
Inhoudsopgave

De eerste stappen	2
Installatie	3
Na de installatie	5
SecurityCenter	6
Virusbeveiliging	8
Virushandtekeningen	10
Webbeveiliging	11
Instellingen	12
Wetenswaardigheden	21

De eerste stappen

Beste gebruiker,

Het doet ons genoegen dat u voor een product van G Data hebt gekozen en wij hopen dat u tevreden bent over uw nieuwe software. Als iets niet meteen duidelijk is, kan onze Help-documentatie u wellicht op weg helpen. Voor overige vragen, opmerkingen en feedback kunt u terecht bij onze experts in het **G Data ServiceCenter** .

Deze beknopte gebruiksaanwijzing helpt u bij het installeren van uw nieuwe G Data-software en geeft u een paar praktische tips.



Hebt u nog vragen? In de software kunt u op elk moment de uitgebreide Help-documentatie raadplegen. Druk hiervoor in het programma op de **F1**-toets of klik op de hier afgebeelde Help-knop.

ServiceCenter

Het installeren en bedienen van de G Data-software is eenvoudig en wijst zich vanzelf. Als zich toch een probleem zou voordoen, kunt u contact opnemen met de deskundige medewerkers van ons ServiceCenter:

www.gdata.nl

Installatie

Voor een vlekkeloze werking van de software moet uw computer afhankelijk van het besturingssysteem aan een van de volgende **minimumvereisten** voldoen:

- Microsoft Windows 7/Vista (32/64 bit), 1 GB beschikbaar werkgeheugen,
- Microsoft Windows XP (SP2 of hoger, 32 bit), 512 MB beschikbaar werkgeheugen.

Wanneer uw computer gloednieuw is of al door antivirussoftware werd beveiligd, kunt u de installatie via de volgende stappen uitvoeren. Als u echter vermoedt dat uw computer al met een virus geïnfecteerd is, is het aanbevolen voor de installatie van de G Data-software een **BootScan** uit te voeren. Lees hiervoor ook het hoofdstuk **BootScan**.

Stap 1

Naast de klassieke installatie van software via cd's of dvd's zijn er inmiddels ook andere mogelijkheden om software te installeren:

- **Installatie vanaf cd/dvd:** Om de installatie te starten, plaatst u de G Data-software-cd of -dvd in het cd- of dvd-station. Automatisch wordt een installatievenster geopend.
- **Installatie vanaf USB-stick:** Als u de software op een USB-stick hebt gekocht, sluit u de USB-stick aan op uw computer. Automatisch wordt een installatievenster geopend.
- **Software downloaden:** Om de installatie van een via internet gedownloade versie van de software te starten, dubbelklikt u op het gedownloade bestand. Automatisch wordt een installatievenster geopend.

Stap 2

Klik nu op de knop **Installeren**. Een wizard begeleidt u nu bij de installatie van de software op uw computer.

Stap 3

Tijdens de installatie wordt de **productactivering** uitgevoerd. Hier kunt u de software activeren.

- **Registratienummer invoeren:** Als u de G Data-software voor de eerste keer installeert, selecteert u deze optie en voert u vervolgens het registratienummer van het product in. Afhankelijk van het product vindt u dit registratienummer bijvoorbeeld op de achterkant van de gebruikershandleiding, in de bevestigingsmail bij de software-download of op het insteekhoesje van de cd.

Wanneer u het registratienummer invoert, wordt het product geactiveerd en ontvangt u bovendien per e-mail de toegangsgegevens die u later kunt gebruiken.

Indien er zich problemen voordoen bij het invoeren van het registratienummer, controleer dan of het registratienummer correct is ingegeven. Afhankelijk van het gebruikte lettertype wordt een hoofdletter "I" (als in Ida) vaak voor het cijfer "1" of de letter "l" (als in Lodewijk) aangezien. Hetzelfde geldt voor: "B" en "8", "G" en 6, "O" en "0", "Z" en "2".

- **Toegangsgegevens invoeren:** Als u de G Data-software al eens hebt geactiveerd, hebt u toegangsgegevens (**gebruikersnaam** en **wachtwoord**) ontvangen. Als u de G Data-software opnieuw wilt installeren of – bij meervoudige licenties – andere computers wilt aanmelden, voert u hier de toegangsgegevens in.

Toegangsgegevens worden uitsluitend per e-mail verzonden. Bij het product zitten geen toegangsgegevens.

Als u uw toegangsgegevens niet meer vindt of vergeten bent, klik dan in de aanmelding op **Toegangsgegevens kwijt?** Er wordt een website geopend waar u uw registratienummer opnieuw kunt invoeren. Wanneer u het registratienummer hebt ingevoerd, ontvangt u de toegangsgegevens op het e-mailadres dat u bij de registratie hebt opgegeven. Als uw **e-mailadres** intussen is gewijzigd, neemt u contact op met ons **ServiceCenter**.

- **Testversie:** Als u gratis wilt kennismaken met de G Data-software, kunt u toegangsgegevens aanvragen voor een beperkte testversie. Geef een geldig e-mailadres en uw naam op en u ontvangt de toegangsgegevens per e-mail.
- **Later activeren:** Als u de software gewoon eens wilt bekijken, kunt u deze ook installeren zonder gegevens in te voeren. In dat geval worden er echter geen updates van internet gedownload en is uw computer dus niet afdoende beschermd tegen schadelijke software. U kunt uw registratienummer of toegangsgegevens altijd achteraf nog invoeren zodra u een update uitvoert.

De G Data-software kan uw computer alleen effectief beschermen als er dagelijks updates worden uitgevoerd. Als u de software gebruikt zonder deze te activeren, wordt uw computer onvoldoende beschermd.

Stap 4

Na de installatie moet u mogelijk uw computer opnieuw opstarten. Daarna is de G Data-software klaar voor gebruik.



Als de installatie niet van start gaat: Het is mogelijk dat u de **functie voor automatisch starten** van uw computer niet op de juiste manier hebt ingesteld. Als u in dat geval de programma-cd plaatst (of de USB-stick aansluit bij de USB-versie van de G Data-software), kan de software de installatie niet automatisch starten en wordt er geen venster geopend waarmee u de G Data-software kunt installeren.

- Wanneer in plaats daarvan een keuzevenster voor een automatische weergave wordt geopend, klikt u de optie **AUTOSTRT.EXE uitvoeren**.
- Als er geen keuzevenster wordt geopend, zoekt u via Windows Verkenner de gegevensdrager met de G Data-software en start u het bestand **Setup** of **Setup.exe**.

Het installatievenster van de G Data-software wordt geopend en u kunt met de installatie beginnen.

Na de installatie



Om de interface van de software te openen, dubbelklikt u op het hier afgebeelde **bureaubladsymbool**. Hoe u het SecurityCenter gebruikt, leest u in het hoofdstuk: [SecurityCenter](#).



G Data-symbool: De G Data-software beschermt uw computer constant tegen schadelijke software en aanvallen. Het G Data-symbool in de taakbalk van uw computer geeft aan wanneer u als gebruiker actie moet ondernemen via de software. Meer informatie vindt u in het hoofdstuk: [Wat is de functie van het G Data-symbool?](#)

Snelcontrole: Met de snelcontrole kunt u bestanden heel eenvoudig controleren zonder de software te hoeven starten. Selecteer met de muis bestanden of mappen, bijvoorbeeld in Windows Verkenner. Als u op de rechtermuisknop klikt, wordt een dialoogvenster geopend. Selecteer **Op virussen controleren**. Nu worden de betreffende bestanden automatisch op virussen gecontroleerd.



G Data Shredder: Als u tijdens de installatie de shredder hebt geselecteerd, wordt deze weergegeven als symbool op uw bureaublad. Gegevens die u in de shredder plaatst, worden verwijderd en kunnen niet worden teruggehaald, ook niet met professionele tools voor gegevensherstel. U kunt ook met de rechtermuisknop op een bestand klikken en **Shredderen** selecteren. De shredder is niet beschikbaar in de programmaversie **G Data AntiVirus**.





Uw computer start na de installatie van de G Data-software niet op de gebruikelijke manier: Als u de G Data-software hebt geïnstalleerd, de computer vervolgens opnieuw hebt opgestart en Microsoft Windows niet meteen wordt gestart, is het mogelijk dat de G Data-cd nog in het station zit. Deze cd dient ook als opstart-cd waarmee een BootScan kan worden uitgevoerd voordat het besturingssysteem start. Als u de cd uit het station haalt, start uw computer weer zoals u gewend bent. Meer informatie vindt u in het hoofdstuk: [BootScan](#)

SecurityCenter

Na de installatie werkt de viruscontrole in principe volledig automatisch. U hoeft het SecurityCenter alleen maar te openen als u een van de vele extra functies van de software wilt gebruiken. Zodra u zelf bepaalde handelingen moet uitvoeren, wordt u hiervan automatisch op de hoogte gebracht via de informatie in de taakbalk van uw computer.


Met één klik kunt u mogelijke gevaren voor uw computer uit de weg ruimen. Dat doet u via het symbool **Beveiligingsstatus**.

-  Zolang naast **Beveiligingsstatus** een groen vinkje wordt weergegeven, is uw systeem beveiligd.
-  Een rood uitroepteken wijst op direct gevaar voor uw systeem. U moet dan zo snel mogelijk maatregelen nemen om de beveiliging van uw gegevens te blijven waarborgen.



Als u op de knop **Corrigeren** klikt, ziet u welke acties u moet ondernemen om uw systeem weer optimaal te beveiligen. Selecteer de getoonde acties een voor een tot de beveiligingsstatus weer groen oplicht. De knop wordt dan automatisch inactief en kan pas weer worden gebruikt als de beveiligingsstatus opnieuw verslechtert. De software is nu up-to-date en u kunt het SecurityCenter weer sluiten. Verder zijn er nog de volgende statusmeldingen:

-  Een geel symbool geeft aan dat u op korte termijn moet ingrijpen.
-  Het jokerteken geeft aan dat u de desbetreffende beveiligingsfunctie (bijvoorbeeld de spambeveiliging) niet hebt geactiveerd.

Alle functies en instellingen die u onder het Beveiligingsstatus-symbool ziet (zoals **Viruscontrole** of **Virushandtekeningen**), kunt u gebruiken als u zich actief met de beveiliging van uw systeem wilt bezighouden – maar dat is niet verplicht! Beslis zelf in welke mate u bij het thema virusbeveiliging betrokken wilt zijn. In de verschillende venstergedeelten ziet u in detail welke onderdelen van de software optimaal zijn ingesteld en welke eventueel moeten worden verbeterd. De volgende symbolen verwijzen naar het beveiligingsniveau van het betreffende deel.

-  **Instellingen:** Als u rechtsboven op deze knop klikt, krijgt u toegang tot alle instellingendialoogvensters voor de verschillende onderdelen van de software. Vanuit een bepaald onderdeel kunt u echter ook direct het bijbehorende instellingendialoogvenster selecteren. Meer informatie hierover vindt u in het hoofdstuk: [Instellingen](#)

Rechts van het instellingensymbool vindt u de volgende extra functies:

-  **Help tonen:** U kunt in de software op elk moment de uitgebreide Help-documentatie raadplegen. Druk hiervoor in het programma op de F1-toets of klik op de hier afgebeelde Help-knop.
-  **Logboeken:** Hier vindt u de logboeken over alle recentelijk uitgevoerde acties (viruscontrole, update, gevonden virussen enzovoort).
-  **Opstart-cd maken:** De opstart-cd is een handig hulpmiddel om besmette computers weer virusvrij te maken. Vooral bij computers die voor de installatie van de G Data-software niet tegen virussen waren beveiligd, is het aanbevolen een opstart-cd te gebruiken. Hoe u een **opstart-cd** maakt en gebruikt, leest u in het hoofdstuk: [BootScan voor de installatie](#).

Beschikt u niet over de beschreven functies zoals het maken van een opstart-cd? Het is mogelijk dat u de optie **Opstart-cd maken** bij de installatie van de G Data-software niet hebt geïnstalleerd. U kunt deze optie ook eenvoudig achteraf installeren. Plaats hiervoor de software-cd in het station en voer de installatie met de optie Opstart-cd uit.



Programma bijwerken: Als er nieuwe versies van de software beschikbaar zijn, kunt u de software net als de virusinformatie met één klik op de muis bijwerken. Als u dus hier de melding krijgt dat er een update beschikbaar is, klikt u gewoon op **Programma bijwerken**.

Problemen met de internetupdate? Dit thema komt uitgebreid aan bod in het hoofdstuk: **Updates**



Info: Hier vindt u informatie over de **programmaversie**. Het is bijvoorbeeld handig het versienummer bij de hand te hebben als u contact opneemt met het **ServiceCenter**.

Licentie

Onder het opschrift **Licentie** aan de linkerkant van de programma-interface ziet u hoe lang uw licentie voor virusupdates nog geldig is. Bij geen enkele andere software zijn updates zo belangrijk als bij antivirussoftware. Voordat uw licentie verloopt, wordt u er automatisch aan herinnerd dat de licentie moet worden verlengd. Dat kan gemakkelijk en probleemloos via internet.

Wat gebeurt er bij afloop van mijn licentie?

Een paar dagen voor uw licentie verloopt, verschijnt een informatievenster op de taakbalk. Als u hierop klikt, wordt een dialoogvenster geopend waarin u de licentie via een paar eenvoudige stappen direct kunt verlengen. Klik op de knop **Nu kopen**, vul uw gegevens in en uw computer is onmiddellijk weer beschermd tegen virussen. De factuur ontvangt u een aantal dagen daarna per post.

Dit dialoogvenster verschijnt alleen na afloop van het eerste jaar. Daarna wordt uw G Data -licentie elk jaar automatisch verlengd. U kunt dit abonnement echter te allen tijde zonder opgave van redenen opzeggen.

Hoe kom ik in het bezit van extra of uitgebreide licenties?

U kunt natuurlijk altijd extra licenties aanvragen of upgraden naar een product met meer functies. Wanneer u in het SecurityCenter op het item **Licenties uitbreiden** klikt, wordt u rechtstreeks naar de website van onze onlineshop geleid.

Copyright © 2011 G Data Software AG

Engine A: De virusscan-engine en de spywarescan-engines zijn op BitDefender-technologieën gebaseerd © 1997-2011 BitDefender SRL.

Engine B: © 2011 Alwil Software

OutbreakShield: © 2011 Commtouch Software Ltd.

[G Data - 06.07.2011, 11:05]

CPU-belasting

Onder het opschrift **G Data** ziet u de huidige belasting van uw computer door de software. Onder het opschrift **Systeem** daaronder ziet u de huidige totale belasting van uw computer. Tijdens controles kan de G Data-software uw systeem in hoge mate belasten. In de normale bewakersmodus heeft de G Data-software echter weinig invloed op het prestatievermogen van de processor. Als uw computer trager reageert dan normaal, ziet u hier in één oogopslag of de G Data-software net een intensieve controle uitvoert of dat de oorzaak van de vertraging buiten de systeemcontrole ligt.

Standaard is de G Data-software overigens zo ingesteld dat uw computer alleen wordt gecontroleerd als u er niet mee werkt. Net zoals bij een screensaver wordt de viruscontrole dus alleen uitgevoerd als u er niet door wordt gestoord. De permanente virusbeveiliging van de virusbewaker is natuurlijk wel altijd volledig geactiveerd.

- **Viruscontrole:** De regelmatige controle van uw computer op virussen of schadelijke programma's.
- **Virusbewaker:** De continue bescherming van uw computer tegen schadelijke software.

Virusbeveiliging

Hier ziet u wanneer uw computer voor het laatst op virussen is gecontroleerd en of de virusbewaker het systeem momenteel actief tegen infecties beschermt.

Laatste viruscontrole

Hier kunt u zien, wanneer uw computer voor het laatst volledig op virussen werd gescand. Een rode aanduiding betekent dat u zo snel mogelijk een viruscontrole moet uitvoeren. Klik op de aanduiding, vervolgens kunt u de controle starten door op de knop **Computer nu controleren** te klikken. Na de controle is de aanduiding groen, d.w.z. dat de viruscontrole recent gebeurde.

Hoe een viruscontrole precies werkt en wat u moet doen als u daadwerkelijk een virus vindt, leest u in het hoofdstuk: **Wat gebeurt er bij een viruscontrole?**

Virusbewaker

De virusbewaker moet steeds geactiveerd zijn. Wilt u de bewaker toch een keertje uitschakelen of iets aan de instellingen wijzigen, klik dan de optie **Virusbewaker uitschakelen** aan.

Viruscontrole en virusbewaker: Beide functies beschermen uw computer tegen infecties, maar de manier waarop ze dat doen verschilt.

- De **virusbewaker** scant uw computer doorlopend op virussen en controleert schrijf- en leesprocessen. Zodra een programma probeert schadelijke functies uit te voeren of schadelijke bestanden te verspreiden, wordt dat door de bewaker verhinderd. De virusbewaker is uw belangrijkste bescherming! Schakel hem nooit uit.
- De **viruscontrole** is een bijkomende bescherming. Deze functie controleert of zich niet toch een virus in het systeem bevindt. Met een viruscontrole worden ook virussen gevonden die op uw computer zijn gekopieerd voordat u de G Data-software had geïnstalleerd of die in uw systeem zijn terechtgekomen toen de virusbewaker een keer niet was ingeschakeld. Het is belangrijk dat er regelmatig een viruscontrole wordt uitgevoerd. Dit kan het beste automatisch gebeuren op tijdstippen dat uw computer niet wordt gebruikt.

Keuzemenu

Als u op het kopje **Virusbeveiliging** klikt, opent u een keuzemenu met acties die u direct kunt uitvoeren.



Computer controleren: Als u naast de automatische controle een eigen controle wilt uitvoeren (vanwege een actuele virusverdenking bijvoorbeeld), klikt u op deze optie. Uw computer wordt dan meteen op virussen gescand. Raadpleeg ook het hoofdstuk: **Wat gebeurt er bij een viruscontrole**.

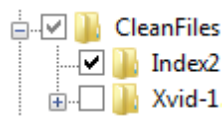


Geheugen en automatisch starten controleren: Hiermee worden voor alle lopende processen de programmabestanden en programmabibliotheken (DLL's) gecontroleerd. Schadelijke programma's kunnen zodoende direct uit het **geheugen** en het gedeelte **Automatisch starten** worden verwijderd. Actieve virussen kunnen dus direct worden verwijderd, zonder dat u de complete vaste schijf hoeft te doorzoeken. Aangezien deze controle relatief snel kan worden uitgevoerd, is het raadzaam deze bijvoorbeeld binnen het kader van een automatische viruscontrole regelmatig uit te voeren. Deze functie is een aanvulling en geen vervanging van een regelmatige virusscan van opgeslagen gegevens.



Mappen/bestanden controleren: Hiermee controleert u de geselecteerde stations, mappen of bestanden op virussen. Als u op deze optie klikt, opent u een venster waarin u mappen en bestanden kunt selecteren. Hier kunt u gericht afzonderlijke bestanden, maar ook hele mappen op virussen controleren.

In de mappenstructuur kunt u mappen openen en selecteren door te klikken op de (+)-symbolen. Hun inhoud wordt dan in het bestandsoverzicht weergegeven. De mappen en bestanden waarvoor u een vinkje plaatst, worden gecontroleerd. Als in een map niet alle bestanden worden gecontroleerd, staat bij deze map een grijs vinkje.



Verwisselbare media controleren: Met deze functie kunt u **cd-roms**, **dvd-roms**, **geheugenkaarten** en **USB-sticks** op virussen controleren. Als u deze actie aanklikt, worden alle verwisselbare media die met uw computer zijn verbonden (d.w.z. ook geplaatste cd's en geheugenkaarten of de via USB-poort verbonden harde schijven of USB-sticks) gecontroleerd. Houd er rekening mee dat u met de software natuurlijk geen virussen kunt verwijderen van media die geen schrijftoegang toestaan (zoals gebrande cd-roms). Hier worden de gevonden virussen vervolgens bijgehouden.



Op RootKits controleren: **RootKits** proberen gebruikelijke virusherkenningsmethodes te snel af te zijn. U kunt met deze functie doelgericht naar rootkits zoeken zonder een volledige controle van de harde schijven en opgeslagen gegevens te hoeven uitvoeren.



Afwezigheidsscan uitschakelen: Terwijl de virusbewaker uw systeem permanent beschermt tegen infecties door schadelijke software, controleert de **afwezigheidsscan**, een intelligente viruscontrole, alle bestanden op uw computer steeds opnieuw op virussen. De afwezigheidsscan werkt net zoals een screensaver alleen wanneer u de computer even niet gebruikt en stopt meteen als u weer aan het werk gaat. De scan staat de prestaties van de computer dus niet in de weg.

Uw computer wordt uiteraard altijd door de virusbewaker tegen virusaanvallen beschermd, ook als de afwezigheidsscan is uitgeschakeld. Dit kan bijvoorbeeld zinvol zijn als u de viruscontrole op uw systeem liever handmatig wilt starten.



Virusbewaker uitschakelen: Hiermee kunt u de **virusbewaker** uitschakelen en ook weer inschakelen. Dit kan bijvoorbeeld nuttig zijn als op uw harde schijf grote hoeveelheden gegevens van de ene naar de andere plaats moeten worden gekopieerd of bij intensieve processen (bijv. bij het kopiëren van een dvd). Schakel de virusbewaker echter niet langer uit dan strikt noodzakelijk. Zorg er zo mogelijk voor dat het systeem gedurende deze tijd niet met internet verbonden is of toegang heeft tot nieuwe, niet-gecontroleerde gegevens (bijvoorbeeld via cd's, dvd's, geheugenkaarten of USB-sticks).



Quarantaine: De quarantaine is een afgeschermd gedeelte binnen de software, waarin de besmette bestanden gecodeerd worden opgeslagen. Op die manier kan het virus niet verder worden verspreid. Lees hierover ook het hoofdstuk: **Hoe werkt de quarantaine?**



Instellingen: Met deze knop kunt u de instellopties weergeven. Raadpleeg voor meer informatie het hoofdstuk: **Instellingen - AntiVirus**

Virushandtekeningen

In dit gedeelte vindt u informatie over de programma-updates.

Laatste update

Hier ziet u wanneer uw computer voor het laatst recente virushandtekeningen via internet heeft ontvangen. Een rode aanduiding betekent dat u zo snel mogelijk een virusupdate moet uitvoeren. Klik daarvoor op de aanduiding en selecteer de optie **Virushandtekeningen bijwerken**.

Volgende update

Onder dit kopje ziet u wanneer de volgende update wordt uitgevoerd.

Virushandtekeningen: Virussen en andere schadelijke programma's zijn te herkennen aan specifieke kenmerken. De G Data-software bevat functies waarmee virussen ook op basis van hun gedrag kunnen worden opgespoord. Met een virushandtekening – de definitie van een virus – kan het desbetreffende schadelijke programma echter vele malen sneller en effectiever worden gedetecteerd en bestreden. Voor een optimale virusbeveiliging moeten deze definities regelmatig worden bijgewerkt via de G Data-databases op internet.

Keuzemenu

Als u op het kopje **Virushandtekeningen** klikt, opent u een keuzemenu met acties die u direct kunt uitvoeren.



Virushandtekeningen bijwerken: Normaal gesproken worden de updates van de virushandtekeningen automatisch uitgevoerd. Als u een update direct wilt uitvoeren, klikt u op deze knop.



Automatische updates uitschakelen: Selecteer deze optie als u niet wilt dat de G Data-software de virushandtekeningen automatisch up-to-date houdt. Bedenk wel dat uitschakeling van automatische updates een hoog veiligheidsrisico met zich meebrengt. Selecteer deze optie dus alleen in uitzonderlijke gevallen.



Instellingen: Met deze knop kunt u de instellopties weergeven. Raadpleeg voor meer informatie het hoofdstuk: [Instellingen - AntiVirus](#)

Webbeveiliging

In dit gedeelte kunt u de webbeveiliging in- of uitschakelen. De webbeveiliging is een module die tijdens surfen en downloaden op internet automatisch bedreigingen herkent en onschadelijk maakt. De webbeveiliging werkt als nuttige ondersteuning voor de virusbewaker: de module blokkeert schadelijke websites en downloads al voordat ze kunnen worden opgeroepen.

Als een internetpagina door de G Data-software als bedreiging wordt herkend en geblokkeerd, krijgt u in plaats van de website een informatiepagina van G Data in de browser te zien.

Keuzemenu

Als u op het kopje **Webbeveiliging** klikt, opent u een keuzemenu met acties die u direct kunt uitvoeren.

Uitzonderingen vastleggen: De webbeveiliging zorgt ervoor, dat u op het internet niet het slachtoffer wordt van geïnfecteerde of misleidende websites. Heel af en toe kan het voorvallen dat een internetsite niet juist wordt weergegeven, hoewel ze van een betrouwbare aanbieder afkomstig is. In dat geval kunt u dit internetadres op de whitelist (witte lijst) zetten, u kunt ze m.a.w. als uitzondering definiëren. De webbeveiliging zal deze website niet meer blokkeren. In het hoofdstuk **Uitzonderingen vastleggen** leest u hoe dit in zijn werk gaat.

Whitelist: Een selectie van objecten (zoals internetpagina's) die door de gebruiker als ongevaarlijk worden beschouwd en daarom niet afzonderlijk worden gecontroleerd.



Webbeveiliging uitschakelen: Als u de webbeveiliging uitschakelt, kunt u bijvoorbeeld heel grote downloads van veilige sites sneller binnenhalen. In principe wordt uw computer ook zonder webbeveiliging door de virusbewaker beschermd. Toch is het raadzaam de webbeveiliging alleen in uitzonderlijke gevallen uit te schakelen.



Instellingen: Met deze knop kunt u de instellingsopties weergeven. Raadpleeg voor meer informatie het hoofdstuk: **Instellingen - Webbeveiliging**

Instellingen

In het gebied **Instellingen** kunt u de programmamodules aan uw wensen aanpassen. Normaal gesproken is het echter niet nodig om hier wijzigingen aan te brengen, omdat de G Data-software bij de installatie al optimaal geconfigureerd is voor uw systeem.

AntiVirus

Hier vindt u alle instellingsmogelijkheden voor de viruscontrole.

Bewaker

Hieronder staan de instellingen die u kunt opgeven in het dialoogvenster **Opties** van de **virusbewaker**. Hier hoeven alleen in uitzonderlijke gevallen wijzigingen te worden aangebracht:

- **Bewakerstatus:** Geef hier aan of u de bewaker wilt in- of uitschakelen.
- **Engines gebruiken:** De software werkt met twee **engines** (Engels voor machines/motors), dus twee viruscontroleprogramma's die in principe onafhankelijk van elkaar functioneren. Elke engine apart zou u al in heel hoge mate tegen virussen beschermen. Maar net de combinatie van beide engines levert de allerbeste resultaten op. Bij oude of trage computers kan men door het gebruik van één engine de viruscontrole versnellen. Over het algemeen kunt u echter beter de instelling **Beide engines** behouden.
- **Geïnfecteerde bestanden:** Als een virus wordt aangetroffen, wordt u standaard gevraagd wat u met het virus en het geïnfecteerde bestand wilt doen. Als u steeds dezelfde actie wilt uitvoeren, kunt u dat hier instellen. De instelling **Desinfecteren (wanneer niet mogelijk: in quarantaine)** biedt de hoogste beveiliging voor uw gegevens.
- **Geïnfecteerde archieven:** Geef hier aan of **archiefbestanden** (dus bijvoorbeeld bestanden met de extensie **RAR**, **ZIP** of **PST**) anders behandeld moeten worden dan normale bestanden. Houd er echter rekening mee dat een archief zo beschadigd kan raken wanneer het in quarantaine wordt geplaatst dat het ook na eventuele terugplaatsing niet meer kan worden gebruikt. Om die reden is het bij geïnfecteerde archieven verstandig per geval te bekijken wat u wilt doen en hier dus de optie **Vragen welke actie gewenst is** te selecteren.
- **Systeembeveiliging:** Als de gedragscontrole is geactiveerd, wordt elke activiteit op het systeem onafhankelijk van de virusbewaker bewaakt. Daardoor worden ook schadelijke programma's herkend waarvoor nog geen handtekening beschikbaar is. De gedragscontrole is vooral gericht op wijzigingen in het onderdeel Automatisch starten en in het hostbestand.

Uitzonderingen

Als u op de knop **Uitzonderingen** klikt, kunt u bepaalde stations, mappen en bestanden uitsluiten van controle, wat de virusherkenning vaak aanzienlijk sneller maakt. Daarvoor gaat u als volgt te werk:

- 1** Klik op de knop **Uitzonderingen**.
- 2** Klik in het venster **Uitzonderingen voor de bewaker** op **Nieuw**.
- 3** Geef nu aan of u een station, map, bestand of bestandstype wilt uitsluiten.
- 4** Selecteer vervolgens daaronder de map die of het station dat u wilt beveiligen. Om bestanden te beveiligen, voert u de volledige bestandsnaam in het invoerveld onder Bestandsmasker in. U kunt hier ook met **jokertekens** werken.

De werkwijze van jokertekens is als volgt:

- Het **vraagteken-symbool** (?) neemt de plaats in van afzonderlijke tekens.
- Het **asterisk-symbool** (*) neemt de plaats in van complete tekenreeksen.

Als u bijvoorbeeld alle bestanden met de extensie **.sav** wilt beveiligen, voert u ***.sav** in. Om een speciaal aantal bestanden met opeenvolgende bestandsnamen te beschermen (bijv. tekst1.doc, tekst2.doc, tekst3.doc), voert u bijvoorbeeld **tekst?.doc** in.

U kunt deze procedure zo vaak als u wilt herhalen en aanwezige uitzonderingen ook weer verwijderen of wijzigen.

Uitgebreid

Via de knop **Uitgebreid** kunt u opgeven welke extra controles de virusbewaker moet uitvoeren. Normaal gezien moet u hier geen bijkomende instellingen opgeven.

- **Modus:** Hier kunt u aangeven of bestanden bij het uitvoeren, alleen bij het lezen of bij het lezen én schrijven moeten worden gecontroleerd. Als een bestand bij het schrijven wordt gecontroleerd, wordt meteen bij het maken van een nieuw bestand of nieuwe bestandsversie gecontroleerd of een onbekend proces het bestand geïnfecteerd heeft. In het andere geval worden bestanden alleen gecontroleerd wanneer ze door programma's worden gelezen.
- **Netwerktogangen controleren:** Wanneer voor uw computer een netwerkverbinding met onbeveiligde computers bestaat (bijv. vreemde notebooks), is het nuttig om ook de netwerktogangen te controleren op de overdracht van schadelijke programma's. Als u uw computer als autonome computer zonder netwerktoegang gebruikt, dan hoeft deze optie niet te worden geactiveerd. Wanneer u op alle computers in het netwerk een virusbescherming hebt geïnstalleerd, is het aan te raden om deze optie uit te schakelen, omdat bepaalde bestanden anders dubbel worden gecontroleerd, wat negatieve gevolgen voor de snelheid heeft.
- **Heuristiek:** In de heuristische analyse worden virussen niet alleen herkend aan de hand van virusupdates, die u regelmatig online van ons krijgt, maar ook op basis van bepaalde virustypische kenmerken. Deze methode zorgt voor extra veiligheid, maar kan in sommige gevallen ook een vals alarm veroorzaken.
- **Archieven controleren:** De controle van gecomprimeerde gegevens in archieven (te herkennen aan extensies als **ZIP**, **RAR** en **PST**) is heel tijdrovend en kan normaal gesproken achterwege worden gelaten als de virusbewaker op het systeem is geactiveerd. Om de snelheid van de viruscontrole te verhogen, kunt u de grootte van de archiefbestanden die worden doorzocht beperken tot een bepaald aantal megabytes.
- **E-mailarchieven controleren:** Aangezien de software de binnenkomende en uitgaande e-mails al op virussen controleert, is het in de meeste gevallen zinvol om de regelmatige controle van e-mailarchieven over te slaan; afhankelijk van de grootte van de e-mailarchieven kan dit namelijk wel een aantal minuten duren.
- **Systeemgebieden bij het starten van het systeem controleren:** Systeemgebieden (bijv. bootsectoren) van uw computer mogen over het algemeen niet van de viruscontrole worden uitgesloten. Hier kunt u aangeven of u deze bij het **starten van het systeem** of bij het **wisselen van medium** (zoals een nieuwe cd-rom) wilt controleren. Normaal gezien moet u minstens een van beide functies geactiveerd hebben.
- **Systeemgebieden bij wisselen van medium controleren:** Systeemgebieden (bijv. bootsectoren) van uw computer mogen over het algemeen niet van de viruscontrole worden uitgesloten. U kunt hier bepalen of u dit controleert bij het starten van het systeem of bij het **wisselen van medium** (nieuwe cd-rom e.d.). Normaal gezien moet u minstens een van beide functies geactiveerd hebben.
- **Op dialers / spyware / adware / riskware controleren:** Met de software kunt u uw systeem ook controleren op **dialers** en andere schadelijke programma's (**spyware**, **adware** en **riskware**). Het gaat hier bijvoorbeeld om programma's die ongeraagd dure internetverbindingen maken en die voor uw portemonnee net zo schadelijk zijn als virussen voor uw computer. Deze programma's slaan bijvoorbeeld uw surfgedrag en zelfs volledig getypte teksten op (en op die manier ook uw wachtwoorden) en sturen deze via het internet door aan onbekenden.
- **Alleen nieuwe of gewijzigde bestanden controleren:** Als u deze functie inschakelt, worden alleen bestanden gecontroleerd die al langere tijd niet zijn gewijzigd en eerder als onschadelijk zijn aangemerkt. Hierdoor kunt u – zonder veiligheidsrisico – ongestoord en snel op uw computer blijven werken.

Handmatige viruscontrole

Hier kunt u basisprogramma-instellingen voor **Viruscontrole** bepalen. Dit is bij normaal gebruik niet nodig.

- **Engines gebruiken:** De software werkt met twee **engines** (Engels voor machines/motors), dus twee viruscontroleprogramma's die in principe onafhankelijk van elkaar functioneren. Elke engine apart zou u al in heel hoge mate tegen virussen beschermen. Maar net de combinatie van beide engines levert de allerbeste resultaten op. Bij oude of trage computers kan men door het gebruik van één engine de viruscontrole versnellen. Over het algemeen kunt u echter beter de instelling **Beide engines** behouden.
- **Geïnfekteerde bestanden:** Heeft de software een virus gevonden? Bij de standaardinstelling vraagt de software nu wat u met het virus en het geïnfekteerde bestand wilt doen. Als u steeds dezelfde actie wilt uitvoeren, kunt u dat hier instellen. De instelling **Desinfecteren (wanneer niet mogelijk: in quarantaine)** biedt de hoogste beveiliging voor uw gegevens.
- **Geïnfekteerde archieven:** Geef hier aan of **archiefbestanden** (dus bijvoorbeeld bestanden met de extensie **RAR, ZIP** of **PST**) anders behandeld moeten worden dan normale bestanden. Houd er echter rekening mee dat een archief zo beschadigd kan raken wanneer het in quarantaine wordt geplaatst dat het ook na eventuele terugplaatsing niet meer kan worden gebruikt. Om die reden is het bij geïnfekteerde archieven verstandig per geval te bekijken wat u wilt doen en hier dus de optie **Vragen welke actie gewenst is** te selecteren.
- **Bij zware systeembelasting de viruscontrole onderbreken:** Normaal gezien zou een viruscontrole moeten gebeuren als u de computer niet gebruikt. Indien u de computer op dat moment toch gebruikt, wordt de viruscontrole onderbroken. Zo blijft de computer voor u op een normaal tempo werken. De viruscontrole gebeurt dus tijdens uw pauze.

Uitzonderingen

Als u op de knop **Uitzonderingen** klikt, kunt u bepaalde stations, mappen en bestanden uitsluiten van controle, wat de virusherkenning vaak aanzienlijk sneller maakt. Daarvoor gaat u als volgt te werk:

- 1 Klik op de knop **Uitzonderingen**.
- 2 Klik in het venster **Uitzonderingen voor de handmatige controle van de computer** op **Nieuw**.
- 3 Geef nu aan of u een station, map, bestand of bestandstype wilt uitsluiten.
- 4 Selecteer vervolgens daaronder de map die of het station dat u wilt beveiligen. Om bestanden te beveiligen, voert u de volledige bestandsnaam in het invoerveld onder Bestandsmasker in. U kunt hier ook met **jokertekens** werken.

De werkwijze van jokertekens is als volgt:

- Het **vraagteken-symbool** (?) neemt de plaats in van afzonderlijke tekens.
- Het **asterisk-symbool** (*) neemt de plaats in van complete tekenreeksen.

Als u bijvoorbeeld alle bestanden met de extensie **.sav** wilt beveiligen, voert u ***.sav** in. Om een speciaal aantal bestanden met opeenvolgende bestandsnamen te beschermen (bijv. tekst1.doc, tekst2.doc, tekst3.doc), voert u bijvoorbeeld **tekst?.doc** in.

U kunt deze procedure zo vaak als u wilt herhalen en aanwezige uitzonderingen ook weer verwijderen of wijzigen.

Uitzonderingen ook voor de afwezigheidsscan gebruiken: Tijdens een handmatige viruscontrole wordt in het systeem gericht naar virussen gezocht en kunt u de computer beter niet voor andere taken gebruiken. Bij de intelligente viruscontrole **Afwezigheidsscan** daarentegen, worden alle bestanden op uw computer steeds opnieuw op virussen gecontroleerd. De afwezigheidsscan werkt net zoals een screensaver alleen wanneer u de computer even niet gebruikt en stopt meteen als u weer aan het werk gaat. De scan staat de prestaties van de computer dus niet in de weg. Hier kunt u aangeven of ook voor de afwezigheidsscan uitzonderingsbestanden of uitzonderingsmappen moeten worden gedefinieerd.

Uitgebreid

Als u op de knop **Uitgebreid** klikt, kunt u extra instellingen voor de viruscontrole opgeven. Meestal volstaat het om de opgegeven standaardinstellingen te gebruiken.

- **Bestandstypen:** Hier kunt u vastleggen welke bestandstypen door de software op virussen moeten worden gecontroleerd. Het selecteren van de optie **Alleen programmabestanden en documenten** zorgt voor voordelen op het gebied van snelheid.
- **Heuristiek:** In de heuristische analyse worden virussen niet alleen herkend aan de hand van de virusdatabases die u bij elke update van de antivirussoftware krijgt, maar ook aan de hand van bepaalde virustypische kenmerken opgespoord. Deze methode zorgt voor extra veiligheid, maar kan in sommige gevallen ook een vals alarm veroorzaken.
- **Archieven controleren:** De controle van gecomprimeerde gegevens in archieven (te herkennen aan extensies als **ZIP**, **RAR** en **PST**) is heel tijdrovend en kan normaal gesproken achterwege worden gelaten als de virusbewaker op het systeem is geactiveerd. Om de snelheid van de viruscontrole te verhogen, kunt u de grootte van de archiefbestanden die worden doorzocht beperken tot een bepaald aantal megabytes.
- **E-mailarchieven controleren:** Hier kunt u aangeven of ook uw e-mailarchief op infecties moet worden gecontroleerd.
- **Systeemgebieden controleren:** Systeemgebieden (bijv. bootsectoren) van uw computer mogen over het algemeen niet van de viruscontrole worden uitgesloten.
- **Op dialers / spyware / adware / riskware controleren:** Met deze functie kunt u uw systeem ook op **dialers** en andere schadelijke software (**spyware**, **adware** en **riskware**) controleren. Het gaat hier bijvoorbeeld om programma's die ongevraagd dure internetverbindingen maken en die voor uw portemonnee net zo schadelijk zijn als virussen voor uw computer. Deze programma's slaan bijvoorbeeld uw surfgedrag en zelfs volledig getypte teksten op (en op die manier ook uw wachtwoorden) en sturen deze via het internet door aan onbekenden.
- **Op rootkits controleren:** **Rootkits** proberen gebruikelijke virusherkenningmethoden te snel af te zijn. Het is steeds aan te raden een extra controle op deze schadelijke software uit te voeren.
- **Alleen nieuwe of gewijzigde bestanden controleren:** Als u deze functie inschakelt, worden alleen bestanden gecontroleerd die al langere tijd niet zijn gewijzigd en eerder als onschadelijk zijn aangemerkt. Hierdoor kunt u – zonder veiligheidsrisico – ongestoord en snel op uw computer blijven werken.
- **Logboek samenstellen:** Als u dit vakje aanvinkt, wordt het viruscontroleproces vastgelegd in een logboek. Dit kan dan onder **Logboeken** worden bekeken.

Updates

Als het niet lukt om de software of virushandtekeningen via internet bij te werken, kunt u in dit gedeelte de gegevens invoeren die nodig zijn voor automatische updates. Typ bij Opties de toegangsgegevens (**gebruikersnaam** en **wachtwoord**) die u bij de online-aanmelding van de software per e-mail hebt ontvangen. Op basis van deze gegevens wordt u herkend bij de G Data-updateserver. De updates kunnen nu volledig automatisch worden uitgevoerd.

Als u een nieuwe licentie hebt en deze wilt activeren, selecteert u **Bij server aanmelden**. Bij de internetinstellingen staan speciale opties die slechts in een paar uitzonderingsgevallen (proxyserver, andere regio) worden gebruikt. Schakel de versiecontrole alleen – tijdelijk – uit als u problemen ondervindt bij het bijwerken van de virushandtekeningen.

Virushandtekeningen automatisch bijwerken

Verwijder het vinkje bij deze optie als u niet wilt dat de G Data-software de virushandtekeningen automatisch up-to-date houdt. Bedenk wel dat uitschakeling van automatische updates een hoog veiligheidsrisico met zich meebrengt. Selecteer deze optie dus alleen in uitzonderlijke gevallen. Als u vindt dat de frequentie waarmee de updates worden uitgevoerd te hoog is, kunt u deze hier wijzigen en bijvoorbeeld instellen dat er alleen updates worden uitgevoerd als u verbinding maakt met internet. Dat is bijvoorbeeld een zinvolle instelling voor computers die niet permanent met internet verbonden zijn.

Logboek samenstellen: Als u dit vakje aanvinkt, wordt elke update van de virushandtekeningen vastgelegd in een logboek. U vindt dit logboek bij de extra functies van de G Data-software (in het **SecurityCenter** onder **Meer > Logboeken**). Naast deze gegevens vindt u in het logboek bijvoorbeeld informatie over gevonden virussen en andere acties die door het programma zijn uitgevoerd.

Bij server aanmelden

Als u de G Data-software nog niet hebt geregistreerd, kunt u dat nu doen en uw registratienummer en klantgegevens invoeren. Afhankelijk van het product vindt u het **registratienummer** bijvoorbeeld op de achterkant van de gebruikershandleiding, in de bevestigingsmail bij de software-download of op het insteekhoesje van de cd.

Als u het registratienummer invoert, wordt het product geactiveerd.

Als u op de knop **Aanmelden** klikt, worden uw toegangsgegevens op de updateserver gegenereerd. Wanneer de aanmelding geslaagd is, verschijnt een informatiescherm met de melding **Het aanmelden is gelukt**. Dit scherm kunt u met de knop Sluiten weer verlaten.

Let op: Voor uw administratie en eventuele nieuwe installaties van de software ontvangt u uw **toegangsgegevens** ook via e-mail. Zorg er daarom bij uw onlineregistratie voor dat het opgegeven e-mail adres juist is, anders zijn uw toegangsgegevens niet beschikbaar.

Vervolgens worden de toegangsgegevens automatisch in het oorspronkelijke invoerscherm overgenomen en kunt u voortaan virushandtekeningen via internet bijwerken.

Kunt u zich niet bij de server aanmelden? Als u zich niet bij de server kunt aanmelden, ligt dat misschien aan een proxyserver. Klik op de knop **Internetinstellingen**. Hier kunt u de instellingen voor uw internetverbinding opgeven. Als u problemen ondervindt bij de update van de virushandtekeningen, controleer dan eerst of het lukt om via een browser (bijvoorbeeld Internet Explorer) op internet te komen. Als u helemaal geen verbinding kunt maken met internet, is er waarschijnlijk iets mis met de internetverbinding en niet met de instellingen van de proxyserver.

Internetinstellingen

Als u gebruikmaakt van een proxyserver, vink dan **Proxyserver gebruiken** aan. Wijzig deze instelling alleen als de update van de virushandtekeningen niet werkt. Neem eventueel contact op met uw systeembeheerder of uw internetprovider voor het proxy-adres. Indien nodig kunt u hier ook de toegangsgegevens voor de proxyserver invoeren.

Proxyserver: Een proxyserver bundelt netwerkaanvragen en verdeelt ze over de aangesloten computers. Als uw computer bijvoorbeeld is aangesloten op een bedrijfsnetwerk, kan het goed zijn dat u via een proxyserver verbinding maakt met internet. Als u problemen ondervindt bij de update van de virushandtekeningen, controleer dan eerst of het lukt om via een browser op internet te komen. Als u helemaal geen verbinding kunt maken met internet, is er waarschijnlijk iets mis met de internetverbinding en niet met de instellingen van de proxyserver.

Webbeveiliging

Hier zijn volgende instellingen beschikbaar.

- **Internetinhoud (HTTP) verwerken:** In de webbeveiligingsopties kunt u instellen dat de gehele **HTTP-webinhoud** al bij het browsen op virussen wordt gecontroleerd. Geïnfecteerde webinhoud wordt dan überhaupt niet uitgevoerd en de bijbehorende pagina's worden niet weergegeven. Zet hiervoor een vinkje bij **Internetinhoud (HTTP) verwerken**.

Als u internetinhoud niet laat controleren, grijpt de **virusbewaker** natuurlijk in als geïnfecteerde bestanden worden uitgevoerd. Uw systeem is dus ook zonder de controle van internetinhoud beschermd zolang de virusbewaker actief is.

Websites die u vertrouwt, kunt u als uitzonderingen definiëren. Raadpleeg voor meer informatie het hoofdstuk **Uitzonderingen vastleggen**. Als u op de knop **Uitgebreid** klikt, kunt u extra opties voor de behandeling van internetinhoud instellen. Voor de browsers **Internet Explorer** en **Firefox** zijn plug-ins beschikbaar waarmee u de bovengenoemde uitzonderingen rechtstreeks vanuit de browser kunt definiëren.

- **Phishingbeveiliging:** Met behulp van **phishing** proberen oplichters via het internet klanten van een bepaalde bank of shop naar een vervalste website te lokken om daar hun gegevens te stelen. De Webfilter krijgt continu online de nieuwste informatie over nieuwe phishing-websites zodat deze dan automatisch kunnen worden onderdrukt. Het activeren van de phishingbeveiliging: wordt sterk aanbevolen.
- **Adressen van geïnfecteerde internetpagina's inzenden:** Via deze functie kunt u – vanzelfsprekend anoniem – automatisch internetpagina's melden die door de software als gevaarlijk worden bestempeld. Zo helpt u mee aan de veiligheid van alle gebruikers.

- **Inhoud van chatberichten verwerken:** Aangezien virussen en andere schadelijke programma's ook via chatberichten kunnen worden verspreid, kan de software ook hier de weergave en het downloaden van besmette gegevens tijdig tegenhouden. Als uw chatprogramma's niet via de standaardpoortnummers verlopen, voert u onder **Uitgebreid** de bijbehorende **poorten** in.
- **Koppelen aan de Messenger-toepassing:** Als u **Microsoft Messenger** of **Trillian** gebruikt, kunt u door het aanvinken van het betreffende programma een contextmenu instellen waarin u verdachte bestanden direct op virussen kunt controleren.

Uitzonderingen vastleggen

Om een internetsite als uitzondering in de whitelist op te nemen, gaat u als volgt te werk:

- 1 Klik op de knop **Uitzonderingen vastleggen**. Het Whitelist-venster wordt weergegeven. Hier worden de websites getoond die u veilig vindt en hier hebt opgegeven.
- 2 Om nog een internetsite toe te voegen, klikt u nu op de Nieuw-knop. Er verschijnt een invoerscherm. Geef bij **URL** het adres van de website op, bijvoorbeeld www.vertrouwdesite.nl, en bij **Opmerking** eventueel de reden waarom u de website opneemt. Klik op OK om de ingevoerde gegevens te bevestigen.
- 3 Klik nu op OK om alle wijzigingen in de whitelist te bevestigen.

Om een website uit de whitelist te verwijderen, selecteert u deze in de lijst en klikt u vervolgens op de knop [Verwijderen](#).

Uitgebreid

Hier kunt u vastleggen welke **serverpoortnummers** door de webbeveiliging moeten worden bewaakt. Voor de bewaking bij normaal browsen wordt meestal poortnummer 80 gebruikt.

- **Tijdoverschrijding in de browser voorkomen:** Aangezien de software de internetinhoud vóór de weergave in de internetbrowser bewerkt en daarvoor afhankelijk van de hoeveelheid gegevens een bepaalde tijd nodig heeft, kan het gebeuren dat er een foutmelding in de browser verschijnt. De browser krijgt immers niet meteen de gegevens door omdat deze door de antivirussoftware op schadelijke processen worden gecontroleerd. Als u het vakje **Tijdoverschrijding in de browser voorkomen** selecteert, wordt deze foutmelding niet getoond. Zodra de browsergegevens op virussen zijn gecontroleerd, worden deze vervolgens op normale wijze overgedragen aan de internetbrowser.
- **Maximale grootte voor downloads:** Met deze functie kunt u de HTTP-controle voor te grote webinhoud blokkeren. De inhoud wordt door de virusbewaker gecontroleerd zodra eventuele schadelijke inhoud actief wordt. Het voordeel bij deze groottebegrenzing is dat het surfen op het internet niet door de viruscontrole wordt vertraagd.

E-mailcontrole

Met de e-mailcontrole kunt u binnenkomende en uitgaande e-mails en de bestandsbijlagen controleren op virussen en de bron van mogelijke besmettingen uitschakelen. De software kan in geval van een virus bestandsbijlagen direct verwijderen of besmette bestanden herstellen.

In **Microsoft Outlook** gebeurt de e-mailcontrole via een **plug-in**. Deze biedt dezelfde bescherming als de **POP3/IMAP**-georiënteerde beveiliging binnen de **AntiVirus**-opties. Na de installatie van deze Plug-in kunt u in het **Outlook**-menu **Extra** de functie **Map op virussen controleren** gebruiken om uw e-mailmappen op virussen te controleren.

Inkomende e-mails

- **In geval van een infectie:** Hier kunt u vastleggen wat bij de ontdekking van een besmette e-mail moet gebeuren. Afhankelijk van het doel waarvoor u uw computer gebruikt, zijn verschillende instellingen aan te bevelen. Normaal gesproken is de instelling **Desinfecteren (indien niet mogelijk: bijlage/tekst verwijderen)** aan te raden.

- **Ontvangen e-mails controleren:** Door het activeren van deze optie worden alle **e-mails**, ontvangen tijdens uw werk op de computer, op virussen gecontroleerd.
- **Ongelezen e-mails bij het starten van het programma controleren (alleen Microsoft Outlook):** E-mails die binnenkomen terwijl er geen verbinding is met internet, worden met deze optie op virussen gecontroleerd. Zodra u **Outlook** start, worden daarom alle ongelezen e-mails in Postvak IN en de onderliggende mappen gecontroleerd.
- **Bericht als bijlage aan ontvangen, geïnfecteerd e-mailbericht toevoegen:** Wanneer u de berichtoptie hebt geactiveerd, verschijnt in het geval een virus wordt gevonden in de onderwerpregel van de geïnfecteerde e-mail de waarschuwing **VIRUS** en aan het begin van de e-mailtekst de mededeling **Opgelet! Deze e-mail bevat het volgende virus** gevolgd door de naam van het virus en de mededeling dat het virus werd verwijderd of dat het geïnfecteerde bestand kon worden hersteld.

Uitgaande e-mails

- **E-mails vóór het verzenden controleren:** Om te voorkomen dat u per ongeluk zelf virussen verzendt, biedt de software ook de mogelijkheid om uw e-mails vóór verzending te controleren op virussen. Als u daadwerkelijk (onopzettelijk) een virus wilt verzenden, verschijnt de melding **De e-mail [onderwerpregel] bevat het volgende virus: [naam virus]**. De e-mail kan niet worden verzonden en de betreffende e-mail wordt niet verstuurd.

Scanopties

- **Engines gebruiken:** De software werkt met twee antivirus-engines. Dit zijn twee analyse-eenheden die in principe onafhankelijk van elkaar werken. Het gebruik van beide engines staat garant voor optimale resultaten bij het voorkomen van virussen.
- **OutbreakShield:** Hiermee activeert u het OutbreakShield. De software maakt bij een geactiveerde OutbreakShield controlesommen van e-mails, vergelijkt deze met continu bijgewerkte antispam-blacklists en is daardoor in staat op massamailings te reageren voordat de betreffende virushandtekeningen beschikbaar zijn. OutbreakShield zoekt daarvoor op internet naar een opvallende groei van verdachte e-mails en dicht dan vrijwel direct het gat tussen de start van een massaal verspreid e-mailvirus en de bestrijding door middel van aangepaste virusdefinities. OutbreakShield is geïntegreerd in de e-mailvirusblokkering.

Uitgebreid

Als u voor uw e-mailprogramma niet de **standaardpoorten** gebruikt, kunt u onder **Serverpoortnummer** ook de **poort** opgeven die u voor inkomende of uitgaande e-mails gebruikt. Via de knop **Standaard** kunt u automatisch de standaardpoortnummers herstellen. U kunt ook meerdere poorten invoeren. Deze moeten altijd door een komma worden gescheiden.

Microsoft Outlook wordt door een speciale plug-in beveiligd. Hiermee kunt u direct in **Outlook** mappen en e-mails controleren. Om een e-mail of map in Outlook op virussen te controleren selecteert u in het menu van Outlook de optie **Extra's > Map op virussen controleren**, waarna de huidig geselecteerde map op virussen wordt gecontroleerd.

Aangezien de software de inkomende e-mails eerder bewerkt dan het eigenlijke e-mailprogramma, kan bij grote hoeveelheden e-mails of trage verbindingen een foutmelding in het e-mailprogramma verschijnen. Dat komt doordat de e-mailgegevens niet direct worden doorgegeven; deze worden immers eerst door de software op virussen gecontroleerd. Als u de optie **Tijdoverschrijding bij de e-mailserver voorkomen** aanvinkt, wordt een dergelijke foutmelding van het e-mailprogramma onderdrukt. Zodra alle e-mailgegevens op virussen zijn gecontroleerd, worden deze door de software zoals gebruikelijk doorgegeven aan het e-mailprogramma.

Automatische viruscontroles

Hier kunt u de **afwezigheidsscan** in- of uitschakelen. Bovendien kunt u in plaats hiervan of in combinatie hiermee (onderdelen van) uw computer regelmatig op infecties controleren. U kunt dergelijke controles dan bijvoorbeeld uitvoeren op momenten dat u de computer niet gebruikt.

Verschillende viruscontroles: In de meeste gevallen is het voldoende als de computer door de afwezigheidsscan wordt gecontroleerd. Met de knop **Nieuw** kunt u echter ook verschillende van elkaar onafhankelijke automatische viruscontroles uitvoeren. Zo kunt u bijvoorbeeld de map **Downloads** dagelijks controleren, terwijl u uw mp3-verzameling maar een keer per maand scant.

Algemeen

Voer hier een naam in voor de automatische viruscontrole die u hebt ingesteld. Gebruik duidelijke namen om jobs van elkaar te onderscheiden, zoals bijv. **Lokale vaste schijven (wekelijkse controle)** of **Archieven (maandelijke controle)**.

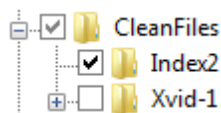
Als u een vinkje plaatst bij **Na voltooiing van de opdracht de computer uitschakelen**, wordt de computer na het uitvoeren van de automatische viruscontrole automatisch uitgeschakeld. Dit is nuttig als u de viruscontrole bijv. na het werk wilt laten uitvoeren.

Taak: Elke automatische opdracht die wordt uitgevoerd ter controle van de computer of bepaalde onderdelen, wordt taak genoemd.

Omvang van de analyse

Bepaal hier of de virusscan op de **lokale vaste schijven** moet worden uitgevoerd, of het **geheugen** en de **gebieden in autostart** moeten worden getest of bepaal of u alleen bepaalde **mappen** en **bestanden** wilt scannen. Als dat het geval is, klikt u op de knop **Selecteren** om de gewenste mappen te selecteren.

Mappen/bestanden selecteren: In de mappenstructuur kunt u mappen openen en selecteren door te klikken op de (+)-symbolen. Hun inhoud wordt dan in het bestandsoverzicht weergegeven. De mappen en bestanden waarvoor u een vinkje plaatst, worden gecontroleerd. Als in een map niet alle bestanden worden gecontroleerd, staat bij deze map een grijs vinkje.



Tijdschema

Via deze tab kunt u bepalen wanneer en volgens welke intervallen de betreffende taak moet worden uitgevoerd. Onder **Uitvoeren** geeft u aan wanneer de taak moet worden gestart en specificeert u dit nader onder **Tijdstip**. Als u **Bij het starten van het systeem** selecteert, vervallen de instellingen van de tijdplanning en voert de software altijd een controle uit als de computer wordt opgestart.

- **Taak alsnog uitvoeren als de computer op de geplande starttijd nog niet werd ingeschakeld:** Als u deze optie inschakelt, worden niet-uitgevoerde automatische viruscontroles alsnog uitgevoerd zodra de computer weer wordt opgestart.
- **Niet in batterijbedrijf uitvoeren:** Om de accu van bijvoorbeeld **notebooks** niet onnodig te belasten, kunt u instellen dat automatische viruscontroles alleen worden uitgevoerd wanneer de draagbare computer op het lichtnet is aangesloten.

Scan-instellingen

Hier legt u vast op basis van welke instellingen de automatische viruscontrole moet worden uitgevoerd.

- **Engines gebruiken:** De software werkt met twee **engines**, dus twee viruscontroleprogramma's die in principe onafhankelijk van elkaar functioneren. Elke engine apart zou u al in heel hoge mate tegen virussen beschermen. Maar net de combinatie van beide engines levert de allerbeste resultaten op. Bij oude of trage computers kan men door het gebruik van één engine de viruscontrole versnellen. Over het algemeen kunt u echter beter de instelling **Beide engines** behouden.
- **Geïnfecteerde bestanden:** Heeft de software een virus gevonden? Bij de standaardinstelling vraagt de software nu wat u met het virus en het geïnfecteerde bestand wilt doen. Als u steeds dezelfde actie wilt uitvoeren, kunt u dat hier instellen. De instelling **Desinfecteren (wanneer niet mogelijk: in quarantaine)** biedt de hoogste beveiliging voor uw gegevens.

- **Geïnfekteerde archieven:** Geef hier aan of **archiefbestanden** (dus bijvoorbeeld bestanden met de extensie **RAR**, **ZIP** of **PST**) anders behandeld moeten worden dan normale bestanden. Houd er echter rekening mee dat een archief zo beschadigd kan raken wanneer het in quarantaine wordt geplaatst dat het ook na eventuele terugplaatsing niet meer kan worden gebruikt. Om die reden is het bij geïnfekteerde archieven verstandig per geval te bekijken wat u wilt doen en hier dus de optie **Vragen welke actie gewenst is** te selecteren.

Bepaal door het klikken op de knop **Uitgebreid** welke bijkomende viruscontroles wel en welke niet moeten worden uitgevoerd.

Meestal volstaat het om de opgegeven standaardinstellingen te gebruiken.

- **Bestandstypen:** Hier kunt u vastleggen welke bestandstypen door de software op virussen moeten worden gecontroleerd.
- **Heuristiek:** In de heuristische analyse worden virussen niet alleen herkend aan de hand van de virusdatabases die u bij elke update van de software krijgt, maar ook aan de hand van bepaalde virustypische kenmerken opgespoord. Deze methode zorgt voor extra veiligheid, maar kan in sommige gevallen ook een vals alarm veroorzaken.
- **Archieven controleren:** De controle van gecomprimeerde gegevens in archieven (te herkennen aan extensies als **ZIP**, **RAR** en **PST**) is heel tijdrovend en kan normaal gesproken achterwege worden gelaten als de **virusbewaker** op het systeem is geactiveerd. Deze herkent dan bij het uitpakken van het archief het tot dan toe verborgen virus en voorkomt automatisch de verspreiding ervan.
- **E-mailarchieven controleren:** Hier kunt u aangeven of ook uw e-mailarchief op infecties moet worden gecontroleerd.
- **Systeemgebieden controleren:** Systeemgebieden (bijv. **bootsectoren**) van uw computer mogen over het algemeen niet van de viruscontrole worden uitgesloten.
- **Op dialers / spyware / adware / riskware controleren:** Met deze functie kunt u uw systeem ook op **dialers** en andere schadelijke software (**spyware**, **adware** en **riskware**) controleren. Het gaat hier bijvoorbeeld om programma's die ongevraagd dure internetverbindingen maken en die voor uw portemonnee net zo schadelijk zijn als virussen voor uw computer. Deze programma's slaan bijvoorbeeld uw surfgedrag en zelfs volledig getypte teksten op (en op die manier ook uw wachtwoorden) en sturen deze via het internet door aan onbekenden.
- **Op RootKits controleren:** **RootKits** proberen gebruikelijke virusherkenningmethoden te snel af te zijn. Het is steeds aan te raden een extra controle op deze schadelijke software uit te voeren.
- **Logboek samenstellen:** Als u dit vakje aanvinkt, wordt het viruscontroleproces vastgelegd in een logboek. Dit kan dan onder **Logboeken** worden bekeken.

Gebruikersaccount

Hier kan de gebruikersaccount op de computer worden aangegeven waarop de viruscontrole moet gebeuren. Deze account is nodig voor de toegang tot netwerkstations.

Wetenswaardigheden

Hier vindt u informatie over belangrijke programmafuncties van de software.

BootScan

Met de **BootScan** kunt u virussen aanpakken die zich al vóór de installatie van de antivirussoftware op uw computer hebben genesteld en mogelijk de installatie van de G Data-software proberen tegen te houden. Hiervoor is een speciale programmaversie van de software beschikbaar, die al voor de start van Windows kan worden uitgevoerd.

Wat is een bootproces? Als u uw computer aanzet, start uw Windows-besturingssysteem normaal gezien automatisch. Dit proces wordt **boot** genoemd. Het is echter ook mogelijk om andere programma's automatisch op te starten in plaats van uw Windows-besturingssysteem. Om uw computer al voor de start van Windows op virussen te controleren, biedt G Data u naast de Windows-versie nog een speciale opstartversie.

Hoe breek ik een BootScan af? Als na het opnieuw opstarten van uw computer niet de gewone Windows-omgeving wordt weergegeven, maar een speciale interface van de G Data-software, hoeft u zich geen zorgen te maken. Als u geen BootScan hebt gepland, selecteert u met de pijltoetsen de optie **Microsoft Windows** en klikt u op **Return**. Nu start Windows normaal op zonder voorafgaande BootScan.

Wanneer u een **BootScan** wilt uitvoeren, gaat u als volgt te werk:

1a Bootscan met de programma-cd: U gebruikt de G Data-**programma-cd** om uw computer op te starten. - Plaats de G Data-**cd** in het station. Klik op **Annuleren** in het startvenster dat wordt geopend en schakel de computer uit.

1b BootScan met G Data-software die u van internet hebt gedownload: U maakt een nieuwe opstart-cd via de optie **G Data-opstart-cd maken** in de **G Data-programmagroep** (*Windows-symbool in het taakoverzicht > Alle programma's > G Data-software > Opstart-cd maken*).

Plaats uw zelfgebrande opstart-cd in het station. Klik op **Annuleren** in het startvenster dat wordt geopend en schakel de computer uit.

Wanneer u **Windows XP** gebruikt, dat u bij een poging een opstart-cd te maken, een melding krijgt dat **IMAPI 2.x** niet is geïnstalleerd. Het gaat in dit geval om een update van Microsoft voor oudere besturingssystemen, die noodzakelijk is voor het branden van gegevensdragers. U kunt de vereiste update rechtstreeks van de homepage van Microsoft downloaden en installeren.

1c Hebt u een speciale netbookversie van de G Data-software op een USB-stick? Hier kunt u de BootScan rechtstreeks vanaf de USB-stick uitvoeren. Uw netbook moet hiervoor echter in staat zijn vanaf een USB-stick te starten.

Sluit de **G Data-USB-stick** aan op uw netbook. Klik op **Annuleren** in het startvenster dat wordt geopend en schakel de netbook uit.

Na de eerste stap verloopt de bootscan voor de drie varianten hetzelfde:

- 2** Start uw computer opnieuw op. Het startmenu van de G Data-**BootScan** wordt geopend.
- 3** Selecteer met de pijltoetsen de optie **G Data-opstart-cd** en bevestig uw selectie met **Enter**. Vanaf de cd wordt nu een Linux-besturingssysteem gestart en er wordt een speciale G Data-**BootScan-versie** weergegeven.

Als u problemen ondervindt bij de weergave van de programma-interface, start u de computer opnieuw en selecteert u de optie **G Data-opstart-cd - alternatief**.

- 4** Het programma stelt nu voor om de virushandtekeningen bij te werken.

Als u een versie van de G Data-software gebruikt die back-upfuncties ondersteunt, kunt u hier ook meteen back-ups van uw opgeslagen gegevens terugzetten.

- 5** Klik nu op **Ja**. Voer de door u ontvangen toegangsgegevens of uw registratienummer in. Vervolgens kunt u de update uitvoeren. Zodra de gegevens via het internet zijn bijgewerkt, verschijnt de melding **Update voltooid**. Verlaat nu het updatescherm door op de knop **Sluiten** te klikken.

De automatische **internetupdate** is beschikbaar wanneer u een **router** gebruikt die automatisch IP-adressen toekent (**DHCP**). Als de internetupdate niet mogelijk is, kunt u de **BootScan** ook met oude virushandtekeningen uitvoeren. In dat geval moet u na de installatie van de G Data-software zo snel mogelijk een nieuwe BootScan uitvoeren met bijgewerkte gegevens.

- 6** Nu ziet u de programma-interface. Klik op **Computer controleren** en uw computer wordt op virussen en schadelijke software gecontroleerd. De bootscan kan afhankelijk van het type computer en de grootte van de harde schijf een uur of meer duren.

- 7** Als de G Data-software virussen vindt, verwijdert u deze via de door het programma voorgestelde optie. Nadat het virus succesvol werd verwijderd, kunt u weer over het originele bestand beschikken.

- 8** Na afloop van de viruscontrole klikt u rechtsboven in het venster op het kleine kruisje (x) om het systeem af te sluiten.

- 9** Neem de G Data-software-cd uit het station of haal de G Data-**USB-stick** uit uw netbook.

- 10** Schakel uw computer opnieuw uit en weer aan. Nu start uw computer weer met het standaard Windows-besturingssysteem en bent u ervan verzekerd dat u de normale G Data-software op een virusvrij systeem kunt installeren.

Wat doe ik als mijn computer niet opstart (boot) vanaf een cd-rom?

Als het niet lukt om de computer vanaf cd/dvd-rom op te starten, moet u deze optie misschien nog instellen. Dat gebeurt in het zogenaamde **BIOS**, een systeem dat nog voor uw Windows-besturingssysteem automatisch wordt opgestart. Volg de onderstaande stappen om in het BIOS veranderingen door te voeren:

1. Schakel uw computer uit.
2. Start uw computer opnieuw op. Normaal gesproken komt u in de BIOS-setup als u bij het starten (= booten) van de computer de **DEL**-toets (soms ook **F2** of **F10**) ingedrukt houdt.
3. Hoe u de instellingen in uw BIOS-setup precies verandert, hangt van computer tot computer af. Lees hiervoor de documentatie bij uw computer. Het resultaat zou de volgende opstartvolgorde moeten zijn: **cd/dvd-rom**;, **C:**. Met andere woorden wordt het cd/dvd-rom-station het **1st Boot Device** en de vaste-schijfpartitie met uw Windows-besturingssysteem het **2nd Boot Device**.
4. Sla de wijzigingen op en start uw computer opnieuw op. Uw computer is nu klaar voor een bootscan.

Wat doe ik als mijn netbook (of desktop-pc/notebook) niet opstart (boot) vanaf een USB-stick?

Als uw computer niet automatisch vanaf een USB-stick opstart, voert u de volgende stappen uit:

1. Schakel uw computer uit.
2. Steek de G Data-**USB-stick** in een vrije **USB-poort** op uw computer.
3. Schakel uw computer in.
4. Tijdens het opstarten drukt u op de **F2-toets** om naar het **BIOS** van uw computer te gaan.
5. Nu verschijnt er een BIOS-interface met een menubalk, waarin u met de pijltjestoetsen (rechts/links) het menu **Boot** uitkiest. Druk vervolgens op **Enter**.
6. Kies nu met de pijltjestoetsen (omhoog/omlaag) **Harde-schijfstations**. Druk vervolgens op **Enter**.
7. Kies nu **USB** zodat deze als **1st Drive = USB** op de eerste plaats staat (**Enter-toets** en pijltjestoetsen).
8. Druk vervolgens op **F10** om de wijzigingen op te slaan en BIOS te sluiten. Uw computer kan nu vanaf de USB-stick worden opgestart.
9. Start uw computer opnieuw op. Uw computer is nu klaar voor een bootscan.

G Data-symbool

De G Data-software beschermt uw computer constant tegen virussen en schadelijke software. In de taakbalk onderaan wordt naast de tijdsaanduiding een symbool getoond, zodat u kunt zien dat de beveiliging actief is.



Dit G Data-symbool geeft aan dat alles in orde is en dat de beveiliging op uw computer actief is.



Als de bewaker is uitgeschakeld of zich andere problemen voordoen, geeft het G Data-symbool een waarschuwing weer. Start de G Data-software dan zo snel mogelijk en controleer de instellingen.



Als de G Data-software gegevens van het internet downloadt, wordt dit ook met een speciaal symbool aangegeven.

Als u met de rechtermuisknop op het symbool klikt, verschijnt een contextmenu waarmee u basisbeveiligingsonderdelen van de software kunt bepalen.

De volgende functies zijn hier beschikbaar:

- **G Data-software starten:** Hiermee opent u het **SecurityCenter**, waarin u bijvoorbeeld de instellingen van de virusbewaker kunt opgeven. Wat u in het SecurityCenter kunt doen, leest u in het hoofdstuk: **SecurityCenter**
- **Bewaker uitschakelen:** Hiermee kunt u de **virusbewaker** uitschakelen en ook weer inschakelen. Dit kan bijvoorbeeld nuttig zijn als op uw harde schijf grote hoeveelheden gegevens van de ene naar de andere plaats moeten worden gekopieerd of bij intensieve processen (bijv. bij het kopiëren van een dvd). U moet de virusbewaker slechts zo lang uitschakelen als absoluut noodzakelijk is. Let er ook op dat het systeem gedurende deze periode bij voorkeur niet met het internet is verbonden of geen toegang heeft tot nieuwe, niet gecontroleerde gegevens (bijv. via cd's, dvd's, geheugenkaarten of USB-sticks).
- **Firewall uitschakelen:** Als de door u gebruikte versie van de G Data-software een geïntegreerde firewall heeft, kunt u de **firewall** ook uitschakelen via het contextmenu. Uw computer blijft dan verbonden met internet en andere netwerken, maar wordt dan niet langer door de firewall beschermd tegen aanvallen of spionage.
- **Automatische piloot uitschakelen:** De **automatische piloot** is een onderdeel van de **firewall** en beslist volledig zelf welke aanvragen en contacten uw computer via het netwerk of internet mag accepteren. Voor een normaal gebruik is de automatische piloot optimaal. Wij bevelen dan ook aan deze altijd ingeschakeld te laten. De automatische piloot is, net zoals de firewall, beschikbaar in bepaalde versies van de G Data-software.

- **Virusupdate:** Een antivirussoftware moet steeds up-to-date zijn. Het bijwerken van de gegevens kunt u vanzelfsprekend via de software automatisch laten uitvoeren. Als u echter onmiddellijk een update nodig hebt, kunt u deze via de knop **Virusupdate** starten. Waarvoor een virusupdate nodig is, leest u in het hoofdstuk: **Updates**
- **Statistieken:** Hier kunt u een statistisch overzicht over de controles van de Virusbewaker bekijken.

Viruscontrole

Met behulp van de viruscontrole controleert u uw computer op aantasting door schadelijke software. Als u de viruscontrole start, scant deze elk bestand op infectie of op de mogelijkheid andere bestanden te infecteren. Worden er tijdens een viruscontrole virussen of andere schadelijke software ontdekt, dan zijn er verschillende mogelijkheden om het virus te verwijderen of onschadelijk te maken.

- 1** Start de viruscontrole. Hoe u dat doet, leest u in het hoofdstuk: **Virusbeveiliging**
- 2** Uw computer wordt nu op virussen gecontroleerd. Een venster wordt geopend met informatie over de status van de controle.

Een voortgangsbalk bovenaan het venster geeft aan hoe ver de controle van uw systeem al gevorderd is. Tijdens de viruscontrole kunt u het verloop van de controle op verschillende manieren beïnvloeden:

- **Bij zware systeembelasting de viruscontrole onderbreken:** Via dit keuzevakje kunt u aangeven of de software moet wachten met de viruscontrole totdat u klaar bent met andere activiteiten op de computer.
- **Computer na viruscontrole uitschakelen:** Deze functie is heel handig wanneer de viruscontrole 's nachts of aan het einde van de werkdag moet worden uitgevoerd. Zodra de G Data-software klaar is met de viruscontrole, wordt uw computer uitgeschakeld.
- **Met wachtwoord beveiligde archieven:** Als een archief met een wachtwoord is beveiligd, kan de G Data-software de bestanden in dat archief niet op virussen controleren. Als u hier een vinkje plaatst, dan geeft de antivirussoftware aan welke archieven met een wachtwoord zijn beveiligd en niet konden worden gecontroleerd. Zolang deze archieven niet worden uitgepakt, vormt een eventueel virus, dat zich daar bevindt, ook geen bedreiging voor uw systeem.
- **Toegang geweigerd:** Er zijn in Windows bestanden die uitsluitend door bepaalde toepassingen worden gebruikt. Deze kunnen niet worden gecontroleerd zolang die toepassingen actief zijn. Het is daarom aan te raden om tijdens een viruscontrole geen andere programma's op uw systeem te laten draaien. Als u hier een vinkje zet, worden alle niet-gecontroleerde gegevens getoond.

- 3a** Als uw systeem virusvrij is, kunt u na afloop van de controle het wizardvenster verlaten met de knop **Sluiten**.

Uw systeem werd op virussen gecontroleerd en is virusvrij.

- 3b** Als er virussen en andere schadelijke programma's werden gevonden, kunt u bepalen wat er met de gevonden virussen moet gebeuren. Over het algemeen is het voldoende om op de knop **Acties uitvoeren** te klikken.

De G Data-software gebruikt nu een standaardinstelling (*als u deze bij de instellingen onder **AntiVirus > Handmatige viruscontrole voor geïnfecteerde bestanden en archieven niet anders hebt geconfigureerd***) en desinfecteert de aangetaste bestanden. Dat houdt in dat de bestanden worden gerepareerd zodat deze weer zonder beperkingen gebruikt kunnen worden en geen gevaar meer vormen voor de computer.

Bestanden die niet kunnen worden gedesinfecteerd, worden in quarantaine geplaatst. Dat betekent dat ze gecodeerd in een extra beveiligde map worden geplaatst, waarin ze geen schade meer kunnen aanrichten.

Als u deze geïnfecteerde bestanden nog nodig hebt, kunt u ze in uitzonderlijke gevallen opnieuw uit quarantaine halen en gebruiken.

Uw systeem werd op virussen gecontroleerd en is virusvrij.

- 3c** Wanneer u weet welke bestanden/objecten geïnfecteerd zijn, kunt u bepalen welke daarvan u eventueel niet meer nodig hebt en afzonderlijk op elk gevonden virus reageren.

In het overzicht van de gevonden virussen kunt u in de kolom **Actie** voor elk geïnfecteerd bestand apart bepalen wat er met het bestand moet gebeuren.

- **Alleen in logboek registreren:** In de **Logboeken**-weergave wordt de infectie geregistreerd. De betroffen bestanden worden echter niet hersteld of verwijderd. **Let op: Indien een virus alleen in het logboek wordt geregistreerd, is het nog steeds actief en gevaarlijk.**
- **Desinfecteren (indien niet mogelijk: Alleen in logboek registreren):** Hier wordt een poging gedaan om het virus uit het aangetaste bestand te verwijderen. Als dat niet mogelijk is zonder het bestand te beschadigen, wordt het virus in het logboek geregistreerd en kunt u het probleem later via de logboek invoer oplossen. **Let op: Indien een virus alleen in het logboek wordt geregistreerd, is het nog steeds actief en gevaarlijk.**
- **Desinfecteren (indien niet mogelijk: in quarantaine):** Dit is de standaardinstelling. Hier wordt een poging gedaan om het virus uit het aangetaste bestand te verwijderen. Als dat niet mogelijk is zonder het bestand te beschadigen, wordt het bestand in **Quarantaine** geplaatst. Raadpleeg ook het hoofdstuk: **Hoe werkt de quarantaine?**
- **Desinfecteren (indien niet mogelijk: Bestand verwijderen):** Hier wordt geprobeerd het virus uit een aangetast bestand te verwijderen. Als dat niet mogelijk is, wordt het bestand verwijderd. Gebruik deze functie alleen als er zich geen belangrijke gegevens op uw computer bevinden. Het consequent verwijderen van geïnfecteerde bestanden kan in het ergste geval ertoe leiden dat Windows niet meer functioneert en opnieuw moet worden geïnstalleerd.
- **Bestand in quarantaine plaatsen:** Geïnfecteerde bestanden worden direct in **Quarantaine** geplaatst. In de quarantaine worden bestanden gecodeerd opgeslagen. Hier kan het virus dus geen schade aanrichten en kan worden geprobeerd om het geïnfecteerde bestand te herstellen. Lees hierover ook het hoofdstuk: **Hoe werkt de quarantaine?**
- **Bestand verwijderen:** Gebruik deze functie alleen als er zich geen belangrijke gegevens op uw computer bevinden. Het consequent verwijderen van geïnfecteerde bestanden kan in het ergste geval ertoe leiden dat Windows niet meer functioneert en opnieuw moet worden geïnstalleerd.

Als u nu op de knop **Acties uitvoeren** klikt, behandelt de G Data-software elk gevonden virus op de manier die u hebt ingesteld.

Uw systeem werd op virussen gecontroleerd. Als u echter een instelling met de optie In logboek registreren hebt gebruikt, kan het zijn dat uw computer niet virusvrij is.

- 4** Na voltooiing van de viruscontrole kunt u ons een kopie van de geïnfekteerde bestanden sturen. Op basis van deze gegevens kunnen wij de viruscontrole dan voor alle gebruikers verbeteren. Uw gegevens worden uiteraard vertrouwelijk behandeld en er worden geen persoonlijke gegevens doorgegeven of gebruikt.

U bent natuurlijk absoluut niet verplicht deze gegevens door te sturen. Als u wilt, kunt u deze stap overslaan of uitschakelen.

Virus gevonden

Als de G Data-software een virus of een ander schadelijk programma op uw computer vindt, hebt u de volgende mogelijkheden om met het geïnfekteerde bestand om te gaan.

- **Alleen in logboek registreren:** In de **Logboeken**-weergave wordt de infectie geregistreerd. De betroffen bestanden worden echter niet hersteld of verwijderd. Het logboek helpt u wel bij het een voor een controleren en doelgericht verwijderen van de gevonden virussen. **Let op: Indien een virus alleen in het logboek wordt geregistreerd, is het nog steeds actief en gevaarlijk.**
- **Desinfecteren (indien niet mogelijk: In quarantaine plaatsen):** Hier wordt een poging gedaan om het virus uit het aangetaste bestand te verwijderen. Als dat niet mogelijk is zonder het bestand te beschadigen, wordt het bestand in **Quarantaine** geplaatst. Lees hierover ook het hoofdstuk: **Hoe werkt de quarantaine?**
- **Bestand in quarantaine plaatsen:** Geïnfekteerde bestanden worden direct in **Quarantaine** geplaatst. In de quarantaine worden bestanden gecodeerd opgeslagen. Hier kan het virus dus geen schade aanrichten en kan worden geprobeerd om het geïnfekteerde bestand te herstellen. Lees hierover ook het hoofdstuk: **Hoe werkt de quarantaine?**
- **Geïnfecteerd bestand verwijderen:** Gebruik deze functie alleen als er zich geen belangrijke gegevens op uw computer bevinden. Het consequent verwijderen van geïnfekteerde bestanden kan in het ergste geval ertoe leiden dat Windows niet meer functioneert en opnieuw moet worden geïnstalleerd.

Quarantaine en e-mailpostvakken: Sommige bestanden, zoals de archiefbestanden voor e-mailpostvakken, kunt u beter niet in quarantaine plaatsen. Als een e-mailpostvak in quarantaine wordt geplaatst, kan uw e-mailprogramma hiertoe geen toegang meer krijgen, waardoor het mogelijk niet meer werkt. Vooral bij bestanden met de extensie **PST** moet u daarom voorzichtig zijn. Deze bevatten in de meeste gevallen gegevens van uw **Outlook-e-mailpostvak**.

Feedback over malware

In de G Data Security Labs wordt voortdurend onderzoek gedaan naar de mogelijkheden om G Data-klanten tegen malware te beschermen. Des te meer informatie er over malware bestaat, des te snellere en effectievere beveiligingsmechanismen kunnen worden ontwikkeld. Veel informatie is spijtig genoeg enkel beschikbaar op reeds aangevallen of geïnfekteerde systemen. Om deze gegevens ook in de analyses te kunnen opnemen, is het G Data Malware Information Initiative opgericht. Hierbij wordt informatie over malware naar de G Data Security Labs verzonden. Door uw deelname draagt u eraan bij dat alle G Data-klanten internet op een veiligere manier kunnen gebruiken.

Malware: Een verzamelnaam voor alle bestanden, programma's en codes die zijn geprogrammeerd om een computer zonder medeweten van de gebruiker te infecteren, te bespioneren of te controleren. Daaronder vallen onder andere virussen, wormen, rootkit-virussen, trojanen en keyloggers.

Welke gegevens worden verzameld?

In principe worden twee soorten gegevens doorgestuurd. 1. U kunt op vrijwillige basis malware-bestanden naar G Data sturen en 2. op een website wordt schadelijke inhoud ontdekt. Als u malware-bestanden naar de G Data-Internetambulance stuurt, dan verstuurt het systeem naast het bestand ook de vindplaats, de originele bestandsnaam en de aanmaakdatum. Bij het ontdekken van schadelijke internetinhoud worden de volgende gegevens verzonden:

- Versienummer van het G Data-product en de gebruikte engines
- Taal (lokale instelling) van het besturingssysteem
- URL waarvan de toegang is geblokkeerd en de reden voor de blokkering (malware, phishing enzovoort)
- Naam van de malware

Deze informatie is normaal niet daarvoor geschikt om pc-gebruikers te identificeren. Ze bevat geen persoonlijke gegevens.

Hoe worden de verzamelde gegevens gebruikt?

Bij de verwerking en opslag van de gegevens worden de wettelijke bepalingen van de desbetreffende landen met betrekking tot privacy en publicatie van gegevens in acht genomen. G Data besteedt er de grootste zorg aan om de gegevens tegen onbevoegde toegang te beschermen. De evaluatie van de gegevens vindt plaats in de G Data Security Labs en dient ter ondersteuning van het onderzoek naar IT-beveiliging. Het hoofddoel is het onderzoeken van veiligheidsrisico's en de ontwikkeling van beveiligingsmechanismen. Voorbeelden van het gebruik zijn het opmaken van blokkeringslijsten, het opstellen van statistieken ter publicatie in vakartikels en de ontwikkeling van regelsets voor beveiligingstechnologieën. Deelname is op vrijwillige basis en als u hiervan afziet, heeft dit geen negatieve gevolgen voor de werking van uw product. Dankzij uw deelname aan het G Data Malware Information Initiative kunnen alle G Data-klanten in de toekomst nog beter over computerbedreigingen worden geïnformeerd en ertegen worden beschermd.

Melding not-a-virus

Bij bestanden die als **not-a-virus** gekenmerkt zijn, gaat het om potentieel gevaarlijke toepassingen. Dergelijke programma's beschikken niet meteen over schadelijke functies, maar kunnen onder bepaalde omstandigheden door aanvallers tegen u worden gebruikt. Tot deze categorie behoren bijvoorbeeld bepaalde hulpprogramma's voor beheer op afstand, programma's voor het automatisch omschakelen van het toetsenbord, IRC-clients, FTP-servers of verschillende hulpprogramma's voor het maken of verbergen van processen.

Quarantaine

Tijdens de viruscontrole hebt u de mogelijkheid om op verschillende manieren om te gaan met **ontdekte virussen**. Zo kunt u het besmette bestand bijvoorbeeld in quarantaine plaatsen. De quarantaine is een afgeschermd gedeelte binnen de software, waarin de besmette bestanden gecodeerd worden opgeslagen. Op die manier kan het virus niet verder worden verspreid.

De bestanden in quarantaine blijven daarbij in dezelfde toestand als toen de G Data-software een virus aantroef. U kunt dan later beslissen wat u verder met de bestanden wilt doen.

- **Bijwerken:** Als het dialoogvenster voor de quarantaine langere tijd geopend blijft en intussen een virus wordt gevonden en in quarantaine wordt geplaatst (bijvoorbeeld automatisch door de virusbewaker), kunt u met deze knop de weergave bijwerken.
- **Inzenden:** In bepaalde gevallen kunt u een geïnfecteerd bestand dat u niet kunt desinfecteren via internet naar G Data sturen. De inhoud van dit bestand wordt natuurlijk vertrouwelijk behandeld. De resultaten van het onderzoek worden gebruikt om de virushandtekeningen en de software te verbeteren en bij te werken. Lees hiervoor ook het hoofdstuk: [Feedback over malware](#)
- **Desinfecteren:** Vaak kunnen geïnfecteerde bestanden nog worden gered. De software verwijdert dan de virusbestanddelen uit het geïnfecteerde bestand en herstelt op die manier het niet-geïnfecteerde originele bestand. Als het desinfecteren geslaagd is, wordt het bestand automatisch op de oorspronkelijke plek teruggeplaatst en kunt u er weer zonder beperkingen over beschikken.
- **Terugplaatsen:** Soms kan het nodig zijn om een geïnfecteerd bestand dat niet kan worden gedesinfecteerd, uit quarantaine terug te plaatsen naar de oorspronkelijke plek. Dit kan bijvoorbeeld worden gedaan om te trachten gegevens te redden. Gebruik deze functie alleen in uitzonderingsgevallen en na strenge veiligheidsmaatregelen (zorg dat de computer niet meer verbonden is met een netwerk of internet, maak van tevoren een back-up van niet-geïnfecteerde gegevens enzovoort).
- **Verwijderen:** Wanneer u het geïnfecteerde bestand niet meer nodig hebt, kunt u dit gewoon uit de quarantaine verwijderen.

Logboeken

Onder Logboeken worden door de software aangemaakte logboeken weergegeven. Door te klikken op de kolomtitels **Starttijd**, **Type**, **Titel** of **Status** kunt u de beschikbare logboeken overeenkomstig sorteren. Met de knoppen **Opslaan als** en **Afdrukken** kunt u logboekgegevens ook als tekstbestand opslaan of rechtstreeks afdrukken. U kunt een logboek verwijderen door er in het overzicht met de muis op te klikken en vervolgens op de **Delete**-toets of op de knop **Verwijderen** te drukken.

Meervoudige licentie

Met een meervoudige licentie kunt u de G Data-software gebruiken op het aantal computers waarvoor u een licentie hebt. Na de installatie op de eerste computer en de internetupdate worden u online toegangsgegevens toegezonden. Als u de software op de volgende computer wilt installeren, voert u de gebruikersnaam en het wachtwoord in die u bij de registratie op de G Data-updateserver hebt gekregen. Herhaal deze procedure voor elke volgende computer. Gebruik voor de internetupdate voor al uw computers uw **toegangsgegevens** (gebruikersnaam en wachtwoord), die u na de eerste registratie hebt ontvangen. Ga hierbij als volgt te werk:

- 1 Start de G Data-software.
- 2 Klik in het SecurityCenter op **Virushandtekeningen > Virushandtekeningen bijwerken**.
- 3 Voer in het venster dat nu wordt geopend de toegangsgegevens in die u eerder per e-mail hebt ontvangen. Als u nu op OK klikt, krijgt uw computer een licentie.

Licentieverlenging

Een paar dagen voor uw licentie verloopt, verschijnt een informatievenster op de taakbalk. Als u hierop klikt, wordt een dialoogvenster geopend waarin u de licentie via een paar eenvoudige stappen direct kunt verlengen. Klik op de knop **Nu kopen**, vul uw gegevens in en uw computer is onmiddellijk weer beschermd tegen virussen. De factuur ontvangt u in de daaropvolgende dagen per post.

Dit dialoogvenster verschijnt alleen na afloop van het eerste jaar. Daarna wordt uw G Data -licentie elk jaar automatisch verlengd. U kunt dit abonnement echter te allen tijde zonder opgaaf van redenen opzeggen.

Nieuwe computer

U kunt uw G Data-product met de bijbehorende toegangsgegevens op een nieuwe of andere computer gebruiken. Installeer de software en voer uw toegangsgegevens in. De updateserver stelt vervolgens de verbinding met de nieuwe computer in. Als de G Data-software ook nog op uw oude computer staat, moet u de licentie van de oude naar de nieuwe computer overdragen. U kunt een licentie slechts een beperkt aantal keren overdragen. Als het maximumaantal licentieoverdrachten is bereikt, wordt de licentie volledig geblokkeerd. Er kan dan geen enkele update meer worden gedownload.

Deïnstallatie

De gemakkelijkste manier om de G Data-software van uw computer te verwijderen, is door in de G Data-**programmagroep** op de knop **Installatie ongedaan maken** te klikken. De deïnstallatie wordt dan volledig automatisch uitgevoerd. U kunt de installatie echter ook ongedaan maken via het Configuratiescherm van Windows.

- **Windows Vista, Windows 7:** Klik in de Windows-taakbalk op het Start-symbool (meestal links onder op het scherm) en selecteer de map **Configuratiescherm**. Daar vindt u de optie **Programma's > Een programma verwijderen**. Selecteer de G Data-software in de lijst en klik op de knop **Installatie ongedaan maken** om de installatie ongedaan te maken.
- **Windows XP:** Om dit te doen klikt u in de taakbalk van Windows op **Start** en kiest u de map **Instellingen > Configuratiescherm > Software**. Op het tabblad **Installeren/Installatie ongedaan maken** kunt u de G Data-software met de muis markeren. Klik vervolgens op de knop **Toevoegen/Verwijderen** om de installatie ongedaan te maken.

Als bij de deïnstallatie nog bestanden in het gedeelte **Quarantaine** van de G Data-software aanwezig zijn, wordt u gevraagd of u deze bestanden wilt verwijderen. Als u deze bestanden niet verwijdert, blijven ze in een speciale G Data-**map** versleuteld op uw computer opgeslagen, zodat ze geen schade kunnen aanrichten. Deze bestanden zijn pas weer beschikbaar als u de G Data-software opnieuw op uw computer hebt geïnstalleerd. Tijdens de deïnstallatie wordt u gevraagd of u **instellingen en logboeken** wilt verwijderen. Als u deze bestanden niet verwijdert, zijn de logboeken en instellingen weer beschikbaar als de software opnieuw is geïnstalleerd. Klik op de knop **Afsluiten** om de deïnstallatie te beëindigen. De software is nu volledig van uw systeem gedeïnstalleerd.

Schadelijke computeritems

Als men het over **virussen**, **wormen** en **Trojaanse paarden** heeft, dan heeft men het in het algemeen over een schadelijk aspect van software. Inmiddels is het overkoepelende begrip **malware** (een samentrekking van malicious = kwaadaardig en software) ingeburgerd. Onder **malware** vallen programma's die met kwaadaardige bedoelingen elektronische gegevens toegankelijk maken, wijzigen of verwijderen. Deze bezit altijd een schadelijke functie (in het Engels **payload**). Dit kan variëren van een ongevaarlijke melding over de eigen aanwezigheid tot het bespioneren van privégegevens en het wissen van de harde schijf. Malware kan worden onderverdeeld in drie groepen: **Trojaanse paarden**, **wormen** en **virussen**. In bredere zin vallen daar ook **spyware** en **dialers (die stiekem dure betaalnummers bellen)** onder.

- **Trojaanse paarden** Trojaanse paarden onderscheiden zich van wormen en virussen doordat ze zichzelf niet zelfstandig vermenigvuldigen. De naam **Trojaans paard** is afgeleid van het historische voorbeeld en beschrijft een programma dat de gebruiker wijsmaakt een bepaalde en gewenste functie te bezitten. Daarnaast bevatten trojanen nog een verborgen programmaonderdeel, waardoor de besmette computer toegankelijk wordt via een achterdeur, zonder dat de gebruiker dat in de gaten heeft. De mogelijkheden van Trojaanse paarden om zich te verbergen zijn vrijwel onbeperkt. Ze kunnen zich in commandoregels verstoppen (zogenaamde **Rootkits**) of als **Remote Access Trojans** (zogenaamde **RAT's**, ook wel **Backdoor** genoemd) binnendringen. Deze verraderlijke programma's worden echter ook via e-mail verstuurd als zogenaamde screensavers of spelletjes.

- **Overeenkomsten tussen virussen en wormen: Virussen en wormen** zijn opgebouwd uit de volgende componenten:

Reproductiecomponent: Deze programmacomponent zorgt voor de vermenigvuldiging van het virus. Het is een vast onderdeel van alle virussen. De besmetting kan plaatsvinden via USB-sticks (en andere verwisselbare gegevensdragers), vrijgegeven mappen, netwerkscans, peer-to-peer-netwerken of e-mail. Bovendien gebruiken de schadelijke programma's allerlei verschillende aanvalspunten, die gedeeltelijk alleen bij bepaalde combinaties van hardware, software en besturingssysteem functioneren.

Herkenningcomponent: De herkenningcomponent controleert of er al sprake is van een besmetting met dit virus. Elk programma wordt slechts eenmaal besmet om de verspreiding te versnellen en de vermomming in stand te houden.

Schadelijke component: De schadelijke functies (in het Engels **payload**) kunnen in de volgende groepen worden onderverdeeld: Met **backdoor**-programma's verschaft een hacker zich toegang tot de computer en de gegevens. Zo kan hij de gegevens manipuleren of **Denial of Service-aanvallen** starten. Er kunnen **gegevens** worden gemanipuleerd. Dat gaat van (min of meer grappige) meldingen, berichten en geluiden tot en met het wissen van bestanden en stations. Er kan ook **informatie** worden bekeken en verzonden. Het doel van deze aanvallen is het bemachtigen van **wachtwoorden**, **creditcardnummers**, **inlognamen** en andere persoonlijke gegevens. Vaak worden besmette computers misbruikt voor **Denial of Service (DoS)**-aanvallen. Deze doelen er bijvoorbeeld op een website door overbelasting plat te leggen. Als de aanval van slechts één bron afkomstig is, is deze eenvoudig af te weren. In **Distributed Denial of Service (DDoS)**-aanvallen worden daartoe besmette computers misbruikt om de aanvallen te ondersteunen. **DoS** en **DDoS**-aanvallen kunnen tot doel hebben het doelsysteem plat te leggen, de bandbreedte en de opslagcapaciteit te overbelasten of de dienst in het netwerk ontoegankelijk te maken.

Conditiecomponent: Zowel de verspreiding als ook de schadelijke functie kunnen afhankelijk van voorwaarden geprogrammeerd zijn. In het eenvoudigste geval start de schadelijke code automatisch, zonder dat het slachtoffer daar iets van merkt. In een aantal gevallen moet de payload door het slachtoffer zelf worden gestart. Dat kan gebeuren door het oproepen van een besmet programma, het openen van een e-mailbijlage of **phishing** van persoonlijke gegevens. Het starten van de schadelijke code kan ook aan voorwaarden gekoppeld zijn. Bij bepaalde virussen treedt bijvoorbeeld pas op een bepaalde datum of na een bepaald aantal oproepen schade op.

Camouflagecomponent: Wormen, trojaanse paarden en virussen proberen zichzelf te beschermen tegen ontdekking door de gebruiker en door virusscanners. Hiervoor maken ze gebruik van een reeks mechanismen. Zij herkennen dat een debug-programma draait of beschermen zichzelf door overvloedige en verwarrende (assembler)-programmaregels. Ze verbergen de sporen van een infectie. Daarvoor worden onder meer statusmeldingen of logboekgegevens vervalst. Een geheugenresident virus kan bijvoorbeeld het systeem voorspiegelen dat een reeds verwijderd programma nog steeds actief is in het geheugen dat het gebruikt. Om ontdekking tegen te gaan, coderen veel virussen zichzelf en/of hun schadelijke code. Bij het decoderen kunnen altijd dezelfde sleutels worden gebruikt. Deze sleutels kunnen uit een lijst zijn gekopieerd (**oligomorf**) of zij kunnen ongelimiteerd opnieuw worden bijgemaakt (**polymorf**).

- **Wormen:** In tegenstelling tot een virus, koppelt een **worm** zichzelf niet aan uitvoerbare bestanden. De worm verspreidt zich via netwerken of e-mailverbindingen door zichzelf automatisch naar andere computers over te dragen.

Netwerkwormen: In netwerken worden op willekeurig gekozen computers enkele poorten gescand en als een aanval mogelijk is, worden de zwakke plekken in logboeken (bijvoorbeeld IIS) of hun implementering misbruikt voor de verspreiding. Bekende boosdoeners in dit genre zijn **Lovsan/Blaster** en **CodeRed**. **Sasser** misbruikt een **buffer-overflow-fout** in de **Local Security Authority Subsystem Service (LSASS)** en besmet computers als deze met het internet verbonden zijn.

E-mailwormen: Bij de verspreiding per e-mail kan een worm een beschikbaar e-mailprogramma (zoals Outlook of Outlook Express) gebruiken of een eigen SMTP-mailengine bij zich dragen. Afgezien van het ontstane netwerkverkeer en het verhoogde gebruik van systeembronnen kunnen wormen nog meer schadelijke functies bevatten. Prominente leden van deze familie zijn **Beagle** en **Sober**.

- **Virussen:** Ook virussen richten zich op de eigen vermenigvuldiging en verspreiding naar andere computers. Daarvoor koppelen zij zich aan andere bestanden of nestelen ze zich in de bootsector van gegevensdragers. Ze worden vaak ongemerkt een pc binnengesmokkeld via verwisselbare gegevensdragers, via netwerken (ook peer-to-peer), per e-mail of via internet. Virussen kunnen veel verschillende plekken binnen het besturingssysteem aanvallen en werken via diverse kanalen. Men onderscheidt de volgende groepen:

Bootsectorvirussen: Bootsector- of **MBR-virussen** (= Master Boot Record-virussen) plaatsen zichzelf voor de eigenlijke bootsector van een gegevensdrager en zorgen er zo voor dat bij het opstarten vanaf deze gegevensdrager eerst de viruscode wordt gelezen en daarna de oorspronkelijke bootsector. Op deze manier nestelt het virus zich ongemerkt in het systeem en wordt het vanaf dat moment bij het opstarten vanaf de harde schijf uitgevoerd. Vaak blijft de viruscode na de besmetting in het geheugen aanwezig. Dergelijke virussen noemt men **geheugenresident**. Bij het formatteren van gegevensdragers wordt het virus dan doorgegeven en kan het zich ook verspreiden naar andere computers. Afhankelijk van de schadelijke code kunnen bootsector-virussen hinderlijk tot uiterst gevaarlijk zijn. Het oudste en meest verspreide virus van dit type draagt de naam **Form**.

Bestandsvirussen: Veel virussen maken gebruik van de mogelijkheid om uitvoerbare bestanden als verstopplaats te gebruiken. Daartoe wordt een belangrijk bestand gewist of overschreven of koppelt het virus zich aan het bestand. In het laatste geval blijft de uitvoerbare code van het bestand goed functioneren. Als het uitvoerbare bestand wordt opgeroepen, dan wordt de meestal in Assembler geschreven viruscode uitgevoerd en pas daarna het oorspronkelijke programma gestart (indien dit niet gewist is).

Multipartitie-virussen: Deze virussen zijn uiterst gevaarlijk omdat ze zowel de bootsector (respectievelijk partitietabellen) besmetten als ook uitvoerbare bestanden aanvallen.

Companionvirussen: Onder DOS worden .com-bestanden uitgevoerd vóór gelijknamige .exe-bestanden. In de tijd dat computers alleen of vooral via commando-regels werden bediend, was het een manier om ongemerkt schadelijke code op een computer uit te voeren.

Macrovirussen: Ook macrovirussen koppelen zich aan bestanden. Deze zijn echter zelf niet uitvoerbaar. Macrovirussen zijn ook niet geschreven in assembler, maar in een macrotaal als **Visual Basic**. Om het virus uit te voeren, moet het worden vertaald door een macrotaal die is geïntegreerd in Word, Excel, Access en PowerPoint. Bij macrovirussen kunnen dezelfde mechanismen werkzaam zijn als bij bestandsvirussen. Ook kunnen ze zich camoufleren, de bootsector besmetten of companionvirussen aanmaken.

Stealth-virussen: Stealth-virussen of **gemaskeerde virussen** bezitten speciale beschermingsmechanismen om niet door virusscanners te worden ontdekt. Daartoe nemen ze de controle van diverse systeemfuncties over. Is dit eenmaal gelukt, dan kunnen deze virussen bij een normale toegang tot bestanden of systeemgebieden niet meer worden gedetecteerd. Zij spiegelen een virusscanner de niet-besmette toestand van een besmet bestand voor. De camouflagemechanismen van stealth-virussen werken pas nadat het virus zich in het werkgeheugen bevindt.

Polymorfe virussen: Polymorfe virussen bevatten mechanismen om hun uiterlijk bij iedere besmetting te veranderen. Daartoe worden delen van het virus gecodeerd. De in het virus geïntegreerde versleutelingsroutine genereert daarbij voor iedere kopie een nieuwe sleutel en voor een deel zelfs nieuwe versleutelingsroutines. Bovendien kunnen reeksen opdrachten die niet vereist zijn voor het functioneren van het virus worden verwisseld of willekeurig worden tussengevoegd. Op die manier kunnen eenvoudigweg miljarden varianten van een virus ontstaan. Om er zeker van te zijn dat gecodeerde en polymorfe virussen worden herkend en vernietigd, is het gebruik van klassieke virusdefinities (ook handtekeningen genoemd) vaak niet voldoende. Meestal moeten er speciale programma's voor worden geschreven. De onderzoekskosten en het inzetten van speciale tegenmaatregelen kunnen daardoor extreem hoog zijn. Polymorfe virussen zijn dus zonder overdrijving te beschouwen als de hoogste klasse onder de virussen.

Intended virus: Een **intended virus** is een gedeeltelijk defect virus dat er weliswaar in slaagt een bestand een eerste besmetting toe te brengen, maar zich niet verder weet te vermenigvuldigen.

E-mailvirussen: E-mailvirussen behoren tot de groep van zogenaamde **Blended threats** (= vermengde bedreigingen). Deze malware combineert de eigenschappen van trojanen, wormen en virussen. Door het **Bubbleboy-virus** werd bekend dat het mogelijk is om al bij de preview van een HTML-mail een virus op de pc binnen te sluisen. De gevaarlijke viruscode verstopt zich in HTML-e-mails en misbruikt een beveiligingslek in Microsoft Internet Explorer. Het gevaar van dergelijke combivirussen mag niet worden onderschat.

- **Malware in bredere zin:** Volledigheidshalve moet hier nog een aantal andere lastige en deels ook schadelijke categorieën worden genoemd, die wij echter niet rekenen tot de groep malware.

Hoaxes: Hoaxes zijn zogenaamde viruswaarschuwingen die vaak per e-mail worden verspreid. De ontvanger wordt aangespoord de e-mailwaarschuwing door te zenden aan vrienden en bekenden. Meestal gaat het bij deze berichten alleen om paniekzaaij.

Backdoor-programma's: Veel systeembeheerders gebruiken programma's voor beheer op afstand om computers quasi van op een afstand te besturen. Vooral bij grote ondernemingen is dit zeer nuttig. Normaal gesproken heeft de systeembeheerder toegang tot het systeem met medeweten en goedkeuring van de gebruiker van de pc. Pas wanneer deze backdoor-functies zonder medeweten van de pc-gebruiker worden gebruikt en er schadelijke handelingen worden verricht, verandert een backdoor-programma in malware.

Spyware: Spyware houdt de activiteiten en processen op een computer bij en maakt deze gegevens toegankelijk voor derden. Vaak worden deze gebruikt voor het analyseren van het surfgedrag, zodat passende reclamebanners kunnen worden weergegeven.

Dialers: Net als virussen, wormen en trojanen, worden dialers (telefoonkiezers) vaak ongemerkt op de computer geïnstalleerd. Als de verbinding per modem wordt opgebouwd, wordt dan bij de eerstvolgende verbinding een duur servicenummer gebruikt. Een lastige plaag die tot grote financiële schade kan leiden. Met anti-dialerprogramma's als **Dialer Control** kan men zich tegen ongewenste dialers wapenen.

Spam: Een eveneens dure en vervelende plaag is het verzenden van ongewenste reclamemail of propagandamail. Moderne antispamprogramma's combineren statische (tekstanalyse, overzichten van mailservers) en automatische (op de theorie van Bayes gebaseerde) procedures om ongewenste post uit te filteren.

Phishing: Onder **phishing** verstaat men de poging om via vervalste websites of e-mails persoonlijke gegevens te bemachtigen, zoals inlognamen, wachtwoorden, creditcardnummers en toegangsgegevens van bankrekeningen. Vaak wordt men hierbij naar een vervalste website geleid. In de afgelopen jaren is dit fenomeen sterk toegenomen.

Vorzorgsmaatregelen

Hoewel de G Data-software niet alleen bekende virussen ontdekt en verwijdert, maar met behulp van de heuristische analyse ook tot nog toe onbekende schadelijke programma's herkent, is het vanzelfsprekend beter een virusinfectie van tevoren onmogelijk te maken. Daarvoor zouden enkele veiligheidsmaatregelen moeten worden genomen die niet veel moeite kosten, maar de veiligheid van uw systeem en uw gegevens echter aanmerkelijk verhogen.

- **Gebruikersaccounts gebruiken:** U dient twee gebruikersaccounts op uw computer te gebruiken. Een **administrator-account**, die u telkens gebruikt als u software installeert of belangrijke instellingen op uw computer uitvoert, en een **gebruikersaccount** met beperkte rechten. De gebruikersaccount zou bijvoorbeeld niet in staat mogen zijn programma's te installeren of wijzigingen in het besturingssysteem van Windows aan te brengen. Met deze account kunt u met relatief weinig risico's bijvoorbeeld op het internet surfen en gegevens van externe computers overnemen. In de Help-documentatie van het besturingssysteem van Windows wordt uitgelegd hoe u de verschillende gebruikersaccounts instelt.
- **Spammails negeren:** Kettingbrieven en spammails mogen in principe nooit worden beantwoord. Zelfs als zulke e-mails geen virus bevatten, vormt het ongewenste doorzenden een aanzienlijke belasting voor de gegevensstroom via het internet.
- **Virusverdenking controleren:** Als u denkt met een virus van doen te hebben, bijvoorbeeld wanneer pas geïnstalleerde software niet zoals verwacht functioneert of een foutmelding geeft, voert u de viruscontrole voor het betreffende programma uit voordat u de computer opnieuw opstart. Dit maakt het eenvoudiger om Trojaanse paarden op te sporen en te bestrijden, omdat sommige Trojaanse paarden zich pas nestelen en hun sporen uitwissen als de computer opnieuw is opgestart.
- **Regelmatige Windows-updates:** De laatste Microsoft-patches moeten regelmatig worden geïnstalleerd. Die dichten vaak recent ontdekte beveiligingslekken van Windows, nog voordat een maker van virussen op het idee is gekomen deze te gebruiken om schade aan te richten. Windows-update is een functie die geautomatiseerd kan worden.

- **Originele software gebruiken:** In uiterst zeldzame gevallen kunnen de gegevensdragers van originele software geïnfecteerd zijn met virussen, maar de kans op een virusinfectie door illegale kopieën of kopieën op herschrijfbaar gegevensdragers is aanzienlijk hoger. Gebruik daarom uitsluitend originele software.
- **Software vanaf het internet voorzichtig behandelen:** Wees bovendien zeer kritisch bij het downloaden van software vanaf het internet en sta het gebruik van dergelijke software alleen toe als deze ook werkelijk vereist is en als de herkomst van de software betrouwbaar is. Open nooit bestanden die via e-mail door onbekenden, of onverwacht door vrienden, collega's of bekenden, werden toegestuurd. Vraag altijd eerst aan de afzender of de betreffende toepassing al dan niet zonder risico's kan worden gestart.

Index

A

Aanmelden 16
 Aanwijzingen voor deïnstallatie 28
 Achtergrondscan 8
 Adressen van geïnfecteerde internetpagina's inzenden 16
 Adware 12
 Afgelopen licentie 28
 Afwezigheidsscan 18
 Algemeen 19
 Alleen in logboek registreren 24
 Archiefbestanden 12, 14, 19
 Archieven controleren 12, 19
 Asterisk-symbool 12
 Automatische updates uitschakelen 10
 Automatische viruscontroles 18

B

Beknopte handleiding 2
 Bericht bijvoegen bij ontvangen geïnfecteerde e-mails 17
 Bestand in quarantaine plaatsen 24
 Bestand verwijderen 24
 Bestandstypen 19
 Bewaker 12
 Bewakerstatus 12
 Bewerkingsnummer 2
 Bij het starten van het systeem 19
 Bij server aanmelden 15, 16
 Bij zware systeembelasting de viruscontrole onderbreken 14, 24
 BootScan 3, 21
 BootScan voor de installatie 21
 Bootsectoren 19
 Bureaubladsymbool 5

C

Cd-roms 8
 Computer controleren 8
 Computer na de viruscontrole uitschakelen 24
 CPU-belasting 7

D

De aanmelding is met succes uitgevoerd. 16
 Deïnstallatie 28
 Desinfecteren (indien niet mogelijk: alleen in logboek registreren) 24
 Desinfecteren (indien niet mogelijk: Bestand verwijderen) 24
 Desinfecteren (indien niet mogelijk: bijlage/tekst verwijderen) 17
 Desinfecteren (indien niet mogelijk: in quarantaine) 12, 14, 24
 Dialers 12
 Dvd-roms 8

E

E-mailarchieven controleren 12, 19

E-mailcontrole 17
 E-mails 17
 E-mails vóór het verzenden controleren 17
 Engines 12, 14, 19
 Engines gebruiken 12, 14, 17, 19
 Enkel nieuwe of gewijzigde bestanden controleren 12
 Extra 17

F

Firefox 16

G

Gebruikersaccount 20
 Gebruikersnaam 3, 15
 Gedragscontrole 12
 Geheugen 8
 Geheugen en automatisch starten controleren 8
 Geheugenkaarten 8
 Geïnfecteerde archieven 12, 14, 19
 Geïnfecteerde bestanden 12, 14, 19

H

Handmatige viruscontrole 14
 Helptonen 6
 Heuristiek 12, 19
 Hoe kom ik in het bezit van extra of uitgebreide licenties? 7
 HOSTS-bestand 12
 HTTP-webinhoud 16

I

IMAP 17
 In geval van een infectie 17
 Info 6
 Inhoud van chatberichten verwerken 16
 Inkomende e-mails 17
 Installatie 3
 Installatie van de software 3
 Installatie vanaf cd/dvd 3
 Installatie vanaf USB-stick 3
 Internet Explorer 16
 Internetinhoud (HTTP) verwerken 16
 Internetinstellingen 15, 16
 Internetupdate 16

K

Keuzemenu 8, 10
 Klantgegevens 16
 Koppelen aan de Messenger-toepassing 16

L

Laatste update 10
 Laatste viruscontrole 8
 Laatste virusupdate 10
 Laptops 19
 Licentie 7
 Licentieverlenging 28
 Logboek samenstellen 15, 19

Logboeken 6,27

M

Malware Information Initiative 26
Map op virussen controleren 17
Mappen/bestanden controleren 8
Maximale grootte voor downloads 17
Meervoudige licentie 28
Melding not-a-virus 27
Met wachtwoord beveiligde archieven 24
Microsoft Messenger 16
Microsoft Outlook 17
Minimumvereisten 3
Modus 12

N

Na de installatie 5
Na voltooiing van de taak de computer uitschakelen 19
Netwerktogingen controleren 12
Niet in batterijbedrijf uitvoeren 19
Nieuwe computer 28
Nieuwe installatie 28
not-a-virus 27

O

Omvang van de analyse 19
Onderdeel automatisch starten 8
Ontvangen e-mails controleren 17
Op dialers / spyware / adware / riskware controleren 12,19
Op RootKits controleren 8,19
Opstart-cd 6
Opstart-cd maken 6
OutbreakShield 17
Outlook 17

P

Phishing 16
Phishingbeveiliging 16
Plug-in 17
Poort 17
POP3 17
Productactivering 3
Programma bijwerken 6
Programmaversie 6
Proxyserver 16
Proxyserver gebruiken 16
PST 12,14

Q

Quarantaine 8,27

R

RAR 12,14
Registratienummer 2,16
Registratienummer invoeren 3
Riskware 12
RootKits 8,19

S

Scan-instellingen 19
Scanopties 17
Schadelijke computeritems 29
SecurityCenter 6
Security-symbool 5
Serverpoortnummer 17
ServiceCenter 2
Shredder 5
Snelcontrole 5
Software downloaden 3
Spyware 12
Standaardpoorten 17
Symbool 23
Systeembeveiliging 12
Systeemgebieden bij het starten van het systeem controleren 12
Systeemgebieden bij wisselen van medium controleren 12
Systeemgebieden controleren 19
Systeemstart 12

T

Taak alsnog uitvoeren als de computer op de geplande starttijd nog niet werd ingeschakeld 19
Testversie 3
Tijdelijke plaatsaanduidingen 12
Tijdoverschrijding bij de e-mailserver voorkomen 17
Tijdoverschrijding in de browser voorkomen 17
Tijdschema 19
Toegang geweigerd 24
Toeganggegevens 2
Toeganggegevens invoeren 3
toeganggegevens voor de internetverbinding 16
Trillian 16

U

Uitgaande e-mails 17
Uitgebreid 12,14,17,19
Uitzonderingen 12
Uitzonderingen ook voor de achtergrondscan gebruiken 14
Uitzonderingen vastleggen 11,17
Updates 15
USB-sticks 8

V

Verloop van een viruscontrole 24
Versiecontrole 15
Verwisselbare media controleren 8
Virus gevonden 26
Virusbeveiliging 8
Virusbewaker 7,8
Virusbewaker uitschakelen 8
Viruscontrole 7,8,21,24
Virushandtekeningen 10
Virushandtekeningen automatisch bijwerken (aanbevolen) 15

Virushandtekeningen bijwerken 10

Volgende update 10

Voorzorgsmaatregelen 31

Vraagteken-symbool 12

W

Wachtwoord 3,15

Wat gebeurt er bij afloop van mijn licentie? 7

Webbeveiliging 11,16

Wetenswaardigheden 21

Whitelist 11

Wisselen van medium 12

Z

ZIP 12,14