

G DATA AntiVirus

Handbuch

Inhaltsverzeichnis

| | |
|-------------------------------|-----------|
| Allgemeines..... | 5 |
| G DATA ServiceCenter | |
| G DATA Unternehmenslösungen | |
| Tipps zur Virenprophylaxe | |
| Systemvoraussetzungen | |
| Installation..... | 11 |
| Willkommen | |
| Lizenzvereinbarung | |
| Installationsart | |
| Setup-Typ | |
| Zielordner | |
| Angepasstes Setup | |
| Zeitplan | |
| Installationsabschluss | |
| Beim ersten Start..... | 16 |
| Internet-Update | |
| Virenprüfung | |
| Programmaufbau | 24 |
| Windows Kontextmenü | |
| Security-Symbol | |
| G DATA BootCD erstellen | |
| AntiVirus..... | 30 |
| Status | |
| Aktionen | |
| Zeitplan | |
| Quarantäne | |
| Protokolle | |
| Optionen | |
| Anhang | 60 |
| Lizenzvereinbarung | |
| Virengeschichte | |

Virenkategorien

Glossar

Fragen und Antworten (FAQ)

Allgemeines

Der Antiviren-König baut seine Spitzenposition weiter aus: **G DATA AntiVirus** (ehemals **AVK**) bietet mit noch gründlicherer Virenerkennung und verbessertem Schutz vor unbekannten Schädlingen die bestmögliche Sicherheit für Ihren Computer. Jetzt mehr Rechenleistung trotz verbessertem Schutz.



Diese Schnellhilfe beschreibt die Installation und die wesentlichsten Funktionen Ihres neuen G DATA Sicherheitspakets. Bitte lesen Sie auch das beigegefügte Benutzerhandbuch oder die Online-Hilfe (durch Drücken der Taste **F1** in der Programmoberfläche), wo alle Funktionen und Eigenschaften Ihrer G DATA Software beschrieben werden.

Copyright © 2008 G DATA Software AG

Engine A: The Virus Scan Engine and the Spyware Scan Engines are based

on BitDefender technologies © 1997-2008 BitDefender SRL.

Engine B: © 2008 Alwil Software

OutbreakShield: © 2008 Commtouch Software Ltd.

G DATA ServiceCenter

Das **G DATA ServiceCenter** hilft registrierten Kunden bei allen Problemen, die im Zusammenhang mit dem G DATA Produkt auftreten per Telefon, Telefax oder E-Mail. Die Kontaktdaten des ServiceCenters erhalten Sie von uns unmittelbar nach der Anmeldung am **G DATA UpdateServer**.

Bei vielen Problemen können Ihnen oft bereits Hilfetexte und Handbuch weiterhelfen. Bitte versuchen Sie zunächst hier eine Antwort auf Ihre Fragen zu finden. Viele Fragen sind auch bereits in der Online-Datenbank für häufig gestellte Fragen (FAQ) beantwortet worden, die Sie im Support-Bereich der G DATA-Homepage aufrufen können:

www.gdata.de

Sollten Sie dennoch bereits vor der Anmeldung eine Hilfestellung benötigen, können Ihnen unsere Mitarbeiter im ServiceCenter weiterhelfen. Bitte halten Sie für das Gespräch Ihre Kundendaten (Kundennummer, Registriernummer o.ä.) sowie Zettel und Stift bereit.

Deutschland: 0180 555 48 40

(14 Cent/Minute aus dem deutschen Festnetz. Aus dem Mobilfunknetz können ggf. abweichende Preise gelten.)

Österreich/Schweiz: +49 180 555 48 40

(14 Cent/Minute aus dem Festnetz der Schweiz oder Österreich. Aus dem Mobilfunknetz können ggf. abweichende Preise gelten.)

Prüfen Sie vor jedem Gespräch bitte, mit welcher Soft- und Hardware Ihr Computersystem ausgestattet ist. Bitte richten Sie es so ein, das Telefon in der Nähe Ihres angeschalteten Rechners zu haben. Die Software sollte zu diesem Zeitpunkt auf Ihrem Rechner installiert sein.

*Bitte halten Sie - soweit vorhanden - beim Gespräch mit dem ServiceCenter Ihre **Zugangsdaten**, die Sie beim Internet-Update erhalten haben, die **Registriernummer** und bei erneuten Anfragen zur gleichen Problematik gegebenenfalls die **Bearbeitungsnummer** bereit.*

Mehrfachlizenzen

Wenn Sie eine Mehrfachlizenz für dieses Produkt erworben haben, 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 unter **Internet-Update** 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.

Wozu dient die Registriernummer?

*Mit Eingabe der **Registriernummer** bei der Anmeldung fürs Internet-Update erhalten Sie also die **Kundendaten** (Benutzername & Passwort) und mit diesen Kundendaten können Sie die G DATA Software im Rahmen von **Mehrfachlizenzen** auf weiteren Rechnern installieren. **Eine erneute Eingabe der Registriernummer ist hierbei nicht nötig.***

Warum erscheint bei einer Registrierung die Meldung: Das Produkt wurde bereits registriert?

*Wenn Sie das Produkt auf einer Anzahl von Computern installieren möchten, die größer ist, als die Anzahl der Lizenzen, die Sie erstanden haben, dann ist es nicht möglich das Produkt darüber hinaus auf weiteren Rechnern zu installieren. Wenn Sie die Anzahl Ihrer Lizenzen erhöhen möchten, setzen Sie sich bitte mit dem **ServiceCenter** in Verbindung.*

Ich habe meine Zugangsdaten verlegt!

*Sie können sich Ihre Zugangsdaten über den **Support**-Bereich der G DATA-Website (www.gdata.de)zuschicken lassen. Geben Sie dort einfach die vollständige Registriernummer ein, die auf der Rückseite des Benutzerhandbuchs aufgedruckt ist. Ihnen werden dann Ihre Zugangsdaten*

an Ihre hinterlegte E-Mail-Adresse geschickt.

G DATA Unternehmenslösungen

Professionellen Virenschutz mit der preisgekrönten DoubleScan-Technologie gibt es auch für Netzwerke. Hocheffizient, vollautomatisch und fernsteuerbar. Ob als client/server-basierte Komplettausrüstung des Netzwerkes oder als serverunabhängiges Gateway für Ihre Mailkorrespondenz - *G DATA bietet 100% Virenschutz für beliebige Netzwerke jeder Größe.* Informieren Sie sich einfach unverbindlich bei unserem **G DATA Business Vertrieb** während der üblichen Geschäftszeiten unter:

Deutschland



Tel.: 0234 / 9762-170
Fax: 0234 / 9762-298
E-Mail: b-vertrieb@gdata.de

Österreich & Schweiz



Tel.: +49 234 / 9762-170
Fax: +49 234 / 9762-298
E-Mail: b-vertrieb@gdata.de

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

Tipps zur Virenprophylaxe

Obwohl die G DATA Software auf Basis international renommierter Virenerkennungstechnologien nicht nur bekannte Viren entdeckt und beseitigt, sondern mit Hilfe der heuristischen Analyse auch bis dato unbekannte Schadprogramme anhand Ihrer besonderen Spezifika erkennt, ist es fraglos besser, einen Virenbefall von vornherein auszuschließen bzw. die Möglichkeiten dafür zu minimieren. Dazu sollten sowohl bei Einzelplatzrechnern, als auch in Netzwerken einige Sicherheitsvorkehrungen getroffen werden, die nicht viel

Mühe kosten, die Sicherheit Ihres Systems und Ihrer Daten jedoch merklich erhöhen.

- **E-Mail-Vorschaufunktion deaktivieren:** Um HTML-Viren keine unnötige Angriffsfläche zu bieten, ist es empfehlenswert, die Vorschaufunktion in E-Mailprogrammen auszuschalten, die in dieser Hinsicht einen möglichen Infektionsweg eröffnet. Wenn Ihr Mailprogramm das Nachladen und Anzeigen von Grafiken von "unsicheren" Mail-Absendern unterbindet, sollten Sie das Anzeigen dieser Grafiken nur dann erlauben, wenn Sie sich sicher sind, dass der Absender vertrauenswürdig ist.
- **Benutzerkonten verwenden:** Sie sollten auf Ihrem Computer zwei Benutzerkonten verwenden. Ein Administrator-Konto, das Sie immer dann verwenden, wenn Sie Software installieren oder grundlegende Einstellungen an Ihrem Computer vornehmen und ein Benutzerkonto mit eingeschränkten Rechten. Das Benutzerkonto mit eingeschränkten Rechten sollte z.B. nicht in der Lage sein Programme zu installieren oder Modifikationen im Windows-Betriebssystem vorzunehmen. Mit diesem Konto können Sie dann relativ gefahrlos z.B. im Internet surfen, Daten von Fremdrechnern übernehmen usw. Wie Sie unterschiedliche Benutzerkonten anlegen, wird Ihnen in der Hilfe-Dokumentation Ihres Windows-Betriebssystems erläutert.
- **Spam-Mails ignorieren:** Auf Kettenbriefe und Spam-Mail sollte grundsätzlich nicht geantwortet werden. Selbst wenn solche E-Mails keinen Virus enthalten sollten, belastet Ihre unerwünschte Weiterleitung den Datenfluss im Internet erheblich.
- **Virenverdacht überprüfen:** Sollten Sie einen begründeten Virenverdacht haben, z.B. weil eine neu installierte Software nicht das tut, was erwartet wurde oder eine Fehlermeldung erscheint, dann überprüfen Sie das entsprechende Programm am besten noch vor dem Neustart des Rechners auf Virenbefall. Dies ist sinnvoll, da z.B. einige Trojanische Pferde Löschbefehle erst beim nächsten Neustart des Rechners ausführen und auf diese Weise vorher einfacher zu entdecken und bekämpfen sind.
- **Makro-Befehle deaktivieren:** In der Regel ist es empfehlenswert, das Ausführen von Makro-Befehlen der Windows-Office-Anwendungen zu deaktivieren, da gerade dadurch die größten wirtschaftlichen Schäden entstehen. Generell gibt es nur sehr wenige Dateien, die wirklich notwendige Makrofunktionen enthalten. Wie Sie die Makrofunktionen in Office-Anwendungen deaktivieren, wird Ihnen in der Hilfe-Dokumentation Ihres Office-Programmpakets erläutert.
- **Regelmäßige Windows-Updates:** Es sollte es zur regelmäßigen Routine werden, die aktuellen Patches von Microsoft einzuspielen, da diese neu entdeckte Sicherheitslücken von Windows oftmals schon schließen, bevor ein Virenprogrammierer überhaupt auf die Idee kommt, diese für neue

Schadroutinen auszunutzen. Das Windows-Update lässt sich auch automatisieren.

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

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

Systemvoraussetzungen

Zur problemlosen Verwendung der Software benötigt Ihr Computersystem folgende Mindestvoraussetzungen:

- PC mit Windows Vista oder Windows XP (ab SP 2)
- Ab 512 MB RAM Arbeitsspeicher, Internet-Zugang, MS InternetExplorer 5.5 oder höher

Installation

Stellen Sie sicher, die G DATA Software auf einem virenfreien System zu installieren. Führen Sie hierzu gegebenenfalls den oben beschriebenen **BootScan** durch.

*Es ist empfehlenswert, **Vorgängerversionen** der G DATA Software vor der Installation der neuen Software zu deinstallieren.*

Um mit der Installation zu beginnen, legen Sie die G DATA Software CD in Ihr CD/DVD-ROM-Laufwerk ein. Es öffnet sich automatisch ein Installationsfenster.



*Sollten Sie die Autostart-Funktion Ihres CD/DVD-ROM-Laufwerks nicht aktiviert haben, kann die Software den Installationsvorgang nicht automatisch starten. Suchen Sie dann alternativ durch Anklicken des Arbeitsplatz-Symbols auf Ihrem Desktop in der obersten Verzeichnisebene Ihres CD/DVD-ROM-Laufwerks die Datei **setup** bzw. **setup.exe** und starten diese.*

Klicken Sie auf den **Installieren**-Button. Ein Assistent begleitet Sie nun bei der Installation der Software auf Ihrem Computer.

Willkommen

Zur Installation der Software auf Ihrem Computer klicken Sie bitte auf den **Weiter**-Button.

*Wenn Sie die Installation aus irgendwelchen Gründen abbrechen möchten, klicken Sie bitte auf den **Abbrechen**-Button, der in jedem Installationsfenster vorhanden ist. Beim Abbruch der Installation werden sämtliche schon auf Ihren Computer installierte Installationsdaten gelöscht und das System in den Zustand zurückversetzt, den es vor dem Beginn der Installation hatte.*

Lizenzvereinbarung

Nun erscheint ein Bildschirm mit den Lizenzvereinbarungen zur Nutzung der Software. Bitte lesen Sie sich diese aufmerksam durch und klicken auf **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** um sämtlichen Bestimmungen des Lizenzvertrags zuzustimmen.

*Um sich die Lizenzvereinbarung komplett durchzulesen, können Sie den Text durch Anklicken der kleinen Pfeilsymbole mit der Maus nach oben und unten verschieben. Über den **Drucken**-Button können Sie sich die Vertragsbedingungen auch ausdrucken. Wenn Sie die Bedingungen ablehnen, wird das Installationsprogramm abgebrochen. Für die Installation der Software müssen Sie dieser Lizenzvereinbarung zustimmen.*

Installationsart

Wenn Sie die Software als Vollversion gekauft haben, wählen Sie hier bitte den Eintrag **Vollversion installieren** aus.

Was ist der Unterschied zwischen Trial- und Vollversion?

*Wenn Sie die Software als Trial-Version z.B. von einer Heft-CD eines Computer-Magazins einfach mal ausprobieren möchten, dann wählen Sie bitte den Eintrag **Trialversion installieren**. Hier haben Sie die Möglichkeit,*

die Software 30 Tage lang kostenfrei und unverbindlich zu testen.

Setup-Typ

Nun haben Sie die Möglichkeit, den Installationsumfang der Software zu bestimmen. Wählen Sie einfach die gewünschte Installationsvariante aus:

- **Vollständig:** Diese Einstellung ist für die meisten Anwender sinnvoll. Hier wird die G DATA Software mit allen Komponenten und Einstellungen so installiert, wie es auf einem Standard-Betriebssystem optimal ist.
- **Angepasst:** Hier kann der erfahrene Anwender Programmfeatures und Speicherort für die Installation frei wählen. Dies ist für Nutzer sinnvoll, die nur bestimmte Komponenten installieren möchten oder spezielle Systemeinstellungen haben, die bei einer Standardinstallation nicht berücksichtigt werden.

*Sie können Komponenten der Software auch nachträglich installieren oder deinstallieren. Starten Sie dazu bei Bedarf einfach das Setup erneut und aktivieren, bzw. deaktivieren über das **angepasste Setup** die gewünschten oder nicht mehr gewünschten Module.*

Zielordner

Wenn Sie das **vollständige Setup** gewählt haben, wird dieser Schritt bei der Installation übersprungen. Beim **angepassten Setup** können Sie die Software an einem anderen Ort als dem Standard-Programmverzeichnis von Windows installieren. Klicken Sie bitte den **Ändern**-Button und wählen das gewünschte **Zielverzeichnis** aus.

Angepasstes Setup

Während bei der **vollständigen Installation** die Auswahl der zu installierenden Module automatisch abläuft, haben Sie bei der benutzerdefinierten Auswahl die Möglichkeit, gezielt die Module auszuwählen, die Sie benötigen. Wenn Sie bei der Auswahl der Komponenten ein Modul anklicken, erscheint ein Auswahldialog, in dem Sie folgende Installations- bzw. Deinstallationsmöglichkeiten haben:



Das Modul wird auf Ihre Festplatte installiert



Das Modul und alle untergeordneten Module werden auf Ihrer Festplatte installiert (also z.B. **AntiVirus** und **BootCD**)



Das Modul wird nicht installiert oder, falls es schon installiert war, deinstalliert.

Folgende Module stehen Ihnen zur Verfügung:

- **AntiVirus:** Virenschutz mit DoubleScan-Technologie
- **BootCD:** Ermöglicht die Erstellung einer selbstgebrannten CD für den **BootScan**. Der BootScan ist ein praktisches Hilfsmittel, um Viren zu entdecken, die sich schon vor der Installation der Antivirensoftware auf Ihrem Rechner eingeknistet haben.

Zeitplan

Sie können schon während der Installation festlegen, ob die Software bestimmte Aktionen von nun an automatisch durchführen soll.

- **Viren-Update stündlich laden:** Hiermit werden die Virensignaturen, die das wichtigste Mittel zur Erkennung und Bekämpfung von Viren und Schadsoftware darstellen, im Rahmen **automatischer Updates** stündlich auf Ihrem Rechner aktualisiert.
- **Rechner wöchentlich auf Viren prüfen:** Eine regelmäßige Kontrolle des Rechners ist gerade dann sinnvoll, wenn Sie viel im Internet surfen. Der im Hintergrund laufende Virenwächter von G DATA schützt Sie wohl permanent, aber eine zusätzliche Kontrolle ist z.B. dann empfehlenswert, wenn Sie z.B. auf alte Datenbestände (z.B. von einer Backup-Festplatte) zurückgreifen. Auch hier können sich Viren befinden, die z.B. vor der Installation der G DATA Software in Ihren Datenbestand gelangt sein können.

Selbstverständlich können Sie alle Aktionen des Zeitplans auch nachträglich in

der installierten Software verwalten, starten, ändern oder unterbrechen. Wenn Sie eine der automatischen Aktionen nicht sofort verwenden möchten, entfernen Sie einfach das Häkchen an dem jeweiligen Eintrag.

Weitere Informationen finden Sie in den Kapiteln:

- AntiVirus > Optionen > Wächter
- AntiVirus > Zeitplan > Automatische Updates
- AntiVirus > Zeitplan > Automatische Virenprüfungen

Installationsabschluss

Nach Eingabe der notwendigen Informationen startet die Installation der Software auf Ihrem System. Der Installationsvorgang kann einige Minuten dauern und Ihnen wird über einen Fortschrittsbalken angezeigt, an welcher Position der Installation Sie sich gerade befinden. Sie können die Software nach einem **Neustart** jetzt direkt, über den Programmgruppeneintrag der **G DATA Software** im Programme-Verzeichnis oder durch Anklicken des entsprechenden **Symbols** auf Ihrem **Desktop** starten.



Nach der Installation sehen Sie unten rechts in der Taskleiste das **Security-Symbol**. Seine Funktion wird in dem Kapitel **Allgemeine Informationen > Security-Symbol** ausführlich erläutert.

Beim ersten Start

Beim ersten Start der Software werden einige Parameter und Einstellungsoptionen abgefragt. Die Anzahl dieser Abfragen ist abhängig davon, welche Programm-Module Sie installiert haben und welche weiteren Einstellungen Sie bei der Installation vorgenommen haben.

Internet-Update

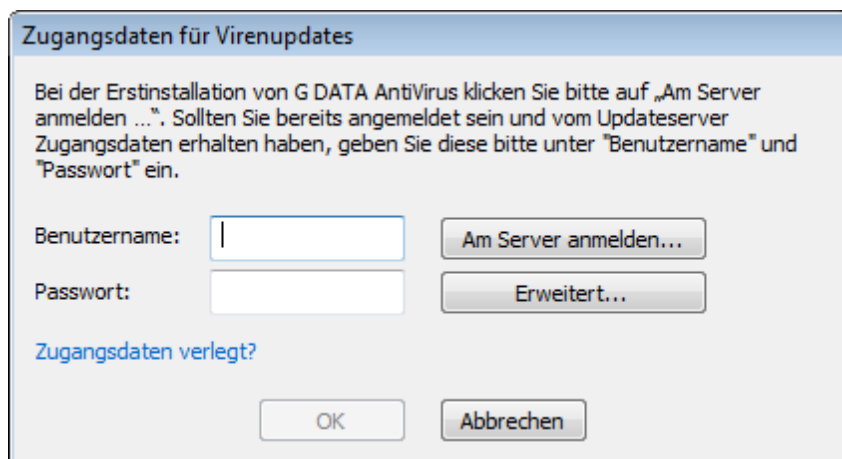
Aktualisierung von Virensignaturen und Software: Das Internet-Update

Wenn Sie die Software nach der Installation zum ersten Mal starten, öffnet sich ein Assistent, über den Sie das Internet-Update der Virensignaturen sowie ein Update eventueller Programm-Aktualisierungen durchführen können. Damit Ihnen der Zeitabstand zwischen der Herstellung der Software und der Installation nicht zum Nachteil gerät, empfehlen wir Ihnen, sofort dieses Update durchzuführen.

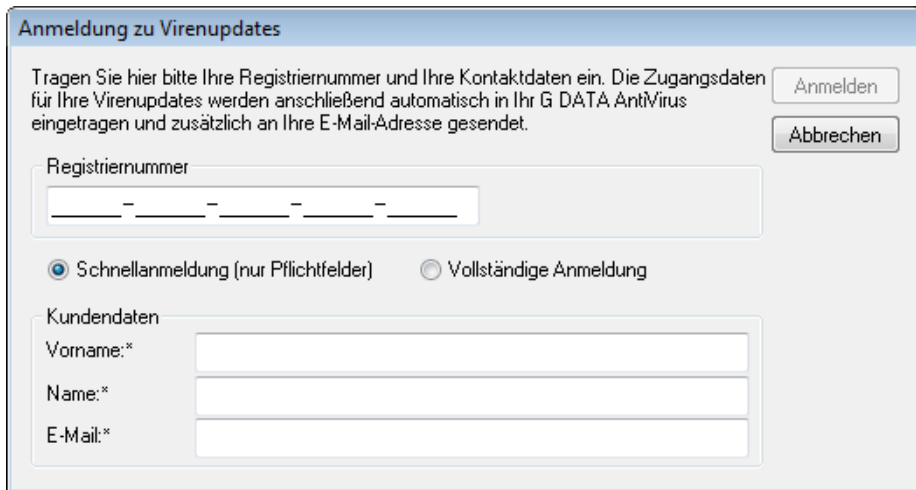
Bei keiner anderen Software sind Updates so wichtig wie bei Security-Software. Halten Sie Ihre G DATA Software stets aktuell!



Klicken Sie dazu einfach auf den Button **Updates durchführen**. Nun erscheint ein Fenster, in dem die Zugangsdaten für Internet Updates abgefragt werden.



Um diese Zugangsdaten zu erhalten, klicken Sie hier einfach auf den Button Am Server anmelden. Es erscheint ein Eingabefenster, in dem Sie ihre Registriernummer und Kundendaten eingeben können.



Anmeldung zu Virenupdates

Tragen Sie hier bitte Ihre Registriernummer und Ihre Kontaktdaten ein. Die Zugangsdaten für Ihre Virenupdates werden anschließend automatisch in Ihr G DATA AntiVirus eingetragen und zusätzlich an Ihre E-Mail-Adresse gesendet.

Registriernummer

☒ Schnellanmeldung (nur Pflichtfelder) ☐ Vollständige Anmeldung

Kundendaten

Vorname:*

Name:*

E-Mail:*

Die **Registriernummer** finden Sie auf der Rückseite des gedruckten Bedienungshandbuchs. Wenn Sie die Software online gekauft haben, erhalten Sie die Registrierungsnummer in einer gesonderten E-Mail.

Bei der Anmeldung haben Sie die Auswahl zwischen einer **Schnellanmeldung** und der Option **Vollständige Anmeldung**. Mit Hilfe der Dateien aus der vollständigen Anmeldung kann unser Support in Problemfällen ein KundenLogin leichter zuordnen, außerdem steht für etwaige Zusendungen unserem Service Ihre postalische Adresse direkt zur Verfügung.

Klicken Sie nun auf den **Anmelden**-Button und Ihre Zugangsdaten werden auf dem G DATA UpdateServer generiert. Wenn die Anmeldung erfolgreich verlief, erscheint ein Info-Bildschirm mit dem Vermerk **Die Anmeldung wurde erfolgreich durchgeführt**, den Sie mit dem **Schließen**-Button verlassen können. Abschließend werden die Zugangsdaten automatisch in die

ursprüngliche Eingabemaske übernehmen und Sie können durch Anklicken des **OK**-Buttons den eigentlichen Update-Vorgang starten.



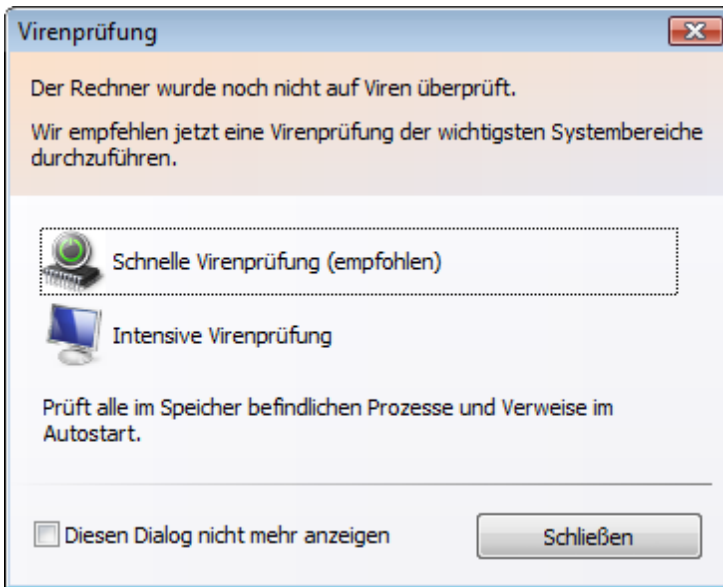
Sofern Sie die Voreinstellungen des Installations-Assistenten übernommen haben, aktualisiert sich Ihre G DATA Software nach dem Erststart automatisch im Hintergrund.

Sie können auf der **Status**-Seite des AntiVirus-Moduls jederzeit den Stand der Virensignaturen (**Datum der Virensignaturen**) ablesen. Sollte dieser Eintrag ein Warnsymbol mit einem veralteten Datum anzeigen, sollten Sie die Funktion **Automatische Updates** aktivieren oder manuell ein Update durchführen. Ein Anleitung hierzu finden Sie im Handbuch oder der Online-Hilfe.

Virenprüfung

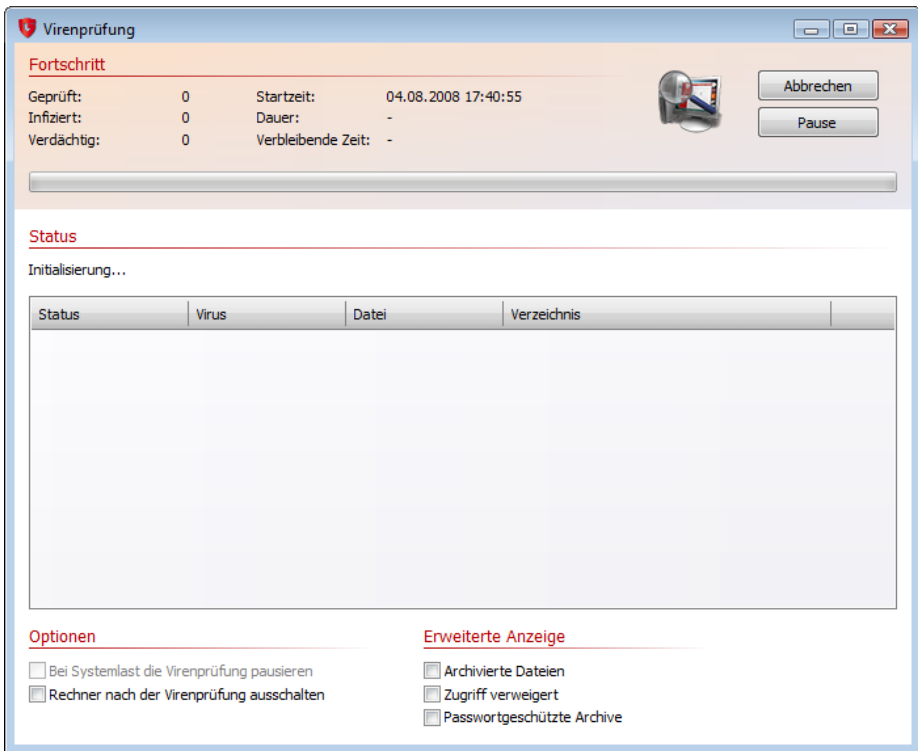
Direkt ab Neustart nach der Installation Ihrer G DATA Software schützt der Virenwächter unsichtbar im Hintergrund vor Schadsoftware und reagiert sofort, wenn Malware mit Ihrem System interagieren will. Trotzdem ist es beim Erststart Ihrer G DATA Software ratsam, nach der Installation und dem Internet-

Update der Virensignaturen sofort eine Überprüfung des Rechners auf Virenbefall vorzunehmen.



Mit dem Virenprüfungs-Assistenten, der beim ersten Start der Software erscheint, können Sie diese Prüfung direkt vornehmen. Sie haben die Auswahl zwischen den Optionen **Schnelle Virenprüfung (empfohlen)** und **Intensive Virenprüfung**. Eine intensive Virenprüfung ist empfehlenswert, dauert aber auch je nach Hardwareausstattung einige Minuten bis über eine Stunde. Sollten Sie in Zeitnot sein, führen Sie wenigstens eine schnelle Virenprüfung durch. Wenn Sie die Virenprüfung starten, erfolgt eine Überprüfung Ihres Rechners auf Virenbefall. Dazu öffnet sich ein Fenster, in dem Sie über den Verlauf der Virenüberprüfung informiert werden.

Unter **Fortschritt** wird Ihnen angezeigt, wie viele Dateien überprüft wurden und wie viele davon gegebenenfalls infiziert sind oder verdächtig wirken. Im Anzeigefenster werden wichtige Informationen und Ergebnisse der Virenprüfung aufgelistet. So werden hier auch infizierte Dateien angezeigt. Virenfunde können Sie hier direkt bearbeiten und entscheiden, wie Sie damit verfahren möchten.



Je nachdem, welche Häkchenfelder Sie unter **Erweiterte Anzeige** aktiviert haben, erhalten Sie hier auch Informationen über archivierte Dateien, passwortgeschützte Archive und Dateien, auf die der Zugriff verweigert wurde.

- **Archivierte Dateien:** Hier können Sie festlegen, ob jeder einzelne Virenfund in einem Archiv angezeigt wird oder nur eine Zusammenfassung für das gesamte Archiv. So werde z.B. bei eingeschalteter Option bei einem Postfach mit 100 infizierten Dateien 101 Einträge angezeigt (also 100 infizierte Dateien UND dazu das infizierte Archiv, in dem diese Dateien enthalten sind). Wenn die Option nicht eingeschaltet ist, wird lediglich mit einem Eintrag darauf hingewiesen, dass sich in dem Postfach-Archiv Viren befinden
- **Zugriff verweigert:** Generell gibt es unter Windows Dateien, die von Anwendungen exklusiv verwendet werden und deshalb von der G DATA Antivirensoftware nicht überprüft werden können, solange diese Anwendungen laufen. Am besten sollten Sie deshalb während einer Virenprüfung möglichst keine anderen Programme auf Ihrem System laufen lassen. Wenn Sie hier

ein Häkchen setzen, werden Ihnen die Daten angezeigt, die nicht überprüft werden konnten.

- **Passwortgeschützte Archive:** Solange ein Archiv passwortgeschützt ist, kann die G DATA Antivirensoftware die Dateien dieses Archives nicht auf Virenbefall überprüfen. Solange dieses Archiv nicht entpackt wird, stellt ein darin enthaltener Virus auch kein Sicherheitsrisiko für Ihr System dar. Wenn Sie Ihren **Virenwächter** aktiviert haben, wird der Virus automatisch erkannt und bekämpft, sobald Sie das Archiv manuell entpacken. Dazu muss im Virenwächter allerdings die Option **Beim Schreiben prüfen** im Virenwächter aktiviert sein. Wenn Sie das Häkchen bei **Passwortgeschützte Archive** setzen, informiert die Antivirensoftware Sie darüber, welche passwortgeschützten Archive es nicht überprüfen konnte.

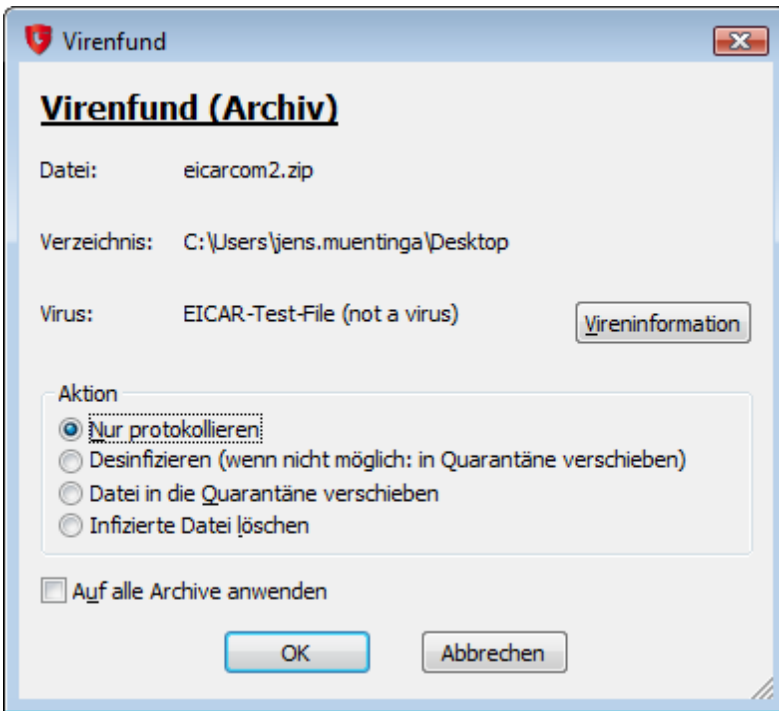
Ein Fortschrittsbalken im oberen Bereich des Fensters zeigt Ihnen, wie viel Prozent Ihres Systems schon überprüft wurden.

*Über das Auswahlfeld **Bei Systemlast die Virenprüfung pausieren** können Sie festlegen, dass die Software so lange mit der Virenprüfung wartet, bis Sie mit anderen Tätigkeiten am Computer fertig sind.*

*Generell können Sie Ihren Computer während der Virenüberprüfung ganz normal weiterverwenden, sollte es bei speicherintensiven Anwendungen doch zu Verzögerungen kommen, können Sie die Virenprüfung über den **Pause-Button** auch anhalten und zu einem späteren Zeitpunkt mit Anklicken von **Fortsetzen** weiterführen. Eine Virenprüfung können Sie jederzeit natürlich auch nachträglich oder sogar automatisch und zeitgesteuert durchführen. Wie das funktioniert, wird Ihnen in der Hilfe-Dokumentation ausführlich erläutert.*

Virenfund

Bei einem Virenfund erscheint ein Info-Fenster, in dem Ihnen das Programm verschiedene Optionen zur Verfügung stellt, wie mit dem Virus zu verfahren ist. In diesem Fenster können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll.



Empfehlenswert ist hierbei **Desinfizieren (wenn nicht möglich: in Quarantäne verschieben)**, da hier die Verbreitung des Virus unterbunden wird und trotzdem keine Datei auf dem Rechner gelöscht wird.

*Sie können auch aus dem **Quarantäne**-Ordner heraus verdächtige Dateien zu G DATA senden, die dann auf Schadcode untersucht werden.*

Programmaufbau

Die Bedienungsoberfläche der Software ist selbsterläuternd und übersichtlich gestaltet. Anhand einer Auswahl auf der linken Seite können Sie das Programm-Modul (z.B. **AntiVirus**) auswählen, an dem Sie Einstellungen vornehmen oder überprüfen möchten. Hier finden Sie dann weitergehende thematische Untergliederungen und Bereiche (z.B. **Status**, **Aktionen**), die Sie ebenfalls anklicken können.

Die Funktionen der jeweiligen Bereiche, werden Ihnen dabei im Programm selbst durch Info-Texte erläutert, die über dem jeweiligen Bereich stehen oder im unteren Teil des Programmfensters erscheinen, wenn sie den Mauszeiger auf ein Bedienelement ziehen.



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



Ein grünes Häkchen weist darauf hin, dass die jeweilige Komponente aktiv ist und ihre Schutzfunktion erfüllt.



Ein gelbes Warnsymbol zeigt Ihnen, dass geringe Beeinträchtigungen der Schutzfunktionen bestehen, dass z.B. die letzte Analyse des Rechners zu lange her ist oder sich Dateien in der Quarantäne befinden. Hier droht keine unmittelbare Gefahr, aber Sie sollten baldmöglichst reagieren, um den Schutz Ihres Systems wieder zu optimieren.

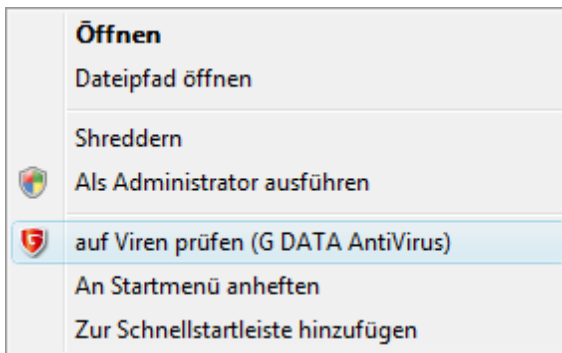


Ein rotes Warnsymbol signalisiert, dass bei dieser Funktion ein ernstes Sicherheitsproblem vorliegt und sofortiger Handlungsbedarf besteht.

Sollte eine Komponente Ihres Securitypakets einer Handlung bedürfen (rotes oder gelbes Warnsymbol), können Sie direkt auf das jeweilige Symbol klicken und gelangen in den gewünschten Bereich, in dem Sie das angezeigte Problem in der Regel mit wenigen Mausklicks beheben können. Genauere Informationen hierzu finden Sie im Handbuch oder der Online-Hilfe.

Windows Kontextmenü

Bei der Installation der Software wird eine Analysefunktion in das Windows-Kontextmenü eingefügt. Hiermit können Sie direkt eine Virenprüfung bestimmter verdächtiger Objekte durchführen: Dazu bewegen Sie die Maus auf das zu analysierende Objekt (Laufwerk, Verzeichnis, Datei) und betätigen dort dann die rechte Maustaste. Das Windows Kontextmenü öffnet sich. Durch Anwählen des Menüpunktes **auf Viren prüfen (G DATA AntiVirus)** wird automatisch eine Virenprüfung des Objektes mit den Standardeinstellungen des Programmbereiches **AntiVirus** durchgeführt.



Security-Symbol

Über das Security-Symbol, das sich in der Regel rechts unten in der **Taskleiste** Ihres Windows Desktops neben der Systemuhr befindet, können Sie immer feststellen, ob der Virenwächter aktiv ist.

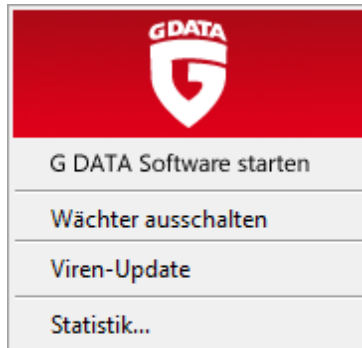


Der aktivierte **Wächter** zeigt ein rotes Schild.



Falls der Virenwächter nicht aktiviert wurde oder andere Probleme mit dem Schutz Ihres Rechners vorliegen, ist das Schild mit einem Warnsymbol markiert. Sie sollten dann die G DATA Software starten, um eine Lösung für dieses Problem herbeizuführen.

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 die Programmoberfläche auf und können dort z.B. die Einstellungen für den Virenwächter vornehmen.
- **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 Rechengvorgängen (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. Sie können den Virenwächter über diese Funktion nur für bestimmte Zeitintervalle (maximal bis zum nächsten Neustart) ausschalten. Wenn Sie den Virenwächter komplett ausschalten wollen, können Sie das über die G DATA-Programmoberfläche durchführen.
- **Viren-Update:** Auch unabhängig von zeitplangesteuerten Virensignatur-Updates können Sie über diese Funktion ihre Virensignaturen jederzeit auf den neuesten Stand bringen.
- **Statistik:** Hier können Sie sich eine Statistik über die Prüfungsvorgänge des Virenwächters anzeigen lassen.

*Wie Sie die Einstellungen für den Wächter verändern und an individuelle Bedürfnisse anpassen können, lesen Sie im Kapitel **AntiVirus > Optionen > Wächter**.*

*Wenn Sie den Autopiloten ausschalten, schalten Sie damit nicht automatisch die komplette Firewall ab. Sollten Sie spezielle Verbindungen wünschen, die vom Autopiloten geblockt werden, ist es deshalb sinnvoll, die Funktion **Autopilot ausschalten** zu wählen. Mit der Funktion **Firewall ausschalten** deaktivieren Sie hingegen komplett die gesamte Firewallfunktionalität. Dies sollten Sie nur in sehr begründeten Ausnahmefällen durchführen. Informationen darüber, wie Sie Firewall und Autopilot einstellen können, erhalten Sie im Kapitel **Firewall > Optionen**.*

G DATA BootCD erstellen

In der Programmgruppe können Sie unter diesem Eintrag eine Linux-basierte Boot-CD für den **BootScan** erstellen. Im Gegensatz zum BootScan mit der **G DATA Programm-CD** werden hier auch offline automatisch die jeweils aktuellsten Virensignaturen verwendet. Die Boot-CD kann Ihnen auf anderen Rechnern, die noch nicht von der G DATA Software geschützt sind, bei Virenbefall schnell und unkompliziert ein virenfreies System erzeugen, auf dem Sie dann eine Antivirensoftware zum permanenten Schutz installieren sollten. Die Erzeugung der Boot-CD erfolgt mit Hilfe eines Assistenten, der Ihnen sämtliche Arbeitsschritte ausführlich erläutert.

*Der **BootScan** ist die wirksamste und sicherste Methode zur Erkennung und Beseitigung aktiver **Rootkits**. Sie sollten in regelmäßigen Abständen einen **BootScan** durchführen. Legen Sie hierzu die Boot-CD wieder ein und starten Ihren Rechner anschließend neu.*

*Informationen zum BootScan erhalten Sie in dem Kapitel **Anhang > Fragen und Antworten (FAQ) > BootScan**.*

*Ein **Rootkit** versucht den in ihm enthaltenen Schadcode (Trojaner, Viren, Würmer) so zu verschleiern, dass er sogar vor Antivirenprogrammen getarnt ist. Wenn sich ein Rootkit erst einmal auf dem Rechner eingenistet hat, ist es für ein nachträglich installiertes Antivirenprogramm fast unmöglich, es zu entdecken. Abhilfe bietet hier der BootScan, da dieser schon vor dem Start des Betriebssystems eingreift und so auch Schadsoftware entdeckt, die sich*

ansonten verbergen könnte.

*Wenn Ihre Virensignaturen regelmäßig aktualisiert werden und Sie den Virenwächter permanent verwenden, schützt die G DATA Software natürlich effektiv gegen **Rootkits**. Ein **BootScan** ist in der Regel dann ratsam, wenn Ihr Computer eine Zeitlang ohne professionellen Virenschutz betrieben wurde.*

AntiVirus

Die Bedienung der **AntiVirus**-Software ist prinzipiell selbsterläuternd und übersichtlich gestaltet. Anhand unterschiedlicher Register, die Sie über die links in der Software angezeigten Symbole anwählen können, wechseln Sie in den jeweiligen **Programmbereich** (z.B. **Status**-Bereich, **Protokolle**-Bereich etc.) und können dort Aktionen durchführen, Einstellungen vornehmen oder Protokolle und Ergebnislisten überprüfen.



Außerdem finden Sie in der oberen **Menüleiste** der **Programmoberfläche** übergreifende Funktionen und Einstellungsmöglichkeiten (siehe Kapitel **AntiVirus > Optionen**) sowie das **Security-Symbol** in der Taskleiste Ihres Desktop (in der Regel unten rechts neben der Windows-Systemuhr).



Sobald **AntiVirus** installiert und der **Virenwächter** aktiviert ist, verfolgt es sämtliche Vorgänge auf Ihrem Computer, die die Infektion oder Verbreitung von Schadsoftware und Viren ermöglichen könnten.

Die Aktivität und das Vorhandensein des Virenwächters erkennen Sie an dem Security-Symbol in der Start-Leiste von Windows. Hierauf können Sie durch einen Klick mit der rechten Maustaste ein **Windows-Kontextmenü** öffnen, in dem Sie sich eine Statistik anzeigen lassen und die Programmoberfläche von AntiVirus öffnen können. Welche Funktionen Sie im einzelnen über das **Security-Symbol** aufrufen können, erfahren Sie in dem Kapitel **Allgemeine Informationen > Security-Symbol**.

*Sollte einer der Programm-Module fehlen, kann es daran liegen, dass Sie das jeweilige Feature (z.B. **Firewall** oder **AntiSpam**) beim angepassten Setup während der Installation nicht mitinstalliert haben. Eine andere Möglichkeit ist die, dass Sie eine Programmversion besitzen, die das entsprechende Feature nicht beinhaltet.*

Status

Im **Status**-Bereich von **AntiVirus** erhalten Sie grundlegende Informationen zum aktuellen Zustand Ihres Systems und der Software. Durch doppeltes Anklicken des jeweiligen Eintrags (oder durch Auswählen des Eintrags und Anklicken des **Bearbeiten**-Buttons) können Sie hier direkt Aktionen vornehmen oder in den jeweiligen Programmbereich wechseln. Sobald Sie die Einstellungen einer Komponente mit Warnsymbol optimiert haben, wechselt das Symbol im **Status**-Bereich wieder auf das grüne Häkchensymbol. Wenn alle Symbole hier grün sind, dann ist Ihr System optimal geschützt.

Virenwächter

Der Virenwächter arbeitet auch dann, wenn Sie die AntiVirus Programmoberfläche nicht geöffnet haben und kontrolliert Ihren Rechner im Hintergrund automatisch auf Viren ohne Sie dabei in Ihrer täglichen Arbeit zu beeinträchtigen. Seine Funktionsweise wird in dem Kapitel **Security-Symbol** erläutert.

Wenn Sie den Eintrag **Virenwächter** anklicken, öffnet sich ein Menü, in dem Sie den Status des Virenwächters schnell zwischen **eingeschaltet** und **ausgeschaltet** umschalten können. Um die Virenwächterfunktionen genauer zu spezifizieren, klicken Sie bitte auf den **Erweitert**-Button. Auf diese Weise gelangen Sie in das **Optionen**-Menü des Virenwächters. Lesen Sie hierzu bitte auch das Kapitel **AntiVirus > Optionen > Wächter**.

Systemschutz

Wenn der Systemschutz aktiviert ist, werden bei jedem Systemstart die **Windows-Registry** und die Systemordner überprüft. Auf diese Weise wird die **HOSTS-Datei** vor Manipulationen geschützt.

E-Mail-Virenblocker

Der **E-Mail-Virenblocker** überprüft neue E-Mails auf Viren. Sie sollten den E-Mail-Virenblocker immer aktiviert haben. Wenn Sie diesen Eintrag doppelt anklicken, öffnet sich eine Infobox, in der statistische Angaben zum E-Mail-Virenblocker angezeigt werden. Über den **Aktualisieren**-Button können Sie diese Statistik auf den neuesten Stand bringen, wenn in der Zwischenzeit neue E-Mails eingetroffen sein sollten. Über den **Optionen**-Button gelangen Sie zum Konfigurationsmenü für den E-Mail-Virenblocker. Hier können Sie z.B. die E-Mail-Überprüfung auf neu installierte E-Mail-Programme ausweiten und globale Einstellungen vornehmen. Informationen hierzu erhalten Sie in dem Kapitel **AntiVirus > Optionen > E-Mail-Prüfung**.

Automatische Updates

Hier wird Ihnen angezeigt, ob die Internet-Updates der Virensignaturen vom **G DATA UpdateServer** automatisch erfolgen oder nicht. Wenn Sie diesen Eintrag anklicken, gelangen Sie in den **Zeitplan**-Bereich der Software, in dem Sie die automatischen Updates definieren können. Lesen Sie hierzu bitte das Kapitel **AntiVirus > Zeitplan** und dessen Unterkapitel.

Datum der Virensignaturen

Je aktueller die **Virensignaturen**, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten. Wenn Sie diesen Eintrag doppelt anklicken, können Sie sofort eine Aktualisierung der Virensignaturen durchführen. Beantworten Sie die Frage **Möchten Sie die Virensignaturen jetzt aktualisieren?** einfach durch Anklicken des **Ja**-Buttons. Nach einem Internet-Update stehen Ihnen die neuen Virensignaturen sofort zur Verfügung. Sie müssen die Software nicht erneut starten, um mit den neuen Virendaten zu arbeiten.

Sie haben auch die Möglichkeit, das Internet-Update neuer Virensignaturen automatisch nach einem bestimmten Zeitplan durchführen zu lassen. Lesen

Sie hierzu bitte das Kapitel **AntiVirus > Zeitplan**.

Sollte es Probleme mit dem Internet-Update geben, kann das daran liegen, dass der Software Informationen zur Verbindung mit dem Internet fehlen. Lesen Sie hierzu bitte das Kapitel **AntiVirus > Optionen > Internet-Update**.

Letzte Analyse des Rechners

Regelmäßige Analysen erhöhen die Sicherheit vor Viren. Überprüfen Sie Ihren Rechner am besten nach jedem Internet-Update der Virensignaturen. Wenn Sie diesen Eintrag doppelt anklicken, können Sie sofort eine Überprüfung des Rechners auf Virenbefall durchführen. Beantworten Sie dazu einfach die Fragen **Möchten Sie Ihren Rechner jetzt auf Viren überprüfen?** einfach durch Anklicken des **Ja**-Buttons. Während der Virenprüfung öffnet sich ein Fenster, in dem statistische Angaben und Informationen zur Virenprüfung angezeigt werden.

Weitere Informationen erhalten Sie im Kapitel **AntiVirus > Optionen Virenprüfung**.

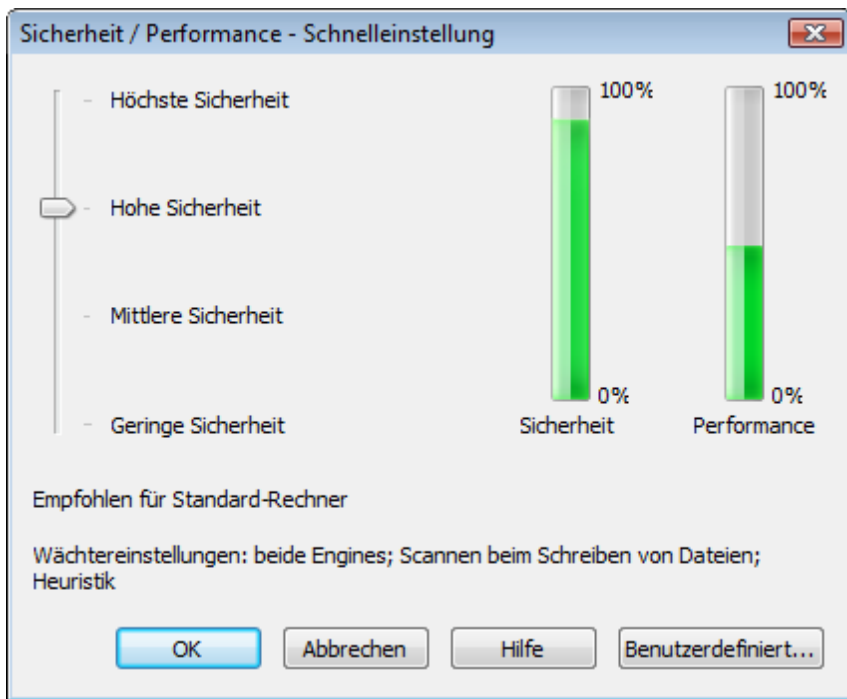
Dateien in der Quarantäne

Im Quarantäne-Bereich werden verdächtige Dateien automatisch durch Verschlüsselung unschädlich gemacht und können von dort aus weiterbearbeitet werden. Wenn die infizierte Datei unbedingt benötigt wird, kann sie auch im infizierten Zustand wieder an ihren Ursprungsort zurückverschoben werden. Durch doppeltes Anklicken des Eintrags **Dateien in der Quarantäne** gelangen Sie automatisch in den Quarantäne-Bereich. Lesen Sie hierzu das Kapitel **AntiVirus > Quarantäne**.

Sicherheit / Performance

Zwangsläufig sorgt eine permanente Überwachung Ihres Rechners für leichte Geschwindigkeitseinbußen. Sollten diese sich bei Ihnen tatsächlich störend bemerkbar machen, können Sie über die Funktion **Sicherheit / Performance** zwischen dem Sicherheitsaspekt und der Performance Ihres Rechners abwägen und auf diese Weise den permanent aktiven Virenwächter auf Ihr

System abstimmen.



Sie haben folgende Einstellungsmöglichkeiten:

- **Höchste Sicherheit** (nur empfohlen für sehr schnelle Rechner): beide Engines aktiv; Archive werden geprüft; Scannen beim Schreiben von Dateien; Heuristische Virenprüfung aktiv.
- **Hohe Sicherheit** (empfohlen für Standard-Rechner): beide Engines aktiv; Archive bis 300 kB Größe werden geprüft; Scannen beim Schreiben von Dateien; Heuristische Virenprüfung aktiv.
- **Mittlere Sicherheit** (nur empfohlen für langsame Rechner): nur Hauptengine aktiv; Archive werden nicht geprüft; Scannen beim Schreiben von Dateien; Heuristische Virenprüfung aktiv.
- **Geringe Sicherheit** (nur empfohlen für sehr langsame Rechner): nur Hauptengine aktiv; Archive werden nicht geprüft; nur Programmdateien und Dokumente werden überprüft; Heuristische Virenprüfung aktiv.

Wenn Sie mit den standardmäßig auszuwählenden Voreinstellungen für den

Virenwächter nicht zufrieden sind, können Sie über den **benutzerdefiniert**-Button den Virenwächter auch individuell konfigurieren. Wie dies funktioniert und welche Bedeutung der hier aufgeführten Leistungsspezifika haben, wird ausführlich im Kapitel **AntiVirus > Optionen > Wächter** erläutert.

Aktionen

Im **Aktionen**-Bereich können Sie Virenprüfungen direkt ausführen, unabhängig von zeitlichen Vorgaben für die automatischen Virenprüfungen, die Sie im **Zeitplan**-Bereich festlegen können. Bei der Virenprüfung haben Sie die Möglichkeit, die Prüfung auf bestimmte Bereiche bzw. Medien zu beschränken. So können Sie z.B. mit der Funktion **Rechner prüfen** Ihren kompletten PC kontrollieren, haben aber auch die Optionen, nur eingelegte Disketten oder CD/DVD-ROMs zu überprüfen. Über **Verzeichnisse/Dateien prüfen** können Sie auch festlegen, dass nur ausgewählte Bereiche Ihres Rechners kontrolliert werden (z.B. freigegebene Eingangsverzeichnisse einer Firewall oder nur die **Eigene Dateien**-Ordner). Außerdem können Sie von hier aus direkt ein Internet-Update für Virensignaturen oder Software-Aktualisierungen von **AntiVirus** starten.

*Die Virenprüfung der einzelnen Bereiche findet in dem Virenprüfungsfenster statt, wie es ausführlich im Kapitel **AntiVirus > Optionen > Virenprüfung** beschrieben wird.*

Rechner prüfen

Mit dieser Funktion haben Sie die Möglichkeit, Ihren Rechner auf möglichen Virenbefall zu kontrollieren (also alle lokalen Festplatten und Systembereiche). Klicken Sie diese Funktion an und die Virenprüfung wird automatisch durchgeführt.

*Wenn Sie möchten, dass Virenprüfungen automatisch in festgelegten Zeitabständen stattfinden sollen, finden Sie die notwendigen Einstellungsmöglichkeiten im Bereich **AntiVirus > Zeitplan > Automatische Virenprüfungen**.*

Wechselmedien prüfen

Prüfen Sie mit dieser Funktion **CD-ROMs** oder **DVD-ROMs**, **Disketten**, **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 **AntiVirus** natürlich keine Viren auf Medien entfernen kann, die keinen **Schreibzugriff** erlauben (z.B. gebrannte CD-ROMs). Hier wird der Virenfund dann protokolliert.*

Verzeichnisse/Dateien prüfen

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

*Im Verzeichnisbaum (links) können Sie durch Anklicken der (+)-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 **AntiVirus** geprüft. Wenn in einem Verzeichnis nicht alle Dateien geprüft werden, findet sich an diesem Verzeichnis ein graues Häkchen, das darauf hinweist, dass sich in diesem Verzeichnis teilweise ausgewählte und teilweise nicht ausgewählte Dateien oder Unterverzeichnisse befinden.*

Speicher und Autostart

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

Auf Rootkits prüfen

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

*Ein **Rootkit** versucht den in ihm enthaltenen Schadcode (Trojaner, Viren, Würmer) so zu verschleiern, dass er sogar vor Antivirenprogrammen getarnt ist. Wenn sich ein Rootkit erst einmal auf dem Rechner eingenistet hat, ist es für ein nachträglich installiertes Antivirenprogramm fast unmöglich, es zu entdecken. Abhilfe bietet hier der **BootScan**, da dieser schon vor dem Start des Betriebssystems eingreift und so auch Schadsoftware entdeckt, die sich ansonsten verbergen könnte. Lesen Sie hierzu bitte das Kapitel **Anhang > Fragen und Antworten (FAQ) > BootScan**.*

*Wenn Sie eine Komplettüberprüfung Ihres Computers im Rahmen einer Virenprüfung durchführen (z.B. über die Funktion **AntiVirus > Aktionen > Rechner prüfen**) wird Ihr Rechner natürlich auch nach Rootkits durchsucht.*

Viren-Update

Je aktueller die **Virensignaturen**, desto sicherer ist Ihr Virenschutz. Sie sollten die Virensignaturen so oft wie möglich updaten. Wenn Sie einen Doppelklick auf diesem Eintrag durchführen, können Sie sofort eine Aktualisierung der Virensignaturen durchführen. Nach einem Internet-Update stehen Ihnen die neuen Signaturen sofort zur Verfügung. Sie müssen AntiVirus nicht erneut starten, um mit den neuen Virendaten zu arbeiten.

*Informationen dazu, wie Sie das Update der Virensignaturen automatisieren, finden Sie im Kapitel **AntiVirus > Zeitplan > Automatische Updates**.*

Programm-Update

Über diese Funktion laden Sie gegebenenfalls **Software-Aktualisierungen** der G DATA Software vom **G DATA UpdateServer** herunter. Wenn keine Software-Aktualisierungen auf dem Server vorliegen, werden Sie darüber durch eine Infobox informiert.

*Beim **Programm-Update** handelt es sich um eine Aktualisierung von Programm-Dateien der aktuellen G DATA Software-Version. Es handelt sich nicht um ein Upgrade auf eine neue Version (also z.B. von **G DATA AntiVirus 2008** auf **G DATA AntiVirus 2009**).*

Zeitplan

Im **Zeitplan**-Bereich können Sie Virenprüfungen und die Internet-Updates der Virensignaturen automatisieren, so dass diese zu bestimmten Zeiten selbständig von Ihrem Computer durchgeführt werden. Sie können verschiedene Schemata anlegen und diese auch parallel nebeneinander verwenden.

*Nur **Virenprüfungen** und **Updates**, bei denen das Häkchenfeld mit einem Häkchen versehen ist, werden auch automatisch durchgeführt.*

Automatische Updates

Über das Häkchenfeld vor dem Eintrag **Virensignaturen** können Sie festlegen, ob ein automatisches Update der Virensignaturen erfolgen soll oder nicht. Wenn Sie das automatische Update nicht verwenden, sollten Sie darauf achten, regelmäßig selbst daran zu denken, die Virensignaturen von **AntiVirus** auf den neuesten Stand zu bringen. Um die Einstellungen des automatischen Updates zu ändern, klicken Sie bitte doppelt auf den Eintrag unter **Automatische Updates** (oder markieren diesen und wählen den **Bearbeiten**-Button). Nun öffnet sich eine Box mit Karteikarten, in denen Sie die notwendigen Einstellungen vornehmen können. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie bitte auf **OK**.

Job

Über das Häkchenfeld **Protokoll anfertigen** können Sie festlegen, dass die Software über den Update-Vorgang ein Protokoll anlegt. Dieses kann dann im **Protokolle**-Bereich (siehe Kapitel **AntiVirus > Protokolle**) eingesehen werden.

Zeitplanung

Über diese Karteikarte können Sie festlegen, wann und in welchem Rhythmus das automatische Update erfolgen soll. Unter **Ausführen** geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter **Zeitpunkt** spezifizieren. Wenn Sie unter **Zeitpunkt** die Option **Internetverbindungsaufbau** auswählen, fallen die Vorgaben der Zeitplanung natürlich fort und die Software führt das Update immer aus, wenn Ihr Rechner mit dem Internet verbunden 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.*

Benutzerkonto

Hier kann ein Benutzerkonto auf dem Rechner angegeben werden, für das der **Internet-Zugang** konfiguriert ist.

*Es handelt sich hierbei **nicht** um den Benutzernamen und das Passwort für das Internet-Update von **AntiVirus**, sondern um die Zugangsdaten für das Benutzerkonto, mit dem eine Internetverbindung möglich ist. Die notwendigen Angaben für das **AntiVirus** Internet-Update geben Sie im Bereich **Internet-Update** ein, wie es im Kapitel **AntiVirus > Optionen > Internet-Update** beschrieben wird.*

Automatische Virenprüfungen

Über das Häkchenfeld unter dem Eintrag **Lokale Festplatten** können Sie festlegen, ob eine automatische Virenprüfung erfolgen soll oder nicht. Wenn Sie die automatische Virenprüfung nicht verwenden, sollten Sie darauf achten, regelmäßig selbst daran zu denken, Ihr System auf Virenbefall zu überprüfen.

Um die Einstellungen des automatischen Virenprüfungen zu ändern, klicken Sie bitte doppelt auf den Eintrag unter **Automatische Virenprüfungen** (oder markieren diesen und wählen den **Bearbeiten**-Button). Nun öffnet sich eine Box mit Karteikarten, in denen Sie die notwendigen Einstellungen vornehmen können. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie bitte auf **OK**.

Sie können natürlich auch mehrere automatische Virenprüfungen zu verschiedenen Zeiten durchführen lassen. Um eine neue automatische Virenprüfung zu definieren, klicken Sie einfach auf den Button **Neue Virenprüfung**. So können Sie z.B. Bereiche, die zur täglichen Nutzung im Internet gedacht sind, auch täglich auf Viren überprüfen, während z.B. Ordner oder Festplatten, die der Archivierung dienen nur wöchentlich überprüft werden.

Job

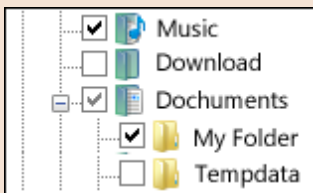
Legen Sie hier fest, welchen Namen der neu eingerichtete Job haben soll. Zur Unterscheidung sind aussagekräftige Namen ratsam wie z.B. **Lokale Festplatten (wöchentliche Überprüfung)** oder **Archive (monatliche Überprüfung)**.

Wenn Sie ein Häkchen bei **Nach Beendigung des Jobs den Rechner ausschalten** setzen, wird der Rechner automatisch heruntergefahren, nachdem die automatische Virenprüfung durchgeführt wurde.

Analyse-Umfang

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

*Im Verzeichnisbaum können Sie durch Anklicken der (+)-Symbole Verzeichnisse öffnen und auswählen, deren Inhalt dann in der Datei-Ansicht (rechts) angezeigt wird. Jedes Verzeichnis oder jede Datei, die Sie mit einem Häkchen versehen, wird von **AntiVirus** 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 die automatische Virenprüfung erfolgen soll. Unter **Ausführen** geben Sie dazu eine Vorgabe vor, die Sie dann mit den Eingaben unter **Zeitpunkt** spezifizieren. Wenn Sie **Beim Systemstart** auswählen, fallen die Vorgaben der Zeitplanung natürlich fort und die Software führt die Prüfung immer aus, wenn Ihr Rechner neu gestartet wird.

*Unter **Täglich** können Sie mit Hilfe der Angaben unter **Wochentage** z.B. bestimmen, dass Ihr Rechner nur an Werktagen die Virenprüfung 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.*

Virenprüfung

In diesem Bereich können Sie festlegen, mit welchen Einstellungen die automatische Virenprüfung stattfinden soll. Welche Bedeutung die hier einstellbaren Optionen haben, wird Ihnen ausführlich in dem Kapitel **AntiVirus > Optionen > Virenprüfung** erläutert.

*Die Einstellungsmöglichkeiten sind im Bereich **AntiVirus > Optionen > Virenprüfung** und im Bereich **AntiVirus > Zeitplan > Automatische Virenprüfungen** identisch, allerdings können Sie beide unabhängig voneinander einstellen. So macht es z.B. Sinn, bei einer automatischen Virenprüfung (die am besten dann stattfinden sollte, wenn der Rechner nicht intensiv genutzt wird, z.B. am Wochenende) eine weit genauere Prüfung vorzunehmen, als bei einer direkten Virenprüfung, wie Sie Sie im Bereich **AntiVirus > Aktionen** durchführen lassen können.*

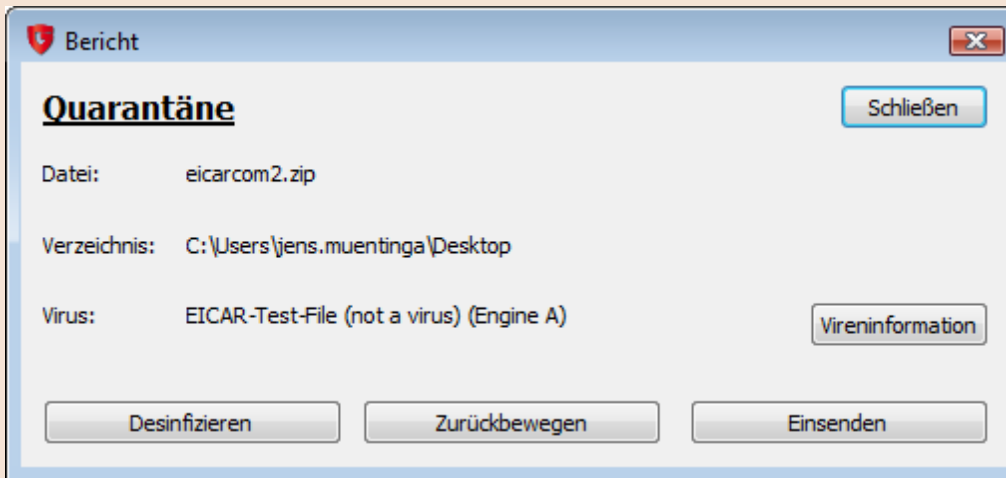
Benutzerkonto

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

Quarantäne

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

*Damit Viren automatisch in die Quarantäne verschoben werden, können Sie bei den Optionen für die Virenprüfung festlegen, was **Im Fall einer Infektion** geschehen soll. Dies wird ausführlich im Kapitel **AntiVirus > Optionen > Virenprüfung** erläutert.*



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 uninfizierter Daten etc.) durchführen.

Einsenden

In bestimmten Fällen können Sie eine infizierte Datei, die Sie nicht desinfizieren können, über das Internet an G DATA übermitteln:

- **Für die Datei wurde ein Virenverdacht gemeldet. Bitte untersuchen Sie die Datei:** Wenn Sie die heuristische Analyse verwenden, kontrolliert **AntiVirus** verdächtige Dateien nicht nur anhand der aktuellen Virensignaturen, sondern schlägt auch automatisch Alarm, wenn eine Datei virenähnliche Elemente enthält. Hierbei handelt es sich in der Regel auch um Viren, in sehr seltenen Fällen aber auch um Fehllalarm. Wenn Sie eine solche Datei einschicken, wird diese eingehend analysiert und untersucht. Das Ergebnis fließt dann in die nächsten Signaturupdates ein.
- **Die Datei wurde als infiziert gemeldet. Ich glaube aber, dass Sie keinen Virus enthält. Bitte untersuchen Sie die Datei:** Sollten Sie ganz sicher davon ausgehen, dass es sich hierbei um keine Infektion handeln kann, schicken Sie die Datei bitte ein. Die Datei wird dann eingehend analysiert und untersucht. Das Ergebnis fließt in die nächsten Signaturupdates ein.
- **Ich benötige Informationen zu dem gefundenen Virus. Im Virenlexikon (www.antiviruslab.com) kann ich keine Informationen finden:** Selbstverständlich wird das **G DATA Virenlexikon** immer auf den neuesten Stand gebracht. Sollten Sie zum angegebenen Virus nichts im

Virenlexikon gefunden haben, dann schicken Sie uns die infizierte Datei und das G DATA Team aktualisiert auf Basis dieser Einsendungen die Informationen im Virenlexikon.

Löschen

Wenn Sie die infizierte Datei nicht mehr benötigen, können Sie diese auch einfach aus der Quarantäne löschen.

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.

Einstellungen

Über doppeltes Anklicken eines Protokolls (oder das Markieren und anschließendes Anklicken von **Öffnen**) öffnet sich die Protokollansicht, die Sie mit den Buttons **Speichern unter** und **Drucken** auch als Textdatei speichern oder direkt ausdrucken können.

Mit dem Auswahlfeld **Einfach / Erweitert** können Sie festlegen, ob Informationen über Archivierte Dateien, Zugriffsverweigerungen und passwortgeschützte Archive angezeigt werden (**Erweitert**) oder nicht (**Einfach**). Um ein Protokoll zu löschen, markieren Sie den Tabelleneintrag mit der Maus und klicken dann bitte auf die Entf-Taste oder betätigen den Löschen-Button. .

*Generell werden nur automatische Vorgänge (automatische Virenprüfung, automatisches Update, Virenfund durch Virenwächter) ins Protokoll eingetragen. Wenn Sie eine manuelle Virenprüfung ins Protokoll aufnehmen wollen, müssen Sie dieses im Bereich **AntiVirus > Optionen > Virenprüfung** vorher einstellen.*

Optionen



Über das Symbol oben rechts in der Menüleiste der Programmoberfläche rufen Sie die den Bereich **Optionen** auf. Hier können Sie grundlegende Einstellungen der Software verändern. Klicken Sie dazu einfach die Registerkarte mit den jeweiligen Einstellungsoptionen an.

Wächter

In diesem Menü können Sie festlegen, wie die **ständige Virenprüfung im Hintergrund** Ihres Systems durch den Virenwächter zu erfolgen hat. Im Gegensatz zu einer Virenprüfung auf Basis eines Zeitplans oder einer manuellen Virenprüfung sollte man beim Virenwächter darauf achten, dass er seine Aufgaben möglichst so erledigt, ohne das System unnötig zu belasten.

*Sollte der Virenwächter mal **Alarm** geschlagen haben, sollte natürlich so bald wie möglich eine ausführliche Virenprüfung erfolgen.*

Wächterstatus



Hier können Sie den Virenwächter ein- oder ausschalten. Generell sollte der Virenwächter natürlich eingeschaltet bleiben, nur in seltenen Ausnahmefällen macht es Sinn, den Virenwächter dauerhaft auszuschalten.

*Um den Virenwächter kurzfristig auszuschalten (für einen bestimmten Zeitraum oder bis zum nächsten Systemstart), empfiehlt es sich, ihn über das Kontextmenü des **Security-Symbols** in der Windows-Taskleiste auszuschalten. Auf diese Weise wird der Virenwächter nach der definierten Zeitspanne automatisch wieder gestartet. Lesen Sie hierzu das Kapitel **Allgemeine Informationen > Security-Symbol**.*

Dass der Wächter aktiv ist, wird Ihnen durch ein Symbol in der Taskleiste

Ihres Systems angezeigt.

Engines benutzen

AntiVirus arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Analyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. In der Regel sollten Sie hier die Einstellung **Beide Engines - performance-optimiert** wählen, da diese die Vorteile einer doppelten Prüfung ohne größere Performance-Einbußen miteinander verbindet.

Im Fall einer Infektion

Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nach dem, für welche Zwecke Sie Ihren Computer verwenden, sind hier unterschiedliche Einstellungen sinnvoll. So ist für Anwender, die viele Daten auf Ihrem Computer verwahren, die Option **Desinfizieren (wenn nicht möglich: Zugriff sperren)** eine empfehlenswerte Möglichkeit, da hier die Verbreitung des Virus unterbunden wird und trotzdem keine Datei auf dem Rechner gelöscht wird. Das direkte Löschen infizierter Dateien wird dagegen nur für die wenigsten Anwender sinnvoll sein. Die Nutzung des Quarantäne-Ordners über die Funktionen **Desinfizieren (wenn nicht möglich: in Quarantäne)** und **Datei in die Quarantäne verschieben** bieten den Vorteil, dass die Dateien im **Quarantäne**-Ordnersicher verwahrt sind, ohne weiteren Schaden anrichten zu können und Sie sich später Gedanken darüber machen können, wie Sie mit den Dateien verfahren möchten.

Infizierte Archive

Legen Sie hier fest, ob die Behandlung von Virenfunden für **Archive** anders als für reguläre Dateien erfolgen soll. Da Viren innerhalb eines Archivs erst Schaden anrichten, wenn Sie entpackt werden, können Sie die Prüfung für Archive unter Umständen auch komplett deaktivieren. Dies bringt bei der Arbeit mit dem Virenwächter gewisse Performance-Verbesserungen mit sich.

Achtung: Sie sollten gerade die Archivdateien großer **E-Mail-Postfächer** nicht löschen oder in die **Quarantäne** verschieben, nur weil sich in diesen eine infizierte Mail befindet. So lange der Virenwächter aktiv ist, können infizierte Mails auch im Postfach keinen Schaden anrichten und bei Bedarf

manuell aus diesem gelöscht werden.

Entfernen Sie das Häkchen bei **Archive prüfen**, um normale Archive von der Kontrolle durch den Wächter auszuschließen. Wenn Sie das Häkchen bei **E-Mail Archive prüfen** entfernen, werden auch E-Mail-Archive nicht mehr vom Wächter überprüft.

Systemschutz und Autostart-Überwachung

Wenn der Systemschutz aktiviert ist, werden bei jedem Systemstart die **Windows-Registry** und die Systemordner überprüft. Auf diese Weise wird die **HOSTS-Datei** vor Manipulationen geschützt.

*Die **HOSTS-Datei** ist eine Textdatei auf Ihrem Rechner, die Hostnamen mit den IP-Adressen abgleicht. Wird diese durch Schadprogramme modifiziert, können Anwender ungewollt z.B. auf Phishing-Websites umgeleitet werden.*

Ausnahmen

Sie können bestimmte Laufwerke, Verzeichnisse und Dateien von der Überprüfung durch den Virenwächter ausschließen und auf diese Weise die Virenerkennung teilweise erheblich beschleunigen. Gehen Sie dazu folgendermaßen vor:

1. Klicken Sie auf den **Ausnahmen**-Button.
2. Klicken Sie in dem **Wächter Ausnahmen**-Fenster 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.
5. Um Dateien zu schützen, geben Sie den kompletten Dateinamen in das Eingabefeld unter **Dateimaske** ein. Sie können hier auch mit Platzhaltern arbeiten (z.B. ? für ein beliebiges Zeichen oder * für eine beliebige Zeichenfolge).
6. Klicken Sie nun auf **OK**.
7. Im **Wächter Ausnahmen**-Fenster klicken Sie ebenfalls auf **OK**.

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

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

Erweitert

Legen Sie hier fest, welche zusätzlichen Virenprüfungen **AntiVirus** durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der Zeitersparnis durch Weglassen dieser Überprüfungen das leicht geringere Maß an Sicherheit aufwiegen.

- **Dateitypen:** Hier können Sie festlegen, welche Dateitypen von **AntiVirus** auf Viren untersucht werden sollen. Der Unterschied zwischen alle Dateien und nur Programmdateien und Dokumente besteht darin, dass bei letzterer Funktion nur Dateien überprüft werden, die eine Dateiendung haben, die auf ausführbare Programme oder Dokumente, die in Programmen ausgeführt werden können, hindeutet.
- **Beim Schreiben prüfen:** Auf diese Weise wird direkt nach dem Erzeugen einer neuen Datei geprüft, ob ein Virus sich in diesen Prozess eingeklinkt hat. Sollte ein Virus hier eingegriffen haben, wird die Aktion durchgeführt, die Sie Im Fall einer Infektion definiert haben.
- **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 Performance auswirkt.
- **Heuristik:** In der heuristischen Analyse werden Viren nicht nur anhand der

ständig aktualisierten Virendatenbanken erkannt, 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 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. Um die Performance durch das unnötige Überprüfen großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail-Archive prüfen:** Da die Software schon den Aus- und Eingang von 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 Mail-Archives teilweise mehrere Minuten dauern kann.
- **Systembereiche beim Systemstart prüfen:** Systembereiche (z.B. **Bootsektoren**) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (z.B. neue CD-ROM). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Systembereiche beim Medium-Wechsel prüfen:** Systembereiche (z.B. Bootsektoren) Ihres Computers sollten in der Regel nicht von der Virenkontrolle ausgeschlossen werden. Sie können hier festlegen, ob Sie diese beim Systemstart überprüfen oder beim Medium-Wechsel (neue CD-ROM o.ä.). Generell sollten Sie zumindest eine dieser beiden Funktionen aktiviert haben.
- **Auf Dialer / Spyware / Adware / Riskware prüfen:** Mit **AntiVirus** können Sie Ihr System auch auf **Dialer** und andere Schadprogramme 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.

Virenprüfung

In diesem Menü können Sie festlegen, wie die Virenprüfung durch die Software zu erfolgen hat. Da eine Virenprüfung auf Basis eines **Zeitplans** oder eines

manuellen Analysebeginns meist zu Zeiten erfolgt, in der der Computer nicht völlig mit anderen Aufgaben ausgelastet ist, können hier in der Regel mehr Systemressourcen für die Virenprüfung verwendet werden, als beim Virenwächter.

Engines benutzen

AntiVirus arbeitet mit zwei Antiviren-Engines, zwei grundsätzlich unabhängig voneinander operierenden Analyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe. Die Verwendung einer einzigen Engine bringt dagegen Performance-Vorteile mit sich, d.h. wenn Sie nur eine Engine verwenden, kann der Analysevorgang schneller erfolgen. In der Regel sollten Sie hier die Einstellung **Beide Engines - performance-optimiert** wählen, da diese die Vorteile einer doppelten Prüfung ohne größere Performance-Einbußen miteinander verbindet.

Im Fall einer Infektion

Hier können Sie festlegen, was bei Entdeckung einer infizierten Datei geschehen soll. Je nach dem, für welche Zwecke Sie Ihren Computer verwenden, sind hier unterschiedliche Einstellungen sinnvoll. Die Nutzung des **Quarantäne**-Ordners über die Funktionen **Desinfizieren (wenn nicht möglich: in Quarantäne)** und **Datei in die Quarantäne verschieben** bieten z.B. den Vorteil, dass die Dateien im **Quarantäne**-Ordner sicher verwahrt sind, ohne weiteren Schaden anrichten zu können und Sie sich später Gedanken darüber machen können, wie Sie mit den Dateien verfahren möchten.

Infizierte Archive

Legen Sie hier fest, ob die Behandlung von Virenfunden für **Archive** anders als für reguläre Dateien erfolgen soll. Da Viren innerhalb eines Archivs erst Schaden anrichten, wenn Sie entpackt werden, können Sie die Prüfung für Archive unter Umständen auch komplett deaktivieren. Wenn Ihr Virenwächter permanent genutzt wird, verhindert dieser eine Infektion, sobald ein infiziertes Archiv entpackt wird. Die Suche nach infizierten Archiven ist also gerade dann sinnvoll, wenn Sie diese Archive an Personen weitergeben wollen, bei denen Sie nicht automatisch erwarten können, dass diese einen Virenschutz installiert haben.

*Generell ist es empfehlenswert, die Überprüfung von Archiven im **Wächter** (der den Rechner kontinuierlich überprüft) abzuschalten und bei einer **Virenprüfung** (die möglichst dann stattfinden sollte, wenn der Rechner nicht*

für andere Zwecke genutzt wird) anzuschalten.

Bei Systemlast die Virenprüfung pausieren

Mit dieser Funktion können Sie interaktiv auf die Auslastung Ihres Rechners reagieren. Sobald er vom Anwender für die Arbeit mit Programmen genutzt wird, wird die systematische Virenprüfung angehalten. Die ständige Hintergrundkontrolle vom Virenwächter wird hierbei natürlich nicht beeinträchtigt. Wenn der Rechner dann nicht benutzt wird, wird die Arbeitspause gezielt dazu genutzt, die systematische Virenprüfung voranzutreiben.

*Wenn Sie diese Funktion aktivieren, ist es natürlich empfehlenswert, unter **Priorität Scanner** die Einstellung **Hoch** zu verwenden. So kann die Virenkontrolle bei der Nichtnutzung des Computers um so schneller erfolgen.*

Erweitert

Legen Sie hier fest, welche zusätzlichen Virenprüfungen **AntiVirus** durchführen soll. Die hier gewählten Optionen sind für sich gesehen durchaus sinnvoll, je nach Anwendungsart kann der Vorteil der **Zeitersparnis** durch Weglassen dieser Überprüfungen das leicht geringere Maß an Sicherheit aufwiegen.

- **Dateitypen:** Hier können Sie festlegen, welche Dateitypen von der Software auf Viren untersucht werden sollen. Der Unterschied zwischen alle Dateien und nur Programmdateien und Dokumente besteht darin, dass bei letzterer Funktion nur Dateien überprüft werden, die eine Dateiendung haben, die auf ausführbare Programme oder Dokumente, die in Programmen ausgeführt werden können, hindeutet.
- **Priorität Scanner:** Über diese Einstellung können Sie bestimmen, wie viele Systemressourcen von **AntiVirus** für eine Virenprüfung genutzt werden sollen. Wenn während der Virenprüfung auf dem Rechner noch gearbeitet werden soll, empfehlen wir die Einstellung **Niedrig (Lange Laufzeit)**. Bei einem momentan nicht benutzten Rechner die Einstellung **Hoch (Kurze Laufzeit)**.
- **Heuristik:** In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken erkannt, sondern auch anhand bestimmter virentypischer Merkmale ermittelt. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch einen Fehllarm erzeugen.

- **Archive prüfen:** Das Überprüfen gepackter Daten in Archiven 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. Um die Performance durch das unnötige Überprüfen großer Archiv-Dateien, die selten verwendet werden, nicht zu belasten, können Sie die Größe der Archivdateien, die durchsucht werden, auf einen bestimmten Wert in Kilobyte begrenzen.
- **E-Mail-Archive prüfen:** Da **AntiVirus** schon den Aus- und Eingang von 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 Mail-Archives teilweise mehrere Minuten dauern kann.
- **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 **AntiVirus** können Sie Ihr System auch auf **Dialer** und andere Schadprogramme 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.
- **Protokoll anfertigen:** Über das Häkchenfeld **Protokoll anfertigen** können Sie festlegen, dass **AntiVirus** über den Virenprüfungsvorgang ein Protokoll anlegt. Dies kann dann im **Protokolle**-Bereich eingesehen werden. Wenn Sie das Häkchen hier nicht setzen, werden weiterhin nur automatische Vorgänge (automatische Virenprüfung, automatisches Update, Virenfund durch Virenwächter) im Protokoll eingetragen.

Weitere Informationen zum **Protokolle**-Bereich erhalten Sie unter **AntiVirus > Protokolle**.

Rootkits, die schon vor der Installation der Antivirensoftware auf den Rechner gelangt sind, sind in dieser Form nur schwer zu entdecken. Sollten Sie den Verdacht haben, dass Ihr Rechner ohne adäquaten Virenschutz benutzt wurde, empfehlen wir einen BootScan, der die Schadsoftware schon vor dem

Start des Betriebssystems ermitteln und bekämpfen kann. Lesen Sie hierzu bitte das Kapitel **Anhang > Fragen und Antworten (FAQ) > BootScan.**

Internet-Update

Geben Sie hier die Zugangsdaten (Benutzername und Passwort) ein, die Sie bei der Anmeldung von **AntiVirus** erhalten haben. Mit Hilfe dieser Daten werden Sie vom **G DATA UpdateServer** erkannt und das Update der Virensignaturen kann vollautomatisch erfolgen.

*Generell geben Sie die Zugangsdaten gleich beim ersten Start von **AntiVirus** ein und die Software merkt sich diese Einstellungen. Im Bereich "Internet-Update" müssen Sie eigentlich nur Änderungen vornehmen, wenn Sie die Software nach einer Deinstallation erneut installieren oder sich die Einstellungen Ihres Internet-Zugangs verändert haben.*

Am Server anmelden

Wenn Sie noch keine Anmeldung am Server durchgeführt haben, können Sie diese jetzt nachholen, indem Sie auf den Button **Am Server anmelden** klicken. Es erscheint ein Eingabefenster, in dem Sie ihre **Registriernummer** und **Kundendaten** eingeben.

*Sollte **AntiVirus** keine Verbindung mit dem Internet aufnehmen können, klicken Sie bitte auf den **Erweitert**-Button und nehmen die notwendigen Internet-Einstellungen vor. In der Regel kann die G DATA Software dann Kontakt mit dem Internet aufnehmen, wenn Ihr Systembrowser, also z.B. der **Internet Explorer** Zugang zum Internet hat.*

*Die **Registriernummer** finden Sie auf der Rückseite des gedruckten Bedienungshandbuchs. Wenn Sie die Software online gekauft haben, erhalten Sie die Registriernummer in einer gesonderten E-Mail.*

Klicken Sie nun auf den **Anmelden**-Button und Ihre Zugangsdaten werden auf dem **G DATA UpdateServer** generiert. Wenn die Anmeldung erfolgreich verlief, erscheint ein Info-Bildschirm mit dem Vermerk **Die Anmeldung wurde erfolgreich durchgeführt**, den Sie mit dem Schließen-Button verlassen können.

Achtung: Für Ihre Unterlagen und für etwaige Neuinstallationen der Software erhalten Sie Ihre **Zugangsdaten** auch per **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 durch Anklicken des **OK**-Buttons den eigentlichen Update-Vorgang starten.

Sie können das **Update** auch jederzeit nachträglich durchführen.

Internet-Einstellungen

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

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

Weitere Informationen zu einem automatisierten zeitplangesteuerten Internet-Update erhalten Sie im Kapitel **AntiVirus > Zeitplan > Automatische Updates**.

Versionsprüfung

Die Versionsprüfung sollten Sie nur dann deaktivieren, wenn es Probleme mit den Virensignaturen gibt (z.B. weil Sie versehentlich hier Dateien gelöscht haben). Bei ausgeschalteter Versionsprüfung dauert das Update etwas länger,

weil für alle Dateien eine Prüfsumme berechnet wird und diese mit der Prüfsumme auf dem Server verglichen wird.

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. **AntiVirus** ist in der Lage, bei Virenfund **Datei-Anhänge** direkt zu löschen oder infizierte Dateien zu reparieren.

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

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 auf Viren prüfen

Mit Aktivierung dieser Option werden sämtliche E-Mails auf Viren überprüft, die Sie während Ihrer Arbeit am Computer erreichen.

Ungelesene Mails beim Programmstart prüfen

Nur für Microsoft Outlook: Diese Option dient dazu, E-Mails auf Virenbefall zu kontrollieren, die Sie erreichen, während Sie nicht mit dem Internet verbunden sind. Sobald Sie Outlook starten, werden deshalb sämtliche ungelesenen Mails im Posteingang-Ordner und den darin enthaltenen Unterordnern von **AntiVirus** kontrolliert.

Bericht an empfangene, infizierte Mails anhängen

Wenn Sie die Berichtsoption 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.

Mails vor dem Senden prüfen

Damit Sie nicht versehentlich selber Viren verschicken, bietet **AntiVirus** 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.

Bericht an ausgehende Mails anhängen

Ein Prüfbericht wird bei jeder ausgehenden E-Mail unter dem eigentlichen Mailtext angezeigt. Sie können hier außerdem festlegen, ob dieser Bericht Informationen über die verwendete **AntiVirus Version (Versionsinformation)** und einen Internet-Link zum **AntiVirusLab** enthält (**Virus News**), in dem Anwender online ständig aktualisierte Informationen über Viren erhalten können. Ein kompletter Bericht würde also in etwa folgendermaßen aussehen:

Virus checked by G DATA AntiVirus

Version: GDAV 15.0.37 from 06.10.2008

Virus news: www.antiviruslab.com

Engines benutzen

AntiVirus arbeitet mit zwei **Antiviren-Engines**, zwei grundsätzlich unabhängig voneinander operierenden Analyseeinheiten. Prinzipiell ist die Verwendung beider Engines der Garant für optimale Ergebnisse bei der Virenprophylaxe.

OutbreakShield

Hiermit aktivieren Sie das OutbreakShield. **AntiVirus** erstellt bei aktiviertem OutbreakShield Prüfsummen von Mails, gleicht diese im Internet mit stets aktualisierten **Anti-Spam-Blacklists** ab und ist dadurch in der Lage, auf ein Massenmailing zu reagieren, bevor entsprechende Virensignaturen zur

Verfügung stehen. Das **OutbreakShield** erfragt dabei über das Internet besondere Häufungen von verdächtigen Mails und schließt dabei quasi in Echtzeit die Lücke, die zwischen dem Beginn eines Massenmailings und seiner Bekämpfung durch speziell angepasste Virensignaturen besteht. Das **OutbreakShield** ist in den E-Mail-Virenblocker integriert.

*Falls Sie einen Rechner hinter einer **Firewall** verwenden oder andere besondere Einstellungen bezüglich Ihres Internetzugangs haben, verwenden Sie bitte einen **Proxyserver**. Klicken Sie dazu auf den Button **Internet-Einstellungen** und nehmen die entsprechenden Änderungen vor. Sie sollten diese Einstellung nur ändern, wenn das **OutbreakShield** nicht funktioniert. Wenden Sie sich wegen der Proxy-Adresse gegebenenfalls an Ihren Systemadministrator oder Internetzugangsanbieter.*

Erweitert

AntiVirus schützt nach der Installation automatisch auch Ihre E-Mails. Dazu verwendet es für **Microsoft Outlook** ein spezielles PlugIn und für **POP3/IMAP basierte E-Mail-Programme** (wie z.B. **Outlook Express**, **Thunderbird**, **Pegasus**, **Opera** etc.) einen speziellen Client, der die Mails überprüft, bevor Sie von Ihrem E-Mail-Programm empfangen bzw. versendet werden.

Durch Entfernen der jeweiligen Häkchens können Sie den Schutz für **eingehende Mails (POP3/IMAP)** und **ausgehende Mails (SMTP)** auch abschalten.

Da **AntiVirus** 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 **AntiVirus** auf Viren überprüft werden. Mit Aktivieren des Häkchenfeldes bei **Zeitüberschreitung beim Mail-Client vermeiden** wird eine solche Fehlermeldung des Mailprogramms unterdrückt und sobald sämtliche Maildaten auf Viren überprüft wurden, werden diese von **AntiVirus** dann ganz normal an das Mailprogramm überreicht.

*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 des **Standard**-Buttons können Sie automatisch die Standardportnummern*

wiederherstellen.

Sie können auch **mehrere Ports** eintragen. Trennen Sie diese jeweils durch ein Komma.

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

Web / IM

In diesem Bereich können Sie grundlegende Einstellungen für den Umgang von **AntiVirus** mit Webinhalten und Messaging-Diensten einstellen.

Internetinhalte (HTTP)

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

Wenn Sie die Internetinhalte nicht prüfen lassen wollen, greift natürlich der Virenwächter dann ein, wenn infizierte Dateien zur Ausführung geraten. Ihr System ist also auch ohne die Überprüfung von Internetinhalten geschützt, solange der **Virenwächter** aktiviert ist. Sollten Sie **AntiVirus** jedoch zusammen mit dem Modul **Kindersicherung** und dem Modul **Webfilter** verwenden wollen (z.B. im Rahmen des **G DATA InternetSecurity Pakets**), muss das Häkchen bei **Internetinhalte (HTTP) verarbeiten** gesetzt sein, da sonst die **Kindersicherung** und der **Webfilter** nicht korrekt funktionieren.

Da **AntiVirus** die Web-Inhalte vor Ihrer Darstellung im Internet Browser bearbeitet und dafür je nach Datenaufkommen eine gewisse Zeit benötigt, kann es vorkommen, dass eine Fehlermeldung im Internet Browser erscheint, weil dieser nicht sofort die Daten zugestellt bekommt, da diese ja von **AntiVirus** auf

Schadroutinen überprüft werden. Mit Aktivieren des Häkchenfeldes **Zeitüberschreitung im Browser vermeiden** wird eine solche Fehlermeldung unterdrückt und sobald sämtliche Browserdaten auf Viren überprüft wurden, werden diese von **AntiVirus** dann ganz normal an den Internetbrowser überreicht. Mit der **Größenbegrenzung für Downloads** können Sie die HTTP-Überprüfung für zu große Webinhalte unterbrechen. 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.

Inhalte, die wegen Ihrer Größe nicht VOR Ihrer Anzeige im Browser auf Viren und Schadprogramme überprüft werden, werden vom Virenwächter natürlich spätestens dann erkannt und geblockt, wenn sie Schadroutinen ausführen möchten.

Instant Messaging

Da auch über Instant Messaging-Tools Viren und andere Schadprogramme verbreitet werden können, kann **AntiVirus** auch hier die Anzeige und den Download infizierter Daten im Vorfeld unterbinden. Sollten Ihre Instant Messaging-Anwendungen nicht über die Standardportnummern ablaufen, geben Sie bitte unter **Serverportnummer(n)**, die entsprechenden **Port-Adressen** ein.

Instant Messaging (Integration in der IM-Anwendung)

Sollten Sie **AOL AIM (ab Version 4.7)**, den **Microsoft Messenger (ab Version 4.7)** oder **Trillian (ab Version 3.0)** verwenden, können Sie durch Setzen des Häkchens für das jeweilige Programm ein Kontextmenü definieren, in dem Sie verdächtige Dateien direkt auf Viren überprüfen können.

Anhang

Lizenzvereinbarung

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

1. Gegenstand des Vertrages: Gegenstand des Vertrages ist das auf einem Datenträger aufgezeichnete oder aus dem Internet geladene **G DATA AntiVirus** und die Programmbeschreibung. Sie werden im Folgenden auch als **Software** bezeichnet. **G DATA** macht darauf aufmerksam, dass es nach dem Stand der Technik nicht möglich ist, Software so zu erstellen, dass sie in allen Anwendungen und Kombinationen fehlerfrei arbeitet.

2. Umfang der Benutzung: **G DATA** gewährt Ihnen für die Dauer dieses Vertrages das einfache, nicht ausschließliche und persönliche Recht (im Folgenden auch als **Lizenz** bezeichnet), die Software auf einer vertraglich vereinbarten Anzahl von Computern zu benutzen. Die Nutzung der Software kann sowohl in Form einer Installation auf einer physikalischen Einheit (CPU), einer virtuellen / emulierten Maschine (wie z.B. VMWare) oder einer Instanz einer Terminal Session erfolgen. Ist dieser Computer ein Mehrbenutzersystem, so gilt dieses Benutzungsrecht für alle Benutzer dieses einen Systems. Als Lizenznehmer dürfen Sie Software in körperlicher Form (d.h. auf einem Datenträger abgespeichert) von einem Computer auf einen anderen Computer übertragen, vorausgesetzt, dass sie zu irgendeinem Zeitpunkt immer nur auf der vertraglich vereinbarten Anzahl von Computern genutzt wird. Eine weitergehende Nutzung ist nicht zulässig.

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

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

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

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

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

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

9. Gewährleistung & Haftung von G DATA:

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

b) Sollte der Datenträger oder der Download aus dem Internet fehlerhaft sein, so kann der Erwerber Ersatzlieferung während der Gewährleistungszeit von 6 Monaten ab Lieferung verlangen. Er muss dazu den Erwerb der Software belegen.

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

von im Sinne von 1. brauchbarer Software mit angemessenem Aufwand nicht möglich ist.

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

10. Gerichtsstand: Alleiniger Gerichtsstand bei allen aus dem Vertragsverhältnis mittelbar oder unmittelbar sich ergebenden Streitigkeiten ist der Firmensitz von **G DATA**.

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

Virengeschichte

Viele **Meilensteine** in der Entwicklung von Viren, Würmern und Trojanern finden Sie in der folgenden Übersicht:

1961: Die Anfänge der Computerviren lassen sich bis 1961 zurückverfolgen. Zu dieser Zeit entwickelten Victor A. Vyssotsky, Robert Morris Sr. und M. Douglas McIlroy auf einem IBM 7090 ein Spiel namens **Darwin**, in dem es darum ging, dass sich selbstgeschriebene Programme auf einem Computer den Speicherplatz streitig machen und gegenseitig löschen. In diesem Zusammenhang wurden auch Programmversionen entwickelt, die sich selber vervielfältigen konnten und hier liegen die eigentlichen Wurzeln der Computerviren. In den 1980er Jahren waren Varianten dieses Spieles als **Core War** unter Programmieren sehr beliebt.

1981: Professor Leonard M. Adleman verwendet im Gespräch mit seinem Doktoranden Fred Cohen zum ersten Mal den Begriff **Computervirus**.

1982: Selbstgeschriebene Bootsektorviren für **Apple II Rechner** werden innerhalb eines kleinen Kreises interessierter Programmierer per Diskette ausgetauscht. Der Virus **Elk Cloner** plagt als erster **in the wild**-Virus Apple-Nutzer mit Schüttelreimen, invertierten oder falschen Anzeigen und Klickgeräuschen. Er verbreitete sich über Disketten. Als **In the wild** werden Viren bezeichnet, wenn sie sich tatsächlich unkontrolliert von Rechner zu

Rechner verbreiten. Neben *in the wild*-Viren gibt es in Forschungslabors und auf Rechnern von Antivirenspezialisten auch Schadsoftware, die zu Testzwecken entwickelt, aber nie weiterverbreitet wurde.

1983: Im November präsentiert Fred Cohen in einem Seminar das Konzept eines erste funktionsfähigen Virus unter UNIX.

1984: Fred Cohen veröffentlicht erste Artikel über *Experimente mit Computerviren*, die in seine 1986 erschienene Doktorarbeit *Computer Viruses - Theory and Experiments* einfließen. Seine eher mathematisch ausgerichtete Definition eines Virus ist heute noch anerkannt und umfasst nicht den negativen Beiklang, den der Begriff Virus heute bekommen hat.

1985: Weitere Viren in freier Wildbahn lassen nicht lange auf sich warten. Oft sind es eher Scherzprogramme, die den Computernutzer nur belästigen. Richtig bösartig ist das Trojanische Pferd *Gotcha*. Nach dem Start des Programms werden die Daten auf der Festplatte gelöscht und auf dem Bildschirm steht *Arf, arf, Gotcha*.

1986: Die Brüder Basit und Amjad Farooq Alvi betreiben ein kleines Computergeschäft namens *Brain Computer Services* in Lahore, Pakistan. Um das illegale Kopieren ihrer Software zu bestrafen, schufen sie einen *Bootsektorvirus* für das Betriebssystem *DOS*. Über pakistanische Studenten verbreitete sich der Virus auch an amerikanischen Hochschulen wie eine Epidemie. Mit *Virdem* wurde der erste *Datei-Virus* freigesetzt und *PC-Write* war das erste *Trojanische Pferd*, das sich auf Basis eines Shareware-Programmes verbreitete. Viren gerieten durch *Pakistani-Brain* in das öffentliche Interesse. John McAfee und weitere Computerspezialisten gründeten erste AntiViren-Firmen.

1987: Immer häufiger erscheinen jetzt Viren, die Dateien befallen. Mit *Lehigh* rückt erstmals ein Virus in das öffentliche Interesse. Lehigh befällt die *command.com* und nach vier Kopien auf Disketten werden die Daten auf allen im Computer befindlichen Datenträgern gelöscht. Diese radikale Aktion führt allerdings auch zu seiner schnellen Ausrottung. Im Zusammenhang mit *Lehigh* wird die *VIRUS-L/comp.virus-Mailingliste und -Newsgroup* gegründet und wird zu einer wichtigen Informationsquelle im Kampf gegen Viren. Der *Cascade-Virus* ist der erste verschlüsselte Virus. Der erste Virus für *Amiga* befällt den Bootsektor und gibt ab und an eine Meldung aus. Im Dezember legte ein wohlmeinender amerikanischer Student mit dem ersten Computer-Wurm weltweit den Mailverkehr und die Netzwerke lahm. Der *Tannenbaum*-Wurm zeichnet einen Tannenbaum auf den Bildschirm, während er sich im Hintergrund an alle Mailadressen, die er auf dem System finden kann verschickt.

1988: Die wachsende Vernetzung von Computern wird 1988 erstmals von einem

neuartigen Schädling ausgenutzt: Dem **Wurm**. Würmer nutzen bis heute Schwachstellen in Netzwerken aus. In dieser Zeit organisierten sich sowohl die Virenautoren als auch die Antiviren-Spezialisten. Antivirensoftware etablierte sich. Der **MacMag Virus** war der erste für **Macintosh** Rechner und hatte eine Reihe weiterer Innovationen zu bieten. Er war der erste Virus, der auf Bestellung (von Chefredakteur des MacMag) entwickelt wurde. Er war auch der erste Virus, der Datendateien befahl, um sich zu verbreiten. Am Freitag dem 13. Mai platzt in Jerusalem zum ersten Mal eine **logische Bombe** (in diesem Fall eine Zeitbombe). Damit war eine neue Virengattung begründet. Robert T. Morris jr. - der Sohn des Computer-Sicherheitsexperten der NSA - setzt einen **Internet Wurm** frei, der sich mit einer kleinen Passwortliste Zugang zu zahlreichen UNIX-Rechnern verschaffte und sich dann wie der Tannenbaum-Virus weiter versendet, was wiederum den Zusammenbruch der Netzwerke und des Mailverkehrs zur Folge hat. Der **Internet-Wurm** wie er genannt wurde, konnte nur noch durch telefonische Absprachen bekämpft und zur Strecke gebracht werden. Als Reaktion auf die allgemein erhöhte Aktivität der Virenentwickler und speziell den **Internet-Wurm** wurde in den USA das **Computer Emergency Response Team/Coordination Center (CERT/CC)** gegründet. Es bietet bis heute Rat und Tat rund um den Datenschutz und die Datensicherheit.

1989: Der Virus **DataCrime** verursacht einen riesigen Medienrummel. Mit **Vienna (V2Px)** von Mark Washburn erscheinen erste **polymorphe Viren**. Er verschlüsselt sich selbst mit variablen Schlüsseln und ändert auch die Form der Entschlüsselungsroutinen. Er ist deshalb durch AntiViren-Software nur mit komplexen Algorithmen aufzuspüren, die zudem zu Fehlalarmen neigten. Das war das Aus für viele Antivirensoftware-Hersteller. Im Juli erscheint die erste Ausgabe des **Virus Bulletin**. Seither entwickelte es sich zum renommiertesten Fachmagazin für Virenforscher. In Bulgarien führt **Dark Avenger** zwei Neuheiten ein: 1. Mit dem **Fast Infector** werden nicht nur ausführbare Dateien, sondern auch zum Lesen geöffnete und kopierte Dateien befallen. So ist nach kurzer Zeit die gesamte Festplatte befallen. 2. In unregelmäßigen Abständen werden einzelne Sektoren der Festplatte überschrieben. Das bleibt in den meisten Fällen unbemerkt. **Backups**, die häufig zum Schutz vor Virenbefall angelegt wurden, sind damit wirkungslos. Ein Trojaner wird von der Firma **PC Cyborg** mit Sitz in Panama auf Disketten verteilt, die als AIDS-Information getarnt sind. AIDS ersetzte die autoexec.bat und fing nach einer bestimmten Zahl (90) von Neustarts an die Festplatte zu verschlüsseln. Danach wurde man mit einer Rechnung für den Entschlüsselungscode konfrontiert.

1990: Viren züchten wird jetzt Mode. In **VX (Virus Exchange) Bulletin Boards** werden alte und neue Viren ausgetauscht. **4096 Bytes** ist die Größe des gleichnamigen Virus, der im Januar erscheint. Er hängt sich an ausführbare und geöffnete Datendateien an. Der Mechanismus, der das zu verbergen versuchte

fürhte oft dazu, dass Dateien zerstört wurden. Der Versuch die Nachricht **Frode Lives** anzuzeigen, führte zu einem Systemabsturz. Der Verband deutscher Virenliebhaber verbreitet das erste **Virus Construction Kit für DOS**. Damit ist es auch Anfängern möglich, Viren nach Maß zu erstellen. Im Dezember wird das **European Institute for Computer Antivirus Research** (kurz **EICAR**) gegründet. Es spielt bis heute eine wichtige Rolle im Kampf gegen Viren und Virenautoren.

1991: **Michelangelo** ist ein Bootsektor-Virus, der am 6. März - dem Geburtstag Michelangelos - die ersten 256 Sektoren des Datenträgers überschreibt. Damit wird der Rechner unbrauchbar. Im darauffolgenden Jahr wird Michelangelo in den Medien breit getreten, was sicher etlichen Schaden verhindert hat. Er ist trotzdem noch lange Jahre aktiv. **Polymorphe Viren** werden jetzt immer häufiger. **Tequila** ist der erste weit verbreitete polymorphe Virus. **Maltese Amoeba** überschreibt an zwei bestimmten Tagen des Jahres den ersten Sektor des Datenträgers. Robert Slade beginnt seine Reihe mit Computer-Viren-Tutorials. Kurz darauf beginnt er mit den Arbeiten am **VIRUS-L-FAQ**. Der **Saddam-Hussein**-Virus verschlüsselt auf Amiga-Rechnern Teile des Datenträgers, so dass diese nur noch gelesen werden können, wenn der Virus im Speicher ist.

1992: Der **Commodore Amiga** und der **Atari ST** verlieren ihre Bedeutung und **MS-DOS** setzt sich immer mehr durch. Entsprechend steigt die Anzahl der **DOS-Viren**. **Altair** für Atari ST gibt sich als Antivirensoftware aus. Er überschreibt alle Viren, die er im Bootsektor findet. Er scheitert wie viele andere **Antiviren-Viren**. Ein Virenautor, der sich **Dark Avenger** nennt, veröffentlicht die **Self Mutating Engine (MtE)**. Damit lassen sich aus normalen Viren mit wenig Aufwand polymorphe Viren erzeugen. **MtE** ist damit das erste **Toolkit** zur Erzeugung von polymorphen Viren. Ebenfalls von Dark Avenger stammt **Commander Bomber**, der einen neuen Tarnmechanismus verwendet. Er befällt COM-Dateien, hängt sich aber nicht in einem Block an die Datei, sondern verteilt seinen Code auf mehrere Fragmente, die untereinander durch Links verbunden sind. Um ihn zu erkennen, muss die gesamte Datei gescannt werden.

1993: Neue Toolkits zur Erzeugung von polymorphen Viren erscheinen: **Trident Polymorphic Engine (TPE)**, **Nuke Encryption Device (NED)** und **Dark Angel's Multiple Encryption (DAME)** bauen auf der MtE auf. **Virensignaturen** werden aber weiterhin verwendet. In MS-DOS 6 ist erstmal ein (mittelmäßiger) Virens Scanner enthalten. Der Amiga-Virus **Fuck**, der durch einen als Modem-Testprogramm getarnten Trojaner verbreitet wurde, ersetzte zunächst die Systemdatei loadWB. Nach einem Neustart des Rechners wurde der Virencode ausgeführt: Nach einer bestimmten Zeit, die durch die Bildwiederholfrequenz festgelegt war, wurde die gesamte Festplatte mit dem

bösen F-Wort voll geschrieben, was zur Zerstörung aller Daten führte. Joe Wells veröffentlicht die erste **Wildlist**. Er möchte damit die Aktivitäten von Viren auflisten, die im Umlauf sind. Aus dieser Liste ist später die **Wildlist Organization** entstanden. Erste Computerviren für **Windows** tauchen auf.

1994: Die ersten **Multipartite Viren** tauchen auf. Diese Viren nutzen mehrere Infektionsmechanismen und können gleichzeitig neben Dateien auch Bootsektoren bzw. Partitionstabellen befallen. Black Baron veröffentlicht **Smeg.Pathogen** (und **Smeg.Queen**). Smeg.Pathogen zeigt eine Meldung an und überschreibt anschließend die ersten 256 Sektoren der Festplatte. Das hat in einigen Firmen zu erheblichen Schäden geführt. Er wurde im darauf folgenden Jahr zu einer Gefängnisstrafe verurteilt. **Kaos4** verbreitete sich über eine **Newsgroup**, die auf Erotikbilder spezialisiert war. Diese Strategie wurde seitdem häufiger angewandt. **Virus Hoaxes** (= Warnungen vor Viren oder anderen Schadprogrammen, die gar nicht existieren) werden mit den **Good-Times**-Warnungen zu einem ernsthaften aber verkannten Problem.

1995: 1995 tauchen mit **DMV** und **Nachtwächter** die ersten **Makroviren** auf. Bis dahin wurden nur ausführbare Dateien und Bootsektoren befallen. **Melissa**, **Loveletter**, **Sobig** und Konsorten stellen immer wieder neue Geschwindigkeitsrekorde bei der Verbreitung auf. **Concept 1995** war der erste Makrovirus der öffentlich ausbrach und sich ungehindert in englischen Systemen verbreitete. Mit **Hunter.c** erscheint der erste polymorphe Makrovirus in Deutschland. **Wm.Concept** war der erste **in the wild** Makrovirus. Er enthielt nur die Meldung **That's enough to prove a point** (etwa: **das reicht als Beweis**) und war kurze Zeit später der weltweit verbreitetste Virus. Wm.Concept begründete die Gattung der **Proof of Concept**-Viren. PoC-Viren zeigen nur, dass es möglich ist eine bestimmte Schwachstelle auszunutzen, ohne wirklich Schaden anzurichten. Die Erkennung von Makroviren stellt hohe Anforderungen an die Virens Scanner, nicht zuletzt wegen der ständig wechselnden Formate von Scriptsprachen und Office-Dateien.

1996: Es erscheinen erste **Makro-Generatoren** für deutsche oder englische Makroviren. Makroviren beschränken sich nicht länger auf **Word**, sondern zielen auch auf **Excel** und **AmiPro** Dateien ab. Sie überspringen auch die Grenzen zwischen Betriebssystemen und befallen sowohl PCs als auch Macs. **Laroux** infiziert als erster MS-Excel-Dateien. **Boza** befällt als erster Virus das PE-EXE-Format von Windows 95-Dateien.

1997: Viren werden jetzt immer spezieller und greifen gezielt Schwachstellen in Programmen, Betriebssystemen oder Hardware an. Das erste Virus für das Betriebssystem **Linux** taucht auf.

1998: **Strange Brew** ist der erste Virus für **Java**. Abgesehen von Makroviren

waren PCs mit **MacOS** seit mindestens drei Jahren nicht von Viren geplagt. Mit dem Wurm **Autostart.9805** ändert sich das. Autostart nutzt den Quicktime AutoStart Mechanismus auf PowerPCs und kopiert sich auf Festplatten und andere Datenträger. Bestimmte Dateien werden mit Datenmüll überschrieben und damit unbrauchbar gemacht. AutoStart verbreitet sich von HongKong über die ganze Welt. **CIH (Spacefiller, Chernobyl)** hat eine der massivsten **Payloads** (= Schadteil eines Virus). Er belebt die Frage, ob Viren in der Lage sind, Hardware zu zerstören. Wenn seine Schadensfunktion (am 26. eines Monats) aktiv wird, überschreibt er das **Flash-BIOS** und die Partitionstabelle der Festplatte. Damit lässt sich der Rechner nicht mehr booten. Auf einigen Motherboards mussten die BIOS-Bausteine ausgetauscht oder neu programmiert werden. Aber selbst nach der Wiederherstellung des Systems waren die Daten verloren.

1999: Im Zusammenhang mit **Back Orifice** wird diskutiert, ob es eine Fernwartungs- oder eine Fernsteuerungs-Software ist. Da die Fernsteuerungs-Funktionen ohne Wissen des Nutzers ausgeführt werden können, ist Back Orifice als **Trojaner** zu bezeichnen. Mit Back Orifice gelingt einem Angreifer Mitte 2000 ein Einbruch ins interne Firmennetz von Microsoft. Im März befällt der Wurm **Melissa** bereits am ersten Tag seines Erscheinens zigtausende Computer und verbreitet sich in Windeseile weltweit. Er versendet E-Mails an die ersten 50 Adressen im Adressbuch und die befallenen Rechner brechen unter der Last eingehender E-Mails zusammen. **Happy99** erzeugt von jeder vom Nutzer versendeten Mail eine Kopie und verschickt sie erneut mit dem gleichen Text und der gleichen Betreffzeile plus dem Wurm im Datei-Anhang. Das funktioniert auch bei **Usenet**-Postings. Abgesehen von E-Mail verbreitet sich **PrettyPark** auch über **Internet Relay Chats (IRC)**. Er hat sehr effektive Schutz- und Tarnmechanismen, die verhindern, dass der Wurm gelöscht werden kann. Beim nächsten Virenskan wird der Wurm als legitim erkannt. Manchmal werden Virenskan auch blockiert. Für Nutzer von Outlook wird mit **Bubbleboy** die **Good-Times** Vision wahr, dass ein Virus den Rechner allein schon dadurch infiziert, dass man eine E-Mail liest. **ExploreZip** tarnt sich als sich selbst entpackendes Archiv, das als Antwort auf eine eingegangene E-Mail gesendet wird. Er verbreitet sich über Netzwerkfreigaben und kann einen Rechner auch dann infizieren, wenn ein anderer Nutzer unvorsichtig ist. Die Schadensfunktion durchsucht die Festplatte nach C und C++ Programmen, Excel-, Word- und Powerpoint-Dateien und löscht sie.

2000: Trotz aller Prophezeiungen gibt es keinen **Millenium-Wurm**, der diesen Namen verdient hätte. **Palm/Phage** und **Palm/Liberty-A** sind zwar selten aber durchaus in der Lage **PDAs** mit **PalmOS** zu befallen. Der **VB-Script-Wurm VBS/KAKworm** nutzt eine Schwachstelle in Scriptlets und Typelibs des Internet Explorers. Ähnlich wie **Bubbleboy** verbreitete er sich beim Öffnen einer

E-Mail (auch in der Voransicht). Im Mai versendet ein Wurm lawinenartig E-Mails aus dem Outlook-Adressbuch mit der Betreffzeile ***I love you*** und richtet vor allem in großen Unternehmens-Netzen Milliarden Schäden an. Auch hier sind die Netze binnen Kurzem völlig überlastet. Von der Urfassung eines philippinischen Studenten namens Onel de Guzman werden zahlreiche Varianten abgeleitet. US-Experten sprechen vom bösartigsten Virus der Computergeschichte. Nach dem ***Loveletter*** und seinen vielen Varianten wurden an den MailGateways einfach die Mails mit den entsprechenden Betreffzeilen herausgefiltert. ***Stages of Life*** variierte die Betreffzeile und schlüpfte so durch die Maschen. Der Autor von ***W95/MTX*** hat sich alle Mühe gegeben, um den Wurm/Virus-Hybriden vom Rechner zu entfernen. Er versendete eine PIF Datei mit doppelter Dateieindung per E-Mail. Er sperrt den Zugriff des Browsers auf einige Websites von Antiviren-Herstellern, versucht Dateien mit der Viruskomponente und einige Dateien werden durch die Wurmkomponente ersetzt.

2001: CodeRed nutzt einen **Buffer Overflow**-Fehler in der **Internet Information Server (IIS) Indexing Service DLL** von Windows NT, 2000 und XP. Er scant zufällig IP Adressen auf dem Standardport für Internetverbindungen und überträgt einen Trojaner, der zwischen dem 20. und 27. eines Monats eine **Denial of Service (DoS) Attacke** gegen die Webseite des Weißen Hauses startet. Die Entfernung des Virus ist sehr aufwändig und verschlingt Milliarden.

2002: Der Wurm **MyParty** zeigt Anfang des Jahres, dass nicht alles, was mit **.com** endet eine Webseite ist. Wer den Mailanhang **www.myparty.yahoo.com** doppelklickt bekommt anstelle der erwarteten Bilder einen Wurm mit Backdoor-Komponente. Im Frühjahr und Sommer nutzt **Klez** die IFRAME-Sicherheitslücke im Internet Explorer um sich automatisch beim Betrachten einer Mail zu installieren. Er verbreitet sich per E-Mail und Netzwerk und hängt sich an ausführbare Dateien. Am 13. von geraden Monaten (in späteren Versionen waren es andere Tage) werden alle Dateien auf allen erreichbaren Laufwerken mit zufälligen Inhalten überschrieben. Die Inhalte lassen sich nur durch Backups wiederherstellen. Im Mai verbreitet sich **Benjamin** als erster Wurm über das **KaZaA-Netzwerk**. Er kopiert sich unter vielen verschiedenen Namen in einen Netzwerkordner. Auf infizierten Rechnern wird eine Webseite mit Werbung angezeigt. Zuvor waren auch **Gnutella** basierte **P2P Netzwerke** befallen. **Lentin** ist ein Wurm, der es ausnutzt, dass viele Leute nicht wissen, dass **SCR-Dateien** nicht nur einfache Bildschirmschoner, sondern auch ausführbare Dateien sind. Verglichen mit Klez ist sein Videoeffekt als Schadensfunktion nur störend. Auch seine Verbreitung erreicht nicht die von Klez. Ende September verbreitet sich **Opasoft** (auch **Brazil** genannt) wie eine Epidemie. Auf Port 137 scant er Rechner im Netzwerk und prüft, ob es dort Datei- und/oder Drucker-Freigaben gibt. Dann versucht er sich auf den Rechner

zu kopieren. Wenn es einen Passwortschutz gibt, wird eine Liste mit Passwörtern durchlaufen und eine Schwachstelle in der Speicherung von Passwörtern ausnutzt. **Tanatos** alias **BugBear** ist der erste Wurm, der Klez seit dem Frühjahr von seinem Spitzenplatz verdrängt. Der Wurm verbreitet sich per E-Mail und Netzwerk, installiert eine **Spyware-Komponente** und versendet Aufzeichnungen der Tastaturanschläge.

2003: Im Januar legt **W32/SQL-Slammer** für Stunden das Internet lahm, weil er eine Schwachstelle im **Microsoft SQL-Server** ausnutzt, um Datenbankinhalte zu versenden. Der Massenmailwurm **Sobig.F** stellt mit seiner eigenen Mailengine einen neuen Rekord für die Verbreitungsgeschwindigkeit auf. Er verbreitet sich zehn Mal schneller als bisherige Würmer.

2004: **Rugrat** ist der erste Virus für 64-bit Windows. Cabir, der erste Virus für **Mobiltelefone** mit **Symbian** Betriebssystem und **Bluetooth** Schnittstelle wird von der für ihre Proof-of-Concept-Viren bekannte Gruppe **29A** entwickelt. Kurz darauf folgt von der gleichen Gruppe mit **WinCE4Dust.A** der erste **PoC-Virus** für **Windows CE**.

2005: Als erster Wurm für **Symbian Smartphones** verbreitet sich **CommWarrior.A** per **MMS**. Die MMS-Nachrichten werden von variablen begleitenden Texten als Antivirensoftware, Spiele, Treiber, Emulatoren, 3D Software oder interessante Bilder dargestellt und an alle Einträge des Telefonbuchs versendet.

2006: In diesem Jahr versucht der Schallplattenkonzern Sony BMG mit einer Installation von **Rootkit-Software** auf seinen Audio-CDs, ein Kopieren dieser CDs zu verhindern. Abgesehen von der Diskussion über Sinn, Zweck und Imageschaden dieser Aktion rückt das RootKit in den Focus der Virenentwickler und immer mehr RootKits mit Backdoor-, Trojaner- und Schadfunktionen überschwemmen den Markt. Einmal installierte Rootkits sind selbst für moderne Antivirenprogramme schwer zu erkennen.

2007: Neben **Phishing**- und **Pharming**-Attacken, bei denen versucht wird, Anwendern sensible Informationen (wie z.B. **Onlinebanking-Daten**) zu entlocken, werden die Schreiber von Schadsoftware auch in anderer Hinsicht zunehmend geschäftstüchtig. Über **BotNetze** werden viele Computer argloser Anwender ferngesteuert (Stichwort: **Zombie-PC**) und für Spam-Mails oder gezielte Attacken auf die Internet-Infrastruktur verwendet.

Virenkategorien

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

Trojaner

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

Gemeinsamkeiten von Viren und Würmern

Viren und Würmer sind aus folgenden Teilen aufgebaut:

Reproduktionsteil

Mit diesem Programmteil wird die Vermehrung des Virus durchgeführt. Dieser Teil ist obligatorisch für alle Viren. Die Infektion kann über **Disketten**, **USB-Sticks** (und andere wechselbare Datenträger), **freigegebene Ordner**, **Netzwerkscans**, **Peer-to-Peer Netzwerke** oder **E-Mail** erfolgen. Dabei nutzen

die Schädlinge viele verschiedene Angriffspunkte, die teilweise nur auf bestimmten Kombinationen von Hardware, Software und Betriebssystem funktionieren.

Erkennungsteil

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

Schadensteil

Die **Schadensfunktionen** (engl. **Payload**), die mit Viren und Würmern einhergehen kann man in folgende Gruppen einordnen:

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

Ein expliziter Schadensteil kann aber auch fehlen. Aber die verschwendete Rechenzeit und der erhöhte Speicherplatz stellt ohnehin eine Payload dar.

Bedingungsteil

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

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

Tarnungsteil

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

- Sie erkennen z.B. wenn **Debugger** laufen oder schützen sich durch überflüssige und verwirrende (Assembler-) Codezeilen.
- Sie verbergen die Spuren einer Infektion. Dazu wird u.a. die Ausgabe von Statusmeldungen oder Log-Einträge gefälscht. Z.B. kann ein speicherresidenter Virus dem System vorgaukeln, dass der Speicher den er belegt immer noch von dem zuvor entfernten Programm stammt.
- Um der Entdeckung zu entgehen verschlüsseln manche Viren sich selbst und/oder Ihren Schadenscode. Bei der **Entschlüsselung** können immer die gleichen Schlüssel verwendet werden, die Schlüssel können aus einer Liste entnommen sein (**oligomorph**) oder die Schlüssel können unbegrenzt neu erzeugt werden (**polymorph**).

Würmer

Ein **Wurm** hängt sich im Gegensatz zu einem Virus nicht an ausführbare Dateien an. Er verbreitet sich dadurch, dass er sich automatisch über Netzwerke oder Mailverbindungen auf andere Rechner überträgt.

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

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

Viren

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

- **Bootsekturviren**: Bootsektor- oder **MBR-Viren** (= **Master Boot Record-Viren**) setzen sich vor den eigentlichen Bootsektor eines Datenträgers und sorgen so dafür, dass bei einem Bootvorgang über diesen Datenträger erst der Viruscode gelesen wird und danach der Original-Bootsektor. Auf diese Weise kann sich der Virus unbemerkt in das System einnisten und wird von da ab auch beim Booten von der Harddisk mit ausgeführt. Oft bleibt der Virencode nach der Infektion im Speicher bestehen. Solche Viren nennt man **speicherresident**. Beim **Formatieren** von Disketten wird der Virus dann weitergegeben und kann sich so auch auf andere Rechner ausbreiten. Aber nicht nur bei Formatier-Vorgängen kann der Bootbereichvirus aktiv werden. So kann durch den DOS-Befehl DIR die Übertragung des Virus von einer infizierten Diskette in Gang gesetzt werden. Je nach Schadensroutine können Bootbereichviren hochgradig gefährlich oder einfach nur störend sein. Der älteste und verbreitetste Virus dieser Art trägt den Namen "**Form**".
- **Datei-Viren**: Viele Viren nutzen die Möglichkeit, **ausführbare Dateien** als Versteck zu nutzen. Dazu kann die Wirtsdatei entweder gelöscht/ überschrieben werden oder der Virus hängt sich an die Datei an. In letzterem Fall bleibt der ausführbare Code der Datei weiterhin funktionsfähig. Wenn die ausführbare Datei aufgerufen wird, wird zunächst der meist in Assembler geschriebene Virencode ausgeführt und danach das ursprüngliche Programm gestartet (sofern nicht gelöscht).
- **Multipartite Viren**: Diese Virengruppe ist besonders gefährlich, da ihre Vertreter sowohl den **Bootsektor** (bzw. **Partitionstabellen**) infizieren als auch **ausführbare Dateien** befallen.
- **Companion Viren**: Unter DOS werden COM Dateien vor gleichnamigen EXE Dateien ausgeführt. Zu den Zeiten als Rechner nur oder häufig über

Kommandozeilenbefehle bedient wurden war dies ein wirkungsvoller Mechanismus um unbemerkt schädlichen Code auf einem Rechner auszuführen.

- **Makroviren:** Auch Makroviren hängen sich an Dateien an. Diese sind aber nicht selbst ausführbar. Die Makroviren sind auch nicht in Assembler, sondern in einer **Makrosprache** wie etwa **Visual Basic** geschrieben. Um die Viren auszuführen bedarf es eines Interpreters für eine Makrosprache wie sie in **Word, Excel, Access** und **PowerPoint** integriert sind. Ansonsten können die Makroviren die gleichen Mechanismen wirken wie bei Datei-Viren. Auch sie können sich tarnen, zusätzlich den Bootsektor verseuchen oder Companion-Viren erstellen.
- **Stealth-Viren:** Stealth-Viren oder **Tarnkappen-Viren** besitzen spezielle **Schutzmechanismen**, um sich einer Entdeckung durch Virensuchprogramme zu entziehen. Dazu übernehmen sie die Kontrolle über verschiedene Systemfunktionen. Ist dieser Zustand erst einmal hergestellt, so können diese Viren beim normalen Zugriff auf Dateien oder Systembereiche nicht mehr festgestellt werden. Sie täuschen dem Virensuchprogramm einen nicht infizierten Zustand einer infizierten Datei vor. Die Tarnmechanismen von Stealth-Viren wirken erst, nachdem der Virus im Arbeitsspeicher resident geworden ist. Einige Viren benutzen Teilfunktionen von echten Stealth-Viren.
- **Polymorphe Viren:** Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern. Dazu werden Teile des Virus verschlüsselt. Die im Virus integrierte Verschlüsselungsroutine generiert dabei für jede Kopie einen neuen Schlüssel und teilweise sogar neue **Verschlüsselungsroutinen**. Zusätzlich können Befehlssequenzen ausgetauscht oder zufällig eingestreut werden, die nicht für das Funktionieren des Virus erforderlich sind. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensignaturen häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.
- **Intended Virus:** Als Intended Virus wird ein teilweise defekter Virus bezeichnet, der zwar eine Erstinfektion einer Datei vollbringt, sich von dort aus aber nicht mehr reproduzieren kann.
- **E-Mail-Viren:** E-Mail-Viren gehören zur Gruppe der sog. **Blended threats** (= vermischte Bedrohung). Solche Malware kombiniert die Eigenschaften von Trojanern, Würmern und Viren. Im Rahmen des **Bubbleboy**-Virus wurde bekannt, dass es möglich ist, schon über die **Voransicht einer HTML-Mail** einen Virus auf den PC einzuschleusen. Der gefährliche Virencode versteckt

sich in HTML-Mails und nutzt eine Sicherheitslücke des Microsoft Internet Explorers. Die Gefahr dieser **Kombi-Viren** nicht zu unterschätzen.

Malware im weiteren Sinn

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

- **Hoaxes:** Hoaxes sind angebliche Viren-Warnungen, die oftmals per E-Mail verbreitet werden. Die Empfänger werden aufgefordert die E-Mail-Warnung an Freunde und Bekannte weiterzuleiten. Meistens handelt es sich bei diesen Hinweisen allerdings nur um Panikmache.
- **Backdoor-Programme:** Viele Systemadministratoren verwenden **Fernwartungsprogramme**, um Rechner von seinem aktuellen Standort zu administrieren. Insbesondere bei großen Unternehmen ist dies sehr nützlich. Üblicherweise erfolgt der Eingriff des Systemadministrators dabei mit dem Wissen und Einverständnis des PC-Users. Erst wenn diese Backdoor-Funktionen ohne Wissen des PC-Users eingesetzt werden und schädliche Aktionen ausgeführt werden wird ein Backdoorprogramm zur Malware.
- **Spyware:** Spyware zeichnet die Aktivitäten und Prozesse auf einem Rechner auf und machen sie Fremden zugänglich. Oft werden sie verwendet um das Surfverhalten zu analysieren, um passende Werbebanner einzublenden. Spyware lässt sich durch **AdAware** oder **SpyBot-Search&Destroy** entfernen. **SpywareBlaster** verhindert, dass Spyware auf Ihren Rechner gelangt.
- **Dialer:** Ähnlich wie Viren, Würmer und Trojaner werden Dialer oft unbemerkt auf dem Rechner installiert. Sofern die DFÜ-Verbindung über ein **Modem** hergestellt wird, wird dann beim nächsten Verbindungsaufbau eine teure Service-Telefonnummer verwendet. Mit dem "Gesetz zur Bekämpfung des Missbrauchs von (0)190er/(0)900er Mehrwertdiensternummern" sind zwar seit dem 15.Aug. 2003 einige Auflagen (Preisobergrenzen, Registrierung) in Kraft getreten. Dennoch sind Dialer immer noch eine lästige Plage, die mitunter zu hohen finanziellen Schäden führen können. Mit Anti-Dialer-Programmen wie **Dialer Control** kann man sich vor unerwünschten Dialern schützen.
- **Spam:** Eine ebenfalls teure und lästige Plage ist das Versenden unerwünschter **Werbe-E-Mail** oder Propagandamail. Moderne **Anti-Spam Programme** kombinieren statische (Textanalyse, Mailserverlisten) und automatische (basierend auf Bayes Theorem) Verfahren um die unerwünschte Post zu filtern.

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

Glossar

Abgesicherter Modus: Nach einem Systemabsturz startet Windows automatisch im **Abgesicherten Modus**. Dabei werden nur die unbedingt benötigten Systemdateien und Treiber geladen. So lassen sich Änderungen am System vornehmen, die im normalen Betrieb nicht möglich wären. Dies kann man auch dazu nutzen, um fehlerhafte Programme oder Viren, Würmer und Trojaner zu beseitigen.

Account: Als Account bezeichnet man die Zugangsberechtigung zu einem Computersystem. Dieser untergliedert sich in der Regel in eine

Benutzerkennung (User-Identification) und ein geheimes **Passwort**.

Active Scripting: Eine der ursprünglichen Stärken des Internet Explorers sind die umfassenden Möglichkeiten **aktive Inhalte** (d.h. ausführbare) darzustellen. Um dies zu gewährleisten, unterstützt der Internet Explorer die Ausführung von **JavaApplets**, **ActiveX Controls** und **Scriptsprachen** wie **JavaScript**, **VB-Script** etc. Neuerdings gehören auch **.NET Komponenten** dazu. Leider bieten aktive Inhalte nicht nur Vorteile. Immer wieder nutzen Anbieter von Webseiten die Möglichkeiten, um Ihre Besucher auszuspionieren. Auch Viren, Würmer und Trojaner verbreiten sich auf diesem Weg. Daher wird häufig empfohlen aktive Inhalte zu deaktivieren. In den Sicherheitseinstellungen des Internet Explorers lassen sich diese Komponenten für die verschiedenen Zonen ein- oder ausschalten. Mehr dazu erfahren Sie bei Microsoft.

ActiveX: ActiveX bezeichnet eine Technologie, die auf dem **Component Object Model (COM)** von Microsoft beruht. Sie ermöglicht es Softwarekomponenten, miteinander zu interagieren, auch wenn sie von unterschiedlichen Personen, zu unterschiedlichen Zeiten, mit unterschiedlichen Tools in unterschiedlichen Programmiersprachen geschrieben wurden. Die Komponenten - auch **ActiveX Steuerelemente** (engl. **ActiveX Controls**) genannt - müssen noch nicht einmal auf dem gleichen Rechner vorhanden sein. Durch ihren modularen Charakter lassen sich ActiveX Controls einfach in eigene Programme einbinden. Der Programmierer muss dazu lediglich die Spezifikation der Schnittstelle kennen. Nicht nur in Anwendungen von Microsoft werden ActiveX Controls eingesetzt. Sie werden z.B. dafür verwendet, um Word-, Excel- oder PowerPoint-Dokumente im Internet Explorer zu öffnen. Man spricht dann von ActiveX Dokumenten.

Administrator: Administrator ist die Bezeichnung für den Systemverwalter eines Netzwerks, der uneingeschränkte Zugriffsrechte hat und für die Betreuung und Verwaltung des Netzwerks zuständig ist.

API: Das **Application Programming Interface** ist eine standardisierte Schnittstelle, über die ein Programm auf ein anderes Programm oder Peripheriegeräte zugreifen kann.

Applet: Ein Applet ist eine Softwarekomponente, die nicht eigenständig benutzt wird, sondern das Leistungsspektrum eines Programms ergänzt. Auch Java-Programme werden als Applets bezeichnet, wenn sie in einem Browser ausgeführt werden.

Archiv: In einem Archiv sind mehrere Dateien und Verzeichnisse in eine Datei zusammengefasst. Um Festplattenspeicherplatz zu sparen oder Daten schneller zu versenden, können Sie diese mit diversen **Packprogrammen** (z.B. Winzip, WinRAR) je nach Datentyp auf ein erheblich geringeres Maß komprimieren. Diese Dateien haben Endungen wie z.B. **zip**, **rar** oder **arj** und können in der Regel erst nach dem Entpacken durch das jeweilige Packprogramm von anderen Anwendungen wieder genutzt werden. Der Zugriff auf ein Archiv kann mittels eines Passwortes eingeschränkt werden.

ASCII: Der **American Standard Code for Information Interchange** ist der weltweit geltende Standard um Buchstaben, Ziffern und Sonderzeichen in Byte zu kodieren.

ASP: Active Server Pages ist eine von Microsoft entwickelte WebServer Technologie, die **HTML-Seiten** aus Datenbanken dynamisch generieren kann.

Attachment: Attachment ist die englische Bezeichnung für einen Datei, die an eine E-Mail angehängt wurde.

Auslagerungsdatei: Jeder Rechner enthält einen Speicherbereich, in dem die Daten, die gerade vom Rechner gebraucht werden abgelegt werden. Diesen Bereich nennt man RAM (Random Access Memory). Der Zugriff auf den RAM-Speicher ist viel schneller als der Zugriff auf die Festplatte. Die Größe des RAMs ist allerdings beschränkt (z.B. auf 512 MB). Wenn jetzt sehr viele und/oder große Dateien geöffnet sind, kann es vorkommen, dass nicht alle Dateien im RAM Platz haben. Dann wird ein Teil des RAMs auf die Festplatte ausgelagert - und zwar in die **Auslagerungsdatei**.

BootScan: Der BootScan prüft vor der Installation des Virenschutzprogramms, ob Ihr System bereits von Viren befallen ist. Falls Sie versäumen, den BootScan durchzuführen, kann es Ihnen passieren, dass **Stealth-Viren** den Virenschutz umgehen und erst später oder gar nicht auffallen.

BCC: Mit einer **Blind Carbon Copy** können E-Mails an mehrere Empfänger versandt werden, ohne dass die Adressaten die E-Mail-Adressen der anderen Empfänger mitgeteilt bekommen.

BIOS: Das Basic Input Output System ist die erste Software, die nach dem Einschalten eines Computers geladen wird. Es führt beim Einschalten einen Selbsttest durch (POST = Power On Self Test), initialisiert die Hardware und lädt den Code aus dem ersten Sektor (Master Boot Record MBR) eines Datenträgers. Es umfasst zusätzlich Ein-/ und Ausgaberroutinen für Hardware, auf die das Betriebssystem zugreift. Da es von der Hardware abhängig ist, kann das BIOS nicht beliebig ausgetauscht werden. Das BIOS ist auf einem speziellen Chip auf dem Motherboard gespeichert, wo diese Daten auch erhalten bleiben, wenn die Stromzufuhr unterbrochen ist. Auf vielen Computern kann das BIOS mit Hilfe von Software des BIOS- Herstellers aktualisiert werden. Es kann auch von Viren, wie W95/CIH-10xx beschädigt werden, so dass der PC nicht mehr booten kann. Wenn der BIOS-Chip nicht ersetzt werden kann (einige BIOS-Chips sind verlötet), muss sogar das Motherboard des Computers ausgetauscht werden.

Bit. Abkürzung für **Binary digIT**. Ein Bit ist die kleinste Informationseinheit in der Computertechnik und kann die Werte 0 oder 1 annehmen.

Bluetooth: Bluetooth ermöglicht die Kommunikation zwischen Computern, PDAs, Mobiltelefonen und Peripheriegeräten wie Tastatur oder Maus. 1994 begann die Entwicklung der Schnittstelle bei Ericsson. Mittlerweile ist Bluetooth als IEEE Standard 802.15.1 für drahtlose Vernetzung über kurze Entfernungen etabliert. Der Name Bluetooth ist von dem dänischen König Harald I. Blauzahn Gormson abgeleitet, dem es im zehnten Jahrhundert gelang die skandinavischen Völker zu einen. Analog sollte Bluetooth zu einer Einigung bei der Kommunikation von elektronischen Kleingeräten führen. Technisch basiert Bluetooth auf einem kostengünstigen und stromsparenden Mikrochip das im ISM-Band zwischen 2,402 GHz und 2,480 GHz sendet - und zwar weltweit und lizenzfrei.

Bookmark: Über Bookmarks (= **Lesezeichen**) konnte man ursprünglich in einem Web-Browser interessante **Internet-Adressen** speichern. Die **Favoriten** - wie die Bookmarks bei Microsoft heißen - können zusätzlich in Word, Excel, PowerPoint, Outlook und anderen MS-Programmen auf interessante Objekte verweisen.

Boot Record: Dieser Eintrag enthält Informationen zum Inhalt einer Diskette oder HardDisk und Informationen, die ein Rechner braucht, um von diesem Medium zu booten. Auf den Boot Record wird vom Bootsektor aus verwiesen.

Bootsektor: Der Bereich auf einer Diskette oder einem Laufwerk, der den Boot Record enthält.

Browser Hijacker. Browser Hijacker installieren sich unbemerkt und ändern Einstellungen des Browsers (z.B. die Startseite) und dessen Funktionen (z.B. Suchfunktion). Daher gehören sie eigentlich zu den **Trojanern**. Browser Hijacker leiten den Nutzer ungewollt auf (oft pornografische) Webseiten indem

die Startseite oder die Suchfunktion umgeleitet wird. Manchmal werden auch zusätzliche Menüleisten oder Fenster angezeigt, die sich nicht entfernen oder schließen lassen. Oft nutzen Browser Hijacker Sicherheitslücken und Schwachstellen des Systems, um sich tief darin einzunisten. Meist wird der Internet Explorer angegriffen. Die Beseitigung der Fehlfunktionen ist oft sehr umständlich. Einer der berüchtigtsten Browser Hijacker ist CoolWeb.

Brute-Force Angriff: ein Brute-Force Angriff ist eine Möglichkeit, um Passwörter von verschlüsselten Dateien zu knacken. Dabei probiert man alle möglichen Kombinationen aus. Mit schnellen Rechnern und schwacher Verschlüsselung oder schwachen Passwörtern funktioniert das. Bei den aktuellen Sicherheitsstandards sind die Chancen für Brute-Force Angriffe aber äußerst gering.

Buffer Overflow: Bei einem Buffer Overflow überflutet ein Angreifer Datenfelder mit einer zu großen Datenmenge. Unter Umständen ist es so möglich, im Speicher der Rechner eigenen Programmcode auszuführen und versteckte Befehle zu übermitteln, die dem Angreifer einen Zugang auf diesen Rechner ermöglichen.

Bug: Der Begriff stammt aus den Zeiten als Rechnern noch mit Relais betrieben wurden. Hier sorgten Käfer (engl. Bug) für Programmfehler. Als Bug bezeichnet man seither einen Fehler in einem Software-Programm. Die meisten Hersteller bieten in so einem Fall einen sogenannten Patch an, der den Fehler behebt.

Bulk Mail: Bulk Mail steht für Massenpost. Der Begriff ist eine etwas mildere Bezeichnung für **Spam**.

Button: Button (engl.: Knopf) bezeichnet die oft stilisiert dargestellten Eingabetasten, die in Programmen und Internetseiten verwendet werden. Bewegen Sie die Maustaste über den Button und klicken Sie mit der linken Maustaste einfach oder doppelt auf den Knopf um die dort hinterlegten Funktionen auszuführen.

Byte: Ein Byte sind 8 Bit.

Cache: Der Cache ist eine schneller Zwischenspeicher, der dafür sorgt, dass oft abgerufene Daten nicht ständig neu übertragen werden müssen.

CC: Per **Carbon Copy** können beliebig viele Kopien einer E-Mail an weitere Empfänger verschickt werden. Die Nachricht muss dazu nur einmal geschrieben und versendet werden.

CGI: Das **Common Gateway Interface** ermöglicht einem Web-Browser, auf einen Web-Server Programme auszuführen. Sogenannte **CGI-Scripts** können dabei z.B. HTML-Formulare auswerten oder Datenbankabfragen durchführen.

Client: Client-Programme empfangen Daten von einem **Server**. Ein Computer wird dann Client genannt, wenn er auf diese Weise Daten von einem Server

empfängt. Web-Browser sind z.B. klassische Client-Programme.

Companion Virus: Wenn sich zwei ausführbare MS-DOS Programme nur im Dateityp (also der Dateierendung) unterscheiden, wird das mit der Endung .COM vor dem mit der Endung .EXE ausgeführt. Diese Eigenschaft machen sich Companion-Viren zu Nutze. Z.B. könnte ein Companion Virus sich unter dem Namen **DIR.COM** in das DOS-Verzeichnis kopieren. Wenn dann ein Anwender den Inhalt eines Verzeichnisses anzeigen möchte, wird der Virus aufgerufen und nicht das gewünschte Programm **DIR.EXE**.

Compiler: Compiler übersetzen Programmiersprachen in einen Maschinencode, der vom Rechner verarbeitet werden kann.

Cracker: Cracker sehen Ihre Lebensaufgabe darin, den **Kopierschutz** von Software durch sogenannte Cracks oder das Herausfinden von Seriennummern zu umgehen. Zu den Crackern zählen auch Personen, die das Datennetz dazu missbrauchen, sich Zugriff auf fremde Rechner zu verschaffen, um sich persönlich zu bereichern oder einfach nur Schaden anzurichten.

CRC: Der **Cyclic Redundance Check** ist ein Prüfsummenverfahren, mit dem festgestellt werden kann, ob Datenpakete fehlerfrei übertragen wurden.

Cross Site Scripting: Eine Sicherheitslücke, bei der Scripte von einer Webseite in einer anderen Webseite ausgeführt werden. Der Nutzer merkt nicht, dass ein fremdes Script ausgeführt wird, da sich die angezeigte URL-Adresse nicht ändert.

CSS: Mit **Cascading Style Sheets** können Formatvorlagen für Internetseiten definiert werden.

Cyberspace: Der Autor William Gibson verwendete 1984 in seinem Cyber-Thriller **Neuromancer** das erste Mal den Ausdruck **Cyberspace** und bezeichnete damit den virtuellen Raum eines globalen Computernetzwerks.

Daemon: Der **Disk And Execution MONitor** ist ein Programm, das im Hintergrund eines Netzwerks auf bestimmte Ereignisse wartet und bei Eintritt eines solchen Ereignisses bestimmte Aktionen startet. So wartet ein **Mailer Daemon** etwa auf eingehende E-Mails und ein Spooler wartet auf Druckaufträge.

Data Encryption Standard: Der **Data Encryption Standard (DES)** ist ein Datenverschlüsselungsstandard.

Datenkompression: Zur effizienteren Übertragung (z.B. per Modem) oder zum Einsparen von Speicherplatz (z.B. auf Datenträgern) werden Daten durch spezielle **Pack-Programme** verlustfrei komprimiert. Bekannte Dateiformate für komprimierte Dateien und Archive sind **ZIP**, **RAR** und **ARJ**. Auch Viren verbreiten sich oft komprimiert und bringen dann ihre eigenen Dekomprimierungsroutinen mit.

Debugger: Ein Debugger ist ein Tool für Software-Entwickler, mit dem sie Fehler im Programmablauf aufspüren können. Das Programm lässt sich an bestimmten Punkten anhalten und schrittweise ausführen. Im Debugger werden dann die jeweiligen Werte der aktiven Variablen angezeigt.

Defacement: Böswillige Umgestaltung von Webseiten durch einen Hacker.

Denial of Service: Bei einer Denial of Service-Attacke (**DoS**) werden Rechner (meist Webserver) mit gezielten und/oder sehr vielen Anfragen bombardiert. Dadurch können sie ihre Dienste nicht mehr ausführen und brechen unter der Last zusammen.

DHCP: Über das **Dynamic Host Configuration Protocol** werden automatisch feste oder dynamische IP-Adressen an Clients vergeben. Außerdem werden Gateway-Einstellungen für Netzwechsel sowie DNS-Informationen verwaltet.

DHTML: Mittels dynamischem HTML (**Dynamic HTML**) können Internetseiten in Verbindung mit **Active Scripting** und **Cascading Style Sheets** auch nach dem Herunterladen im Browser verändert werden. DHTML macht das Internet bunt und schön, birgt aber auch zahlreiche Gefahren.

Dialer: Dialer sind Einwahlprogramme, die eine meist kostenpflichtige Verbindung über Modem oder ISDN-Karte, zum Internet herstellt. Meist werden Dialer für die Bezahlung von sog. Mehrwertdienste im Internet verwendet und stellen eine einfache Bezahlmethode dar. Leider wurde in der Vergangenheit mit Dialern sehr viel Schindluder getrieben: - Dialer wurden ohne Wissen des Nutzers installiert - es wurden teure Auslandsnummern verwendet - die Verbindung zum Internet wurde automatisch hergestellt und nicht wieder beendet So entstanden einigen Kunden horrenden Kosten.

DirectX: Windows-Applikation zu schnelleren Grafikkarten-Ansteuerung bei Spielen oder Multimedia-Anwendungen.

DNS: Das **Domain Name System** ist ein Protokoll zur Umwandlung von Host-Namen in **IP-Adressen**. Der dazugehörige DNS-Server ordnet auf diese Weise den schwer erinnerbaren IP-Adressen (z.B.: 193.98.145.50) Host-Namen (z.B.: **www.antiviruslab.com**) als Alias zu und regelt die entsprechende Verwaltung.

Domain: Domains sind die Klartextnamen für die **IP-Adressen**. Sie bestehen aus 3 Teilen, die durch Punkte voneinander getrennt sind: Die letzten Buchstaben bezeichnen die Top Level Domains. Sie stehen für einzelnen Länder (.de, .fr) oder Sachgruppen (.mil, .gov, .info). An vorletzter Stelle stehen die Second Level Domains mit einfach zu merkenden Begriffen (z.B. Firmennamen). Im ersten Teil des Domain-Namens stehen die Namen von Rechnern und Subnetzen. Domain-Namen müssen mindestens 3 und dürfen maximal 128 Zeichen lang sein und dürfen bis auf Unterstrich und Bindestrich keine Sonderzeichen oder Satzzeichen enthalten. Neuerdings sind auch deutsche Umlaute erlaubt.

DOS: Als **Disk Operating System** wird generell ein Computerbetriebssystem bezeichnet, welches die Grundlage für Programme darstellt, die auf dieses Betriebssystem aufsetzen. **MS-DOS**, **Windows Vista**, **OS/2**, **UNIX** und **Linux** sind z.B. **Disk Operation Systems**.

Egress Filtering: In einer Firewall kann man sowohl den vom Internet (oder anderen Netzwerken) eingehenden Traffic filtern als auch den Traffic, der das eigene Netzwerk verlässt. Unter Egress Filtering versteht man das Filtern des ausgehenden Datenstroms. Dabei wird sichergestellt, dass alle Pakete, die das eigene Netz verlassen auch wirklich vom eigenen Netz stammen. Wäre dies gängige Praxis, wäre es leichter, DDoS-Angriffe und Netzwerk-Würmer wie SQL-Slammer und CodeRed zu stoppen.

E-Mail: Electronic mail oder elektronische Post ist eine der Hauptanwendungen des Internet. Zahllose geschäftliche und private Briefe werden täglich auf elektronischem Weg verschickt. E-Mails sind aber nicht nur nützlich, sondern auch ein Hauptweg zur Verbreitung von schädlichen Programmen. Würmer verbreiten sich häufig dadurch, dass sie automatisch E-Mails versenden, deren Anhang den Wurm enthält oder auf eine Webseite mit schädlichen Inhalten verweist. Die Virenautoren versuchen dabei den Leser der E-Mail mit allen Mitteln der Tarnung und Täuschung dazu zu bringen, die Datei im Anhang zu öffnen. Es gibt aber auch E-Mails, die Sie dazu verleiten, Webseiten mit infizierten Inhalten zu besuchen. Es gibt sogar **HTML-Mails**, die den Wurm beim Öffnen der E-Mail installieren.

Ethernet: Mit der Ethernet-Hardware können Computer unterschiedlichster Bauart miteinander vernetzt werden.

Exploit: Ein Programm, das eine bestehende Sicherheitslücke im Zielrechner ausnutzt, um beliebigen Programmcode auszuführen.

FAQ: Ein FAQ beantwortet **häufig gestellte Fragen** (engl. **frequently asked questions**) zu einem bestimmten Thema.

FAT: Die Dateizuordnungstabelle (File Allocation Table) besteht aus aufeinanderfolgenden Sektoren eines logischen Laufwerks und enthält eine Tabelle der Zuordnung von Dateien zu logischen Sektoren des Datenträgers. Sie befindet sich in den Sektoren nach dem Bootsektor. Zusätzlich enthält sie Informationen über freie und defekte Sektoren des Datenträgers.

FTP: Das **File Transfer Protocol** (= Protokoll zur Dateiübertragung) ist ein Übertragungsprotokoll für den Datenaustausch zwischen zwei Computern. FTP ist unabhängig vom Betriebssystem und der Art der Übertragung. Anders als beispielsweise **HTTP**, baut **FTP** eine Verbindung auf und hält diese während der kompletten Übertragung aufrecht.

Firewall: Bei Firewalls handelt es sich in der Regel um Software-Produkte, die den Datenstrom zwischen einem Rechner im lokalen Intranet (z.B. ein

Firmennetzwerk oder ein einzelner Heimcomputer) und Rechnern in offeneren Netzen (z.B. dem Internet) reglementieren und dafür sorgen, dass ungewünschte Inhalte (z.B. auch Dateien, die potentiell Viren enthalten können) nicht übertragen werden können. Oft wird dazu der Traffic auf vielen Ports unterbunden.

Flame: E-Mails mit beleidigendem Inhalt werden als Flames bezeichnet.

Flooding: Flooding gilt als Oberbegriff für verschiedene Möglichkeiten, bestimmte Rechner innerhalb eines Netzes durch Überforderung zu behindern bzw. zu überlasten.

FTP-Server: Auf FTP-Servern werden Internetanwendern Dateien und Verzeichnisse zum Download bereitgestellt. Auf öffentlichen FTP-Servern kann man sich oftmals mit der Benutzerkennung **Anonymous** und der eigenen E-Mail-Adresse als Passwort anmelden. Einige Viren und Trojaner installieren eigene FTP-Server, mit denen sie Dateien vom infizierten PC herunterladen können.

Gateway: Ein **Gateway** stellt eine Schnittstelle zwischen verschiedenen Kommunikationssystemen dar, z.B. einem Intranet mit dem Internet.

HBCI: Das **Home Banking Communication Interface** ist ein Internet-Protokoll zur gefahrlosen Kommunikation von Bank und Bankkunde untereinander.

Header: Der **Header** bezeichnet den Kopfteil einer Datei und beinhaltet Informationen zur Datei. In E-Mails stehen im Header u.a. Absender, Empfänger und Betreff.

Heuristik: In der heuristischen Analyse werden Viren nicht nur anhand der ständig aktualisierten Virendatenbanken ermittelt, sondern auch anhand bestimmter virentypischer Merkmale. Diese Methode ist ein weiteres Sicherheitsplus, kann in seltenen Fällen aber auch zu mehr Fehlalarmen führen.

Hijacker: Hijacker installieren sich unbemerkt und ändern Einstellungen des Browsers (z.B. die Startseite) und dessen Funktionen (z.B. Suchfunktion). Daher gehören sie eigentlich zu den Trojanern. Browser Hijacker leiten den Nutzer ungewollt auf (oft pornografische) Webseiten indem die Startseite oder die Suchfunktion umgeleitet wird. Manchmal werden auch zusätzliche Menüleisten oder Fenster angezeigt, die sich nicht entfernen oder schließen lassen. Oft nutzen Browser Hijacker Sicherheitslücken und Schwachstellen des Systems, um sich tief darin einzunisten. Meist wird der Internet Explorer angegriffen. Die Beseitigung der Fehlfunktionen ist oft sehr umständlich. Einer der berüchtigsten Browser Hijacker ist CoolWeb.

Hoax: Hoaxes sind angebliche Warnungen vor Viren und anderen Gefahren, die oftmals per E-Mail verbreitet werden. Die Empfänger werden aufgefordert die E-Mail-Warnung an Freunde und Bekannte weiterzuleiten. Meistens handelt es

sich bei diesen Mitteilungen um Panikmache, die nur Zeit (und damit Geld) kosten.

Hop: Als Hop bezeichnet man einen Rechner oder Knotenpunkt über den ein Datenpaket läuft, das von einem Rechner zu einem anderen geschickt wird.

Host: Host bezeichnet den Rechner, der dem Anwender die Möglichkeit bietet, Dienste (z.B. E-Mail) in Anspruch zu nehmen bzw. eine Datenverbindung (z.B. ins Internet) zu eröffnen.

HTML: Die **HyperText Markup Language** ist eine Seitenbeschreibungssprache des WWW und ermöglicht das Aussehen und Verhalten von Dokumenten plattformübergreifend zu regeln. HTML-Dateien werden innerhalb des WWW über HTTP übertragen.

HTTP: Das **Hyper Text Transfer Protocol** ist ein Client/Server-Protokoll, das im WWW zum Austausch von HTML-Dokumenten dient.

HTTPS: Das **Hyper Text Transfer Protocol (Secure)** dient, wie HTTP zum Austausch von HTML-Dokumenten, verschlüsselt die Daten aber vor der Übertragung.

Hub: Ein Hub ist ein Gerät um Computer oder Peripheriegeräte sternförmig miteinander zu vernetzen.

Hyperlink: Während ein Link innerhalb eines HTML-Dokuments auf einen anderen Textabschnitt verweist, stellt der Hyperlink die Möglichkeit dar, vom aktuellen Dokument in ein anderes Dokument innerhalb des WWW zu wechseln.

Hypertext: Hypertext ist die Bezeichnung für ein Dokument, in welchem durch Querverweise (**Links**) ein nichtlineares Lesen ermöglicht wird.

IANA: Die **Internet Assigned Numbers Authority** ordnet bestimmten Ports des TCP/IP-Protokolls bestimmte Dienste zu. Beispielsweise wird aus dieser Übereinkunft heraus für das **HTTP**-Protokoll Port 80 verwendet und für **FTP** Port 20/21.

ICMP: Das **Internet Control Message Protocol** ermöglicht das Versenden von Fehlermeldungen sowie Test- und Informationspaketen und ist ein Teil des **TCP/IP**.

ICP: Das **Internet Cache Protocol** regelt die Kommunikation von Cacheservern und Proxyservern mit den Clients.

IMAP: Das **Internet Message Access Protocol (IMAP)** ist eine Weiterentwicklung des **POP-Protokolls** und ermöglicht es, Nachrichten bedarfsweise zu übermitteln. Dazu werden erst die Kopfzeilen von Mails übermittelt und erst dann wird entschieden, wie mit der eigentlichen Mail zu verfahren ist.

In the wild: Viren die sich **in the wild (itw)** befinden, sind solche, die bei PC-

Nutzern tatsächlich auftreten. Im Unterschied zu **Zoo-Viren**, die nur in Sammlungen von Virenautoren und Herstellern von Antivirensoftware existieren, aber nie verbreitet wurden. Derzeit verbreitete Viren werden in die Wildlist von **www.wildlist.org** aufgenommen.

Internet: Das Internet ist ein weltweiter Verbund von Millionen Rechnern und hat sich vom militärisch genutzten Arpanet zu einem lebensbestimmenden kultur- und ländergrenzenüberspannenden Netzwerk entwickelt.

Internet Explorer: Der Internet Explorer (**IE**) ist ein Web-Browser von Microsoft.

IP-Adresse: Die Internet Protocol-Adresse ist eine numerische Adresse zur Identifizierung von Rechnern in einem TCP/IP-Netz. Diese Adresse wird in vier Byte dargestellt (z.B. 193.98.145.50). Sie besteht dabei aus zwei Teilen: 1. Adresse des logischen Netzwerks, 2. Adresse eines Hosts innerhalb des logischen Netzwerks. Da Menschen sich IP-Adressen nicht so gut merken können, verwenden sie normalerweise **Domain-Namen** um im Rechner im Internet zu besuchen.

IPX/SPX: Internet Packet Switching Protocol / Service Packet Switching Protocol bezeichnet ein Netzwerkprotokoll, das von Novell entwickelt wurde.

IRC: Über das **Internet Relay Chat-Protocol** können zwei oder mehrere Personen über das Internet eine Textkommunikation in Echtzeit durchführen.

ISDN: Als **Integrated Services Digital Network** wird ein internationaler Standard für digitale Fernsprechnetze bezeichnet, über den Telefongespräche, Datenfernübertragung und andere Mehrwertdienste abgewickelt werden können. ISDN stellt eine Weiterentwicklung des analogen Telefonnetzes dar und bietet jedem Anwender zwei Basiskanäle mit jeweils 64 kBit Übertragungskapazität und einen Steuerkanal mit 16 kBit.

ISP: Die **Internet Service Provider** sind Anbieter und Verwalter von Internet Zugängen.

Java: Java ist eine objektorientierte Programmiersprache, die es aufgrund Ihrer Plattform-Unabhängigkeit ermöglicht, Anwendungen zu erstellen, die auf den unterschiedlichsten Computersystemen funktionsfähig sind.

JavaScript: Eine mit Java nur entfernt verwandte Scriptsprache. Sie bietet eine Möglichkeit HTML um Active Scripting zu erweitern. Webseiten können im Browser (also clientseitig) nach dem Laden der Seite dynamisch verändert werden. Leider eröffnet JavaScript Sicherheitslücken wie z.B. Zugang zu Systeminformationen oder Ausführung von Programmen.

JavaScript Style Sheet: JavaScript StyleSheet (**JSSS**) bezeichnet eine von Netscape vorgeschlagene JavaScript-Modifikation. Um eine Kompatibilität des JavaScripts mit CSS zu erreichen.

JPG/JPEG: Das Grafikformat der **Joint Photographics Experts Group** ist im Internet weit verbreitet, da es aufgrund ausgefeilter Kompressionsalgorithmen die Möglichkeit beinhaltet, große Bilder bei vollem Farbumfang als relativ kleine Dateien zu speichern.

JScript: Jscript stellt eine für die Belange des Internet Explorer modifizierte Version von **JavaScript** dar.

Kaltstart: Starten des PCs nachdem der Rechner ausgeschaltet (und daher meistens abgekühlt) war. Der Inhalt des Arbeitsspeicher wird dabei im Gegensatz zum **Warmstart** vollständig gelöscht und damit auch speicherresidente Viren.

KBit: Ein KiloBit sind 1024 Bit.

KByte: Ein KiloByte sind 1024 Byte.

Keylogger: Mit einem Keylogger werden **Tastatureingaben** aufgezeichnet und ggf. versendet. So lassen sich Passwörter und andere persönliche Daten erschnüffeln. Ein Vertreter dieser Spezies heißt Padodoor.

Kompression/Komprimierung: Durch Komprimierung (also zusammenpressen) kann das Datenvolumen einer Datei teilweise erheblich verringert werden. Das spart Platz beim Archivieren und Bandbreite beim Übertragen von Dateien. Nachteil dieser Platzersparnis ist, dass auf diese Datei dann nur noch mit entsprechender Dekompressionssoftware wie z.B. WinZip, WinRAR oder ARJ zugegriffen werden kann.

Kontextmenü: Das Kontextmenü erhalten Sie, wenn Sie mit der rechten Maustaste in bestimmte Bereiche einer Programmoberfläche klicken. Im Kontextmenü können Sie dann Aktionen auswählen, die mit dem angeklickten Objekt durchgeführt werden können.

Konvertierung: Die Umwandlung eines Dateityps in eine Datei mit gleichem Inhalt aber anderem Format wird als Konvertierung bezeichnet.

LAN: Das **Local Area Network** ist ein Netzwerk, das auf ein überschaubares Areal begrenzt ist; z.B. ein Firmengebäude oder -gelände.

Link: Ein Link bezeichnet die Verknüpfung zwischen zwei HTML-Dokumenten. Er ist ein Spezialfall eines **URL (Uniform Ressource Locator)**.

Login: Der Vorgang der **Einwahl, Anmeldung** und **Authentifizierung** (meist per Passwort) eines Anwenders an ein Computersystem wird **LogIn** genannt.

Logoff: Das Beenden einer Datenverbindung zu einem Computersystem bezeichnet man als **LogOff**.

Mac OS: Betriebssystem von Apple Macintosh Computern.

MAC-Adresse: Die MAC-Adresse (**Media Access Control**) ist die Hardware-Adresse eines Netzwerkgerätes (z.B. Netzwerkkarte, Switch). Die Mac-

Adresse ist weltweit eindeutig. Sie besteht aus 48 bit in denen der Hersteller des Gerätes (24 Bit) und vom Hersteller verwendete Schnittstellen identifiziert werden. So lässt sich das Gerät eindeutig im Netzwerk identifizieren. Oft wird die MAC Adresse zur Erzeugung von Lizenzschlüsseln für Software verwendet.

Mailbomb: Der schädliche Code wird einem ahnungslosen Nutzer per Mail zugesandt.

Mailbox: Eine Mailbox ist ein Computersystem, das E-Mail-Dienste, Chat und Dateidownloads über eine bestimmte Einwahlnummer anbietet und nicht mit dem Internet verbunden ist.

Mailingliste: Mailinglisten stellen einen ggf. moderierten Verbund verschiedener E-Mail-Empfänger dar. Eine E-Mail an die Mailingliste erreicht dabei stets alle Abonnenten der Mailinglist. Die meisten Mailinglisten beschäftigen sich mit einem eng umgrenzten Thema.

MAPI: Die **Messaging API** regelt die Kommunikation zwischen Windows-Anwendungen und Microsoft Mail.

MB: Ein MegaByte sind 1024 KByte.

MBit: Ein MegaBit sind 1024 KBit.

MByte: Ein MegaByte sind 1024 KByte.

MegaByte: Ein MegaByte sind 1024 KByte.

Message: Message bedeutet übersetzt **Nachricht**, **Botschaft**, und bezeichnet in der Regel eine **E-Mail-Nachricht** oder eine **InstantMessage**.

MIME: Multipurpose Internet Mail Extensions ist eine Kodierung zur Kombination von E-Mails mit Binärdateien. Sobald Absender und Adressat ein MIME-fähiges E-Mail-Programm verwenden, können Sie Binärdateien wie z.B. ausführbare EXE Dateien, gezippte Archive oder DOC Dateien von Word direkt in E-Mails einfügen.

Modem: Mit Hilfe eines **MOdulator / DEModulators** lassen sich Computer für die Datenfernübertragung aufrüsten. Die Modem-Hardware ermöglicht - mit entsprechender Software - die Einwahl ins Internet oder andere lokale oder offene Computernetzwerke.

MPEG: Ein von der **Motion Picture Experts Group** entwickelter Kompressionsstandard für die digitale Verarbeitung von Audio- und Videodaten.

NAT: Die **Network Address Translation** ermöglicht es, private IP-Adressen eines Local Area Networks auf öffentliche IP-Adressen umzusetzen. Auf diese Weise ist es z.B. möglich, mehrere Rechner über eine einzige, vom Provider gelieferte IP-Adresse ins Internet zu bringen.

Netiquette: Netiquette ist eine Wortschöpfung, die sich aus **Netz** und **Etiquette** ableitet und eine Art Verhaltenskodex im Internet bezeichnet. Im Prinzip gelten

laut der Netiquette dieselben grundlegenden Höflichkeitsformen wie im echten Leben (RL = real life), bloß dass diese aufgrund der einfachen Möglichkeiten zur Anonymisierung der Teilnehmer offenbar einer besonderen Erwähnung bedürfen.

Netzwerk: Als Netzwerk wird ein Verbund von Computern und Peripheriegeräten bezeichnet, die auf Basis eines gemeinsamen Netzprotokolls miteinander kommunizieren können.

Newsgroup: Newsgroups sind Öffentliche Diskussionsforen im Internet zu eng umrissenen Themen. Sie sind die Nachfolger des **Usenet**.

NIC: Die **Network Information Center** sind für die Vergabe von IP-Adressen verantwortlich. Für Deutschland erfolgt dies z.B. durch die **DE-NIC**. Für allgemeine Toplevel Domains ist die **Inter-NIC** verantwortlich.

NullSession: Von NullSessions spricht man, wenn bei der Anmeldung an einem fremden System kein Nutzernamen und kein Passwort angegeben wird. Windows stellt dann dem anfragenden System etliche Informationen zur Verfügung. U.a. Domainname, Adresse(n) des Rechners uvm. Diese NullSessions sind Grundlage für einige Windows-Funktionen. Sie bieten allerdings auch eine Reihe konzeptueller Schwachstellen, die von einem Cracker ausgenutzt werden können, um unbefugt auf die Daten eines Rechners zuzugreifen.

ODBC: Open Database Connectivity sind Schnittstellen die von Microsoft entwickelt wurden. Mit Hilfe dieser Schnittstellen kann auf SQL-Datenbanken zugegriffen werden.

Offline: Offline bedeutet, dass ein Client-Rechner keine Verbindung zum Server oder dem Internet hat.

Offline-Reader: Über **Offline-Reader** kann man Informationen aus dem Internet auf den lokalen Rechner herunterladen. Nach dem Download kann man auch ohne Internetverbindung die ausgewählten Webseiten in Ruhe lesen oder durchstöbern. Dies hat den Vorteil, dass während dieser Zeit keine Verbindungs- und Providerkosten anfallen.

Online: Ein Rechner ist online wenn er eine Verbindung (z.B. über Telefonleitung) zum Server oder dem Internet hat.

P2P: Bei **Peer-to-Peer**-Netzwerken existiert kein zentraler Server und alle Computer im Verbund agieren gleichberechtigt nebeneinander.

Packeting: Eine Form des **Flooding**, bei der ICMP-Pakete an bestimmte IP-Adressen gesendet werden, um auf diese Weise einen **Denial of Service** zu erreichen.

PAP: Das **Password Authentication Protocol** dient als Teil der IETF-Protokollsuite, dem Austausch von Passwörtern. Weil das PAP das User-

Passwort unkodiert zur Überprüfung an einen zentralen Server überträgt, bietet es nur einen geringen Schutz.

Patch: Ein Patch behebt Fehler oder schließt Sicherheitslücken in einer Software. Das Patch ersetzt dabei nur die fehlerhaften Dateien und ersetzt nicht die Vollversion der Software.

Payload: Payload ist die englische Bezeichnung für die **Schadensfunktion eines Virus**. Die Auslösung der Schadensfunktion kann mit einer Bedingung, dem sog. Payload-Trigger verbunden sein. Die Definition von Schadensfunktion ist umstritten, da einige Forscher auch den Verbrauch von Systemressourcen und Übertragungsbandbreite als Payload ansehen.

Payload-Trigger: Bedingung, die einen Payload auslöst. Oft ist es ein Datum oder die Anzahl von Programmaufrufen.

PDC: Der **Primary Domain Controller** verwaltet als Server innerhalb eines Windows-Netzwerkes, die Benutzer und deren Rechte.

PDF: Das **Portable Document Format** ist ein von Adobe entwickeltes Format, um bebilderte Texte auf verschiedenen Rechnersystemen gleichartig darstellen zu können.

PE Datei: Portable Executable. Ausführbare Datei für Win32 Betriebssysteme. Nachfolger der ausführbaren Dateien unter DOS (.EXE und .COM).

Peer: Bei einem Netzwerk ohne zentralen Server bezeichnet man die jeweils andere Station einer Vernetzung als **Peer**.

PGP: Als **Pretty Good Privacy** wird ein Programm zur Verschlüsselung von Daten bezeichnet, das auf dem Public - Private Key Prinzip basiert. Dabei können Nachrichten mit dem Public Key (öffentlichen Schlüssel) verschlüsselt, anschließend allerdings nur mit dem Private Key (privaten Schlüssel) entschlüsselt und gelesen werden.

Phishing: Unter Phishing versteht man den Versuch persönliche Daten wie Loginnamen, Passwörter, Kreditkartennummern, Bankzugangsdaten etc. durch gefälschte Webseiten oder unerwünschte E-Mails zu erhalten. Meist richten sich Phishing-Versuche an Kunden von Banken mit Online-Banking Angeboten (CityBank, Postbank), Bezahlendienste (Paypal), Internet Service Provider (AOL) oder Online-Shops (eBay, Amazon). Oft wird man dazu per E-Mail oder Instant Messenger auf gefälschte Webseiten geleitet, die den Seiten der Vorbilder sehr genau nachempfunden sind.

PIN: Die **Personal Identification Number** dient z.B. beim Online-Banking oder bei Mobiltelefonen zur Identifikation des Nutzers.

PING: Mit dem **Packet Internet Grouper** können IP-Verbindungen getestet werden. Der Befehl **ping** gibt die Dauer an, wie lange ein Packet unterwegs ist. Für Online-Spieler interessant: Je kleiner der Ping-Wert, desto schneller

(=besser) ist die Verbindung.

Polymorphe Viren: Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern. Dazu gehört unter anderem der Austausch von Befehlssequenzen und zufallsgesteuertes Einstreuen von unsinnigen Befehlsgruppen. Diese sind in keiner Weise für das Funktionieren des Virus erforderlich. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensignaturen häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.

POP3: POP3 ist die Abkürzung für **Post-Office Protocol 3**. Mit Hilfe dieses Protokolls werden E-Mail-Daten von einem E-Mail-Server mit Hilfe eines POP3-basierten E-Mail-Programms auf den Rechner des Adressaten heruntergeladen.

Popup: Popups sind Browserfenster, die sich parallel zur aufgerufenen Seite öffnen. Da sie meist Werbung enthalten, kann man das Öffnen der Fenster mit sog. **Popup Blockern** unterbinden.

Port: Vernetzte Anwendungen kommunizieren untereinander durch eine Kombination aus IP-Adresse und Port-Nummer und spezifizieren damit den Dienst, der auf dem jeweiligen Zielrechner angesprochen werden soll. So dient z.B. in der Regel Port 80 für HTTP oder die Ports 20 und 21 für FTP. Mit einer Firewall kann der Datenaustausch für einzelne Port geregelt werden.

Posting: Posting bezeichnet eine Nachricht, die im Internet meist in **Newsgroups**, **Mailinglisten** oder in **Foren** veröffentlicht wird.

PPP: Das **Point to Point Protocol** ist ein Übertragungsprotokoll, das die Verbindung zwischen dem Modem eines Computeranwenders und dem Einwahlknoten eines Providers regelt.

Private Key: Der Private Key ist notwendig, um bei PGP mit dem Public Key verschlüsselte Dokumente, entschlüsseln zu können.

Protokoll: Ein Protokoll dient der Kommunikation zwischen verschiedenen Rechnern in einem Netzwerk. Das Protokoll enthält eine formale Zusammenstellung von Regeln, die den Nachrichtenaustausch steuern. Beispiele für Protokolle sind FTP, HTTP, POP3 oder TCP/IP.

Provider: Anbieter eines Internetzugangs.

Proxy: Der Proxyserver stellt eine Art Zwischenspeicher dar, der dazu dient, die Menge der übertragenen Daten in einem Netzwerk zu verringern. So werden Dateien, die von vielen Anwendern heruntergeladen werden, in einem Zwischenspeicher gelagert und können auf diese Weise schneller verwendet

werden, ohne dass der eigentliche Ladevorgang (z.B. aus dem Internet) erneut erfolgen müsste. Dieser Zwischenspeicher kann in Verbindung mit einer Firewall auch für eine erhöhte Datensicherheit und einen grundlegenden Schutz vor möglicherweise virenverseuchten Dateien dienen.

Public Key: Der Public Key wird bei **PGP** verwendet, um Dokumente zu verschlüsseln.

Quellcode: Als Quellcode wird der Programmtext einer beliebigen Programmiersprache bezeichnet. Der Quellcode selbst kann keine Aktionen auslösen, da er zunächst kompiliert werden muss. Wenn der Quellcode eines Programms (z.B. eines Virus) verfügbar wird, können sehr leicht Varianten entwickelt werden.

Quicktime: Quicktime ist der Multimedia-Player von Apple.

RADIUS: Beim **Remote Dial-In User Service** kommunizieren Anwender und Server nicht nur verschlüsselt miteinander auch die Benutzerdaten werden verschlüsselt gespeichert.

Raubkopie: Eine Raubkopie ist eine nicht lizenzierte, nicht genehmigte Kopie eines Programms, die illegal von einem Originalprodukt angefertigt wurde. Jegliches Besitzen oder Anfertigen einer Raubkopie ist nach dem Urheberschutz strafbar.

Registry: Registrierdatenbank in Windows, die zahlreiche für das Betriebssystem und installierte Anwendungen wichtige Einstellungen enthält. Sie können Sie editieren, indem Sie im Start-Menü **Ausführen** wählen und dort **regedit** eintippen. **Achtung: Erstellen Sie vor Änderungen eine Sicherungskopie Ihrer Registrierdatenbank.**

Re-Mailer: Ein Re-Mailer ist ein Server der E-Mails anonymisiert weitersendet. Er entfernt alle persönlichen Informationen (Absenderadresse) und verschickt die Nachricht weiter. Normalerweise werden auf diesen Servern keine Daten über eingegangene E-Mails gespeichert.

Reply: engl. Antwort. Antwort auf eine E-Mail oder eine andere elektronische Nachricht.

RFC: Als **Request For Comment** (engl. **Bitte um Kommentare**) bezeichnet man Entwürfe und Arbeitspapiere die öffentlich z.B. in Mailinglisten besprochen werden.

Robot: Robots sind Programme, die in Datenbanken, Servern oder dem Internet relativ autonom bestimmte Aufgaben ausführen. Z.B. verwenden Suchmaschinen Robots, um die Inhalte von Webseiten für die Suchanfragen zu erfassen und zu indizieren.

Router: Als Router werden Computer bezeichnet, die speziell für Routing-Aufgaben eingesetzt werden.

Routing: Der Transport von Daten innerhalb eines Netzes wird als Routing bezeichnet. Als passives Routing wird der Transport von Daten innerhalb eines Netzes bezeichnet. Die für den Transport festgelegte Verbindung wird im Header der Daten definiert. Im Gegensatz zum passiven Routing ermittelt der Router beim aktiven Routing die kürzeste, schnellste, billigste oder nächstbeste Leitung aus der Routingtabelle. Dabei macht sich der ständige Austausch der Routingtabellen unter den Routern innerhalb eines Netzes besonders bezahlt.

RTF: RTF steht für **Rich Text Format**. Dieses Textformat wurde von der Firma Microsoft für den Ex- und Import von Texten entwickelt.

S/MIME: Secure MIME ist ein **DES** basiertes Verfahren, das zum Verschlüsseln und elektronischen Unterschreiben von E-Mails genutzt wird.

Secure Sockets Layer Protocol: Das Secure Sockets Layer-Protocol (**SSLP**) bietet durch Datenver- und -entschlüsselung einen gesicherten Datenaustausch und wird oft für das Home-Banking genutzt.

Sektor: Ein Sektor ist die kleinste Einheit der Festplattenaufteilung (d.h. der kleinste adressierbare Teil eines Datenträgers). Ein Datenträger wird während der Formatierung in Sektoren aufgeteilt.

Server: Als Server werden Computer bezeichnet, die innerhalb eines Netzes (z. B. lokales Netzwerk oder auch über das Internet) Daten oder Dienste anderen Computern zur Verfügung stellen. Alternativ werden auch im Hintergrund laufende Programme, die Server-Aufgaben erfüllen, als Server bezeichnet.

SET: Das **Secure Electronic Transaction**-Protokoll dient der verschlüsselten Übertragung von Benutzerdaten übers Internet.

SGML: In der **Standard Generalized Markup Language** werden die Grundlage aller Dokumentenbeschreibungssprachen wie HTML und XML festgelegt.

Site: Einzelne Internetseiten werden oft auch als Site bezeichnet.

Slash: Der Slash (engl. Schrägstrich = /) ist ein Zeichen, das u.a. bei der Eingabe von Internetadressen und Verzeichnispfaden verwendet wird.

SMB: SMB ist ein Protokoll, das in Windows zur Kommunikation zwischen Computern genutzt wird und Freigaben von Druckern, Dateien und Serial Ports regelt.

SMS: Der **Short Messages Service** dient zur kostengünstigen und schnellen Versendung von Kurznachrichten auf Handys.

SMTP: Das **Simple Mail Transfer Protocol** ist ein Protokoll, das den Versand von E-Mail steuert. Für den E-Mail-Empfang wird auf das POP3-Protokoll zurückgegriffen. Normalerweise wird für SMTP der Port 25 verwendet.

Snail-Mail: Da der klassische Briefverkehr im Gegensatz zur E-Mail erheblich langsamer ist, wird er auch als Schneckenpost (engl. snail-mail) bezeichnet.

Sniffer: Sniffer sind Programme oder Personen, die den Datenverkehr abhören.

Social Engineering: Als Social Engineering werden Überredungstaktiken bezeichnet, mit denen ein Hacker einen Anwender dazu veranlasst Informationen preiszugeben, mit denen er dem Anwender oder seiner Organisation Schaden zufügen kann. Oft wird dazu Autorität vorgespiegelt, um Zugangsdaten oder Passwörter zu erlangen.

Sourcecode: Als **Quellcode** wird der Programmtext einer beliebigen Programmiersprache bezeichnet. Der Quellcode selbst kann keine Aktionen auslösen, da er zunächst kompiliert werden muss. Wenn der Quellcode eines Programms (z.B. eines Virus) verfügbar wird, können sehr leicht Varianten entwickelt werden.

Spam: Mitte der 90er Jahre bezeichnet Spam die übermäßige Verbreitung der gleichen Nachricht in Usenet Foren. Der Begriff selbst geht auf einen Sketch von Monty Python zurück. Mittlerweile verwendet man Spam in mehreren Bedeutungen. Als Oberbegriff steht Spam für alle unaufgefordert zugesandten E-Mails. In einem engeren Sinne beschränkt sich der Begriff Spam auf WerbE-Mails; d.h. Würmer, Hoaxes, Phishing-Mails und AutoResponder werden nicht dazugezählt.

Spammer: Jemand, der Spam versendet.

Spyware: Als Spyware bezeichnet man Software, die Aktivitäten und Prozesse auf einem Rechner aufzeichnet und Fremden ohne Wissen und/oder Einverständnis des Besitzers zugänglich macht. Oft wird Spyware verwendet, um für Werbeeinblendungen das Surfverhalten zu analysieren, oder um Zugangsdaten für Bank- oder Online-Accounts zu erschnüffeln.

SQL: Die **Structured Query Language** erlaubt die Abfrage, Erzeugung und Änderung von Datenbanken und Datenbankeinträgen. Im Internet werden die Ergebnisse der Datenbanksuche oft in HTML-Seiten angezeigt. Der verbreitetste Dialekt von SQL ist **MySQL**.

SSL: Das **Secure Sockets Layer-Protocol** bietet durch Datenver- und -entschlüsselung einen gesicherten Datenaustausch und wird oft für das Home-Banking genutzt.

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

Steganografie: Über die Steganographie werden geheime Daten innerhalb anderer Daten versteckt werden. So kann man z.B. in Grafiken Textbotschaften verbergen oder Bilddaten in einer Soundfile.

Subdomain: Eine Subdomain ist ein untergeordneter Teil einer Domain.

Subject: Das Subject ist die Betreffzeile einer E-Mail. Sie befindet sich im Header einer Nachricht.

SysOp: Als System Operator bezeichnet man den **Administrator** eines Rechnernetzwerks. Im Sinne eines Verwalters ist der Administrator für den korrekten Betrieb des Netzwerks zuständig.

Tab: Als Tab bezeichnet man eine **Registerkarte** oder einen **Karteireiter**, das es erlaubt in einem Programmfenster zwischen unterschiedlichen Inhalten umzuschalten. Tabellenblätter sind in Tabellenkalkulationsprogrammen wie Excel schon lange üblich. Seit kurzem gibt es auch viele Browser und Browseroberflächen, die es ermöglichen die Inhalte von mehreren Webseiten, in jeweils einem eigenen Tab anzuzeigen. Man spricht dann von Tabbed Browsing.

Tabbed Browsing: Als Tab bezeichnet man eine Registerkarte oder ein Tabellenblatt, das es erlaubt in einem Programmfenster zwischen unterschiedlichen Inhalten umzuschalten. Tabellenblätter sind in Tabellenkalkulationsprogrammen wie Excel schon lange üblich. Seit kurzem gibt es auch viele Browser und Browseroberflächen, die es ermöglichen die Inhalte von mehreren Webseiten, in jeweils einem eigenen Tab anzuzeigen. Man spricht dann von Tabbed Browsing.

TAPI: Als **Telephony API** wird eine von Microsoft entwickelte Programmierschnittstelle bezeichnet, die es Entwicklern ermöglicht auf die Funktionen von TAPI-konformen Modems zuzugreifen.

Taskleiste: Die Task- oder **Startleiste** von Microsoft Windows befindet sich voreingestellt am unteren Bildrand des Bildschirmhintergrunds (Desktop) und enthält links den Start-Button, über den Sie Programme und Einstellungen aufrufen können. Auf der rechten Seite des Balkens finden Sie neben der Systemuhr, Symbole von aktiven Programmen. Dies kann z.B. die Lautstärkeregelung Ihrer Soundkarte sein, aber z.B. auch der **G DATA AntiVirus Virenwächter**. Durch Anklicken des Symbols mit der linken oder rechten Maustaste können Sie hier weitere Einstellungen vornehmen.

TCP/IP: Die beiden Protokolle **Transmission Control Protocol/Internet Protocol** sind für die Adressierung und Weiterleitung von Daten im Netzwerk zuständig. Sie werden für die Kommunikation zwischen Computern mit unterschiedlichen Betriebssystemen eingesetzt. Sie entsprechen den Schichten 3 und 4 im OSI-Schichtenmodell.

Telnet: Mit Telnet wird ein Internet-Dienst bezeichnet, der dem Benutzer die

Möglichkeit bietet sich auf einem Server einzuloggen, der dann vom Benutzer über bestimmte Befehle gesteuert werden kann. Ein Fenster präsentiert dem Benutzer das Bild des angewählten Rechners. Die Steuerung des Programms läuft über die eigene Tastatur, die dabei vom entfernten Rechner behandelt wird als sei sie direkt mit ihm verbunden.

Terminal: Terminals stellten während der Großrechner-Ära über eine Kombination von Tastatur und Bildschirm eine Verbindung zum Großrechner her. Heute simuliert ein Terminalprogramm eine ähnliche Funktion, beispielsweise als Verbindung zu einer Mail-Box. Dementsprechend kann auch Telnet als eine Art Terminalprogramm bezeichnet werden.

Thumbnail: Als Thumbnails bezeichnet man kleine Kopien von Bilddateien in der Größe eines Daumennagels. Sie werden als Vorschaubilder in großen Bildersammlungen genutzt.

Top Level Domain: Die einzelnen Bestandteile einer Webadresse sind durch Punkte voneinander getrennt. Die Top Level Domain (**TLD**) bezeichnet den letzten Teil der Adresse. In **www.antiviruslab.com** wäre es **com**. Die Top Level Domain stellt die oberste Ebene der Namensauflösung dar. Überregional gültige TLDs sind: .com (weltweite, kommerzielle Firmen), .mil (Militär), .gov (US-Regierung), .org (nicht-kommerzielle Organisationen), .edu (amerikanische Bildungseinrichtungen), .net (Netzverwaltungseinrichtungen), .int (internationale Behörden), .info, .museum, .name (natürliche Personen), .coop (Kooperationen), .aero (Luftfahrtorganisationen). Andere Top Level Domains sind nur für einzelne Länder gültig. Die Kennung enthält eine Kombination von 2 Buchstaben. Hier die bekanntesten: .de (Deutschland), .at (Österreich), .ch (Schweiz), .fr (Frankreich), .nl (Niederlande), .pl (Polen), .es (Spanien), .ca (Kanada).

Traceroute: Als Traceroute wird ein Tool bezeichnet, das alle Server aufzeichnet, die ein IP-Paket während seiner Reise durchs Internet durchläuft.

Trojaner: Der Name **Trojanisches Pferd** ist angelehnt an das geschichtliche Vorbild und beschreibt ein Programm, das dem Anwender vorgibt, eine bestimmte und gewollte Funktion zu besitzen. Zusätzlich dazu beinhalten Trojaner jedoch noch einen versteckten Programmteil, der gleichsam eine Hintertür zum befallenen Rechner öffnet und so nahezu vollen Zugriff auf das betroffene System gewährt ohne, dass der Benutzer dies bemerkt. Die Methoden von Trojanern, sich zu verstecken sind dabei schier unbegrenzt, so werden diese heimtückischen Programme oftmals als Bildschirmschoner oder Spiele per E-Mail verschickt. Ein einmaliges Starten genügt bereits und der Schädling infiziert das System.

Tunneling: Beim Tunneling werden Daten eines Protokolls in ein anderes Netzwerkprotokoll eingebettet. So können sichere (verschlüsselte) Verbindungen (wie **SSH**) über ungesicherte Netzwerke (**TCP/IP**, **SMTP**)

aufgebaut werden. Ein Tunnel kann auch dazu genutzt werden, um eine Firewall zu umgehen. Mit einem ausgehenden Tunnel kann ein Nutzer aus dem Intranet auf externe Rechner, Netze oder Dienste zugreifen. Bei eingehenden Tunnels, kann ien externer Nutzer auf einen Dienst, Rechner oder Daten des Intranet zugreifen.

UCE: Unsolicited E-Mail stellt ein Synonym zu Spam dar und ist daher ebenfalls eine Bezeichnung für unerwünschte E-Mails.

Uniform Resource Identifier. Der Uniform Ressource Identifier (**URI**) ist der Oberbegriff für eine Zeichenfolge, die eine Ressource (in einem Rechner) eindeutig bestimmt. Man kann URIs auch als Namen ansehen, wobei diese allerdings im Gegensatz zu Namen bei Menschen genau einmal vorkommen. URIs werden meist verwendet, um Webseiten, Webdienste oder E-Mail-Empfänger im Internet zu bezeichnen.

Upload: Upload bezeichnet das Gegenteil von **Download**. Dabei werden Daten vom eigenen Rechner an einen anderen geschickt. Wenn z.B. Dateien für einen Webserver vom lokalen Rechner auf den Webserver übertragen werden, spricht man von einem Upload.

URL: Der **Uniform Ressource Locator** ist vereinfacht gesagt die Adresse einer Datei (Text, Grafik, Software, o.ä.) im Internet.

USB: Der **Universal Serial Bus** ermöglicht den Anschluss peripherer Geräte wie Datenspeicher, Maus oder Drucker an den PC auch während das System in Betrieb ist.

Usenet. Als Usenet wird ein Computernetz bezeichnet, das zwar unabhängig vom Internet entstand, heute aber weitgehend über das Internet abgewickelt wird und dem Austausch von Mitteilungen sowie Meinungen in diversen **Newsgroups** dient. Das **USErs NETWORK** ist genaugenommen ein Diskussionsbrett, das auf speziellen News-Servern läuft. Als Transportmittel für die Nachrichten werden hierbei ganz unterschiedliche Netzwerke ebenso wie natürlich auch Teile des Internet benutzt. Im Usenet gibt es nur öffentlich zugängliche Nachrichten. Das heißt, dass auf eine einmal gepostete Nachricht beliebig viele Teilnehmer antworten können. Das führt oft zu langen und komplizierten Ketten von Rede und Gegenrede, die man **Threads** (engl. **Faden**) nennt.

User: Als User (engl. **Nutzer**) wird der Benutzer und Anwender eines ComputerSystems bezeichnet.

VB-Script: Als VB-Script wird eine Scriptsprache bezeichnet, die auf der Programmiersprache **Visual Basic** aufbaut und von Microsoft als Ergänzung von **HTML** entwickelt wurde.

Viren, polymorphe: Polymorphe Viren enthalten Mechanismen, um ihr Aussehen bei jeder Infektion zu verändern. Dazu gehört unter anderem der

Austausch von Befehlssequenzen und zufallsgesteuertes Einstreuen von unsinnigen Befehlsgruppen. Diese sind in keiner Weise für das Funktionieren des Virus erforderlich. So können leicht Milliarden von Varianten eines Virus entstehen. Um verschlüsselte und polymorphe Viren sicher zu erkennen und zu beseitigen, reicht der Einsatz klassischer Virensignaturen häufig nicht aus. Meist müssen spezielle Programme geschrieben werden. Der Aufwand zur Analyse und zur Bereitstellung geeigneter Gegenmittel kann dabei extrem hoch sein. So sind polymorphe Viren ohne Übertreibung als die Königsklasse unter den Viren zu bezeichnen.

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

Virensignatur: Ein sehr effektives Mittel zur Erkennung und Beseitigung von Viren ist der Vergleich der möglichen Viren mit der jeweiligen Virensignatur. Die Virensignatur ist im Prinzip eine Schablone, die genau auf einen Virus oder Virentyp passt und ihn auf diese Weise schnell erkennt. Da diese Schablonen erst dann erstellt werden können, wenn der Virus das erste Mal auftauchte und von Antivirenexperten analysiert wurde, ist es um so wichtiger, dass Sie möglichst immer die aktuellsten Virensignaturen auf Ihrem Computer zur Verfügung haben.

Virtuell: Als virtuell wird eine Umgebung dann bezeichnet, wenn sie nicht auf dem realen Leben (RL engl. real life) basiert, sondern vom Computer generiert wird. Verwirrenderweise spricht man dann von virtueller Realität (VR).

Virtueller Speicher: Jeder Rechner enthält einen Speicherbereich, in dem die Daten, die gerade vom Rechner gebraucht werden abgelegt werden. Diesen Bereich nennt man RAM (Random Access Memory). Der Zugriff auf den RAM-Speicher ist viel schneller als der Zugriff auf die Festplatte. Die Größe des RAMs ist allerdings beschränkt (z.B. auf 256 MB). Wenn jetzt sehr viele und/oder große Dateien geöffnet sind, kann es vorkommen, dass nicht alle Dateien im RAM Platz haben. Dann wird ein Teil des RAMs auf die Festplatte ausgelagert - und zwar in die Auslagerungsdatei.

Virtual Server: Mit einem Virtual Server-System kann man durch die Zuordnung verschiedener IP-Adressen auf einem Computer mehrere Server simulieren.

Visit: Als Visit wird der Besuch einer Website durch einen Anwender

bezeichnet, der anhand seiner IP-Adresse erkannt wird.

VNC: Durch **Virtual Network Computing**-Programme ist es möglich, einen Rechner von einem anderen Rechner fernzusteuern, so als ob man direkt davor sitzt. Mit VNC-Programmen wie TightVNC oder RealVNC können Systemadministratoren die Rechner des Netzwerks von Ihrem Arbeitsplatz aus warten und konfigurieren oder Privatanwender können den heimischen PC vom Rechner am Arbeitsplatz ansteuern. Der VNC-Server überträgt den Bildschirminhalt des ferngesteuerten PCs. Auf dem Rechner des SysAdmins sorgt der VNC-Viewer dafür, dass die lokalen Mausbewegungen und Tastaturbefehle an den entfernten Rechner übertragen werden. VNC wurde von AT&T und der University Cambridge entwickelt und ist plattformunabhängig nutzbar. Es kann sogar in Browser integriert werden.

VRML: Die **Virtual Reality Modeling Language** ist wie XML und HTML eine SGML-konforme, plattformunabhängige Beschreibungssprache für dreidimensionale virtuelle Welten.

WAN: Als **Wide Area Network** wird ein Computer-Netzwerk bezeichnet, das sich über eine größere Fläche erstreckt.

Wardriver: Als Wardriver bezeichnet man (böse) Menschen, die mit einem Laptop auf dem Beifahrersitz herumfahren und nach ungesicherten **WLANs** (kabellose Netzwerke) suchen. Sind sie fündig geworden surfen sie im günstigsten Fall auf Kosten des WLAN-Betreibers. Es ist aber auch möglich, dass ein Wardriver Zugang zu Dateien auf dem Netzwerk bekommt und diese stiehlt. So können die Urlaubsbilder, die Kundendaten oder die Datei mit Passwörtern in unbefugte Hände gelangen.

Warmstart: **Neustart** des Rechners, durch (längeres) Drücken der **Reset-Taste**. Im Gegensatz zum **Kaltstart**, können speicherresidente Viren einen Warmstart überdauern.

Warwalker: Siehe Wardriver. Im Gegensatz zum Wardriver sucht der Warwalker auf der Suche nach ungesicherten WLANs auf Schusters Rappen (d.h. zu Fuß).

Webmaster: Als Webmaster wird der Verwalter eines Webangebots bezeichnet.

Webserver: Ein Server-Dienst, der Daten über das HTTP-Protokoll zur Verfügung stellt und über eine eindeutige HTTP-URL erreichbar ist. Oft wird auch der Rechner, auf dem der Server-Dienst läuft als Webserver bezeichnet. Meistens liefert ein Webserver HTML Dateien aus. Er stellt aber auch Grafiken, Stylesheets, und andere Date(ien) zur Verfügung.

Whois: In sog. Whois-Datenbanken werden Informationen zu Eigentümern und Betreibern von Domains gespeichert und über das gleichnamige Protokoll allen Internetnutzern zugänglich gemacht. So kann man z.B. herausfinden, in

welchem Land der Server für eine bestimmte IP-Adresse steht und wer ihn angemeldet hat.

WiFi: *Wireless Fidelity* ist eine Vereinigung von Unternehmen und Organisationen, die ursprünglich Wireless Ethernet Compatibility Alliance (WECA) hieß. Ziel der Organisation ist es Produkte aus dem Bereich kabelloses Netzwerk, die zwischen Ethernet und dem WLAN-Standard IEEE 802.11 vermitteln, auf Kompatibilität zu testen. Die Mitglieder vergeben für ihre Produkte ein kostenpflichtiges Prüfsiegel, sofern die Produkte den selbst erstellten Richtlinien entsprechen.

WLAN: Ein *Wireless LAN (Wireless Local Area Network)* bezeichnet ein kabelloses, lokales Netzwerk, das per Funk betrieben wird. Die meisten lokalen Funknetze basieren auf den Standards *IEEE 802.11* oder *HIPERLAN*.

WWW: Das *World Wide Web* wurde 1981 von Tim Berners-Lee am CERN entwickelt. Es ist eine Art *Unternetz* des Internet, das von WWW-Servern gebildet wird, die Daten über bestimmte Transfer Protokolle (wie z.B. HTTP) zum Abruf bereitstellen. Im Gegensatz zur früheren reinen Textdarstellung im *Internet* bietet das WWW die Möglichkeit, Textinformationen, Grafiken, Töne, Animationen, Virtuelle 3D Welten und sogar Videos im Internet zu übertragen. Eine weitere Kernfunktion ist der Einsatz von *Hyperlinks*, die das schnelle Springen zu verwandten Sites im WWW erlauben. Um sich im WWW zu bewegen, ist außer der Internet-Verbindung ein WWW-Browser notwendig. Das WWW verdrängte Bulletin Boards und Gopher fast vollständig und wurde zum Informationsträger Nummer 1. Viele Anwender die vom Internet sprechen, meinen eigentlich das WWW.

XSS: Eine Sicherheitslücke, bei der Scripte von einer Webseite in einer anderen Webseite ausgeführt werden. Der Nutzer merkt nicht, dass ein fremdes Script ausgeführt wird, da sich die angezeigte URL-Adresse nicht ändert.

ZIP: *ZIP* ist ein Dateiformat, das es ermöglicht, mehrere Dateien auch mit Unterverzeichnissen zu einem *Archiv* zusammenzufassen. Die im Archiv enthaltenen Dateien werden einzeln komprimiert. So lassen sie sich später auch einzeln wieder extrahieren. Das ZIP-Format wurde 1989 von Phil Katz als Public Domain Software entwickelt und mit den Programmen PKZIP und PKUNZIP verbreitet. Mittlerweile hat sich *ZIP* zum Synonym für ein komprimiertes Archiv entwickelt und kann von vielen anderen Packprogrammen verarbeitet werden.

Zombie-PC: Als Zombie bezeichnet man einen PC, der über eine Backdoor fernsteuerbar ist. Analog zum filmischen Vorbild gehorcht der Zombie-PC nur noch dem verborgenen Master und führt dessen oftmals verbrecherische Befehle aus. Meist werden viele Zombies zu sogenannten Botnetzen zusammengefasst.

Zoo-Viren: Viren, die nur beim 'Virenautor' und in einschlägigen

Virensammlungen (z.B. bei Virensammlern, Hersteller von Antivirensoftware oder Testern) zu finden sind, nennt man Zoo-Viren. Diese Viren tauchen nie beim Anwender, also **in the wild** auf.

Zugriffsrechte: Die Zugriffsrechte werden innerhalb eines Computersystems vom Administrator an den Nutzer vergeben, um den Handlungsspielraum des Nutzers genau zu definieren.

Fragen und Antworten (FAQ)

Hier finden Sie häufig gestellte Fragen, die Ihnen vielleicht schon bei Problemen weiterhelfen könnten.

BootScan mit der G DATA BootCD

Bereits vor der Installation: Der BootScan

Führen Sie die Installation ihrer G DATA Software nur auf einem virenfreien Computer durch. Um dies sicherzustellen, können Sie einen **BootScan** durchführen.

Sie können diesen Schritt überspringen, wenn Sie

- *über einen neuen Computer verfügen, der noch keinen Kontakt zum Internet hatte*
- *bereits vorher Ihren Rechner mit G DATA Software geschützt hatten.*

Fahren Sie in dem Fall mit der Installation fort.

Beim BootScan gehen Sie bitte folgendermaßen vor:

1. Legen Sie die G DATA Software CD in das CD/DVD-ROM-Laufwerk Ihres Computers. 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 BootCD** und bestätigen die Auswahl mit **Enter**. Der Computer wird nun auf ein Linuxsystem gebootet und es erscheint die G DATA Spezialversion für BootScans.

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

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



5. Klicken Sie hier auf **Ja** und führen Sie das Update durch. Sobald die Daten über das Internet aktualisiert wurden, erscheint die Meldung **Update erledigt**. Verlassen Sie nun den Update-Bildschirm mit Anklicken des **Schließen**-Buttons.

*Das automatische Internet Update steht Ihnen dann zur Verfügung, wenn Sie einen Router verwenden, der IP-Adressen automatisch vergibt (**DHCP**). Sollte das Internet Update nicht möglich sein, können Sie den BootScan auch mit alten Virensignaturen durchführen. Dann sollten Sie allerdings nach der Installation der G DATA Software möglichst bald einen neuen BootScan mit aktualisierten Daten durchführen. Wie das funktioniert, wird Ihnen in der Online-Hilfe im Kapitel **G DATA BootCD erstellen** erläutert.*

6. Nun sehen Sie die Programmoberfläche. Klicken Sie auf den Eintrag **Überprüfe Computer** und Ihr Computer wird nun auf Viren und Schadsoftware untersucht.

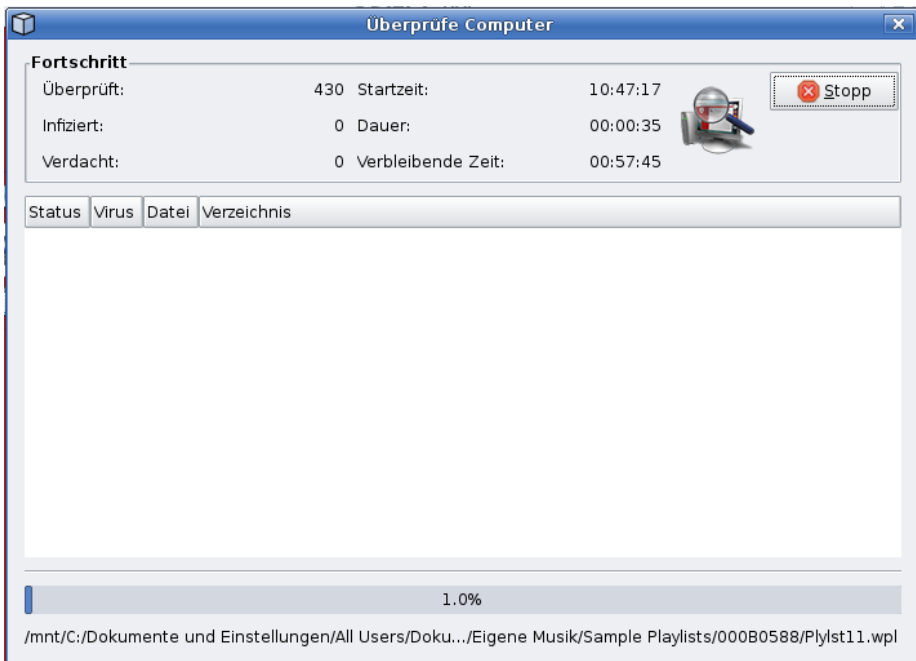


Der BootScan kann je nach Rechnerart und Festplattengröße eine Stunde

oder länger dauern.

7. Sollte die G DATA Software Viren finden, entfernen Sie die bitte mit Hilfe der im Programm vorgeschlagenen Optionen (**Virus entfernen** / **Datei löschen**).

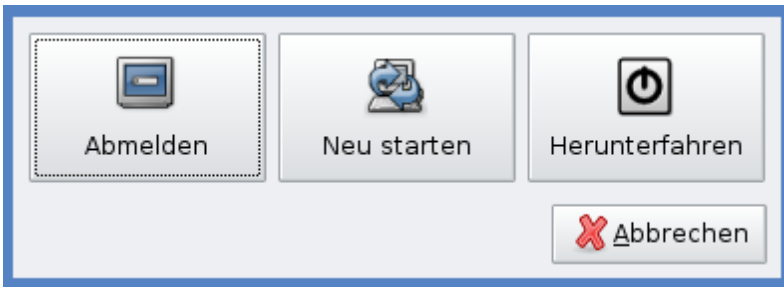
*In der Regel sollten Sie hier die Option **Virus entfernen** verwenden, da Ihnen bei einer erfolgreichen Entfernung des Virus die Originaldatei weiterhin zur Verfügung steht. Die Option **Datei löschen** sollten Sie nur dann verwenden, wenn Sie sich ganz sicher sind, dass sie die jeweilige Datei nicht mehr benötigen und diese nicht für den Betrieb Ihres Windows-Systems relevant ist.*



8. Nach Abschluss der Virenüberprüfung verlassen Sie nun bitte das System, in dem Sie auf den **Beenden**-Button klicken und anschließend **Neu Starten** auswählen.



Der **Beenden**-Button befindet sich unten rechts in der Linux-Programmoberfläche.



9. Entfernen Sie die G DATA Software CD aus den CD/DVD-Laufwerk, sobald sich das die Lade Ihres CD/DVD-Laufwerks öffnet.
10. Schalten Sie ihren Computer wieder aus und starten Sie ihn erneut. Nun startet Ihr Computer wieder mit Ihrem Standard-Windows-Betriebssystem (also z.B. Windows XP oder Windows Vista) und sie haben die Gewähr, die reguläre G DATA Software auf einem virenfreien System installieren zu können.

Die Zugangsdaten sind ungültig

1. Bitte überprüfen Sie die **Zugangsdaten** auf korrekte Eingabe. Beachten Sie Groß- und Kleinschreibung; die Zugangsdaten enthalten keine Leerzeichen.
2. Sollten Sie Ihre Zugangsdaten verlegt oder vergessen haben, so klicken Sie im Anmeldedialog auf **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 Mailadresse geschickt.

Sollte sich Ihre E-Mail-Adresse zwischenzeitlich geändert haben, so wenden Sie sich bitte an unseren Kundenservice.

Bei der Registrierung erscheint die Meldung: Registriernummer ungültig

Überprüfen Sie bitte die **Registriernummer** auf die korrekte Eingabe: je nach verwendeten Schriftsatz wird ein großes "l" (wie lda) oft als die Ziffer "1", bzw.

dem Buchstaben "l" (wie Ludwig) fehlinterpretiert. Das Gleiche gilt für: "B" und 8 "G" und 6 "Z" und 2.

Kann ich an einem neuen Rechner mit meinen Zugangsdaten Updates beziehen?

Ja. Der Updateserver richtet in dem Fall die Verbindung zu dem neuen Computer ein – der alte Computer kann fortan keine Updates mehr beziehen.

Ich habe eine Mehrfach-Lizenz. Wie kann ich diese nutzen?

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. Gehen Sie in der Software bitte auf das Modul **AntiVirus** und wählen **Optionen**.
3. Wählen Sie nun bitte den Karteireiter **Internet-Update**.
4. Tragen Sie hier bitte die **Zugangsdaten** ein, die Sie zuvor per E-Mail erhalten haben.

Kann ich zu meinem Softwarepaket auch weitere Lizenzen für mehr PCs oder weitere Funktionen erwerben?

Natürlich. Hierzu wenden Sie sich bitte an den G DATA Kundendienst.

Wie registriere ich mich mit meiner (neuen) Lizenz, so dass ich wieder Updates herunterladen kann?

Gehen Sie hierfür bitte wie folgt vor:

1. Starten Sie bitte die G DATA Software.
2. Wählen Sie im Karteireiter **AntiVirus** den Punkt **Optionen**.
3. Wählen Sie im neuen Fenster den Karteireiter **Internet-Update** und klicken auf **Am Server anmelden**.
4. Tragen Sie hier nun bitte Ihre (neue) Registriernummer sowie Ihre persönlichen Daten ein.
5. Sie erhalten nun die neuen Zugangsdaten per E-Mail zugestellt.

Bei einer Virenprüfung wurden Dateien als "not-a-virus" gekennzeichnet

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 als Hilfskomponenten eines schädlichen Programmes verwendet werden, weil sie Schwachstellen oder Fehler enthalten.

Unter bestimmten Umständen entsteht durch das Vorhandensein bzw. die Aktivität solcher Programme auf dem Computer ein Sicherheitsrisiko für Ihre Daten. 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.

Oft sind diese Anwendungen aber auch ungewollt zusammen mit anderen Programmen installiert worden. In diesem Falle können Sie sie unter **Start > Systemsteuerung** entfernen.

Einen Hinweis darauf, von welchen Programmen die gefundene Anwendung genutzt wird, gibt unter Umständen der Ordner, in dem sie sich befindet.

Deinstallationshinweise

Wenn Sie die G DATA Software irgendwann wieder deinstallieren möchten, können Sie dies am einfachsten durchführen, indem Sie im **G DATA Programmgruppeneintrag** auf das **Deinstallation**-Icon klicken. Die Deinstallation erfolgt auf diese Weise vollautomatisch. Alternativ können Sie auch über die Windows-Systemsteuerung eine Deinstallation durchführen.

- **Windows XP:** Klicken Sie in der Windows-Taskleiste auf **Start** und wählen

Sie den Ordner **Einstellungen** > **Systemsteuerung** > **Software**. Dort finden Sie auf der Karteikarte **Installieren/Deinstallieren** die Möglichkeit, die *G DATA Software* mit der Maus zu markieren. Klicken Sie dann auf den **Hinzufügen/Entfernen**-Button, um die Deinstallation durchzuführen.

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

Sollten Sie während der Deinstallation noch Dateien im **Quarantäne**-Bereich der *G DATA Software* liegen haben, erfolgt eine Abfrage, ob diese Dateien gelöscht werden sollen oder nicht. Wenn Sie die Dateien nicht löschen, befinden diese sich weiterhin in einem speziellen *G DATA Ordner* verschlüsselt auf Ihrem Computer und können auf diese Weise keinen Schaden anrichten. Diese Dateien stehen Ihnen erst wieder zur Bearbeitung 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 des Beenden-Buttons ab. Die Software ist nun vollständig von Ihrem System deinstalliert.

Index

A

- Abbrechen 11, 12
- Abgesicherter Modus 76
- Access 73
- Account 76
- Achtung 46, 53, 76
- Achtung! Diese Mail enthält folgenden Virus 56
- Active Scripting 76
- Active Server Pages 76
- ActiveX 76
- ActiveX Controls 76
- ActiveX Steuerelemente 76
- AdAware 75
- Administrator 76
- Aktionen 24, 35
- aktive Inhalte 76
- Aktualisieren 11, 32
- Alarm 45
- alle Dateien 48, 51
- Allgemeine Informationen 24
- Allgemeines 5
- Altair 62
- Am Server anmelden 16, 53
- American Standard Code for Information Interchange 76
- Amiga 62
- AmiPro 62
- Analyse-Umfang 40
- andere Antivirensoftware 11
- Ändern 13
- Angepasst 13
- angepasste Setup 13
- angepassten Setup 13
- Angepasstes Setup 13
- Anhang 60
- Anmelden 16, 53
- Anmeldung 76
- AntiSpam 13, 24, 30
- Anti-Spam Programme 75
- Anti-Spam-Blacklists 56
- Antiviren-Engines 56
- Antiviren-Viren 62
- AntiVirus 13, 15, 24, 25, 30, 31, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 48, 49, 50, 51, 53, 54, 55, 56, 57, 58, 59, 105
- AntiVirus Optionen 55
- AntiVirus Programmoberfläche 31
- AntiVirus Version 56
- AntiVirusLab 56
- AOL AIM (ab Version 4.7) 59
- API 76
- Apple II Rechner 62
- Applet 76
- Application Programming Interface 76
- Archiv 76
- Archive 46, 50
- Archive (monatliche Überprüfung) 40
- Archive prüfen 46, 48, 51
- Archivierte Dateien 19
- ARJ 76
- Art 44
- ASCII 76
- ASP 76
- Atari ST 62
- Attachment 76
- Attacke 62
- Auf Dialer / Spyware / Adware / Riskware prüfen 48, 51
- Auf Rootkits prüfen 37, 51
- auf Viren prüfen (G DATA AntiVirus) 25
- ausführbare Dateien 73
- Ausführen 38, 39, 41
- ausgehende Mails (SMTP) 57

- ausgeschaltet 31
- Auslagerungsdatei 76
- Ausnahmen 47
- Auswahl 40
- Authentifizierung 76
- Automatische Updates 32, 38
- Automatische Virenprüfungen 39
- automatischer Updates 14
- Autopilot 26
- Autopilot ausschalten 26
- Autostart 36
- Autostart.9805 62
- Autostartbereiche 40
- Autostart-Funktion Ihres CD/DVD-ROM-Laufwerks 11
- AVK 5

- B**

- Back Orifice 62
- Backdoor 70, 71
- Backdoor-Programme 75
- Backup 13, 14
- Backups 62
- BCC 76
- Beagle 72
- Bearbeiten 31, 38, 39
- Bedingungsteil 71
- Bei der Online-Registrierung erscheint die Meldung: Registriernummer ungültig 104
- Bei einer Virenprüfung wurden Dateien als "not-a-virus" gekennzeichnet 106
- Bei Systemlast die Virenprüfung pausieren 19, 51
- Beide Engines - performance-optimiert 46, 50
- Beim ersten Start 16
- Beim Schreiben prüfen 19, 48
- Beim Systemstart 41
- Benjamin 62
- benutzerdefiniert 33
- Benutzererkennung 76
- Benutzerkonten verwenden 8
- Benutzerkonto 39, 42
- Benutzername 7, 105
- Benutzernamen 7, 54
- Bericht an ausgehende Mails anhängen 56
- Bericht an empfangene, infizierte Mails anhängen 56
- BIOS 76, 100
- Bit 76
- Blended threats 73
- Blind Carbon Copy 76
- Bluetooth 62, 76
- Bookmark 76
- Boot Record 76
- BootCD 13
- BootScan 11, 13, 28, 76, 100
- BootScan mit der G DATA BootCD 100
- BootScans 11
- Bootsektor 73, 76
- Bootsektoren 48
- Bootsekturviren 73
- Bootsekturvirus 62
- BotNetze 62
- Botschaft 76
- Boza 62
- Brazil 62
- Browser Hijacker 76
- Brute-Force Angriff 76
- Bubbleboy 62, 73
- Buffer Overflow 62, 72, 76
- Bug 76
- BugBear 62
- Bulk Mail 76
- Button 76
- Byte 76

C

Cache 76
 Carbon Copy 76
 Cascade-Virus 62
 Cascading Style Sheets 76
 CC 76
 CD/DVD-ROM; C: 100
 CD-ROMs 36
 CGI 76
 CGI-Scripts 76
 CIH 62
 Client 76
 CodeRed 62, 72
 Commander Bomber 62
 Commodore 62
 Common Gateway Interface 76
 CommWarrior.A 62
 Companion Viren 73
 Companion Virus 76
 Compiler 76
 Component Object Model (COM) 76
 Computer Emergency Response Team /Coordination Center (CERT/CC) 62
 Computervirus 62
 Concept 62
 Core War 62
 Cracker 76
 CRC 76
 Cross Site Scripting 76
 CSS 76
 Cyberspace 76
 Cyclic Redundance Check 76

D

Daemon 76
 DAME 62

Dark Angel's Multiple Encryption 62
 Dark Avenger 62
 Darwin 62
 Data Encryption Standard 76
 DataCrime 62
 Datei in die Quarantäne verschieben 22, 46, 50
 Datei-Anhänge 55
 Dateien 40
 Dateien in der Quarantäne 33
 Dateimaske 47
 Dateitypen 48, 51
 Datei-Viren 73
 Datei-Virus 62
 Datenkompression 76
 Datenmanipulationen 71
 Datum der Virensignaturen 32
 DDoS 71
 Debugger 72, 76
 Defacement 76
 Deinstallation 106
 Deinstallationshinweise 106
 Deinstallieren 106
 Denial of Service 62, 71, 76
 DE-NIC 76
 DES 76
 Desinfizieren 43
 Desinfizieren (wenn nicht möglich: Anhang/Text löschen) 55
 Desinfizieren (wenn nicht möglich: in Quarantäne verschieben) 22
 Desinfizieren (wenn nicht möglich: in Quarantäne) 46, 50
 Desinfizieren (wenn nicht möglich: Zugriff sperren) 46
 DHCP 76, 100
 DHTML 76
 Dialer 48, 51, 70, 75, 76
 Dialer Control 75
 Die Anmeldung wurde erfolgreich durchgeführt 16, 53

- Die Datei wurde als infiziert gemeldet. Ich glaube
aber, dass Sie keinen Virus enthält. Bitte
untersuchen Sie die Datei 43
- Die Mail [Betreffzeile] enthält folgenden Virus:
[Virusname] Die Mail kann nicht verschickt
werden 56
- Die Zugangsdaten sind ungültig 104
- DirectX 76
- Disk And Execution MONitor 76
- Disk Operating System 76
- Disketten 36, 70, 73
- Distributed Denial of Service 71
- DMV 62
- DNS 76
- Domain 76
- Domain Name System 76
- Domain-Namen 76
- DOS 62, 71, 76
- DOS-Viren 62
- Download 76
- Drucken 12, 44
- Durchsuchen 11
- DVD-ROMs 36
- Dynamic Host Configuration Protocol 76
- Dynamic HTML 76
- E**
- Egress Filtering 76
- EICAR 62
- Eigene Dateien 35
- Eine erneute Eingabe der Registriernummer ist
hierbei nicht nötig. 7
- Einfach 44
- Einfach / Erweitert 44
- eingehende Mails (POP3/IMAP) 57
- eingeschaltet 31
- Einsenden 43
- Einstellungen 106
- Einstellungen und Protokolle 106
- Electronic mail 76
- Elk Cloner 62
- E-Mail 16, 70, 72, 73, 76
- E-Mail Archive prüfen 46
- E-Mail-Adresse 16, 53
- E-Mail-Archive prüfen 48, 51
- E-Mail-Nachricht 76
- E-Mail-Postfächer 46
- E-Mail-Prüfung 32, 55
- E-Mail-Schutz 32
- E-Mail-Viren 73
- E-Mail-Virenblocker 32
- E-Mail-Vorschaufunktion deaktivieren 8
- E-Mail-Würmer 72
- Empfangene Mails auf Viren prüfen 55
- Engines benutzen 46, 50, 56
- Entschlüsselung 72
- Erkennungsteil 71
- Erweitert 31, 44, 48, 51, 53, 57
- Erweiterte Anzeige 19
- Ethernet 76
- European Institute for Computer Antivirus
Research 62
- Excel 62, 73
- Exploit 76
- ExploreZip 62
- Extras 55, 57
- F**
- F1 5
- FAQ 76, 100
- Fast Infector 62
- FAT 76
- Favoriten 76
- Fernwartungsprogramme 75
- Festplatten 36
- File Transfer Protocol 76

Firefox 13
 Firewall 13, 24, 30, 54, 56, 76
 Firewall ausschalten 26
 Flame 76
 Flash-BIOS 62
 Flooding 76
 Foren 76
 Form 73
 Formatieren 73
 Fortschritt 19
 Fortsetzen 19
 Fragen und Antworten (FAQ) 100
 Fragezeichen-Symbol 47
 freigegebene Ordner 70
 frequently asked questions 76
 Frode Lives 62
 FTP 76
 FTP-Server 76
 Fuck 62
 Für die Datei wurde ein Virenverdacht gemeldet.
 Bitte untersuchen Sie die Datei 43

G

G DATA 8, 14, 43
 G DATA Antivirensoftware 8, 11, 12, 14, 19, 100, 106
 G DATA Antivirensoftware Version 100
 G DATA AntiVirus 5, 56
 G DATA AntiVirus 2008 37
 G DATA AntiVirus 2009 37
 G DATA AntiVirus Software 32
 G DATA AntiVirus Virenwächter 76
 G DATA BootCD 100
 G DATA BootCD - Vesa Driver 100
 G DATA BootCD erstellen 28
 G DATA Boot-CD erstellen 100
 G DATA Business Vertrieb 8
 G DATA CD/DVD-ROM 100

G DATA InternetSecurity 5
 G DATA InternetSecurity Pakets 58
 G DATA NotebookSecurity 5
 G DATA Ordner 106
 G DATA Programm-CD 28
 G DATA Programmgruppeneintrag 106
 G DATA Security-Produkt 7, 105
 G DATA Service 16
 G DATA ServiceCenter 6, 7, 8
 G DATA Software 5, 7, 11, 12, 13, 14, 15, 16, 28, 32, 37, 53, 100, 105, 106
 G DATA Software CD 11, 100
 Windows XP 100
 G DATA Software starten 26
 G DATA Software-CD 24
 G DATA Software-Version 37
 G DATA Team 43
 G DATA TotalCare 5
 G DATA Unternehmenslösungen 8
 G DATA Update-Server 6, 7, 16, 32, 37, 53
 G DATA Virenlexikon 8, 22, 43
 G DATA-Antivirensoftware 28
 G DATA-Homepage 6
 G DATA-Programmoberfläche 26
 G DATA-Website 7
 G DATA Virenlexikon 6
 Gateway 76
 Gemeinsamkeiten von Viren und Würmern 70
 Geringe Sicherheit 33
 Glossar 76
 Gnutella 62
 Good-Times 62
 Gotcha 62
 Größenbegrenzung für Downloads 58

H

Happy99 62
 häufig gestellte Fragen 76

- HBCI 76
- Header 76
- Heuristik 48, 51, 76
- Hijacker 76
- Hilfe 5
- Hintertür 70
- Hinzufügen/Entfernen 106
- Hoax 76
- Hoaxes 75
- Hoch 51
- Hoch (Kurze Laufzeit) 51
- Höchste Sicherheit 33
- Hohe Sicherheit 33
- Home Banking Communication Interface 76
- Hop 76
- Host 76
- HOSTS-Datei 32, 47
- HTML 76
- HTML-Mails 76
- HTML-Seiten 76
- HTTP 76
- <http://user:passwort@www.gdata.de/trade/productview/472/index.php?param1=0¶m2=1> 76
- HTTPS 76
- HTTP-Webinhalte 58
- Hub 76
- Hunter.c 62
- Hyper Text Transfer Protocol 76
- Hyper Text Transfer Protocol (Secure) 76
- Hyperlink 76
- Hyperlinks 76
- Hypertext 76
- HyperText Markup Language 76
- I
- I love you 62
- IANA 76
- Ich akzeptiere die Bedingungen der Lizenzvereinbarung 12
- Ich benötige Informationen zu dem gefundenen Virus. Im Virenlexikon (www.antiviruslab.com) kann ich keine Informationen finden 43
- Ich habe eine Mehrfach-Lizenz. Wie kann ich auf dem zweiten und dritten Rechner Updates laden? 105
- Ich habe eine Mehrfach-Lizenz. Wie kann ich diese nutzen? 105
- Ich habe meine Zugangsdaten verlegt! 7
- ICMP 76
- ICP 76
- IE 76
- IIS 62, 72
- Im Fall einer Infektion 42, 46, 48, 50, 55
- IMAP 76
- in the wild 62, 76
- Indexing Service DLL 62
- Infizierte Archive 46, 50
- Infizierte Datei löschen 22
- Informationen ausgespäht 71
- Installation 11, 100
- Installationsabschluss 15
- Installationsart 12
- Installieren 11, 15
- Installieren/Deinstallieren 106
- Instant Message 76
- Instant Messaging 59
- Instant Messaging (Integration in der IM-Anwendung) 59
- Integrated Services Digital Network 76
- Intended Virus 73
- Intensive Virenprüfung 19
- Internet 73, 76
- Internet Assigned Numbers Authority 76
- Internet Cache Protocol 76
- Internet Control Message Protocol 76
- Internet Explorer 13, 53, 76
- Internet Information Server 62
- Internet Message Access Protocol 76

Internet Packet Switching Protocol 76
 Internet Relay Chat-Protocol 76
 Internet Relay Chats 62
 Internet Service Provider 76
 Internet Wurm 62
 Internet-Adressen 76
 Internet-Einstellungen 54, 56
 Internetinhalte (HTTP) 58
 Internetinhalte (HTTP) verarbeiten 58
 Internet-Update 6, 7, 16, 39, 53
 Internetverbindungsaufbau 38, 39
 Internet-Zugang 39
 Inter-NIC 76
 IP-Adresse 76
 IP-Adressen 76
 IPX/SPX 76
 IRC 62, 76
 ISDN 76
 ISP 76
 itw 76

J

Java 62, 76
 JavaApplets 76
 JavaScript 76
 JavaScript Style Sheet 76
 Job 38, 40
 Joint Photographics Experts Group 76
 JPG/JPEG 76
 JScript 76
 JSSS 76

K

Kaltstart 76
 Kann ich an einem neuen Rechner mit meinen Zugangsdaten Updates beziehen? 105

Kann ich zu meinem Softwarepaket auch weitere Lizenzen für mehr PCs oder weitere Funktionen erwerben? 105
 Kaos4 62
 Karteireiter 76
 KaZaA-Netzwerk 62
 KBit 76
 KByte 76
 Keylogger 76
 Kindersicherung 13, 58
 Klez 62
 Kombi-Viren 73
 Kompression/Komprimierung 76
 Kontaktdaten 6
 Kontextmenü 76
 Konvertierung 76
 Kopierschutz 76
 Kreditkartennummern 71
 Kundendaten 7, 16, 53
 Kundennummer 6

L

LAN 76
 Laroux 62
 Lehigh 62
 Lentin 62
 Lesezeichen 76
 Letzte Analyse des Rechners 33
 Link 76
 Links 76
 Linux 62, 76
 Lizenzvereinbarung 12, 60
 Local Area Network 76
 Local Security Authority Subsystem Service 72
 Login 76
 Loginnamen 71
 logische Bombe 62
 Logoff 76

Lokale Festplatten 39
Lokale Festplatten (wöchentliche Überprüfung)
40
Lokalen Festplattenlaufwerken 40
Löschen 44
Loveletter 62
Lovsan/Blaser 72
LSASS 72

M

Mac OS 76
MAC-Adresse 76
Macintosh 62
MacMag Virus 62
MacOS 62
Mail 53
Mailbomb 76
Mailbox 76
Mailer Daemon 76
Mailingliste 76
Mailinglisten 76
Mails vor dem Senden prüfen 56
Makro-Befehle deaktivieren 8
Makro-Generatoren 62
Makrosprache 73
Makroviren 62, 73
Maltese Amoeba 62
Malware 70
Malware im weiteren Sinn 75
manuellen Analysebeginns 49
MAPI 76
MB 76
MBit 76
MBR-Viren 73
MByte 76
Media Access Control 76
MegaByte 76
mehrere Ports 57

Mehrfachlizenzen 7
Melissa 62
Message 76
Messaging API 76
Michelangelo 62
Microsoft Messenger (ab Version 4.7) 59
Microsoft Outlook 55, 57
Microsoft SQL-Server 62
Microsoft Windows 100
Millenium-Wurm 62
MIME 76
Mittlere Sicherheit 33
MMS 62
Mobiltelefone 62
Möchten Sie die Virensignaturen jetzt
aktualisieren? 32
Möchten Sie Ihren Rechner jetzt auf Viren
überprüfen? 33
Modem 75, 76
Motion Picture Experts Group 76
MPEG 76
MS-DOS 62, 76
MtE 62
Multipartite Viren 62, 73
Multipurpose Internet Mail Extensions 76
MyParty 62
MySQL 76

N

Nach Beendigung des Jobs den Rechner
ausschalten 40
Nachricht 76
nachträglich installieren 24
Nachtwächter 62
NAT 76
NED 62
NET Komponenten 76
Netiquette 76
Network Address Translation 76

Network Information Center 76
 Netzwerk 76
 Netzwerke 73
 Netzwerken 72
 Netzwerkscans 70
 Netzwerk-Würmer 72
 Netzwerkzugriffe prüfen 48
 Neu 47
 Neue Virenprüfung 39
 Neustart 15, 76
 Newsgroup 62, 76
 Newsgroups 76
 NIC 76
 Niedrig (Lange Laufzeit) 51
 not-a-virus 106
 Nuke Encryption Device 62
 NullSession 76
 Nur für Microsoft Outlook 55
 nur Programmdateien und Dokumente 48, 51
 Nur protokollieren 22
 Nutzer 76

O

ODBC 76
 Offline 76
 Offline-Reader 76
 Öffnen 44
 oligomorph 72
 Online 6, 16, 76
 Onlinebanking-Daten 62
 Online-Datenbank für häufig gestellte Fragen (FAQ) 6
 Online-Registrierung 16, 53
 Opasoft 62
 Open Database Connectivity 76
 Opera 57
 Optionen 31, 32, 45, 105
 Ordner auf Viren überprüfen 55, 57

Original-Software verwenden 8
 OS/2 76
 OutbreakShield 56
 Outlook 57, 72
 Outlook Express 57, 72

P

P2P 76
 P2P Netzwerke 62
 Packet Internet Grouper 76
 Packeting 76
 Pack-Programme 76
 Packprogrammen 76
 Pakistani-Brain 62
 Palm/Liberty-A 62
 Palm/Phage 62
 PalmOS 62
 PAP 76
 Partitionstabellen 73
 Password Authentication Protocol 76
 Passwort 7, 54, 76, 105
 Passwörter 71
 Passwortgeschützte Archive 19
 Patch 76
 Pause 19
 Payload 70, 71, 76
 Payloads 62
 Payload-Trigger 76
 PC Cyborg 62
 PC-Write 62
 PDAs 62
 PDC 76
 PDF 76
 PE Datei 76
 Peer 76
 Peer-to-Peer 73, 76
 Peer-to-Peer Netzwerke 70
 Pegasus 57

Personal Identification Number 76
persönliche Daten 71
PGP 76
Pharming 62
Phishing 62, 75, 76
PIN 76
ping 76
Platzhaltern 47
PoC-Virus 62
Point to Point Protocol 76
polymorph 72
Polymorphe Viren 62, 73, 76
POP3 76
POP3/IMAP basierte E-Mail-Programme 57
POP-Protokolls 76
Popup 76
Popup Blockern 76
Port 57, 76
Portable Document Format 76
Portable Executable 76
Port-Adressen 59
Posting 76
Post-Office Protocol 3 76
PowerPoint 73
PPP 76
Pretty Good Privacy 76
Pretty Park 62
Primary Domain Controller 76
Priorität Scanner 51
Private Key 76
Programm deinstallieren 106
Programmaufbau 24
Programmbereich 30
Programme 106
Programmeinstellungen und Protokolle beibehalten 11
Programme-Verzeichnis 15
Programm-Update 37
Proof of Concept 62

Protokoll 76
Protokoll anfertigen 38, 51
Protokolle 30, 38, 44, 51
Provider 76
Proxy 76
Proxyserver 54, 56
Public Key 76

Q

Quarantäne 22, 42, 46, 50, 106
Quellcode 76
Quicktime 76

R

RADIUS 76
RAR 76
RATs 70
Raubkopie 76
Rechner prüfen 35
Rechner wöchentlich auf Viren prüfen 14
Rechnerneustart 15
regedit 76
Regelmäßige Windows-Updates 8
Registerkarte 76
Registrierdatenbank 76
Registriernummer 6, 7, 16, 53, 104
Registry 76
Re-Mailer 76
Remote Access Trojans 70
Remote Dial-In User Service 76
Reply 76
Reproduktionsteil 70
Request For Comment 76
Reset-Taste 76
RFC 76
Rich Text Format 76
Robot 76

Rootkit 28, 37
 Rootkits 28, 37, 51, 70, 100
 Rootkit-Software 62
 Router 76
 Routing 76
 RTF 76
 Rugrat 62

S

S/MIME 76
 Saddam-Hussein 62
 Schadensfunktion 70
 Schadensfunktion eines Virus 76
 Schadensfunktionen 71
 Schadensteil 71
 Schließen 16, 19
 Schnellanmeldung 16
 Schnelle Virenprüfung (empfohlen) 19
 Schreibzugriff 36
 Schutzmechanismen 73
 SCR-Dateien 62
 Scriptsprachen 76
 Secure Electronic Transaction 76
 Secure MIME 76
 Secure Sockets Layer Protocol 76
 Secure Sockets Layer-Protocol 76
 Security-Symbol 15, 26, 31
 Security-Symbols 45
 Sektor 76
 Self Mutating Engine 62
 Server 76
 Serverportnummer 57
 Serverportnummer(n) 59
 Service Packet Switching Protocol 76
 SET 76
 setup 11
 setup.exe 11
 Setup-Typ 13

SGML 76
 Short Messages Service 76
 Shredder 13
 Sicherheit / Performance 33
 Simple Mail Transfer Protocol 76
 Site 76
 Slash 76
 SMB 76
 Smeg.Pathogen 62
 Smeg.Queen 62
 SMS 76
 SMTP 76
 SMTP-Mailengine 72
 Snail-Mail 76
 Sniffer 76
 Sober 72
 Sobig 62
 Sobig.F 62
 Social Engineering 76
 Software 106
 Software aus dem Internet mit Vorsicht
 behandeln 8
 Software-Aktualisierungen 37
 Sourcecode 76
 Spacefiller, Chernobyl 62
 Spam 75, 76
 Spam-Mails ignorieren 8
 Spammer 76
 Speicher 36, 40
 Speicher und Autostart 36
 speicheresident 73
 Speicherkarten 36
 Speichern unter 44
 SpyBot-Search&Destroy 75
 Spyware 70, 75, 76
 SpywareBlaster 75
 Spyware-Komponente 62
 SQL 76
 SSH 76

SSL 76
SSLP 76
Stages of Life 62
Standard 57
Standard Generalized Markup Language 76
ständige Virenprüfung im Hintergrund 45
Start 106
Startleiste 76
Startzeit 44
Statistik 26
Status 24, 30, 31, 44
Stealth-Viren 73, 76, 100
Steganografie 76
Sternchen-Symbol 47
Strange Brew 62
Structured Query Language 76
Subdomain 76
Subject 76
Support 7
Symbian 62
Symbian Smartphones 62
Symbols auf Ihrem Desktop 15
SysOp 76
Systembereiche beim Medium-Wechsel prüfen 48
Systembereiche beim Systemstart prüfen 48
Systembereiche prüfen 51
Systemschutz 32
Systemschutz und Autostart-Überwachung 47
Systemsteuerung 106
Systemvoraussetzungen 10

T

Tab 76
Tabbed Browsing 76
Täglich 41
Tanatos 62
Tannenbaum 62

TAPI 76
Tarnkappen-Viren 73, 76
Tarnungsteil 72
Taskleiste 26, 57
Tastatureingaben 76
TCP/IP 76
technische Fragen 8
Telephony API 76
Telnet 76
Tequila 62
Terminal 76
Threads 76
Thumbnail 76
Thunderbird 57
Tipps zur Virenprophylaxe 8
Titel 44
TLD 76
Toolkit 62
Top Level Domain 76
TopSecret 10, 13
TPE 62
Traceroute 76
Transmission Control Protocol/Internet Protocol 76
Trialversion installieren 12
Trident Polymorphic Engine 62
Trillian (ab Version 3.0) 59
Trojaner 62, 70, 76
Trojanern 76
Trojanische Pferd 62
Trojanische Pferde 70
Trojanisches Pferd 70, 76
Tuner 13
Tunneling 76

U

UCE 76
UNBEDINGT VOR DER INSTALLATION 11

Ungelesene Mails beim Programmstart prüfen 55
 Uniform Resource Identifier 76
 Uniform Ressource Locator 76
 Universal Serial Bus 76
 UNIX 76
 Unsolicited E-Mail 76
 Update 53
 Updates 38
 Updates durchführen 16
 Upload 76
 URI 76
 URL 76
 USB 76
 USB-Sticks 36, 70
 Usenet 62, 76
 User 76
 User-Identification 76

V

V2Px 62
 VB-Script 76
 VB-Script-Wurm VBS/KAKworm 62
 Verschlüsselungsroutinen 73
 Versionsinformation 56
 Versionsprüfung 54
 Verzeichnisse 40
 Verzeichnisse/Dateien prüfen 35, 36
 Vesa Driver 100
 Vienna 62
 Virdem 62
 Viren 70, 73
 Viren, polymorphe 76
 Viren, Stealth 76
 virenfreien System 11
 Virenfund 22
 Virengeschichte 62
 Vireninformation 22

Virenkategorien 70
 Virenprüfung 19, 41, 49, 50
 Virenprüfungen 38
 Virensignatur 76
 Virensignaturen 32, 37, 38, 62
 Viren-Update 26, 37
 Viren-Update stündlich laden 14
 Virenverdacht überprüfen 8
 Virenwächter 19, 31, 58
 Virenwächters 19
 Virtual Network Computing 76
 Virtual Reality Modeling Language 76
 Virtuell 76
 Virtueller Speicher 76
 VIRUS 56
 Virus Bulletin 62
 Virus Construction Kit für DOS 62
 Virus Hoaxes 62
 Virus News 56
 VIRUS-L/comp.virus-Mailingliste und -Newsgroup 62
 VIRUS-L-FAQ 62
 Virtual Server 76
 Visit 76
 Visual Basic 73, 76
 VNC 76
 Vollständig 13
 Vollständige Anmeldung 16
 vollständige Setup 13
 vollständigen Installation 13
 Vollversion installieren 12
 vor der Installation 100
 Voransicht einer HTML-Mail 73
 Vorgängerversionen 11
 VRML 76
 VX (Virus Exchange) Bulletin Boards 62

W

- W32/SQL-Slammer 62
- W95/MTX 62
- Wächter 26, 31, 45, 50
- Wächter Ausnahmen 47
- Wächter ausschalten 26
- Wächterstatus 45
- WAN 76
- Wardriver 76
- Warmstart 76
- Warum erscheint bei einer Registrierung die Meldung Das Produkt wurde bereits registriert?
7
- Warwalker 76
- Was ist eine Boot-CD? 100
- Web / IM 58
- WebFilter 13, 58
- Webmaster 76
- Webserver 76
- Wechselmedien 36
- Wechselmedien prüfen 36
- Weiter 12
- Werbe-E-Mail 75
- Whois 76
- Wide Area Network 76
- Wie kann mein Computer von CD/DVD-ROM booten? 100
- Wie registriere ich mich mit meiner (neuen) Lizenz, so dass ich wieder Updates herunterladen kann? 105
- WiFi 76
- Wildlist 62
- Wildlist Organization 62
- Willkommen 12
- WinCE4Dust.A 62
- Windows 62
- Windows CE 62
- Windows Kontextmenü 25
- Windows Vista 76, 100, 106
- Windows XP 106
- Windows-Registry 32, 47
- Wireless Fidelity 76
- Wireless LAN 76
- Wireless Local Area Network 76
- WLAN 76
- WLANS 76
- Wm.Concept 62
- Wochentage 41
- Wöchentliches Backup erstellen 14
- Word 62, 73
- World Wide Web 76
- Wurm 62, 72
- Würmer 70, 72
- WWW 76
- www.antiphishing.org 75
- www.Antiviruslab.com 76
- www.wildlist.org 76

X

- XSS 76

Z

- Zeitersparnis 51
- Zeitplan 14, 32, 35, 38, 54
- Zeitplans 49
- Zeitplanung 38, 39, 41
- Zeitpunkt 38, 39, 41
- Zeitüberschreitung beim Mail-Client vermeiden
57
- Zeitüberschreitung im Browser vermeiden 58
- Zielordner 13
- Zielverzeichnis 13
- ZIP 76
- Zombie-PC 62, 76
- Zoo-Viren 76

Zugang 71

Zugangsdaten 7, 16, 53, 54, 104, 105

Zugriff 70

Zugriff verweigert 19

Zugriffsrechte 76

Zurückbewegen 43