eine Engine nutzen wollen und für den Wächter festlegen, ob dieser beim Schreiben und Lesen, nur beim Schreiben (Ausführen) oder gar nicht aktiv werden soll (nicht empfohlen).



# Kennwort

Über die Vergabe eines Kennwortes können Sie die Einstellungen Ihrer G DATA Software schützen. Auf diese Weise kann ein anderer Benutzer Ihres Rechners z.B. nicht den Virenwächter oder den Leerlauf-Scan abschalten.




Um ein Kennwort zu vergeben, geben Sie es bitte erst unter "Kennwort" und dann unter "Kennwort wiederholen" ein, um Rechtschreibfehler zu vermeiden. Zusätzlich können Sie unter "Kennworthinweis" einen Hinweis auf das Kennwort angeben.

> **Hinweis**: Der Kennworthinweis wird angezeigt, wenn ein falsches Kennwort eingegeben wurde. Daher sollte der Kennworthinweis nur für Sie Rückschlüsse auf das Kennwort zulassen.

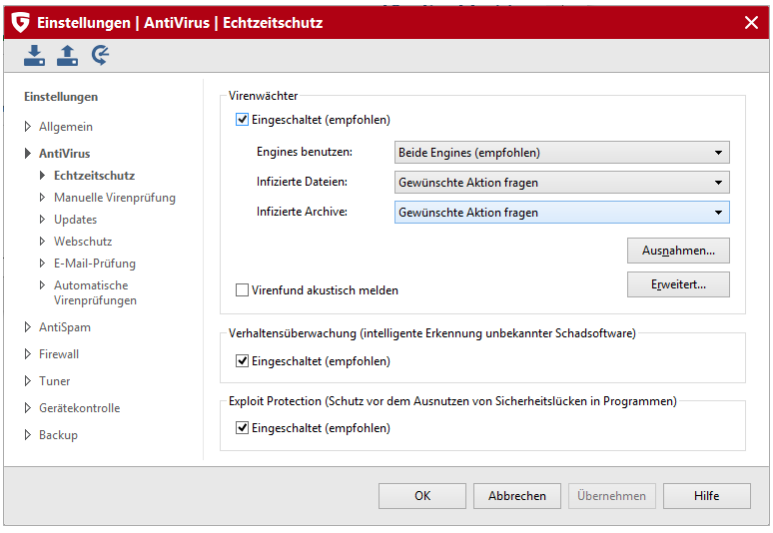
> **Hinweis**: Dieser Kennwortschutz stellt einen erweiterten Schutz der Software dar. Maximale Sicherheit erreichen Sie durch das Arbeiten mit mehreren Benutzerkonten. So sollten Sie - als Administrator - in Ihrem Benutzerkonto z.B. den Virenschutz managen und andere Benutzer (z.B. Kinder, Freunde oder Verwandte) können über ihre Benutzerkonten mit eingeschränkten Rechten hier keine Veränderungen vornehmen.

> **Hinweis**: Wenn Sie - z.B. nach dem Anlegen verschiedener Benutzerkonten - kein Kennwort für Ihre G DATA Software mehr benötigen, können Sie über die Schaltfläche "Kennwort entfernen" die Pflicht zur Kennworteingabe wieder aufheben.

# AntiVirus

# Echtzeitschutz

Der Echtzeitschutz des Virenwächters 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!




Folgende Optionen stehen Ihnen hier zur Verfügung:

- **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 einem Zurückbewegen aus der **Quarantäne** nicht mehr benutzt werden kann.

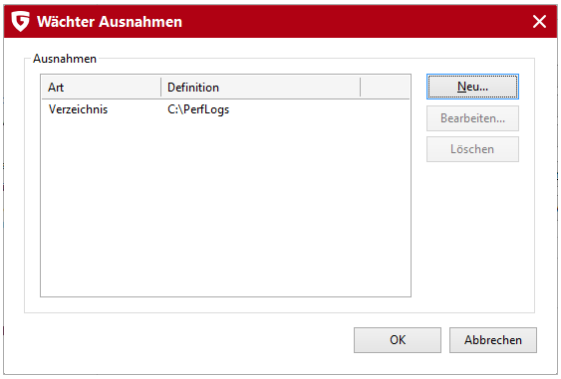
- **Verhaltensüberwachung**: Wenn die Verhaltensüberwachung aktiviert ist, wird jede Aktivität auf dem System unabhängig vom Virenwächter überwacht. Dadurch werden auch Schädlinge erkannt, für die noch keine Signatur existiert.

- **AntiRansomware**: Schutz gegen Verschlüsselungstrojaner.

- **Exploit Protection**: Ein sogenannter Exploit nutzt die Schwachstellen gängiger Anwendersoftware aus und kann über diese Schwachstelle im schlimmsten Fall die Kontrolle über Ihren Rechner übernehmen. Exploits können selbst dann greifen, wenn Anwendungen (wie z.B. PDF-Viewer, Browser usf. ) regelmäßig aktualisiert werden. Die Exploit Protection schützt vor solchen Zugriffen, auch proaktiv gegen bisher unbekannte Angriffe.

## 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.

   **Hinweis**: Die Funktionsweise von Platzhaltern ist folgendermaßen:

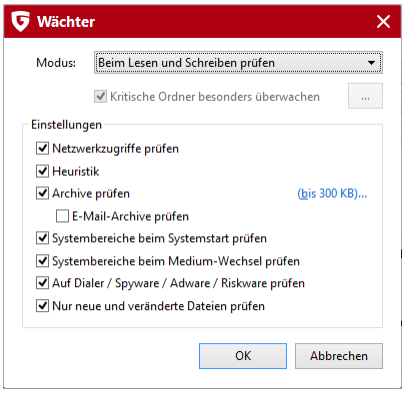
   - Das Fragezeichen-Symbol (?) ist Stellvertreter für einzelne Zeichen.
   - Das Sternchen-Symbol (*) ist Stellvertreter für ganze Zeichenfolgen.

   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.

- **Kritische Ordner besonders überwachen**: Über diese Funktion können Sie für besonders kritische Ordner z.B. die im Netz freigegebene Ordner, persönliche Daten oder Cloud-Dienste (wie z.B. Microsoft Dropbox OneDrive, Google Drive etc.) besonders genau prüfen. Nachdem Sie diese im Dialogfeld ausgewählt haben, werden diese dann - unabhängig von den Einstellungen, die Sie für alle anderen Dateien, Ordner und Verzeichnisse verwenden - immer im Modus **Beim Lesen und Schreiben prüfen** überwacht. Wenn Sie generell den Modus **Beim Lesen und Schreiben prüfen** für alle Dateien ausgewählt haben, ist die Einstellungsmöglichkeit für kritische Ordner ausgegraut.

- **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-Archivs 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 überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen unerwünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen Schadpotential dem Virus in nichts nachstehen, die z.B. Ihr Surf-Verhalten oder sogar sämtliche Tastatureingaben (und damit auch ihre Passwörter) heimlich speichern und bei nächster Gelegenheit über das Internet an fremde Personen weiterleiten.

- **Nur neue bzw. veränderte Dateien prüfen**: Wenn Sie diese Funktion aktivieren, werden bei der Prüfung Dateien übersprungen, die

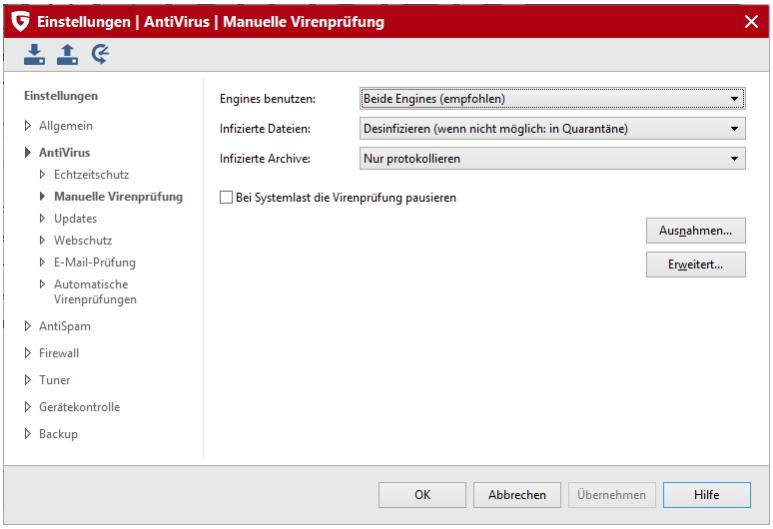
sich seit längerer Zeit nicht verändert haben und die zuvor als unschädlich erkannt worden sind. Das bringt einen Performance-Gewinn bei der täglichen Arbeit – ohne Sicherheitsrisiko.

# Manuelle Virenprüfung

Hier können Sie grundsätzliche Programmeinstellungen zur Virenprüfung vornehmen.

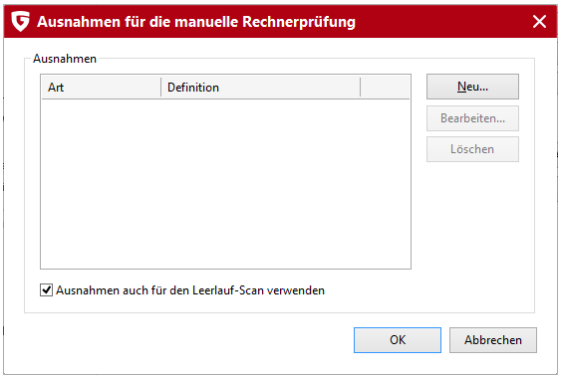
Dies ist aber im Normalbetrieb nicht nötig.

- **Engines benutzen**: Die Software arbeitet mit zwei Engines (= engl. für Maschine/Motor), also zwei aufeinander abgestimmten Virenprüfungsprogrammen. 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 einem Zurückbewegen aus der **Quarantäne** 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. Um Dateien zu schützen, geben Sie den kompletten Dateinamen in das Eingabefeld unter Dateimaske ein. Sie können hier auch mit Platzhaltern arbeiten.

**Hinweis**: Die Funktionsweise von Platzhaltern ist folgendermaßen:

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

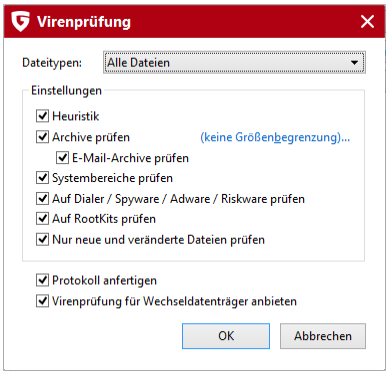
Um z.B. sämtliche Dateien mit der Datei-Endung .sav schützen zu lassen, geben Sie *.sav ein. Um eine spezielle Auswahl an Dateien mit fortlaufenden Dateinamen zu schützen (z.B. text1.doc, text2,doc, text3.doc), geben Sie beispielsweise text?.doc ein.

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

**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 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 über das Internet

an fremde Personen weiterleiten.

- **Auf Rootkits prüfen**: Rootkits versuchen sich herkömmlichen Virenerkennungsmethoden zu entziehen. Eine zusätzliche Kontrolle auf diese Schadsoftware ist immer ratsam.

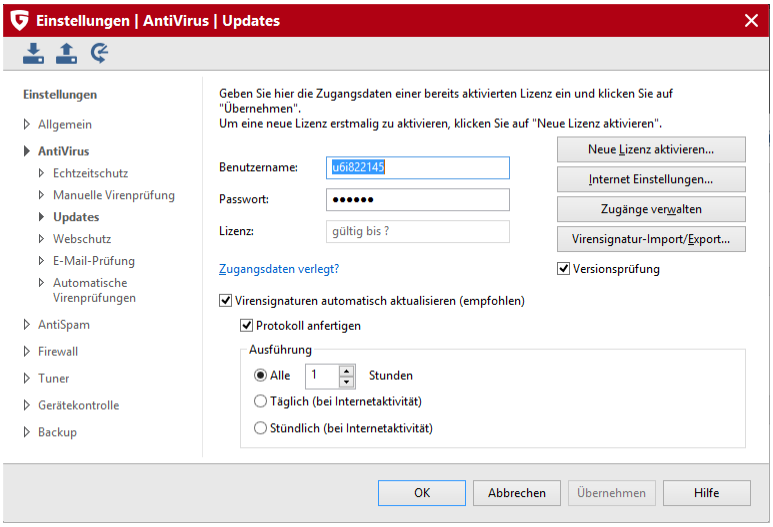
- **Nur neue bzw. veränderte Dateien prüfen**: Wenn Sie diese Funktion aktivieren, werden bei der Prüfung Dateien übersprungen, die sich seit längerer Zeit nicht verändert haben und die zuvor als unschädlich erkannt worden sind. Das bringt einen Performance-Gewinn bei der täglichen Arbeit – ohne Sicherheitsrisiko.

- **Protokoll anfertigen**: Über dieses Häkchen können Sie festlegen, dass die Software über den Virenprüfungsvorgang ein Protokoll anlegt. Dies kann dann im Bereich Protokolle eingesehen werden.

- **Virenprüfung für Wechseldatenträger anbieten**: Wenn Sie dieses Häkchen setzen, wird beim Verbinden eines Wechseldatenträgers (also USB-Sticks, externe Festplatten usw.) mit Ihrem Rechner nachgefragt, ob dieses Gerät auf Viren überprüft werden soll.

# Updates

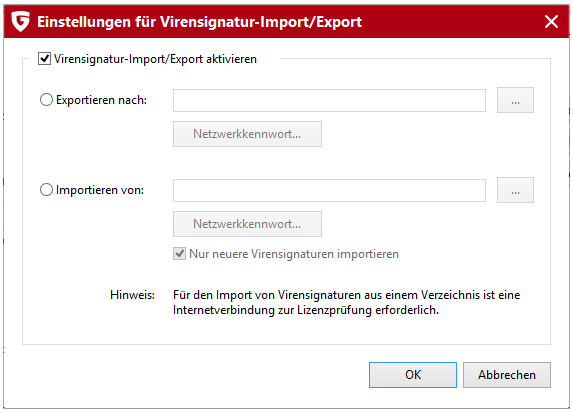
Sollte die Aktualisierung der Software oder der Virensignaturen übers Internet nicht funktionieren, können Sie in diesem Bereich alle notwendigen Angaben machen, um eine automatische Aktualisierung zu ermöglichen. Geben Sie hier in den Optionen die Zugangsdaten (Benutzername und Passwort) ein, die Sie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

**Zugänge verwalten:** Mit dieser Option haben Sie die Möglichkeit, selber zu bestimmen, über welche Internetverbindungen Sie Programm-Updates und Aktualisierungen beziehen möchten. Dies ist besonders nützlich, wenn Sie zeitweise über ein Netzwerk verbunden sind, bei dem der Datentransfer kostenpflichtig ist, also z.B. bei bestimmten Mobilfunktarifen ohne echte Datenflatrate.

**Virensignatur-Import/Export**: Bei Computern, die nur selten oder gar nicht mit dem Internet verbunden sind oder bei denen Einschränkungen bezüglich des Datenvolumens für Downloads bestehen, können Sie Virensignaturen auch über einen Datenträger (z.B. USB-Stick) aktualisieren, also ein **Offline-Update** durchführen. Dazu müssen Sie an einem Rechner, der mit dem Internet verbunden ist und über die notwendigen Rechte verfügt, die Virensignaturen auf den Datenträger exportieren und können diese dann über die Funktion "Importieren von" auf dem Rechner ohne Internetverbindung importieren. Das System auf diesem Rechner ist dann auch mit den neuesten Virensignaturen geschützt. Im Gegensatz zu den regelmäßigen Virensignatur-Updates per Internet ist hier der Anwender in der Pflicht und muss selber dafür sorgen, dass er so oft wie möglich selber Signatur-Updates durchführt.




### 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 **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

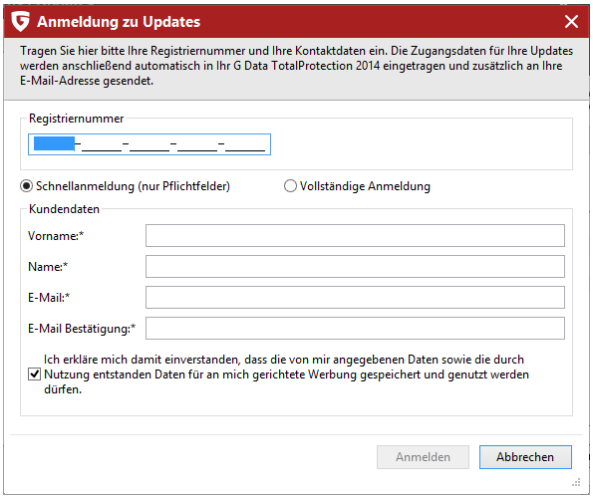
Wenn Sie Ihre G DATA Software noch nicht registriert haben sollten, können Sie dies jetzt nachholen und Ihre Registriernummer und Kundendaten eingeben. Sie finden die Registriernummer je nach Art des Produktes z.B. auf der Rückseite des Bedienungshandbuchs, der Bestätigungsmail beim Softwaredownload 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 Update-Server 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. Internet Explorer) 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

Wenn der Webschutz aktiv ist, werden Internetinhalte schon beim Browsen auf eventuelle Schadsoftware überprüft. Folgende Einstellungen können Sie hier vornehmen.

- **Internetinhalte (HTTP) überprüfen**: 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) überprüfen**.

  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.

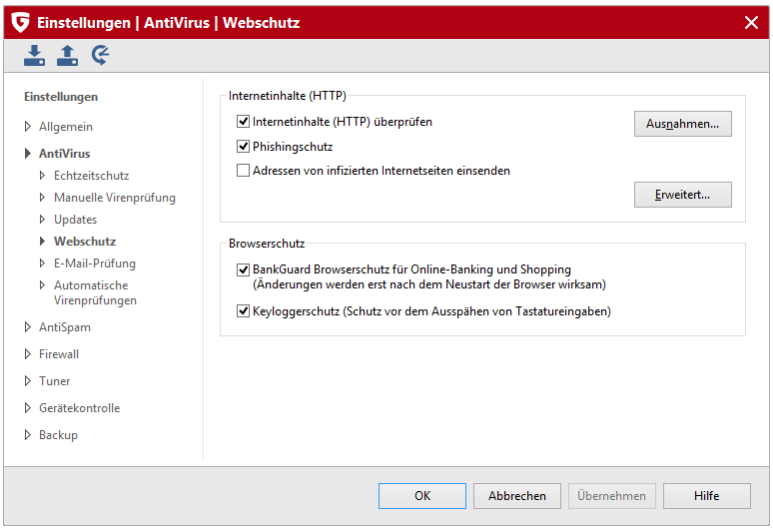
- **Adressen von infizierten Internetseiten einsenden**: Über diese Funktion können Sie - natürlich anonym - automatisch

Internetseiten melden, die von der Software als gefährlich beurteilt werden. Damit optimieren Sie die Sicherheit für alle Anwender.

- **BankGuard Browserschutz**: Banking-Trojaner werden zu einer immer größeren Bedrohung. Im Stundentakt entwickeln Online-Kriminelle neue Malware-Varianten (z.B. ZeuS, SpyEye), um damit Ihr Geld zu stehlen. Banken sichern den Datenverkehr im Internet, jedoch werden die Daten im Browser entschlüsselt und dort greifen Banking-Trojaner an. Die wegweisende Technologie von G DATA BankGuard sichert Ihre Bankgeschäfte jedoch von Anfang an und schützt sofort dort, wo der Angriff stattfindet. Durch eine Prüfung der Echtheit der benutzten Netzwerkbibliotheken stellt G DATA BankGuard sicher, dass Ihr Internet-Browser nicht von einem Banking-Trojaner manipuliert wurde. Es wird empfohlen, den G DATA BankGuard Schutz eingeschaltet zu lassen.

  Info: Neben der Man-in-the-Middle Methode, bei der der Angreifer die Kommunikation zwischen dem Anwender und dem Zielrechner beeinflusst, gibt es auch die Angriffsmethode Man-in-the-Browser (MITB). Bei dieser Methode infiziert der Angreifer den Browser selbst und greift auf die Daten zu, bevor diese verschlüsselt werden. Das Modul BankGuard schützt Sie vor Sie auch vor dieser Art von Angriffen, indem der sogenannte digitale Fingerabdruck einer Datei oder eines Teils einer Internetseite mit einer Datenbank im Internet abgeglichen wird. Auf diese Weise wird ein Betrug sofort entdeckt und die G DATA Software tauscht die betrügerische Datenverbindung automatisch zurück gegen das Original.

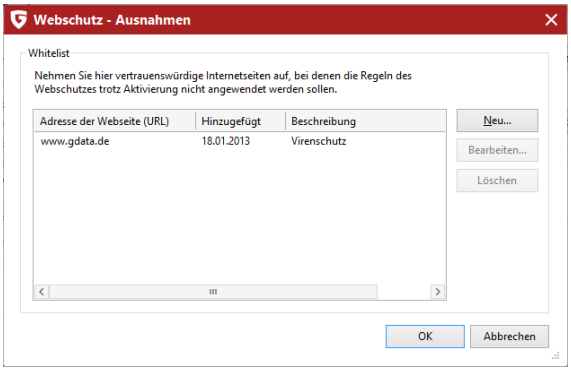
- **Keyloggerschutz**: Der Keyloggerschutz überwacht auch unabhängig von Virensignaturen, ob auf Ihrem System Tastatureingaben ausgespäht werden. Damit wird Angreifern die Möglichkeit genommen, Ihre Passworteingaben mitzuprotokollieren. Diese Funktion sollte immer angeschaltet bleiben.




# 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.

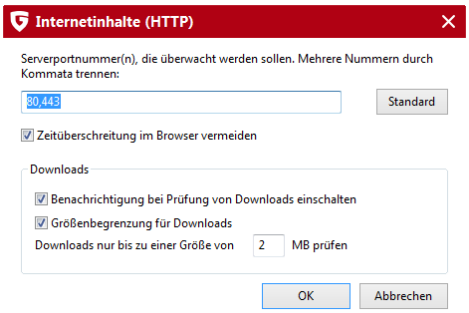
## Erweitert

Hier können Sie festlegen, welche Serverportnummern 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 Internetbrowser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internetbrowser 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 Browser-Daten auf Viren überprüft wurden, werden diese dann ganz normal an den Internetbrowser überreicht.

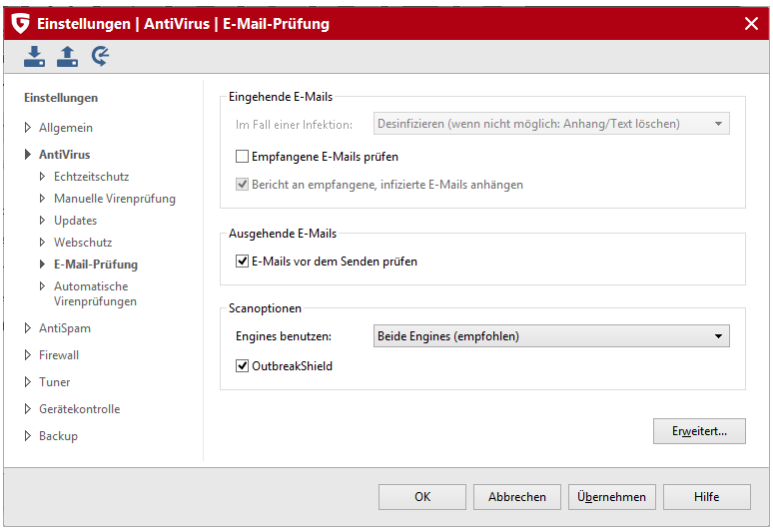
- **Benachrichtigung bei Prüfung von Downloads einschalten**: Hiermit können Sie sich während Downloads geprüft werden eine Benachrichtigung anzeigen lassen.

- **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.




**Achtung**: 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 Antiviren-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

Folgende Optionen können stehen Ihnen zum Virenschutz für eingehende Mails zur Verfügung:

- **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

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. Damit ausgehende Mails auf Viren überprüft werden, setzen Sie bitte das Häkchen bei **E-Mails vor dem Senden prüfen**.

# Scanoptionen

Hier können Sie grundlegende Optionen der Virenüberprüfung zu oder abschalten:

- **Engines benutzen**: Die Software arbeitet mit zwei Antiviren-Engines, zwei aufeinander abgestimmten 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 Massen-Mailing 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 Massen-Mailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht. Das OutbreakShield ist in den E-Mail-Virenblocker integriert.

# Verschlüsselte Verbindungen (SSL)

Viele E-Mail-Anbieter (z.B. GMX, WEB.DE, T-Online und Freenet) haben inzwischen auf die SSL-Verschlüsselung umgestellt. Auf diese Weise sind E-Mails und E-Mailkonten deutlich sicherer geworden. Dennoch ist es weiterhin notwendig, Ihre E-Mails auch durch ein Antivirenprogramm zu schützen. G DATA bietet Ihnen hierzu das Modul **Verschlüsselte Verbindungen (SSL)** an. Sie haben auch die Möglichkeit, SSL-Verschlüsselte E-Mails auf Viren und Schadsoftware zu überprüfen.

Damit die Überprüfung der mit SSL verschlüsselten E-Mails durch die G DATA Software stattfinden kann, muss in das E-Mailprogramm ein Zertifikat der G DATA Software importiert werden. Auf diese Weise wird sichergestellt, dass Ihre G DATA Software die eingehenden E-Mails überprüfen kann.

Unterstützt werden alle Mailprogramme, die entweder Zertifikate importieren können, oder auf den Windows Zertifikatstore zugreifen können, z.B.:

- Outlook 2003 oder höher
- Thunderbird
- The Bat
- Pegasusmail

Gehen Sie bitte folgendermaßen vor, wenn das Zertifikat von G DATA nicht automatisch installiert wurde:

1. Beim Installieren des Zertifikates sollten Ihre E-Mailprogramme nicht aktiv sein. Schließen Sie deshalb einmal alle E-Mailprogramme bevor Sie das Zertifikat erstellen und installieren.
2. Setzen Sie das Häkchen in der G DATA Software bei SSL-Verbindungen prüfen.

3. Klicken Sie auf die Schaltfläche Zertifikat exportieren. Die G DATA Software erzeugt nun ein Zertifikat. Diese Datei heißt GDataRootCertificate.crt.

4. Öffnen Sie nun die Datei GDataRootCertificate.crt. Es erscheint ein Dialogfenster, in dem Sie das Zertifikat auf Ihrem Computer installieren können.

5. Klicken Sie im Dialogfenster auf die Schaltfläche **Zertifikat installieren** und folgen Sie den Anweisungen des Installationsassistenten.

Fertig. Nun enthalten Outlook und alle anderen E-Mailprogramme, die auf den Windowszertifikatstore zugreifen das notwendige Zertifikat, um auch mit SSL verschlüsselt übertragene Emails auf Viren und andere Schadsoftware zu überprüfen.

**Hinweis**: Wenn Sie **Thunderbird (portable)** nutzen, und das Zertifikat nicht automatisch importiert wurde, müssen Sie dies nachträglich importieren und die Vertrauenseinstellungen des erzeugten G DATA Zertifikates verwalten. Wählen Sie dazu bitte in Thunderbird (portable) unter **Einstellungen > Erweitert > Zertifikate** die Schaltfläche **Zertifikate**. Wenn Sie hier klicken erscheinen unterschiedliche Karteireiter. Wählen Sie bitte den Karteireiter **Zertifizierungsstellen** und dann die Schaltfläche **Importieren**. Nun können Sie das Zertifikat **G DATA Mail Scanner Root** auswählen.

Wenn Sie nun bei folgenden Optionsfeldern das Häkchen setzen und auf OK klicken, wird Ihr Thunderbird portable durch G DATA geschützt:

- **Dieser CA vertrauen, um Websites zu identifizieren.**
- **Dieser CA vertrauen, um E-Mail-Nutzer zu identifizieren.**
- **Dieser CA vertrauen, um Software-Entwickler zu identifizieren**.

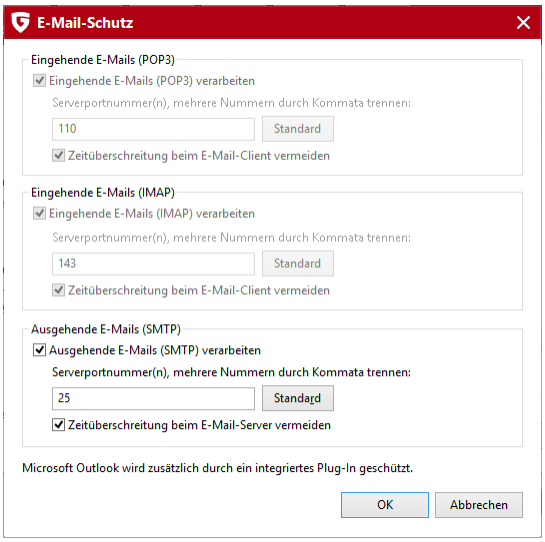
Bei anderen E-Mailprogrammen gibt es ähnliche Funktionen zum Importieren von Zertifikaten. Im Zweifel lesen Sie bitte dazu in der entsprechenden Hilfe nach, wie es für das verwendete E-Mailprogramm funktioniert.

# 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.

**Achtung**: 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, klicken Sie einfach auf das G DATA Symbol und der aktuell ausgewählte Mailordner wird auf Viren überprüft.

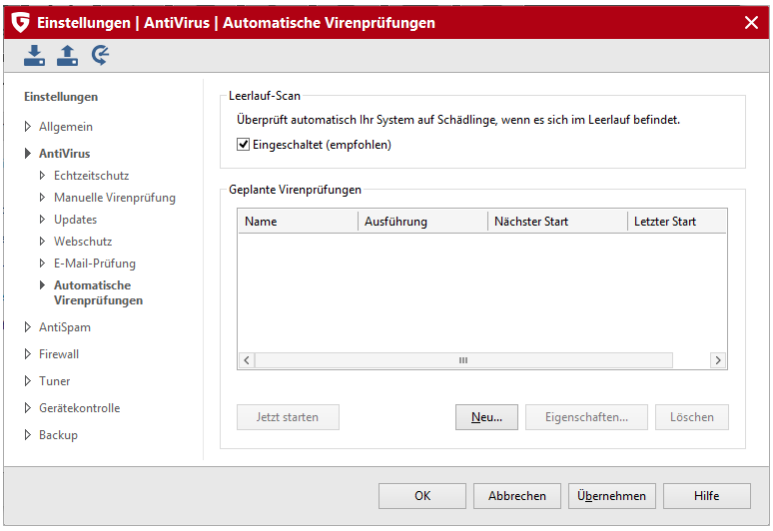
Da die Software die eingehenden Mails zeitlich vor dem eigentlichen Mailprogramm bearbeitet, kann es bei großen Mail-Mengen oder langsamen Verbindungen vorkommen, dass eine Fehlermeldung beim Mailprogramm erscheint, weil es nicht sofort die Maildaten zugestellt bekommt, da diese ja von der Software auf Viren überprüft werden. Mit Aktivieren des Häkchens 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.

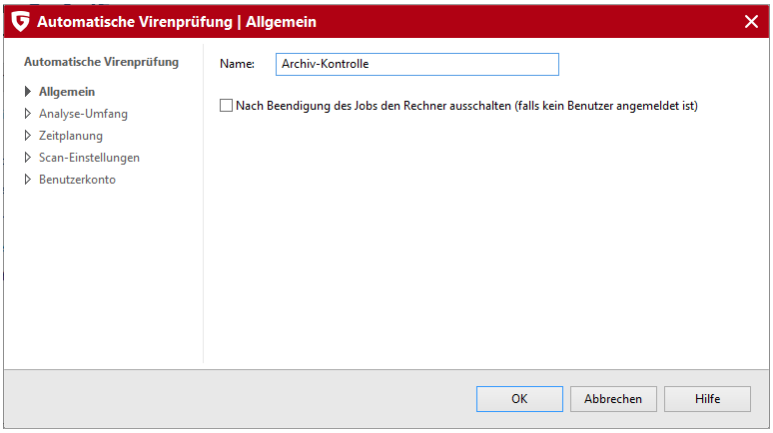
**Geplante Virenprüfungen**: In vielen Fällen reicht es, wenn der Computer durch den Leerlauf-Scan untersucht wird. Über die Schaltfläche **Neu** können Sie aber auch verschiedene, voneinander unabhängige automatische Virenprüfungen erstellen. So ist es z.B. vorstellbar, dass Sie den Ordner Downloads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




In den folgenden Kapiteln wird Ihnen erläutert, wie Sie individuelle Virenprüfungen erstellen.

# 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).*

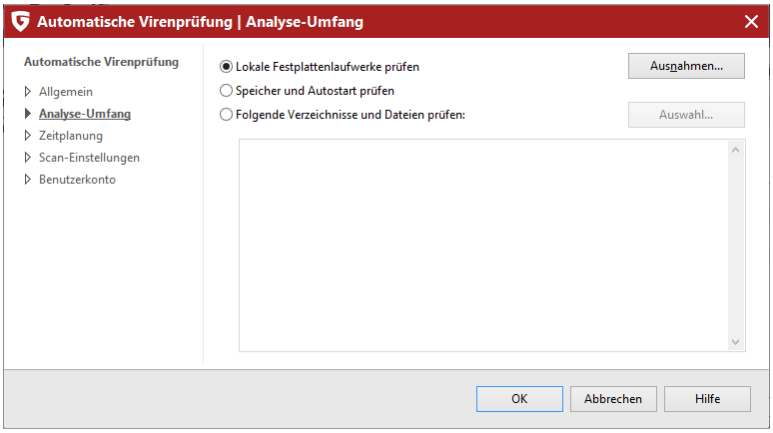


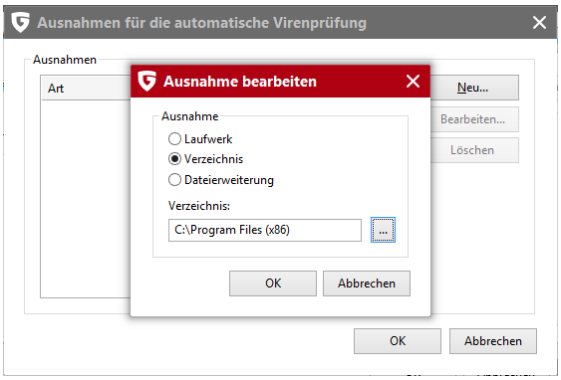

Wenn Sie ein Häkchen bei **Nach Beendigung des Jobs den Rechner ausschalten** setzen, wird der Rechner automatisch heruntergefahren, nachdem die automatische Virenprüfung durchgeführt wurde. Dies macht Sinn, wenn Sie die Virenprüfung z.B. nach der Arbeit im Büro durchführen möchten.

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

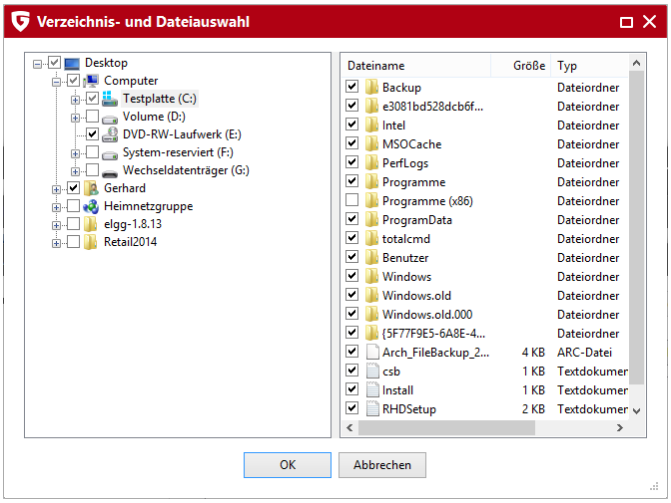
# Analyse-Umfang

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 der Software geprüft. Wenn in einem Verzeichnis nicht alle Dateien geprüft werden, findet sich an diesem Verzeichnis ein graues Häkchen.

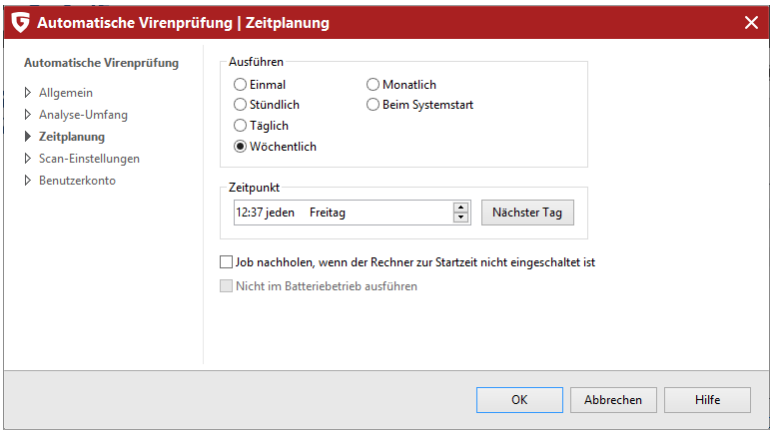



# Zeitplanung

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, müssen Sie keine Zeitvorgaben machen und die Software führt die Prüfung immer dann aus, wenn Ihr Rechner neu gestartet wird.

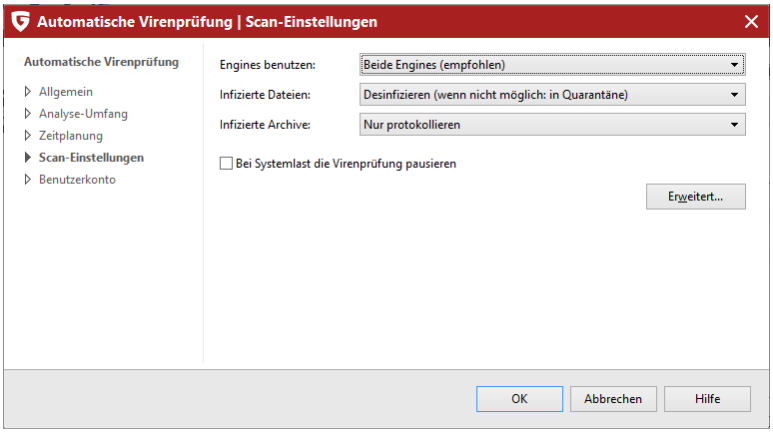
- **Job nachholen, wenn der Rechner zur Startzeit nicht eingeschaltet ist**: Durch Aktivierung dieser Option werden nicht ausgeführte automatische Virenprüfungen automatisch nachgeholt, sobald der Rechner wieder hochfährt.
- **Nicht im Batteriebetrieb ausführen**: Um die Akkulaufzeit nicht unnötig zu 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.

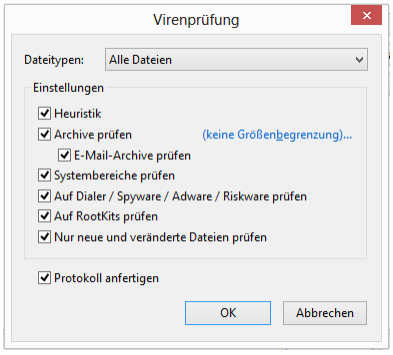



- **Engines benutzen**: Die Software arbeitet mit zwei Engines, also zwei aufeinander optimierten Virenprüfungsprogrammen. Bei älteren und langsamen Rechnern kann man durch die Nutzung einer einzelnen Engine die Virenprüfung beschleunigen, in der Regel sollten Sie jedoch die Einstellung **Beide Engines** 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.

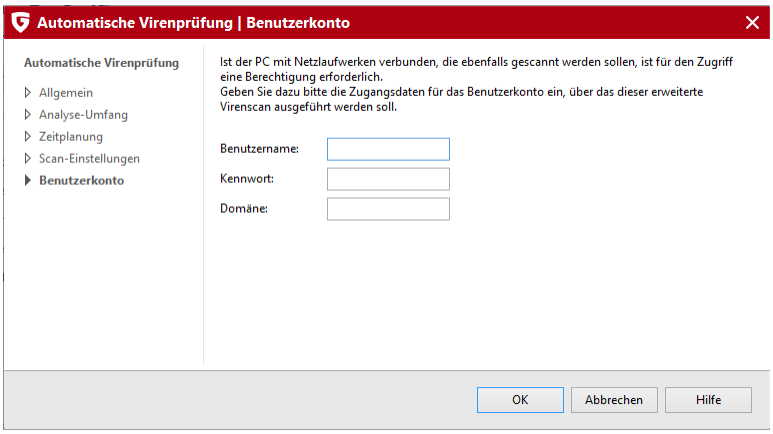
- **Auf Dialer / Spyware / Adware / Riskware prüfen**: Mit dieser Funktion können Sie Ihr System auch auf Dialer und andere Schadsoftware (Spyware, Adware und Riskware) überprüfen. Hierbei handelt es sich z.B. um Programme, die von ihnen ungewünschte teure Internetverbindungen aufbauen und in ihrem wirtschaftlichen 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

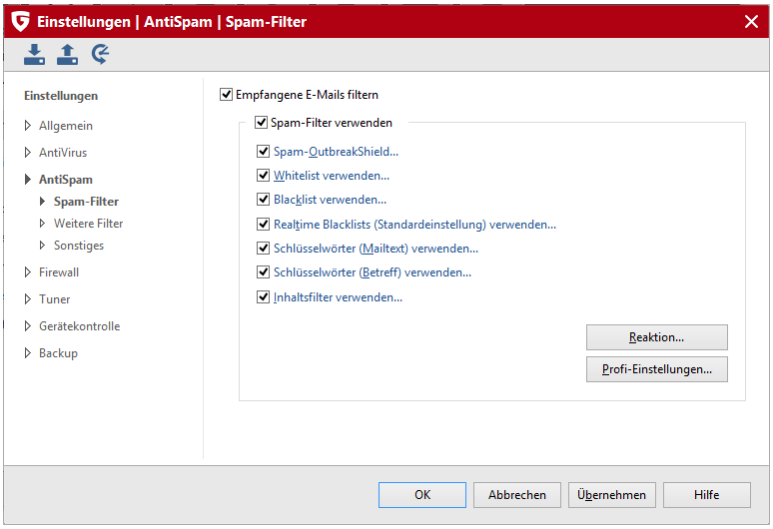
Hier kann das Benutzerkonto auf dem Rechner angegeben werden, auf dem die Virenprüfung stattfinden soll. Dieses Konto wird für den Zugriff auf Netzwerklaufwerke benötigt.



# AntiSpam

## 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 Filterarten 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, woraufhin ein Dialogfenster zur Änderung der Parameter erscheint. 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 verwenden**: 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 verwenden**: 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 (Standardeinstellung) 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

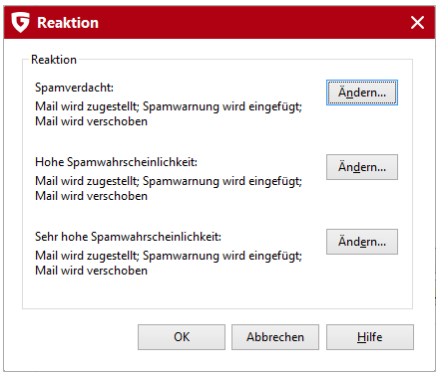
müssen in so einer Liste in einzelnen Zeilen untereinander aufgeführt sein. Als Format wird dabei eine einfache txt-Datei verwendet, wie sie z.B. auch mit dem Windows Notepad erstellt werden kann. Über die Schaltfläche **Export** können Sie eine solche Liste von Schlüsselwörtern auch als Textdatei exportieren. 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.

- **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.




- **Spamverdacht**: Hier 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 Sammel-Mailings, die vom Empfänger durchaus erwünscht sind. Hier empfiehlt es sich, den Empfänger auf den Spam-Verdacht hinzuweisen.

- **Hohe Spamwahrscheinlichkeit**: Hier werden die E-Mails zusammengefasst, die viele Merkmale für Spam in sich vereinen und nur in sehr seltenen Fällen vom Empfänger wirklich erwünscht sind.

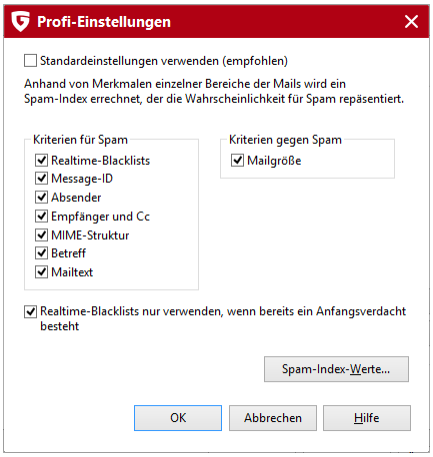
- **Sehr hohe Spamwahrscheinlichkeit**: Hier finden sich die E-Mails, die alle Kriterien einer Spam-E-Mail erfüllen. Hier handelt es sich so gut wie nie um gewünschte E-Mails und das Zurückweisen von derart gestalteten E-Mails ist in den meisten Fällen empfehlenswert.

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.

> **Hinweis**: 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.

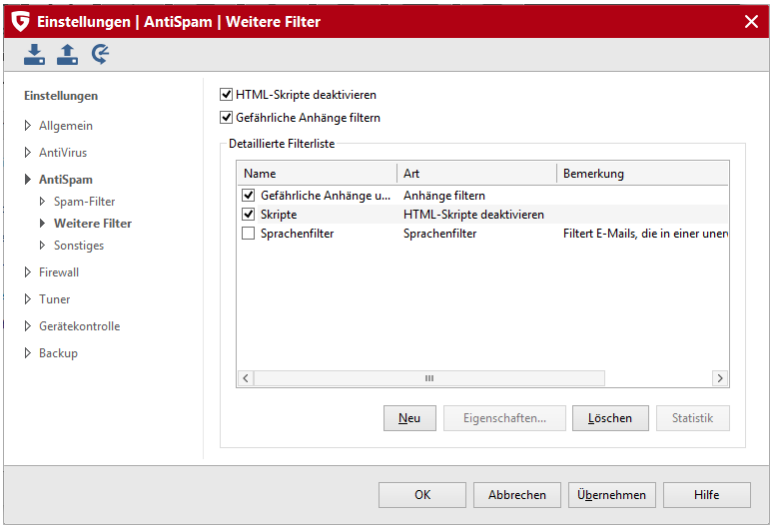



# Weitere Filter

Folgende Filter sind hier standardmäßig 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. Massenmail-Versendern) 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 Absende-Daten 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.

- **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.

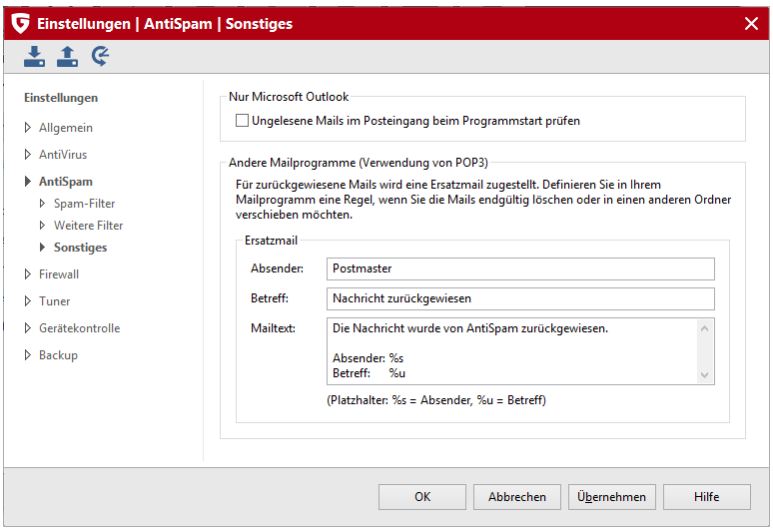
Über **Mail zurückweisen** wird die betreffende E-Mail von Ihrem E-Mailprogramm erst gar nicht in Empfang genommen.

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*

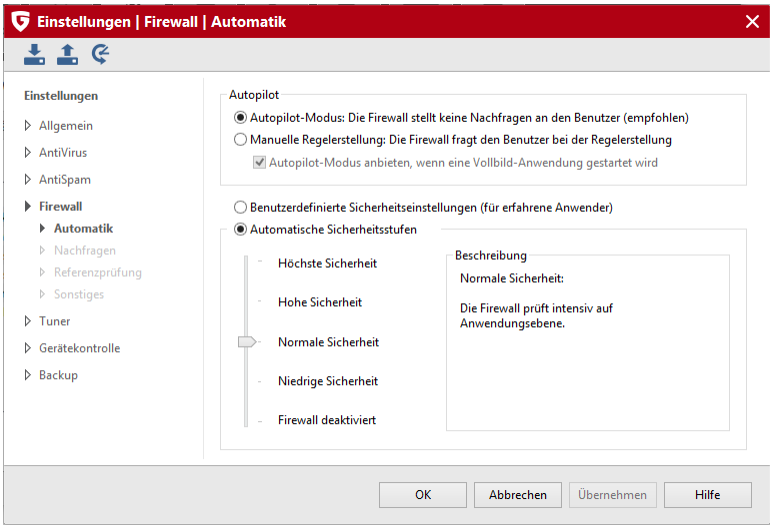
  *%u Betreff*

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

# Firewall

## Automatik

Wenn Sie sich nicht weiter mit der Firewall-Materie befassen möchten, sollten Sie die Einstellung auf Automatik stehen lassen. Neben dem Autopilot-Modus, der für viele Anwender sicherlich die beste Wahl ist, haben Sie darüber hinaus aber auch umfangreiche Optionen, die G DATA-Firewall optimal auf Ihre Bedürfnisse und Anforderungen auszurichten.




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

### Autopilot

Hier können Sie festlegen, ob die Firewall selbstständig und selbst lernend 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 gefragt wird.

- **Autopilot-Modus**: Hier arbeitet die Firewall vollkommen autonom und hält Gefahren automatisch vom heimischen PC ab. Diese Einstellung bietet einen praktischen Rundum-Schutz und ist in den meisten Fällen empfehlenswert.
- **Manuelle Regelerstellung**: Wenn Sie Ihre Firewall individuell konfigurieren möchten, können Sie über die manuelle Regelerstellung Ihren Firewall-Schutz 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 Nachfrage-Fenstern 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.

### Benutzerdefinierte Sicherheitseinstellungen

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.

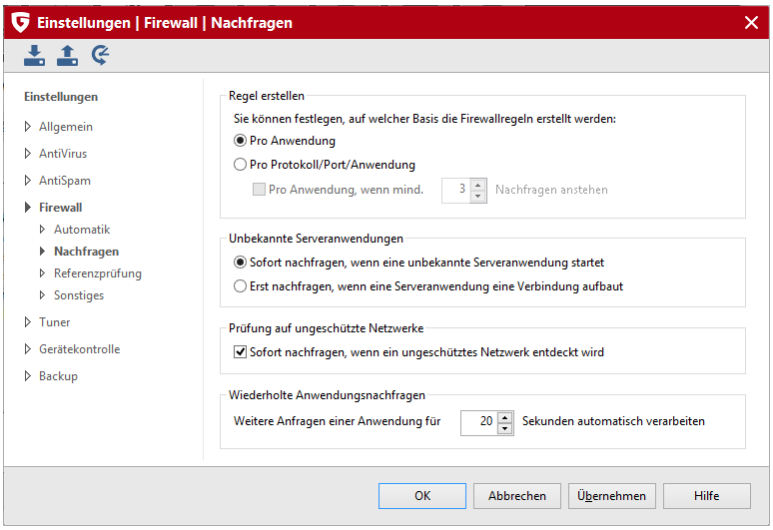
- **Niedrige Sicherheit**: Die Firewall-Regeln werden nur auf Anwendungsebene erstellt. Assistenten halten netzwerkspezifische Details von Ihnen fern und Sie werden während der Lernphase selten gefragt. Höchst sicherer Schutz vor ankommenden Verbindungsanforderungen besteht auch in dieser Sicherheitsstufe.

- **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 Sicherheitseinstellungen**. 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. x 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.

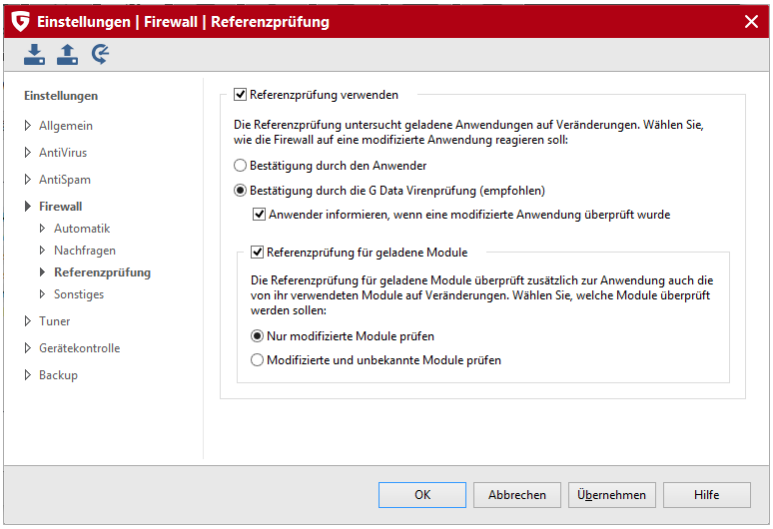
### Wiederholte Anwendungsnachfragen

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

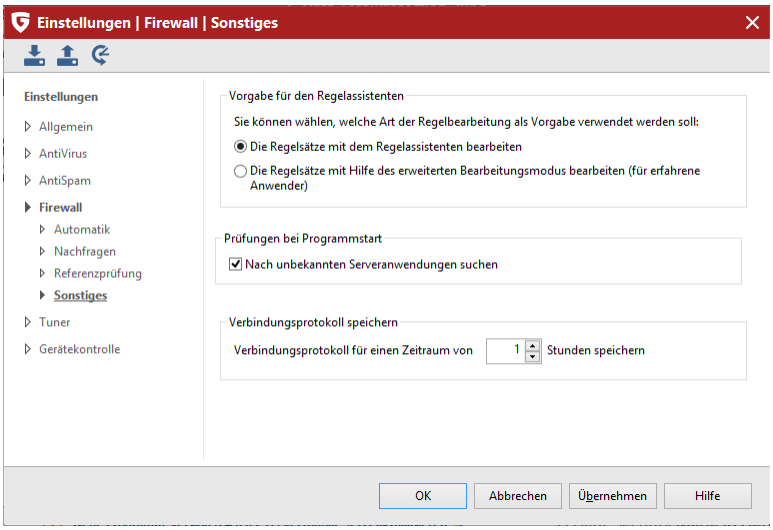
Bei der Referenzprüfung wird für Anwendungen, denen von der Firewall schon der Zugriff auf das Netzwerk erlaubt wurde, eine Prüfsumme auf Basis der Dateigröße und anderer Kriterien ermittelt. Wenn diese Prüfsumme des Programms plötzlich abweicht, kann es daran liegen, dass das Programm durch ein Schadprogramm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

**Referenzprüfung für geladene Module**: Hier werden nicht nur die Anwendungen, sondern auch die Module überwacht, die von den Anwendungen verwendet (z.B. DLLs) werden. 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 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

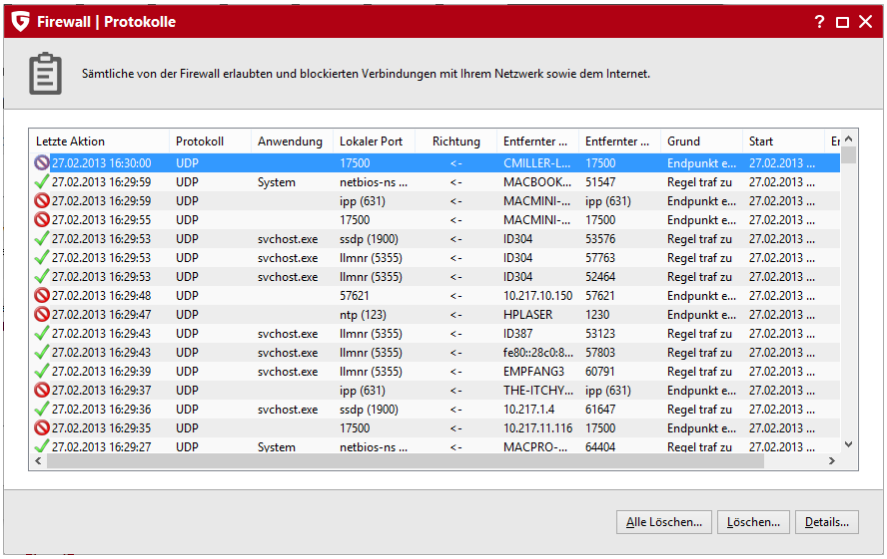
Hier können Sie festlegen, ob Sie das Erstellen neuer Regeln generell über den Regelassistenten oder im erweiterten Bearbeitungsmodus durchführen möchten. Für Anwender, die sich in der Materie der Netzwerksicherheit nicht gut auskennen, empfehlen wir den Regelassistenten.

### 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

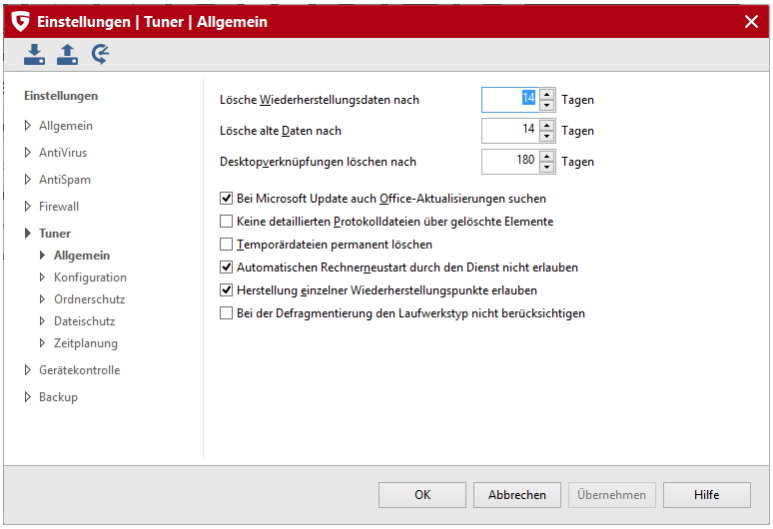
Hier können Sie festlegen, wie lange die Firewall Verbindungsdaten aufbewahren soll. Sie können die Daten von einer Stunde bis zu 60 Stunden nachhalten und im Protokolle-Bereich einsehen.




# Tuner

# Allgemein

Folgende Einstellungen können Sie hier vornehmen:




- **Lösche Wiederherstellungsdaten**: Hier können Sie bestimmen, wann Wiederherstellungsdaten (die die G DATA Software bei Änderungen anlegt) gelöscht werden sollen.
- **Lösche alte Daten**: Hier können Sie bestimmen, wann alte Daten (z.B. alte TEMP-Ordner) gelöscht werden sollen.
- **Desktopverknüpfungen löschen**: Hier können Sie bestimmen, wann unbenötigte Desktopverknüpfungen (wenn sie eine entsprechende Zahl von Tagen nicht verwendet wurden) gelöscht werden sollen.
- **Bei Microsoft Updates auch Office-Aktualisierungen suchen**: Hier können Sie festlegen, ob der Tuner automatisch im Internet neben der Suche nach den aktuellen Windows-Updates auch nach Office-Aktualisierungen suchen soll oder nicht. Eine Aktualisierung beider Elemente spart Zeit und hält Sie auch sicherheitstechnisch auf dem neuesten Stand. Die Suche nach Office-Aktualisierungen funktioniert natürlich nur, wenn Microsoft Office auch auf dem jeweiligen Rechner installiert ist.

- **Keine detaillierten Protokolldateien über gelöschte Elemente erstellen**: Der Tuner ist so aufgebaut, dass er lückenlose Informationen über durchgeführte Änderungen protokolliert. Wenn Sie eine Protokolldatei mit entsprechenden Informationen darüber, was der Tuner gelöscht hat, als Sicherheitsrisiko ansehen, können Sie die Erstellung eines solchen Lösch-Protokolls unterdrücken.

- **Temporärdateien permanent löschen**: Mit dieser Funktion schließen Sie die Webdateien (z.B. Cookies, temporäre Internetdaten) aus der Wiederherstellungsoption des Tuners aus, d.h. Sie können diese Dateien dann nicht wiederherstellen. Indem Sie diese Funktion aktivieren, verringern Sie die Menge der Dateien, die der Tuner im Bereich Wiederherstellen verwalten muss erheblich. Dies bringt Performance-Vorteile mit sich.

- **Automatischen Rechnerneustart durch den Dienst nicht erlauben**: Mit dieser Option unterbinden Sie einen möglichen Rechnerneustart, den der Tuner bei einem zeitgeteuerten Tuning-Vorgang sonst gegebenenfalls durchführen würde. Da der Tuner einen Rechnerneustart ungefragt nur dann durchführen würde, wenn kein Benutzer angemeldet ist, ist es sicherlich in den meisten Fällen ratsam, diese Option nicht zu aktivieren.

- **Herstellung einzelner Wiederherstellungspunkte erlauben**: Ohne diese Funktion kann die G DATA Software keine Wiederherstellung mehr durchführen.

- **Bei der Defragmentierung den Laufwerkstyp nicht berücksichtigen**: Da die meisten Hersteller vom Defragmentieren ihrer SSDs abraten, ist die Defragmentierung für diesen Festplattentyp im G DATA Tuner standardmäßig ausgenommen. Sofern die Laufwerke der G DATA Software nicht automatisch typisiert werden können, Sie sich aber sicher sind, dass sich keine SSD Laufwerke in Ihrem Rechner befinden, können Sie hier den Haken gesetzt lassen. Der Tuner startet dann bei jeder Ausführung die Defragmentierung aller im System befindlichen Festplatten.

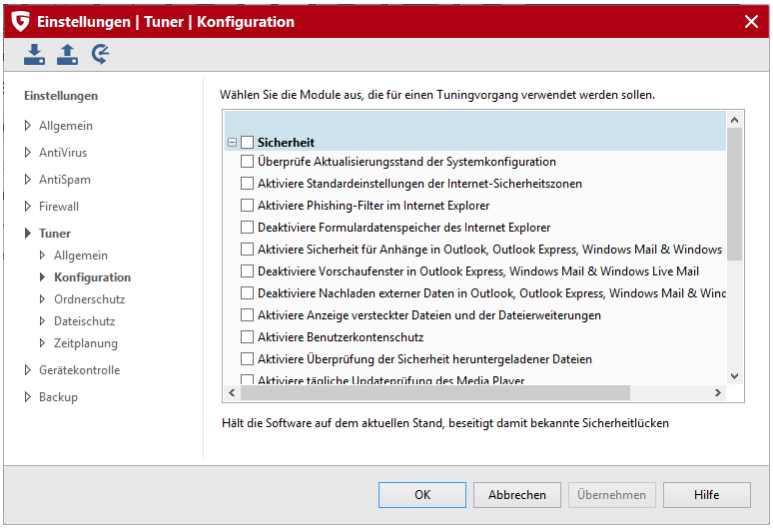
# Konfiguration

Im diesem Bereich können Sie alle Module auswählen, die der Tuner für einen Tuning-Vorgang verwenden soll. Ausgewählte Module werden dabei dann entweder über eine automatische zeitgesteuerte Aktion gestartet (siehe Kapitel **Zeitplanung**) oder manuell. Um ein Modul zu aktivieren, führen Sie einfach einen Doppelklick mit der Maus darauf aus. Folgende großen Tuning-Bereiche können Sie hier individuell optimieren:

- *Sicherheit*: Diverse Funktionen, die automatisch Daten aus dem Internet nachladen, haben lediglich für den Anbieter und nicht für Sie sinnvolle Aspekte. Oftmals wird über solche Funktionen auch Schadsoftware Tür und Tor geöffnet. Mit diesen Modulen schützen Sie Ihr System und halten es auf dem neuesten Stand.

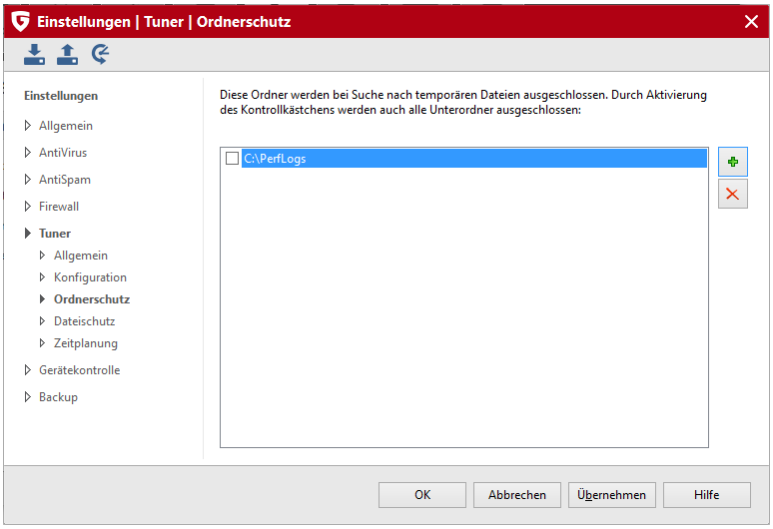
- *Leistung*: Temporäre Dateien, z.B. nicht mehr benötigte Sicherheitskopien, Protokolldateien oder Installationsdaten, die nach der Installation nur noch Festplattenplatz belegen, bremsen Ihre Festplatte aus und belegen wertvollen Speicherplatz. Darüber hinaus verlangsamen nicht mehr benötigte Prozesse und Dateiverknüpfungen Ihr System merklich. Mit den hier aufgelisteten Modulen können Sie Ihren Rechner von diesem überflüssigen Ballast befreien und beschleunigen.

- *Datenschutz*: Hier sind die Module zusammengefasst, die sich mit dem Schutz Ihrer Daten befassen. Spuren, die beim Surfen oder der allgemeinen Computernutzung unfreiwillig entstehen und viel über Ihr Nutzerverhalten oder sogar wichtige Daten und Passwörter verraten, werden hier gelöscht.



# Ordnerschutz

Über diese Karteikarte können Sie bestimmte Ordner (z.B. auch ihre Windows-Partition) von der automatischen Löschung alter Dateien ausnehmen.

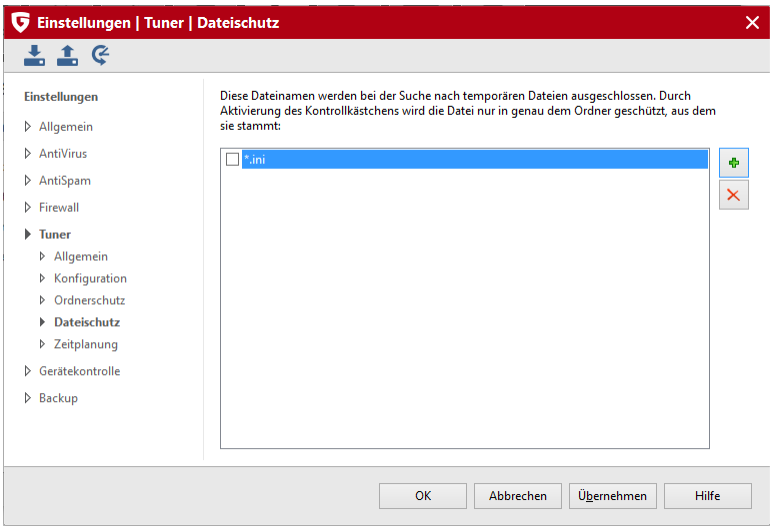



Klicken Sie dazu einfach auf das **Hinzufügen**-Symbol und wählen dann den entsprechenden Ordner bzw. das gewünschte Laufwerk aus.

Um ein Ausnahmeverzeichnis wieder freizugeben, wählen Sie es aus der angezeigten Liste aus und klicken dann auf die Schaltfläche **Löschen**.

# Dateischutz

Mit dem Dateischutz können Sie bestimmte Dateien vor der Löschung durch den Tuner schützen, z.B. Spielstände von Computerspielen oder ähnliche Dateien mit unüblichen Datei-Endungen, die auch als Backup- oder Temp-Dateien interpretiert werden könnten.




Um bestimmte Dateien zu schützen, klicken Sie auf die **Hinzufügen**-Schaltfläche und geben den entsprechenden Dateinamen 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 zu schützen zu lassen, geben Sie also *.sav ein. Um z.B. Dateien unterschiedlichen Typs mit einem anfänglich gleichen Dateinamen zu schützen, geben Sie beispielsweise text*.* ein.

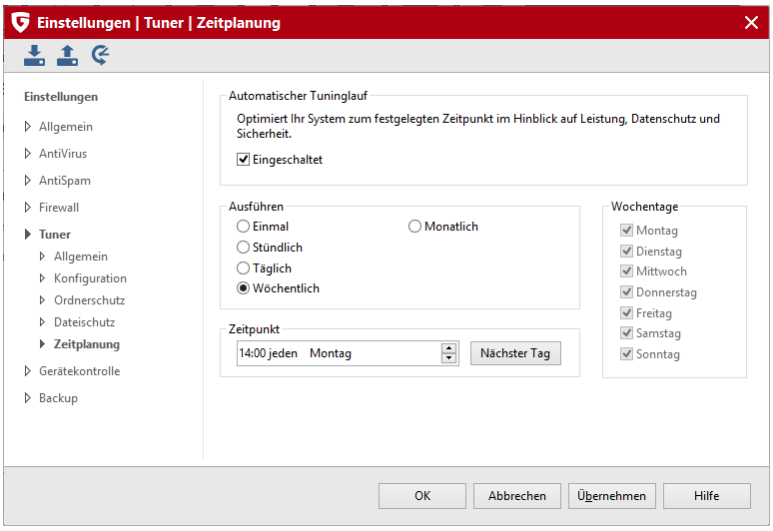
Wählen Sie nun noch den Ordner aus, in dem die Dateien geschützt werden sollen, indem Sie auf die Erweitert-Schaltfläche

klicken. Wählen Sie hier nun den Speicherort aus, an dem sich die zu schützenden Dateien befinden. Der Tuner schützt nun die entsprechend definierten Dateien nur in diesem Ordner (z.B. Spielstände nur im jeweiligen Spiele-Ordner).

Um einen Dateischutz wieder freizugeben, wählen Sie es aus der angezeigten Liste aus und klicken dann auf die Schaltfläche **Löschen**.

# Zeitplanung

Über die Karteikarte **Zeitplanung** können Sie festlegen, wann und in welchem Rhythmus der automatische Tuning-Vorgang erfolgen soll.

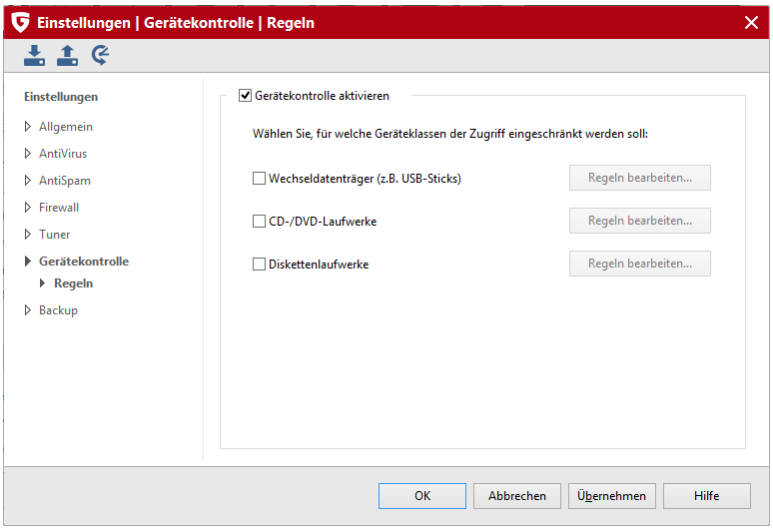



Unter **Täglich** können Sie mit Hilfe der Angaben unter Wochentage z.B. bestimmen, dass Ihr Rechner nur an Werktagen das Tuning durchführt oder eben nur an jedem zweiten Tag oder gezielt an Wochenenden, an denen er nicht zur Arbeit genutzt wird. Um unter **Zeitpunkt** Daten- und Zeiteinträge zu ändern,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

Wenn Sie kein automatisches Tuning durchführen lassen möchten, entfernen Sie einfach das Häkchen am Eintrag **Eingeschaltet** für den automatischen Tuninglauf.

# Gerätekontrolle

Über die Gerätekontrolle können Sie für Ihren Computer festlegen, welche Speichermedien zum Lesen und/oder Schreiben von Daten zugelassen sind. So können Sie z.B. unterbinden, dass private Daten auf einen USB-Stick gezogen oder auf einer CD gebrannt werden. Darüber hinaus können Sie bei Wechseldatenträgern wie USB-Sticks oder externen USB-Festplatten genau festlegen mit welchem Wechseldatenträger Sie Daten herunterladen können. So können Sie z.B. Ihre eigene USB-Festplatte zum Datenbackup nutzen, aber andere Festplatten haben keinen Zugriff.



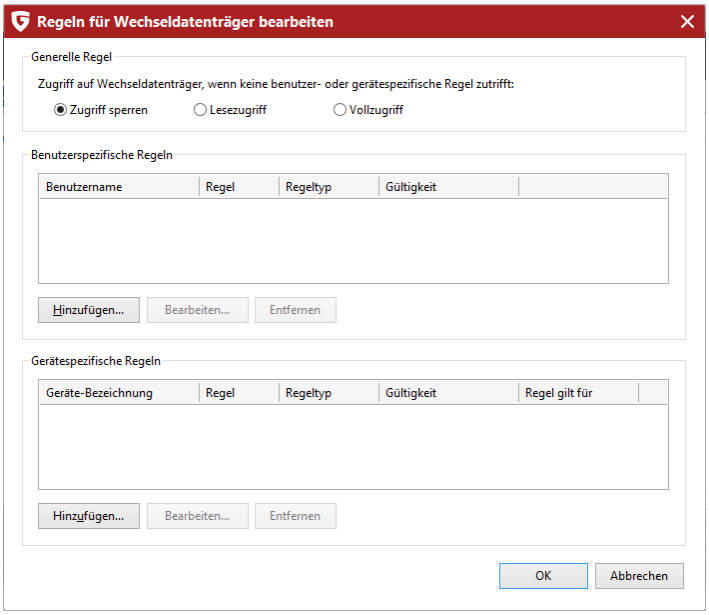

Um die Gerätekontrolle zu nutzen, setzen Sie bitte das Häkchen bei **Gerätekontrolle aktivieren** und wählen dann aus, für welche Geräte Sie Beschränkungen festlegen möchten:

- **Wechseldatenträger (z.B. USB-Sticks)**
- **CD-/DVD-Laufwerke**
- **Diskettenlaufwerke**

Nun haben Sie die Möglichkeit, Regeln für die einzelnen Speichermedien zu definieren.

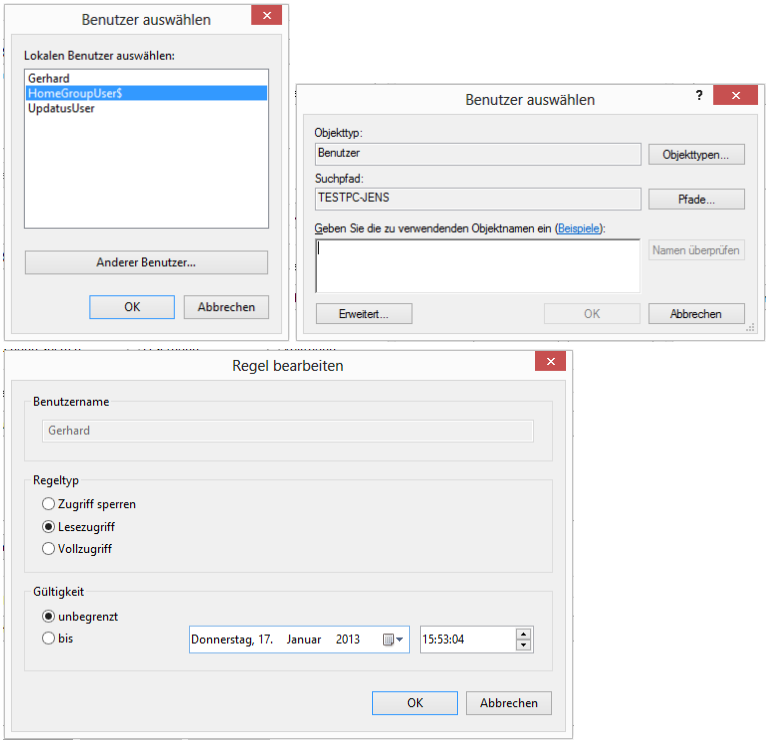
## Generelle Regel

Hier können Sie festlegen, ob das jeweilige Gerät gar nicht genutzt werden kann (**Zugriff sperren**), ob von ihm nur Daten heruntergeladen werden können, ohne dass darauf auch Daten abgespeichert werden können (**Lesezugriff**) oder ob es keine Beschränkungen für dieses Gerät gibt (**Vollzugriff**). Diese Regel gilt dann für alle Benutzer Ihres Rechners.




## Benutzerspezifische Regel

Wenn Sie möchten, dass nur bestimmten Nutzern eingeschränkte Rechte für Speichermedien eingeräumt werden, können Sie in diesem Bereich erst den Benutzernamen des auf Ihrem Rechner eingetragenen Mitbenutzers auswählen und dann den Zugriff auf das jeweilige Speichermedium wie unter **Generelle Regel** beschrieben begrenzen. Auf diese Weise können Sie sich z.B. als Administrator und Besitzer des Rechners Vollzugriff erlauben, anderen Benutzern aber nur eingeschränkte Rechte.

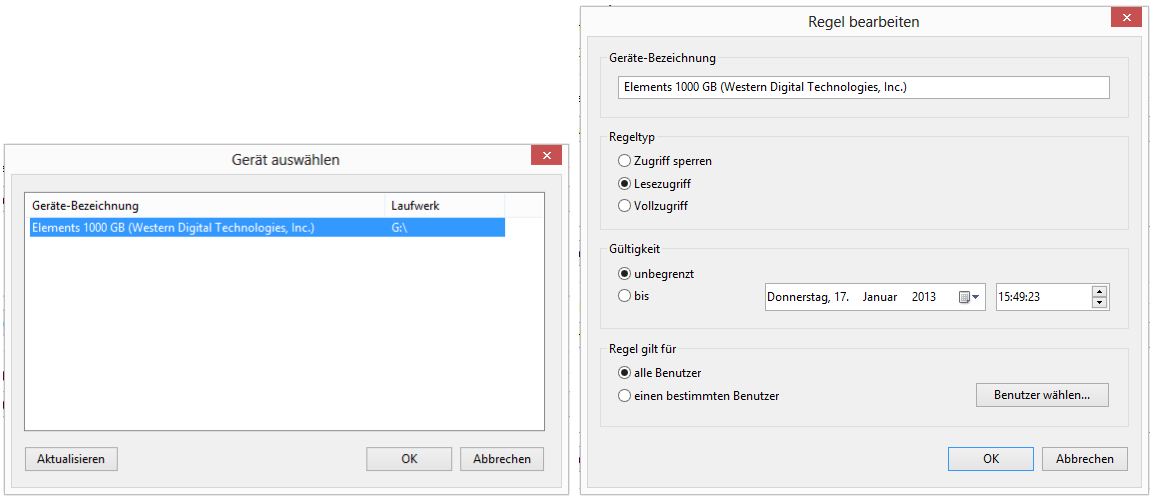


Wählen Sie hier den Benutzer aus. Wenn Sie nun auf OK klicken, öffnet sich ein weiterer Dialog, in dem Sie festlegen können, welche Zugriffsart für diesen Benutzer gewünscht ist und ob die Berechtigung für diesen Nutzer auf eine bestimmte Zeit (z.B. zwei Wochen) begrenzt ist (**Gültigkeit**).

> **Hinweis**: Die benutzerspezifische Regel hebt die generelle Regel auf. D.h. wenn Sie generell bestimmen, dass der Zugriff auf USB-Sticks nicht erlaubt ist, können Sie einem bestimmten Benutzer dennoch die Nutzung über eine benutzerspezifische Regel erlauben. Wenn ein Benutzer über die Gerätekontrolle gewisse Zugriffsbeschränkungen erhalten hat, die zeitlich begrenzt sind, dann gelten nach Ablauf dieser Beschränkung wieder die generellen Regeln für diesen Benutzer.

### Gerätespezifische Regel

Bei der Verwendungen von Wechseldatenträgern wie z.B. USB-Sticks oder externen Festplatten können Sie auch festlegen, dass nur bestimmte Wechseldatenträger auf Ihren Rechner zugreifen dürfen. Verbinden Sie dazu den Wechseldatenträger mit Ihrem Computer und klicken dann auf die Schaltfläche **Hinzufügen**. In dem nun erscheinenden Dialog können Sie den gewünschten Wechseldatenträger auswählen. Wenn Sie nun auf OK klicken, öffnet sich ein weiterer Dialog, in dem Sie festlegen können, welche Zugriffsart für diesen Datenträger gewünscht ist, ob die Verwendung dieses Datenträgers auf eine bestimmte Zeit (z.B. zwei Wochen) begrenzt ist (**Gültigkeit**) und ob jeder Benutzer diesen Datenträger unter seinem Benutzerzugang nutzen darf oder nicht.

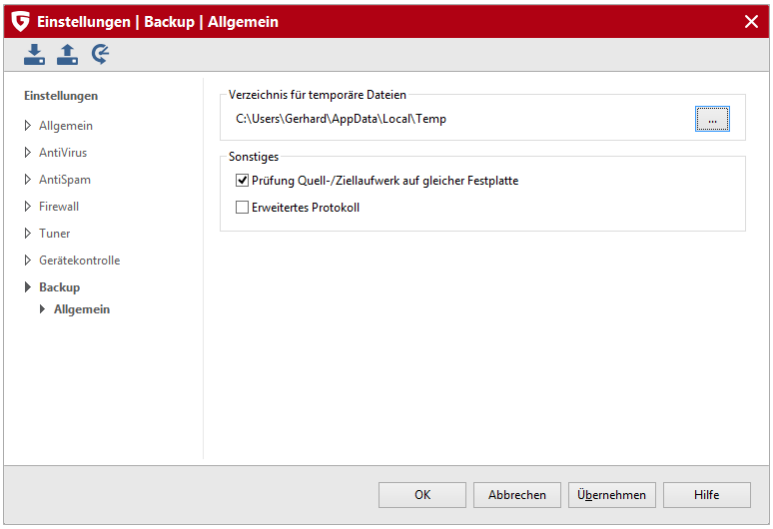



# Backup

In diesem Bereich können Sie allgemeine Einstellungen zur Funktionalität des Backup-Moduls vornehmen.

- **Verzeichnis für temporäre Dateien**: Legen Sie hier fest, wo zwischengespeicherte Daten vom Backup-Modul gespeichert werden sollen. Diese Dateien entstehen beim Erzeugen, aber auch beim Wiederherstellen eines Backups, werden nach dem jeweiligen Vorgang aber auch automatisch wieder gelöscht. Dennoch sollten Sie ausreichend Festplattenspeicherplatz hier zur Verfügung haben, da sonst die Geschwindigkeit von Backup und Wiederherstellung eingeschränkt wird. Diese Einstellung sollte nur dann geändert werden, wenn auf dem ausgewählten Verzeichnis für temporäre Dateien zu wenig Speicherplatz zur Verfügung steht.

- **Prüfung Quell-/Ziellaufwerk auf gleicher Festplatte**: Normalerweise warnt das Backup-Modul jedesmal dann den Anwender, wenn er ein Backup auf demselben Datenträger erstellen möchte, auf dem sich auch die Originaldateien befinden. Das erfolgt aus dem Grund, weil bei einem Ausfall/Verlust dieses Datenträgers automatisch auch das Backup nicht mehr vorhanden wäre. Sollten Sie aus bestimmten Gründen dennoch regelmäßig Backups auf dem Originaldatenträger durchführen wollen, können Sie hier diesen Warnhinweis ausschalten.


Einstellungen | Backup | Allgemein
Einstellungen
Allgemein
AntiVirus
AntiSpam
Firewall
Tuner
Gerätekontrolle
Backup
Allgemein
Verzeichnis für temporäre Dateien
C:\Users\Gerhard\AppData\Local\Temp
...
Sonstiges
Prüfung Quell-/Ziellaufwerk auf gleicher Festplatte
Erweitertes Protokoll
OK
Abbrechen
Übernehmen
Hilfe

# Protokolle

Für die einzelnen Module stehen Ihnen Protokollfunktionen zur Verfügung, mit deren Hilfe Sie jederzeit den Überblick darüber haben, welche Aktionen Ihre G DATA Software zu Ihrem Schutz durchführt.

## Virenschutz-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.

## Firewall-Protokolle

Der Protokolle-Bereich stellt für jede Aktion der Firewall eine umfangreiche Log-Datei bereit. Hier können Sie einzelne Aktionen mit Doppelklick öffnen und gegebenenfalls ausdrucken oder als Textdatei abspeichern. Lesen Sie hierzu auch das Kapitel **Einstellungen: Sonstiges**.

## Backup-Protokolle

Der Protokolle-Bereich stellt für jede Aktion und jeden Backup-Job eine umfangreiche Log-Datei bereit. Hier können Sie einzelne Aktionen mit Doppelklick öffnen und gegebenenfalls ausdrucken oder als Textdatei abspeichern. Lesen Sie hierzu auch das Kapitel **Sichern und Wiederherstellen**.

## Spamschutz-Protokolle

Der Protokolle-Bereich stellt für jede Aktion eine umfangreiche Log-Datei bereit. Hier können Sie einzelne Aktionen mit Doppelklick öffnen und gegebenenfalls ausdrucken oder als Textdatei abspeichern.

## Kindersicherung-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. Lesen Sie hierzu bitte auch das Kapitel **Einstellungen: Protokoll**.

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

## Gerätekontrolle-Protokolle

Der Protokolle-Bereich stellt für jede Aktion des Gerätemanagers eine umfangreiche Log-Datei bereit. Lesen Sie hierzu auch folgendes Kapitel: **Einstellungen: Gerätekontrolle**

# FAQ: BootScan

Wenn Ihr Computer fabrikneu ist oder bisher schon von einer Antivirensoftware geschützt wurde, können Sie die Installation Ihrer G DATA Software einfach wie normale Windows-Software installieren, indem Sie den Installationsassistenten von dem Datenträger (G DATA Software DVD) oder aus ihrem Downloadverzeichnis (beim Online-Kauf) heraus starten und mit der Installation beginnen. Diese Schritte sind alle im Kapitel **Installation** beschrieben.

Sollten Sie jedoch den begründeten Verdacht haben, dass Ihr Computer schon virenverseucht ist, empfiehlt es sich, vor der Installation der G DATA Software und vor dem Start Ihres Windows-Betriebssystems einen BootScan mit der G DATA DVD durchzuführen.

**Was ist ein BootScan?**
Wenn Sie Ihren Computer anschalten, startet normalerweise automatisch Ihr Windows-Betriebssystem. Dieser Vorgang nennt sich Booten. Es gibt aber auch die Möglichkeit, andere Betriebssysteme und Programme 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 für den BootScan zur Verfügung.

**Wie bereite ich meinen Computer auf einen BootScan vor, wenn er nicht entsprechend voreingestellt ist?**
Sollte Ihr Computer nicht von CD/DVD-ROM booten, dann führen Sie bitte vorab 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 (je nach System auch F2 oder F10) drücken.
3. Wie Sie die Einstellungen in Ihrem BIOS-Setup im Einzelnen ändern, ist von Computer zu Computer unterschiedlich. Schauen Sie bitte dazu in der Dokumentation Ihres Computers nach.
4. 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.
5. Speichern Sie die Änderungen und starten Sie Ihren Computer neu. Jetzt ist Ihr Computer bereit für einen BootScan.

**Wie breche ich einen BootScan ab?**
Wenn Ihr Rechner nach einem Neustart einmal nicht die gewohnte Windows-Umgebung anzeigen sollte, sondern die Oberfläche der G DATA BootScan-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.

**Booten von USB-Stick**: Sollten Sie als Bootmedium einen USB-Stick verwenden, können Sie auch diesen als 1st Boot Device auswählen.

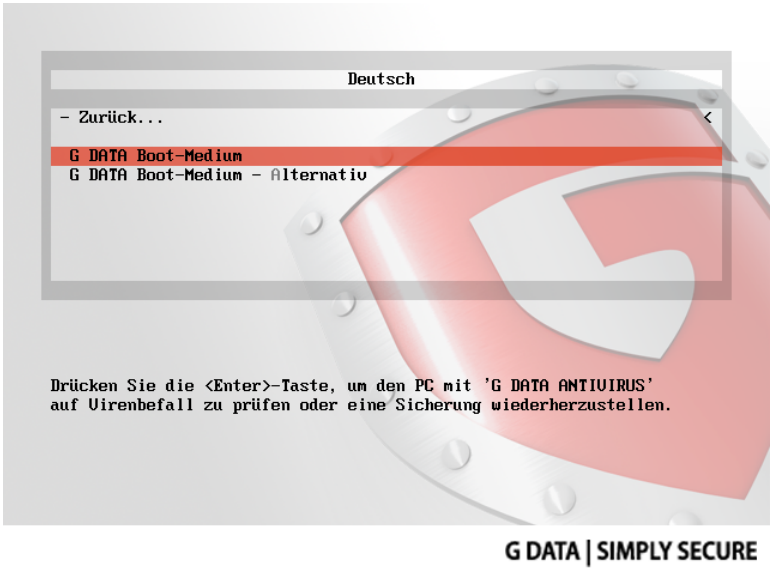
## Schrittweise Durchführung

Einen BootScan führen Sie folgendermaßen durch:

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

**BootScan mit G DATA Software, die Sie aus dem Internet heruntergeladen haben**: Sie erzeugen sich über den Eintrag "G DATA Bootmedium erstellen" in der G DATA Programmgruppe ein eigenes Bootmedium. Legen Sie Ihre selbstgebrannte BootDVD in das Laufwerk bzw. verbinden Sie den Boot-USB-Stick mit Ihrem Computer. Klicken Sie auf dem sich öffnenden Startfenster auf "Abbrechen" und schalten Sie den Computer aus.

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




3 Wählen Sie mit den Pfeiltasten die Option **G DATA Boot-Medium**. Es wird nun ein Linux-Betriebssystem von der DVD gestartet und es erscheint eine G DATA Spezialversion für BootScans.

**Hinweis**: Falls Sie Probleme mit der Ansicht der Programmoberfläche haben, starten Sie den Rechner erneut und wählen bitte die Option **G DATA Boot-Medium – Alternativ** aus.

4 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.

5 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.

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

7 Entfernen Sie die G DATA Software-DVD aus dem Laufwerk, sobald sich die Lade Ihres Laufwerks öffnet oder entfernen Sie den Boot-USB-Stick.

8 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.

# FAQ: Programmfunktionen

## Security-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.

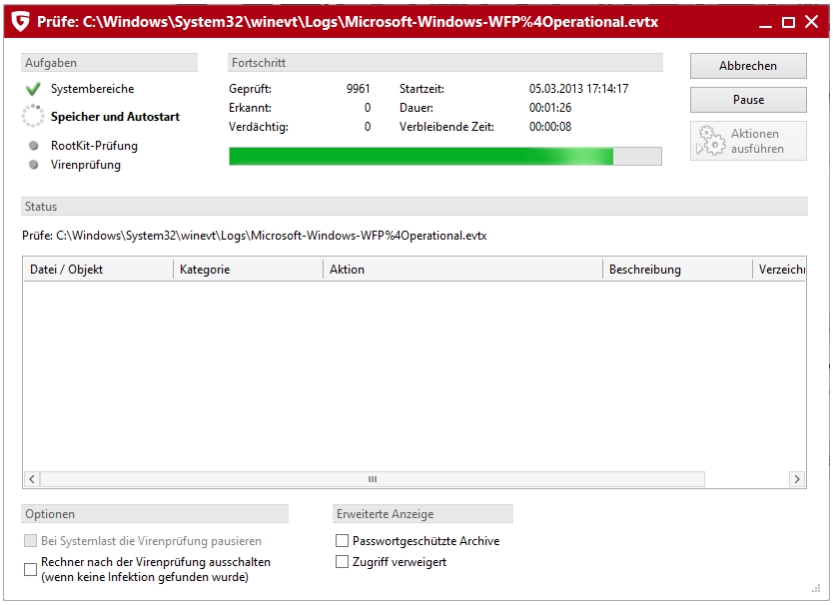
Wenn Sie das Symbol mit der rechten Maustaste anklicken, erscheint ein Kontextmenü, mit dem Sie grundlegende Sicherheitsaspekte der Software steuern können.

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.
- **Virensignaturen aktualisieren**: 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 **Virensignaturen aktualisieren** starten. Wozu ein Virenupdate nötig ist, lesen Sie im Kapitel: **Virenprüfung**
- **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.

# Virenprüfung durchführen

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 Systems 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 **Einstellungen: 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.

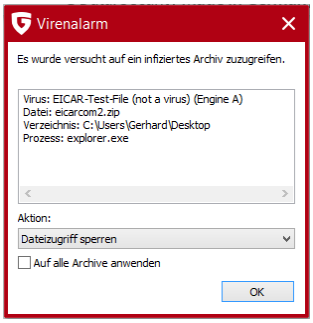
- **Nur protokollieren**: In der **Protokolle**-Ansicht wird die Infektion aufgelistet. Eine Reparatur oder Löschung der betroffenen Dateien findet jedoch nicht statt. **Achtung**: Wenn ein Virus nur protokolliert wird, ist er weiterhin aktiv und gefährlich.
- **Desinfizieren (wenn nicht möglich: nur 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: **Dateien in der 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: **Dateien in der 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.

# Viren-Alarm

Wenn die G DATA Software auf Ihrem Rechner einen Virus oder ein anderes Schadprogramm findet, erscheint ein Hinweisfenster am Bildschirmrand.




Sie haben nun 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: **Dateien in der 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.

# 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.

# 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.

# Deinstallation

Wenn Sie die G DATA Software irgendwann wieder von Ihrem Rechner entfernen möchten, führen Sie die Deinstallation bitte über die Systemsteuerung Ihres Betriebssystems durch. Die Deinstallation erfolgt dann vollautomatisch.

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.

# FAQ: Lizenzfragen

## Mehrfach-Lizenzen

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 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.

## Lizenzverlängerung

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 in den nächsten Tagen dann bequem per E-Mail als PDF.

> **Hinweis**: Dieser Dialog erscheint nur nach Ablauf des ersten Jahres. Danach verlängert sich Ihre G DATA Lizenz jedes Jahr automatisch. Sie können diesen Verlängerungsservice jederzeit ohne Angabe von Gründen kündigen.

## 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.

> **Hinweis**: Die Anzahl der Lizenzübertragungen ist begrenzt - bei Erreichen des Grenzwertes wird die Lizenz vollständig gesperrt, sodass dann keinerlei Updates mehr geladen werden können.

## Copyright

Copyright © 2017 G DATA Software AG
Engine: The Virus Scan Engine and the Spyware Scan Engines are based on BitDefender technologies © 1997-2017 BitDefender SRL.
OutbreakShield: © 2017 Commtouch Software Ltd.
[G DATA - 24/07/2017, 10:15]