G DATA

Security Software

Inhoudsopgave

De eerste stappen

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

> **Opmerking**: in de software kunt u op elk moment de uitgebreide Help-documentatie raadplegen en krijgt u meteen alle relevante informatie. Klik daarvoor in het programma op het daar afgebeelde Help-symbool.

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:

G DATA België	www.gdata.be
G DATA Nederland	www.gdata.nl

Installatie

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 is geïnfecteerd, raden wij u aan een **BootScan** uit te voeren voordat u de software installeert.

> **Opgelet**: Als u tot nu toe antivirussoftware van een andere fabrikant hebt gebruikt, moet u deze van tevoren volledig van uw computer verwijderen. Omdat antivirussoftware heel diep in de systeemstructuur van Windows geïntegreerd is, is het aan te raden de software niet enkel te verwijderen door een normale deïnstallatie uit te voeren, maar indien mogelijk ook de desinfectieprogramma's te gebruiken die de fabrikant online ter beschikking stelt in zijn supportcentrum.

Stap 1 - Begin van de installatie

Start de installatie als volgt:

- **Installatie vanaf cd/dvd**: Om de installatie te starten, plaatst u de software-cd of -dvd in het cd- of dvd-station.
- **Software downloaden**: Om de installatie van een via internet gedownloade versie van de software te starten, klikt u op het gedownloade bestand.

Er wordt nu automatisch een installatievenster geopend.

> **Opmerking**: Als de installatie niet automatisch start: het is mogelijk dat u de functie voor automatisch starten van uw computer niet op de juiste manier hebt ingesteld. In dat geval kan de software de installatie na het plaatsen van de software-cd 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**.
> - Wanneer geen keuzevenster wordt geopend, zoekt u in uw Windows Verkenner de gegevensdrager met de G DATA software en vervolgens start u het bestand **Setup** of **Setup.exe**.

Stap 2 - Taalkeuze

Selecteer nu de taal waarin u de nieuwe G DATA software wilt installeren.

Stap 3 - Installatiemethode

Een wizard begeleidt u verder bij de installatie van de software op uw computer. Bepaal nu of u de standaardinstallatie of een aangepaste installatie wilt uitvoeren. Wij bevelen hier de standaardinstallatie aan.

Malware Information Initiative: De medewerkers van G DATA Security Labs onderzoeken voortdurend manieren om klanten van G DATA te beschermen tegen malware (virussen, wormen en schadelijke programma's). 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 geïnfecteerde systemen. Om deze gegevens ook in de analyses te kunnen opnemen, werd het G DATA Malware Information Initiative opgericht. Hierbij wordt informatie over malware naar G DATA Security Labs verstuurd. Dankzij uw deelname

kunnen alle klanten van G DATA internet op een veiligere manier gebruiken. Tijdens de installatie van de G DATA software kunt u beslissen of u gegevens al dan niet wilt ter beschikking wilt stellen aan G DATA Security Labs.

> **Opmerking**: bij de door de gebruiker gedefinieerde installatie kunt u de locatie voor de programmabestanden individueel selecteren en bepalen welke softwaremodules (bijvoorbeeld spambeveiliging) moeten worden geïnstalleerd.

Stap 4 - Licentieovereenkomst

Lees nu de licentieovereenkomst en ga hiermee akkoord.

Stap 5 - Door gebruiker gedefinieerde installatie

Als u de aangepaste installatie hebt gekozen, verschijnen er nu twee wizardvensters waarin u de installatiemap voor de software en de omvang van de geïnstalleerde modules kunt bepalen. Als u de standaardinstallatie hebt gekozen, kunt u deze stap overslaan.

- **Aangepast**: Hier bepaalt u de installatieomvang door de vinkjes bij de verschillende softwaremodules (zoals AntiSpam enz.) in te schakelen.
- **Volledig**: Alle softwaremodules van uw softwareversie worden geïnstalleerd.
- **Minimaal**: Met de optie wordt enkel de module AntiVirus, de basisbeveiliging tegen virussen, van uw G DATA software geïnstalleerd.

> **Updates**: Via de setup kunt u op elk gewenst moment aanvullende softwaremodules installeren of uw software bijwerken. Start daarvoor de setup opnieuw en selecteer **Installatie aanpassen** om modules aan de software toe te voegen of weg te laten. Als u over een nieuwe softwareversie beschikt en uw softwareversie wilt bijwerken, kunt u met de optie **Aangepaste update** bepalen welke modules moeten worden toegevoegd of weggelaten.

Stap 6 - Softwareversie

Nu kunt u ook bepalen of u de software als volledige versie of als testversie wilt installeren. Als u de software gekocht hebt en een registratienummer hebt, kiest u hier natuurlijk de optie **Volledige versie**. Als u gratis wilt kennismaken met de G DATA software, kunt u ook onze beperkte testversie gebruiken.

Stap 7 - Productactivering

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

- **Een nieuw 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 de productverpakking.

  > **Opmerking**: wanneer u het registratienummer invoert, wordt het product geactiveerd en ontvangt u bovendien de toegangsgegevens via e-mail zodat u deze later kunt gebruiken.

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

  > **Opmerking**: toegangsgegevens worden uitsluitend via 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 ondertussen is gewijzigd, neem dan contact op met ons **ServiceCenter**.

- **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 het internet gedownload en is uw computer dus niet voldoende beschermd tegen schadelijke software. U kunt uw registratienummer of toegangsgegevens altijd achteraf nog invoeren zodra u een update uitvoert.

Stap 8 - Einde van de installatie

Na de installatie moet u mogelijk uw computer opnieuw opstarten. U kunt de G DATA software nu gebruiken.

Na de installatie

Na de installatie kunt u de nieuw geïnstalleerde G DATA software starten met het programmasymbool in de taakbalk. Daarnaast zijn er nog een aantal bijkomende beveiligingsfuncties beschikbaar op uw computer:

Security-symbool Uw G DATA software beveiligt uw computer permanent tegen schadelijke software en aanvallen. Het symbool in de taakbalk van uw computer geeft aan wanneer u als gebruiker actie moet ondernemen via de software. Door met de rechtermuisknop op het symbool te klikken, kunt u de interface van G DATA openen. Lees hierover ook het hoofdstuk **Security-symbool**.

Shredder: als u tijdens de installatie de shredder hebt geselecteerd (niet geïntegreerd in G DATA Antivirus), wordt deze als symbool weergegeven op uw bureaublad. Gegevens die u in de shredder plaatst, worden verwijderd en kunnen niet worden teruggehaald, ook niet met professionele tools voor gegevensherstel. Daarbij worden de gegevens met een vrij definieerbaar aantal doorgangen overschreven. U kunt de instellingen openen door rechts te klikken op het Shredder-pictogram en de eigenschappen op te roepen.

Snelcontrole: Met de snelcontrole kunt u bestanden heel eenvoudig controleren zonder dat u de software hoeft te 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.

Uw computer start na de installatie van de software niet op de gebruikelijke manier: de software-cd bevindt zich mogelijk nog in het station. Als u de cd uit het station haalt, start uw computer weer zoals u gewend bent.

SecurityCenter

U hoeft het SecurityCenter alleen maar te openen als u een van de vele extra functies van de software wilt gebruiken. De daadwerkelijke beveiliging van uw computer tegen virussen en andere bedreigingen gebeurt voortdurend op de achtergrond. Zodra u zelf bepaalde handelingen moet uitvoeren, wordt u hiervan automatisch op de hoogte gebracht via de informatie in de taakbalk van uw computer.

Beveiligingsstatus

Zolang er overal een groen vinkje staat, 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.

Het jokerteken geeft aan dat u de desbetreffende beveiligingsfunctie (bijvoorbeeld de spambeveiliging) niet hebt geactiveerd (bijv. spambeveiliging).

Het gele symbool geeft aan dat u op korte termijn actie moet ondernemen. Dat is bijvoorbeeld het geval wanneer er een programma-update voor de software beschikbaar is.

Alle andere functies en programmaonderdelen van de software (zoals **Viruscontrole** of **Instellingen**) kunt u gebruiken als u zich actief met de beveiliging van uw systeem wilt bezighouden – maar dat is niet verplicht! Bepaal zelf in welke mate u zich wilt bezighouden met het thema virus- en gegevensbeveiliging. In de software kunt u uitgebreide Help-documentatie raadplegen.

Overkoepelende functies

De volgende symbolen verwijzen naar het beveiligingsniveau van het betreffende gebied.

Instellingen: Als u rechtsboven op deze knop klikt, krijgt u toegang tot alle dialoogvensters voor de instellingen voor de verschillende onderdelen van de software. Vanuit een bepaald onderdeel kunt u echter ook direct het bijbehorende instellingendialoogvenster selecteren.

Logboeken: hier vindt u de logboeken over alle recentelijk uitgevoerde acties (viruscontrole, update, gevonden virussen enzovoort).

Rechtsboven in de koptekst van de software vindt u bovendien nog de volgende functies:

Help tonen: U kunt in de software op elk moment de uitgebreide Help-documentatie raadplegen. Klik daarvoor in het programma op de daar afgebeelde Help-knop.

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. 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** .

Statusweergaven

De volgende statusweergaven informeren u over de beveiligingstoestand van uw systeem. Wanneer u op deze items klikt, kunt u direct acties uitvoeren om de beveiligingsstatus te optimaliseren:

Realtimebeveiliging

De realtimebeveiliging van de virusbewaker scant uw computer doorlopend op virussen en controleert schrijf- en leesprocessen. Zodra een programma schadelijke functies probeert uit te voeren of schadelijke bestanden probeert te verspreiden, wordt dat door de bewaker verhinderd. De virusbewaker is uw belangrijkste bescherming! Schakel deze nooit uit!

- **Virusbewaker uitschakelen**: Als u de virusbewaker toch wilt uitschakelen, kunt u dat hier doen. Wanneer u de prestaties van uw computer wilt optimaliseren door de bewaker uit te schakelen, moet u eerst controleren of u eventueel met een andere instelling van de virusbewaker het gewenste resultaat kunt bereiken. Daarom hebt u bij het uitschakelen van de virusbewaker de mogelijkheid de instellingen overeenkomstig te wijzigen. Klik daarvoor op **Beveiliging / prestaties wijzigen** en volg de instructies in het gelijknamige Help-hoofdstuk. U kunt de virusbewaker natuurlijk ook volledig uitschakelen.

- **Gedragscontrole uitschakelen**: Gedragscontrole wordt gebruikt voor het herkennen van onbekende schadelijke software en biedt bijkomende beveiliging onafhankelijk van virushandtekeningen. De gedragscontrole moet in principe ingeschakeld zijn.

- **Meer instellingen**: meer informatie hierover vindt u in het hoofdstuk **Instellingen | AntiVirus | Realtimebeveiliging**.

Laatste afwezigheidsscan

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.

- **Computer controleren**: Wanneer u hiervoor voldoende tijd hebt en u de computer de komende uren niet nodig hebt, kunt u hier direct een volledige controle van de computer starten. U kunt de computer tijdens deze controle blijven gebruiken, maar omdat de viruscontrole bij deze instelling met maximale prestaties wordt uitgevoerd, is het mogelijk dat andere toepassingen trager reageren. Meer informatie hierover vindt u in het hoofdstuk **Viruscontrole**.

- **Afwezigheidsscan nu starten**: de afwezigheidsscan start automatisch in periodes waarin uw computer inactief is en voert zo, met automatisch vastgelegde intervallen, een controle van de volledige computer uit. Als u de afwezigheidsscan wilt starten voor het volgende automatisch vastgelegde tijdstip, selecteert u **Afwezigheidsscan nu starten**. Als u niet wilt dat de G DATA software tijdens uw pauzes automatisch de afwezigheidsscan start, kunt u deze functie ook uitschakelen onder **Afwezigheidsscan uitschakelen** (niet aanbevolen).

Firewall

Een firewall voorkomt dat gegevens op uw computer *bespied* worden. Hij controleert welke gegevens en programma's via het internet of een netwerk op uw computer binnenkomen en welke gegevens via uw computer worden verzonden. Zodra het blijkt dat gegevens op uw computer onrechtmatig moeten worden geïnstalleerd of gedownload, slaat de firewall alarm en blokkeert hij de onrechtmatige gegevensuitwisseling. Deze softwaremodule is beschikbaar in de programmaversies G DATA Internet Security en G DATA Total Security.

- **Firewall uitschakelen**: U kunt de firewall desgewenst ook uitschakelen. Uw computer blijft dan verbonden met internet en andere netwerken, maar wordt dan niet langer door de firewall beveiligd tegen aanvallen of spionage (niet aanbevolen).

- **Automatische piloot uitschakelen**: Over het algemeen is het zinvol de firewall in de functie **Automatische piloot** te gebruiken. Hij werkt dan zo goed als onzichtbaar op de achtergrond en beschermt u zonder dat u al te veel instellingen moet opgeven. Als u de firewall zonder de automatische piloot gebruikt, wordt in geval van twijfel een dialoogvenster weergegeven waarin u de firewall geleidelijk aan optimaal kunt afstemmen op uw systeem. Voor ervaren gebruikers is dit een handige functie. Normaal gesproken is het echter niet aanbevolen om de automatische piloot uit te schakelen.

- **Meer instellingen**: meer informatie hierover vindt u in het hoofdstuk **Instellingen | Firewall | Automatisch systeem**.

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.

- **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.

- **Uitzonderingen vastleggen**: De webbeveiliging zorgt ervoor dat u op 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.

- **Meer instellingen**: meer informatie hierover vindt u in het hoofdstuk **Instellingen | AntiVirus | Webbeveiliging**.

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.

- **E-mailcontrole uitschakelen**: Selecteer deze optie als u niet wilt dat de G DATA software e-mails controleert. Bedenk wel dat uitschakeling van automatische updates een hoog veiligheidsrisico met zich meebrengt. Selecteer deze optie dus alleen in uitzonderlijke gevallen.

- **Meer instellingen**: meer informatie hierover vindt u in het hoofdstuk Instellingen | AntiVirus | E-mailcontrole.

Microsoft Outlook: hier worden de e-mails gecontroleerd door middel van een plug-in. Deze biedt dezelfde bescherming als de beveiliging voor POP3/IMAP in de opties van AntiVirus. 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.

Spambeveiliging

Speciale aanbiedingen, reclame, nieuwsbrieven – het aantal ongewenste e-mails neemt voortdurend toe. Wordt uw e-maibox ook overspoeld door al die ongewenste elektronische post? De G DATA software biedt betrouwbare beveiliging tegen spam, blokkeert afzenders van spam op een efficiënte manier en verhindert foutieve herkenning op basis van een combinatie van de modernste spamcontrolecriteria. Deze softwaremodule is beschikbaar in de programmaversies G DATA Internet Security en G DATA Total Security.

- **Logboek: spam**: Hier vindt u een uitgebreid overzicht van alle e-mails die de G DATA software als spam beschouwt. Klik op de knop **Bijwerken** om de meest actuele gegevens van de software op te roepen. Klik op de knop **Verwijderen** om de in dit overzicht gemarkeerde regels te wissen. De eigenlijke e-mails in uw e-mailprogramma worden daarbij uiteraard niet gewist. Via de knop **Op Whitelist** kunt u een gemarkeerde e-mail aan de whitelist toevoegen. Hierdoor wordt het betreffende e-mailadres van verdere spamcontrole uitgesloten. Via de knop **Op Blacklist** kunt u een gemarkeerde e-mail aan de blacklist toevoegen. Hierdoor wordt het betreffende e-mailadres speciaal op spamelementen gecontroleerd.

- **Logboek: geen spam**: Hier vindt u een uitgebreid overzicht van alle e-mails die de G DATA software niet als spam beschouwt. Klik op de knop **Bijwerken** om de meest actuele gegevens van de software op te roepen. Klik op de knop **Verwijderen** om de in dit overzicht gemarkeerde regels te wissen. De eigenlijke e-mails in uw e-mailprogramma worden daarbij uiteraard niet gewist. Via de knop **Op Whitelist** kunt u een gemarkeerde e-mail aan de whitelist toevoegen. Hierdoor wordt het betreffende e-mailadres van verdere spamcontrole uitgesloten. Via de knop **Op Blacklist** kunt u een gemarkeerde e-mail aan de blacklist toevoegen. Hierdoor wordt het betreffende e-mailadres speciaal op spamelementen gecontroleerd.

- **Whitelist bewerken**: Met de Witte lijst kunt u adressen van afzenders of domeinen uitzonderen van een spamverdenking. Klik daarvoor op de knop **Nieuw** en typ in het veld **Afzender/Afzenderdomeinen** het e-mailadres (bijvoorbeeld newsletter@infopag.nl) of domein (bijvoorbeeld infopag.nl) dat u van spamverdenking wilt uitsluiten. De G DATA software zal e-mails van deze afzender of dit afzenderdomein dan niet als spam behandelen. Met de knop Importeren kunt u ook kant-en-klare lijsten met e-mailadressen of domeinen aan de whitelist toevoegen. De adressen en domeinen moeten in een dergelijke lijst op aparte regels onder elkaar zijn ingevoerd. Als formaat wordt hierbij een eenvoudig txt-bestand gebruikt, zoals dat bijvoorbeeld in Windows Kladblok kan worden aangemaakt. Met de knop **Exporteren** kunt u een dergelijke whitelist ook als tekstbestand exporteren.

- **Blacklist bewerken**: Met de blacklist kunt u adressen van bepaalde afzenders of domeinen identificeren als verzenders van spam. Klik daarvoor op **Nieuw** en typ in het veld **Afzender/Afzenderdomeinen** het e-mailadres (bijvoorbeeld newsletter@megaspam.nl) of domein (bijvoorbeeld megaspam.nl) dat u wilt aanmerken als spam. De G DATA software zal e-mails van deze afzender of dit afzenderdomein voortaan beschouwen als e-mails met een zeer hoge spamwaarschijnlijkheid. Met de knop **Importeren** kunt u ook kant-en-klare lijsten met e-mailadressen of domeinen aan de blacklist toevoegen. De adressen en domeinen moeten in een dergelijke lijst op aparte regels onder elkaar zijn ingevoerd. Als formaat wordt hierbij een eenvoudig txt-bestand gebruikt, zoals dat bijvoorbeeld in Windows Kladblok kan worden aangemaakt. Met de knop **Exporteren** kunt u een dergelijke blacklist ook als tekstbestand exporteren.

- **Spambeveiliging uitschakelen**: Indien gewenst kunt u hier de spambeveiliging op uw computer uitschakelen, bijvoorbeeld omdat er helemaal geen e-mailprogramma op uw computer is geïnstalleerd.

- **Overige instellingen**: meer informatie hierover vindt u in het hoofdstuk Instellingen | AntiSpam | Spamfilter.

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**.

- **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.

- **Meer instellingen**: meer informatie hierover vindt u in het hoofdstuk **Instellingen | AntiVirus | Updates**.

Volgende update

Hier ziet u wanneer de volgende update wordt uitgevoerd. Wanneer u direct een update wilt uitvoeren, klikt u op het item en selecteert u de optie **Virushandtekeningen bijwerken**.

- **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.
- **Meer instellingen**: meer informatie hierover vindt u in het hoofdstuk **Instellingen | AntiVirus | Updates**.

BankGuard

Banktrojanen vormen een steeds grotere bedreiging. Elk uur ontwikkelen cybercriminelen nieuwe malwarevarianten (bv. ZeuS, SpyEye) om uw geld te stelen. Banken beveiligen het gegevensverkeer op internet, maar de gegevens worden gedecodeerd in de browser en daar slaan banktrojanen toe. De toonaangevende technologie van G DATA BankGuard beveiligt uw banktransacties vanaf het begin en biedt meteen beveiliging op de plaatsen waar de aanval plaatsvindt. Door de gebruikte netwerkbibliotheken in realtime te controleren, zorgt G DATA BankGuard ervoor dat uw internetbrowser niet door een banktrojaan wordt gemanipuleerd. We raden u aan om de beveiliging van G DATA BankGuard ingeschakeld te laten.

Keyloggerbeveiliging

de keyloggerbeveiliging controleert ook onafhankelijk van virushandtekeningen, of de toetsenbordinvoer op uw systeem wordt bespioneerd. Op die manier kunnen aanvallers uw wachtwoordinvoer registreren. Deze functie moet altijd ingeschakeld blijven.

Exploit Protection

Een zogenaamde exploit misbruikt de zwakke plekken in populaire gebruikersprogramma's en kan zo in het ergste geval de controle over uw computer overnemen. Exploits kunnen zelfs toeslaan als toepassingen (bv. PDF-viewer, browser) regelmatig worden bijgewerkt. Exploit Protection biedt bescherming tegen dergelijke aanvallen en beschermt ook proactief tegen nog onbekende aanvallen.

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.

Toegangsgegevens

Als u in het gedeelte Licentie op **Toegangsgegevens** klikt, verschijnt een dialoogvenster met uw toegangsgegevens. Meer informatie hierover vindt u in het hoofdstuk **Instellingen | AntiVirus | Updates**. Als u vragen over uw licentie hebt, kunnen we u in het **G DATA ServiceCenter** met deze gegevens beter helpen. Als u uw wachtwoord vergeten bent, kunt u via dit dialoogvenster ook snel en gemakkelijk een nieuw wachtwoord genereren.

Softwaremodules

Afhankelijk van de geïnstalleerde softwareversie zijn de volgende softwaremodules beschikbaar:

SecurityCenter: uw persoonlijk beveiligingscentrum. Hier vindt u alle gegevens die u nodig hebt om uw computer te beveiligen tegen schadelijke software en kunt u doelgericht op bedreigingen reageren.

Virusbeveiliging: in dit gedeelte vindt u informatie over wanneer uw computer de laatste keer op virussen werd gecontroleerd en of de virusbewaker de computer momenteel actief beveiligt tegen infecties. Bovendien kunt u de computer of gegevensdrager direct op schadelijke software controleren, geïnfecteerde bestanden in quarantaine bewerken en een opstartmedium maken.

Firewall: een firewall zorgt ervoor dat uw computer niet kan worden "bespied". Hij controleert welke gegevens en programma's via het internet of een netwerk op uw computer binnenkomen en welke gegevens via uw computer worden verzonden. Zodra het

blijkt dat gegevens op uw computer onrechtmatig moeten worden geïnstalleerd of gedownload, slaat de firewall alarm en blokkeert hij de onrechtmatige gegevensuitwisseling. Deze softwaremodule is beschikbaar in de programmaversies G DATA Internet Security en G DATA Total Security.

Back-up: door de toenemende digitalisering van het dagelijkse leven, het gebruik van online muziekdiensten, digitale camera's en e-mailcorrespondentie wordt de beveiliging van uw persoonlijke gegevens steeds belangrijker. Uw gegevens kunnen door een defect in de hardware, een fout, beschadiging door virussen of aanvallen van hackers verloren gaan. Het is dan ook essentieel dat u regelmatig een back-up maakt van uw persoonlijke documenten. De module Back-up neemt deze taak van u over en beveiligt zo uw belangrijke documenten en bestanden zonder dat u zich daar steeds zorgen over hoeft te maken. Deze softwaremodule is beschikbaar in de programmaversie G DATA Total Security.

Wachtwoordmanager: Met de Wachtwoordmanager kunt u op een eenvoudige manier wachtwoorden beheren en gemakkelijk als invoegtoepassing in uw browser gebruiken. Deze softwaremodule is beschikbaar in de programmaversie G DATA Total Security.

Tuner: met de tuner hebt u een tool in handen die uw Windows-systeem aanzienlijk sneller en overzichtelijker maakt, van de automatische herinnering aan Windows-updates en een tijdgestuurde regelmatige defragmentatie tot het regelmatig verwijderen van overbodige gegevens in het register en het opruimen van tijdelijke bestanden. Deze softwaremodule is beschikbaar in de programmaversie G DATA Total Security.

Kinderbeveiliging: met behulp van de kinderbeveiliging kunt u het surfgedrag en het computergebruik van uw kinderen regelen. Deze softwaremodule is beschikbaar in de programmaversies G DATA Internet Security en G DATA Total Security.

Codering: de coderingsmodule doet dienst als een bankkluis voor de beveiliging van vertrouwelijke gegevens. Een safe kan bijvoorbeeld worden gebruikt als extra station, zoals een bijkomende partitie van de vaste schijf, en is heel eenvoudig te bedienen. Deze softwaremodule is beschikbaar in de programmaversie G DATA Total Security.

Autostart Manager: met de Autostart Manager kunt u de programma's beheren die automatisch worden gestart wanneer Windows start. Normaal worden deze programma's direct bij het opstarten van het systeem geladen. Wanneer u deze met de Autostart Manager beheert, kunt u deze ook met vertraging of afhankelijk van de belasting van het systeem of de vaste schijf starten. Daardoor start het systeem sneller op en presteert uw computer beter.

Apparaatcontrole: Met deze functie kunt u voor bepaalde gebruikers van uw computer het gebruik van apparaten zoals verwisselbare opslagmedia, cd/dvd- en diskettestations beperken. Op die manier kunt u bijvoorbeeld de ongewenste export of import van gegevens of installatie van software verhinderen. Nu ook met USB KeyboardGuard. Meer info hierover vindt u in het hoofdstuk Apparaatcontrole.

Virusbeveiliging

Met deze module kunt u uw computer of geselecteerde gegevensdrager gericht controleren op malware-infecties. Dit is aanbevolen wanneer u bijvoorbeeld zelfgebrande cd's of USB-sticks van vrienden, familie of collega's ontvangt. Ook bij de installatie van nieuwe software en downloads van het internet is een viruscontrole aanbevolen.

> **Opgelet**: Het controleren van de computer of geselecteerde gegevensdrager is bedoeld als extra beveiliging. In principe bent u met de G DATA Screensaver-scanner en de G DATA Virusbewaker, die altijd op de achtergrond actief is, optimaal beveiligd tegen malware. Met een viruscontrole worden ook virussen gevonden die naar uw computer zijn gekopieerd vóór de installatie van de G DATA software of die in uw systeem zijn terechtgekomen toen de virusbewaker een keer niet was ingeschakeld.

Viruscontrole

Selecteer hier welk deel van uw computer of welke gegevensdrager u wilt controleren:

Computer controleren (alle lokale harde schijven): Als u naast de automatische controle door de afwezigheidsscan een eigen controle wilt uitvoeren (vanwege een actuele virusverdenking bijvoorbeeld), klikt u op deze optie. Uw computer wordt dan meteen op virussen gescand. Lees hierover ook het volgende hoofdstuk: **Viruscontrole uitvoeren**.

Geplande viruscontroles: Met deze functie kunt u automatische viruscontroles inplannen. Lees hierover ook het volgende hoofdstuk: **Automatische viruscontroles**.

Geheugen en automatisch starten controleren: Hiermee worden voor alle lopende processen de programmabestanden en programmabibliotheken (DLL's) gecontroleerd. Op die manier kunnen schadelijke programma's meteen uit het geheugen en autostart worden verwijderd. Actieve virussen kunnen dus direct worden verwijderd, zonder dat u de complete vaste schijf hoeft te doorzoeken. Deze functie is een aanvulling en geen vervanging van een regelmatige viruscontrole van de opgeslagen gegevens.

Mappen/bestanden controleren: Hiermee controleert u geselecteerde stations, mappen of bestanden op virussen. Als u op deze optie klikt, opent zich 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 op de (+)-symbolen te klikken. Hun inhoud wordt dan in het bestandsoverzicht weergegeven. De mappen en bestanden waarvoor u een vinkje plaatst, worden gecontroleerd.

Als niet alle bestanden in een map worden gescand, wordt dat aangeduid door een grijs vinkje bij deze map.

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.

Bestanden in quarantaine

Tijdens het scannen op virussen kunt u op verschillende manieren omgaan met eventueel aangetroffen 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.

Quarantaine weergeven: wanneer u op deze knop klikt, wordt de quarantaine geopend.

De bestanden in quarantaine blijven daarbij in dezelfde toestand als toen de G DATA software een virus aantrof. 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.
- **In de toekomst toestaan**: Als de gedragscontrole een bestand foutief naar de quarantaine heeft verplaatst, kunt u het bestand

toevoegen aan de whitelist. De gedragscontrole verplaatst het bestand dan niet meer naar de quarantaine.

- **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.

Opstartmedium

Het opstartmedium is een handig hulpmiddel om besmette computers weer virusvrij te maken. Vooral bij computers die voor de installatie van de G DATA software geen virusbeveiliging hadden, is het aanbevolen een opstartmedium te gebruiken. Meer informatie over het gebruik van een **opstartmedium** vindt u in het hoofdstuk **BootScan**.

Om een opstartmedium te maken, klikt u op de knop **Opstartmedium maken** en volgt u de instructies in de installatiewizard. Hier kunt u actuele virushandtekeningen downloaden zodat uw opstartmedium up-to-date is. Bovendien kunt u hier bepalen of u een cd/dvd wilt branden als opstartmedium of een USB-stick als opstartmedium wilt gebruiken.

Wanneer u de programmaversie G DATA Total Security gebruikt, kunt u met een opstartmedium een back-up van een station ook herstellen op het volume waarop zich het systeem bevindt. De back-up van een station of bestand herstellen op andere doelstations is hier ook mogelijk. Plaats daarvoor het opstartmedium in het station en selecteer de functie **Herstel starten**.

Firewall

Een firewall voorkomt dat gegevens op uw computer *bespied* worden. Hij controleert welke gegevens en programma's via het internet of een netwerk op uw computer binnenkomen en welke gegevens via uw computer worden verzonden.

De firewallmodule bestaat uit drie delen:

- **Status**: in het gedeelte Status van de firewall krijgt u belangrijke informatie over de huidige toestand van uw systeem en de firewall.
- **Netwerken**: in het gedeelte Netwerken vindt u de netwerken (zoals LAN, remote enz.) waarmee de computer verbonden is.
- **Regelsets**: in dit gedeelte kunt u voor verschillende netwerken speciale regels maken om het gedrag van uw firewall te optimaliseren.

Zodra blijkt dat gegevens op uw computer onrechtmatig moeten worden geïnstalleerd of gedownload, slaat de firewall alarm en blokkeert deze de onrechtmatige gegevensuitwisseling.

Instellingen: Als u rechtsboven op deze knop klikt, krijgt u toegang tot meer dialoogvensters voor het instellen van de firewall.

Status

In het onderdeel Status van de firewall krijgt u belangrijke informatie over de huidige toestand van uw systeem en de firewall. Dit vindt u rechts naast de betreffende regel als tekst of getal. Bovendien wordt de status van de componenten ook grafisch voorgesteld. Door op het betreffende item te dubbelklikken, kunt u hier direct acties uitvoeren of naar een bepaald programmaonderdeel overschakelen.

Zodra u de instellingen van een component met waarschuwingssymbool hebt geoptimaliseerd, verandert het symbool in het statusgedeelte weer in het groene vinkje.

- **Beveiliging**: Tijdens het dagelijkse gebruik van de computer leert de firewall automatisch welke programma's u al dan niet gebruikt om toegang te krijgen tot internet en welke programma's een veiligheidsrisico vormen. Afhankelijk van uw kennis over de gebruikte technologie kunt u de firewall zo configureren dat deze zonder al te veel rompslomp een uitstekende basisbescherming biedt, of kiezen voor een professionele bescherming, die precies is afgestemd op de manier waarop u de computer gebruikt, maar ook de nodige kennis van firewall-technologie vereist. Hier kunt u de beveiligingsstatus instellen: **Instellingen | Firewall | Automatisch systeem**.
- **Modus**: Hier ziet u met welke basisinstelling uw firewall werkt. U kunt hier kiezen tussen handmatige regelaanmaak of het automatische systeem (autopiloot).

  Automatische piloot: Hier werkt de firewall volkomen autonoom en houdt automatisch de gevaren voor uw thuis-pc tegen. Deze instelling biedt praktische en volledige beveiliging en is in de meeste gevallen aan te bevelen. De automatische piloot moet standaard ingeschakeld zijn.

  Overige instellingen: Als u de firewall individueel wilt configureren of bepaalde toepassingen niet met de Autopiloot-modus wilt laten werken, kunt u met de handmatige regelaanmaak uw firewall volledig Autopiloot-modus op uw behoeften. Meer informatie vindt u in het volgende hoofdstuk: **Instellingen | Firewall | Automatisch systeem**.
- **Netwerken**: Met deze optie kunt u de netwerken weergeven waarin uw computer zich bevindt. Meer informatie vindt u in het volgende hoofdstuk: **Firewall | Netwerken**.
- **Geregistreerde aanvallen**: Zodra de firewall een aanval op uw computer registreert, wordt deze verhinderd en in het logboek opgenomen. Klik op de menuoptie voor meer informatie.
- **Toepassingsradar**: in dit dialoogvenster ziet u welke programma's momenteel door de firewall worden geblokkeerd. Als u aan een van de geblokkeerde toepassingen toch de toestemming wilt verlenen voor het gebruik van het netwerk, moet u deze hier selecteren en vervolgens op de knop **Toestaan** klikken.

Netwerken

In het gedeelte Netwerken vindt u de netwerken (zoals LAN, remote enz.) waarmee de computer verbonden is. Hier kunt u ook zien volgens welke regelset (zie hoofdstuk **Regelsets**) het betreffende netwerk is beveiligd. Als u het vinkje bij het betreffende netwerk verwijdert, wordt dit van de firewall-beveiliging uitgezonderd. U moet de beveiliging echter uitsluitend met een goede reden uitschakelen. Als u een netwerk met de muis markeert en op de knop **Bewerken** klikt, kunt u de firewall-instellingen voor dit netwerk bekijken resp. wijzigen.

Netwerk bewerken

In dit overzicht worden de volgende gegevens en instelmogelijkheden voor het geselecteerde netwerk weergegeven:

- **Netzwerk-Informatie**: Hier vindt u netwerkgegevens zoals, indien beschikbaar, informatie over het IP-adres, het subnetmasker, de standaardgateway, de DNS- en WINS-server.
- **Firewall actief, op dit netwerk**: Hier kunt u de firewall voor dit netwerk deactiveren, doe dit wel enkel als het echt nodig is.
- **Internetverbinding delen**: bij directe verbindingen met internet kunt u bepalen of alle computers in het netwerk via een met internet verbonden computer internettoegang krijgen. Normaal gesproken kan deze internetverbindingsvrijgave (ICS) voor een thuisnetwerk worden geactiveerd.
- **Automatische configuratie (DHCP) toestaan**: wanneer uw computer verbonden is met het netwerk wordt een dynamisch IP-adres toegewezen (via het DHCP = Dynamic Host Configuration Protocol). Als u via deze standaardconfiguratie met het netwerk bent verbonden, moet u het vakje hier aangevinkt laten.
- **Regelset**: U kunt hier zeer snel kiezen uit voorgeprogrammeerde regelsets en op deze manier, afhankelijk van de beveiligingscriteria, bepalen of u te maken hebt met een betrouwbaar netwerk, een onbetrouwbaar netwerk of een netwerk dat moet worden geblokkeerd. Met de knop **Regelset bewerken** hebt u ook de mogelijkheid om de regelsets afzonderlijk te configureren. Lees hiertoe het hoofdstuk **Regelsets aanmaken**.

Regelsets

Hier kunt u voor verschillende netwerken speciale regels opstellen. Deze regels worden dan telkens tot een regelset samengevoegd. Er zijn standaardregelsets voor directe verbinding met internet, onbetrouwbare netwerken, betrouwbare netwerken en te blokkeren netwerken. In het overzicht wordt de betreffende regelset met naam weergegeven. Met de knoppen **Nieuw**, **Verwijderen** en **Bewerken** kunt u bestaande regelsets veranderen, resp. nieuwe regelsets toevoegen.

De standaardregelsets voor **directe verbinding met internet**, **betrouwbare netwerken**, **onbetrouwbare netwerken** en **te blokkeren netwerken** kunnen niet worden verwijderd. Aanvullende regelsets die u zelf hebt opgesteld kunnen natuurlijk altijd worden verwijderd.

Regelsets aanmaken

U kunt aan elk netwerk een eigen regelset (of een verzameling speciaal daarop afgestemde regels) toewijzen. Op die manier kunt u netwerken met verschillende bedreigingsniveaus door de firewall laten afschermen. Voor een privé-LAN-verbinding is mogelijk minder beveiliging nodig (en dus ook minder administratieve rompslomp) dan voor een extern netwerk, dat rechtstreeks in verbinding staat met internet.

Bovendien kunt u met de knop **Nieuw** ook eigen regelsets voor netwerken aanmaken. Klik daarvoor bij Regelsets op de knop **Nieuw** en voer in het geopende dialoogvenster de volgende gegevens in:

- **Naam regelset**: Voer hier een sprekende naam in voor de regelset.
- **Een lege regelset maken**: Hier kunt u een volledig lege regelset maken en hierin enkel zelf gedefinieerde regels opnemen.
- **Een regelset maken die enkele nuttige regels bevat**: Bij deze optie kunt u beslissen of u een nieuwe regelset wilt aanmaken met als uitgangspunt de regelset voor betrouwbare, onbetrouwbare of te blokkeren netwerken. U kunt deze standaardinstellingen vervolgens naar eigen behoefte aanpassen.

De firewall bevat vooraf gedefinieerde regelsets voor de volgende soorten netwerken:

- **directe verbinding met internet**: hieronder vallen regels die de directe internettoegang regelen.
- **onbetrouwbare netwerken**: hieronder vallen doorgaans open netwerken, zoals externe netwerken die toegang hebben tot internet.

- **betrouwbare netwerken**: thuis- en bedrijfsnetwerken zijn over het algemeen betrouwbaar.
- **te blokkeren netwerken**: Als de verbinding tussen de computer en een netwerk tijdelijk of permanent moet worden geblokkeerd, dan kunt u daar deze instelling voor gebruiken. Dat is bijvoorbeeld zinvol in geval van een verbinding met een onbekend netwerk waarvan u niet zeker weet of dit betrouwbaar is (bijvoorbeeld tijdens een LAN-party, externe bedrijfsnetwerken of openbare werkplekken voor notebooks.)

de nieuwe regelset verschijnt nu in het gedeelte Regelsets onder de bijbehorende naam (bijvoorbeeld *Nieuwe regelset*) in de lijst. Indien u nu op **Bewerken** klikt, wordt er afhankelijk van de instelling, die u bij **Instellingen | Overige** (zie het gelijknamige hoofdstuk) hebt ingevoerd, de Wizard Regels of deuitgebreide bewerkingsmodus. geopend om de afzonderlijke regels van deze regelset te bewerken. Hoe u nieuwe regels kunt maken in de regelsets, leest u in de hoofdstukken **Wizard Regels gebruiken** oftewel **Uitgebreide bewerkingsmodus gebruiken**.

Behalve het rechtstreeks invoeren van regels kunt u natuurlijk ook via het informatievenster van het firewallalarm regels aanmaken. Dit leerproces voor de firewall wordt in het hoofdstuk **Firewallalarm** uitgelegd.

Wizard Regels gebruiken

Met de wizard Regels kunt u bepaalde aanvullende regels definiëren voor de huidige regelset of bestaande regels wijzigen. Vooral gebruikers die minder bekend zijn met de firewalltechnologie kunnen beter de wizard Regels gebruiken dan de uitgebreide bewerkingsmodus.

Met de wizard Regels wijzigt u een of meer regels in de geselecteerde regelset. U maakt dus altijd een regel binnen een regelset die al een aantal regels bevat.

Afhankelijk van de regelset die u voor het betreffende netwerk hebt gedefinieerd, kan een toepassing in de ene regelset (bijv. voor onbetrouwbare netwerken) zijn geblokkeerd en in een andere regelset (bijv. voor betrouwbare netwerken) volledige toegang hebben. Op die manier kunt u een browser door afwijkende regels bijvoorbeeld zo instellen dat deze wel toegang heeft tot een site die in uw LAN-verbinding klaarstaat, maar niet tot de inhoud van diezelfde site via een remote netwerk.

Via de wizard Regels beschikt u over de volgende basisregels:

- **Toepassingen vrijgeven of blokkeren**: Hiermee kunt u gericht een toepassing (programma) op uw harde schijf selecteren en die toepassing uitdrukkelijk toestemming geven of ontzeggen om verbinding te maken met het in die regelset gedefinieerde netwerk. Selecteer hiervoor in de wizard het gewenste programma (**programmapad**) en geef daarna bij **Richting** aan of het programma moet worden geblokkeerd voor inkomende of uitgaande verbindingen, of voor verbindingen in beide richtingen. Op die manier kunt u bijvoorbeeld voorkomen dat de software voor uw mp3-speler gegevens doorgeeft over uw luistergewoonten (uitgaande verbindingen) of ervoor zorgen dat programma-updates niet automatisch worden uitgevoerd (inkomende verbindingen).
- **Netwerkdiensten vrijgeven of blokkeren**: Een **poort** is de benaming voor een speciaal adresbereik dat de gegevens die via een netwerk zijn verzonden, automatisch via een bepaald protocol naar bepaalde software doorstuurt. Zo gaat bijvoorbeeld de gegevensoverdracht van normale websites via poort 80, e-mails versturen gaat via poort 25, e-mails ontvangen via poort 110 enz. Zonder firewall staan over het algemeen alle poorten op uw computer open, hoewel de meeste door normale gebruikers helemaal niet worden gebruikt. Door een of meerdere poorten te sluiten, kunnen dus snel gaten worden gedicht die anders door hackers zouden kunnen worden misbruikt voor aanvallen. In de wizard hebt u de mogelijkheid de poorten helemaal te sluiten of alleen voor een bepaalde toepassing (bijv. voor de software van uw mp3-speler).
- **Bestands-/printerdeling**: wanneer u toegang verleent, kunt u vrijgegeven mappen en printers in het netwerk gebruiken. Tegelijk krijgen ook andere computers en gebruikers in het netwerk toegang tot uw shares (voor zover ingesteld).
- **Domeindiensten vrijgeven of blokkeren**: een domein is een soort register voor computers in een netwerk, dat een gecentraliseerd beheer mogelijk maakt van de aan het netwerk gekoppelde computers. Vrijgave van domeinservices binnen onbetrouwbare netwerken moet over het algemeen worden geweigerd.
- **Internetverbinding delen**: bij directe verbindingen met internet kunt u bepalen of alle computers in het netwerk via een met internet verbonden computer internettoegang krijgen. Normaal gesproken kan deze internetverbindingsvrijgave voor een thuisnetwerk worden geactiveerd.
- **VPN-diensten vrijgeven of blokkeren**: VPN is de afkorting van Virtual Private Networks en verwijst naar de mogelijkheid om computers exclusief met elkaar te verbinden en als het ware een directe verbinding tussen die computers tot stand te brengen. Om VPN-diensten te kunnen gebruiken, moeten deze door de firewall worden vrijgegeven.
- **Geavanceerde regelseteditor (expertmodus)**: Hiermee schakelt u over van de wizard Regels naar de uitgebreide bewerkingsmodus. Raadpleeg voor meer informatie over de uitgebreide bewerkingsmodus het hoofdstuk **Uitgebreide bewerkingsmodus gebruiken**.

Uitgebreide bewerkingsmodus gebruiken

In de uitgebreide bewerkingsmodus kunt u – mits u over voldoende kennis van netwerkbeveiliging beschikt – uw eigen regels definiëren voor het betreffende netwerk. U kunt hier natuurlijk alle regels instellen die u ook met de wizard Regels kunt definiëren, maar daarnaast kunt u nog meer instellingen opgeven.

Hiervoor staan de volgende instelmogelijkheden ter beschikking:

- **Naam**: Hier kunt u eventueel de naam van de huidige regelset wijzigen. Onder deze naam wordt de regelset dan in de lijst in het onderdeel Regelsetsweergegeven en kan daar met de door de firewall geïdentificeerde netwerken worden gecombineerd.
- **Stealth-modus**: In de Stealth-modus (Engels: verborgen, stiekem) worden aanvragen aan de computer die ertoe dienen om de bereikbaarheid van bepaalde poorten te controleren, niet beantwoord. Dit maakt het voor hackers moeilijker om op deze manier informatie over het systeem te verkrijgen.
- **Actie als er geen regel voorhanden is**: Hier kunt u bepalen of de toegang tot het netwerk in het algemeen toegestaan, geweigerd of na controle moet worden geregeld. Als er in de automatisch leren-stand van de firewall uitzonderingsregels zijn gedefinieerd voor bepaalde programma's, dan wordt hier uiteraard rekening mee gehouden.
- **Adaptieve modus**: De adaptieve modus ondersteunt u bij toepassingen die de zogenaamde terugkoppelingstechniek gebruiken (zoals FTP en veel online spelletjes). Dergelijke toepassingen maken verbinding met een externe computer en delen daarmee een terugkoppeling waarmee de externe computer wordt *terugverbonden*. Als de adaptieve modus is geactiveerd, herkent de firewall deze terugkoppeling en wordt de toegang zonder verdere controle vrijgegeven.

Regels

In het regeloverzicht vindt u alle regels die voor deze regelset zijn gedefinieerd. Op die manier kunt u bijvoorbeeld aan geselecteerde programma's uitgebreide netwerktoegang toekennen, ook al is het betreffende netwerk gedefinieerd als onbetrouwbaar. De regels die hierin voorkomen, kunnen op verschillende manieren worden aangemaakt:

- Via de **Wizard Regels**
- Direct via de **uitgebreide bewerkingsmodus.** Via de knop **Nieuw**
- Via het informatievenster dat bij een **Firewallalarm** wordt weergegeven.

Elke regelset heeft natuurlijk zijn eigen lijst met regels.

Omdat de firewallregels deels een bepaalde hiërarchische indeling hebben, is het in veel gevallen belangrijk om op de rangorde van de regels te letten. Zo kan een vrijgave voor een poort weer worden geblokkeerd door de weigering om toegang te geven tot een protocol. U kunt de rang van een regel wijzigen door deze te markeren met de muis en vervolgens met de pijltoetsen onder **Rangorde/Positie** in de lijst omhoog of omlaag te brengen.

Als u een nieuwe regel maakt via de uitgebreide bewerkingsmodus of een bestaande regel wijzigt via de optie **Bewerken**, wordt het dialoogvenster **Regel bewerken** geopend. Hierin vindt u de volgende instelmogelijkheden:

- **Naam**: Als vooraf ingestelde en automatisch gegenereerde regels worden gebruikt, dan staat hier de naam van het programma waarop deze regel van toepassing is.
- **Regel actief**: U kunt een regel inactief maken zonder de regel direct te verwijderen, door het vakje uit te vinken.
- **Opmerking**: Hier ziet u op welke manier de regel is aangemaakt. Bij de standaardregels voor de regelset staat Standaardregel, bij regels die via het dialoogvenster uit het **Firewallalarm** ontstaan, staat na controle aangemaakt en bij regels die u zelf via de uitgebreide bewerkingsmodus genereert, kunt u uw eigen opmerkingen invoegen.
- **Verbindingsrichting**: Met de richting wordt bepaald of deze regel van toepassing is voor inkomende of uitgaande verbindingen, of geldt voor beide soorten verbindingen.
- **Toegang**: Hier stelt u in of het betreffende programma binnen deze regelset al dan niet de toestemming krijgt om verbinding te maken.
- **Protocol**: Hier selecteert u welke verbindingsprotocollen u toegang wilt toestaan of weigeren. U kunt hierbij protocollen altijd blokkeren of vrijgeven, of het gebruik van het protocol koppelen aan een of meer toepassingen (**Toepassingen toewijzen**). Op dezelfde manier kunt u ongewenste of gewenste poorten via de knop **Internetservice toewijzen** nauwkeurig definiëren.
- **Tijdsduur**: U kunt de toegang tot netwerkbronnen ook tijdafhankelijk maken en er zo bijvoorbeeld voor zorgen dat de toegang

alleen wordt verleend tijdens uw werkuren en niet daarbuiten.

- **IP-adresbereik**: Vooral bij netwerken met vaste IP-adressen is het zinvol het gebruik te reglementeren door een beperking van het IP-adresbereik. Een duidelijk gedefinieerd IP-adresbereik vermindert het gevaar van een aanval door hackers aanzienlijk.

Back-up

Door de toenemende digitalisering van het dagelijkse leven, het gebruik van online muziekdiensten, digitale camera's en e-mailcorrespondentie wordt de beveiliging van uw persoonlijke gegevens steeds belangrijker. Uw gegevens kunnen door een defect in de hardware, een fout, beschadiging door virussen of aanvallen van hackers verloren gaan. Het is dan ook essentieel dat u regelmatig een back-up maakt van uw persoonlijke documenten. De G DATA software neemt deze taak van u over en beveiligt zo uw belangrijke documenten en bestanden zonder dat u zich daar steeds zorgen over hoeft te maken.

Back-up maken en herstellen

Zodra u een back-upopdracht hebt aangemaakt via de functie **Nieuwe opdracht**, kunt u deze direct bewerken en beheren via de volgende symbolen:

Herstel: met deze optie zet u de in de back-up gearchiveerde bestanden terug op uw systeem. Het verloop van het herstel wordt in het hoofdstuk **Back-up herstellen** uitgelegd.

Back-up: met deze optie start u het back-upproces voor de gedefinieerde back-upopdracht meteen en afzonderlijk, onafhankelijk van een vooraf gedefinieerd schema voor deze back-up.

Instellingen: Met deze optie kunt u voor de betreffende back-upopdracht de instellingen wijzigen die u hebt opgegeven toen u deze back-upopdracht voor het eerst onder **Nieuwe back-upopdracht** hebt aangemaakt.

Logboeken: Hier vindt u een overzicht van alle processen die via deze back-upopdracht zijn uitgevoerd. U vindt hier gegevens over uitgevoerde handmatige of tijdgestuurde back-upprocessen, informatie over eventueel herstelde back-ups en eventuele foutmeldingen, bv. wanneer de doelmap onvoldoende schijfruimte voor de uit te voeren back-up had.

Nieuwe back-upopdracht

Om een nieuwe back-upopdracht te maken, klikt u op **Nieuwe opdracht**.

Bestanden/vaste schijven/partities selecteren

De wizard Back-up vraagt nu welke soort back-up u wilt uitvoeren.

Back-up van bestand: Het gaat hier om een back-up van bepaalde geselecteerde bestanden en mappen in een archiefbestand.

Selecteer in de mapweergave welke bestanden en mappen u wilt opslaan. Het is doorgaans aanbevolen bij de gegevensback-up persoonlijke bestanden op te slaan en geen back-up van de geïnstalleerde programmabestanden uit te voeren. In de mappenstructuur kunt u mappen openen en selecteren door op de (+)-symbolen te klikken. Hun inhoud wordt dan in het bestandsoverzicht weergegeven. De mappen en bestanden waarvoor u een vinkje plaatst, worden door de software gecontroleerd voor de back-up. Als niet alle bestanden en mappen in een map voor de back-up worden gebruikt, wordt dat aangeduid door een grijs vinkje bij deze map.

Back-up van station: Het gaat hier om een complete back-up van vaste schijven of partities in een archiefbestand.

Doel selecteren

Hier selecteert u het doel, of de plaats, waar de G DATA software de back-up van de bestanden en mappen of vaste schijven en partities moet opslaan. Dit kan een cd- of dvd-romstation zijn, een andere harde schijf, een USB-stick, andere verwisselbare media of een map in het netwerk.

Naam van het archief: hier kunt u het archiefbestand een betekenisvolle naam geven, bv. *Wekelijkse back-up eigen bestanden, MP3-back-up* enz.

Nieuwe map: Als u een nieuwe map wilt aanmaken voor de back-up, selecteert u in de mapweergave de gewenste opslaglocatie en klikt u daarna op knop **Nieuwe map**.

> **Opmerking**: let er echter wel op dat de back-up niet op dezelfde vaste schijf als de originele bestanden mag worden opgeslagen. Bij een defect van deze schijf, gaan zowel uw originele als uw back-upgegevens verloren. U kunt uw back-up het beste op een locatie bewaren die fysiek gescheiden is van de originele bestanden, bijvoorbeeld in een andere kamer op een harde USB-schijf

of op een cd- of dvd-rom gebrand.

Archief in de cloud aanmaken: U kunt een gangbare cloudservice zoals Dropbox, Microsoft OneDrive*, TeamDrive** of Google Drive gebruiken om uw back-up op te slaan. Meld u daarvoor gewoon aan met de toegangsgegevens voor uw cloudservice en uw back-uparchief wordt meteen aan uw cloud gekoppeld.

> **Opmerking**: Let er bij een back-up in de cloud op dat uw back-upgegevens versleuteld zijn. Onder **Opties** onder **Nieuwe back-upopdracht** kunt u de versleuteling van de gegevens in- en uitschakelen.
>
> **(*) Opmerking over OneDrive**: u kunt OneDrive gebruiken wanneer u deze service als virtueel station in Windows Verkenner hebt geïntegreerd. Het archief wordt dan echter volledige normaal via de gegevensmap gemaakt en niet via de functie **Archief in de cloud aanmaken**.
>
> **(**) Opmerking over TeamDrive**: u kunt TeamDrive gebruiken nadat u via de TeamDrive-software een TeamDrive-Space hebt aangemaakt en ingesteld.

Tijdschema

Enerzijds kunt u hier bepalen met welk interval de geselecteerde bestanden door een back-up moeten worden beveiligd, anderzijds kunt u bepalen welke soort back-up moet worden uitgevoerd. Standaard is dat de volledige back-up, waarbij alle geselecteerde bestanden volledig worden beveiligd. U hebt ook de mogelijkheid om via gedeeltelijke back-ups enkel de wijzigingen sinds de laatste back-up op te slaan.

Als u **Handmatig** selecteert, wordt de back-up niet automatisch uitgevoerd, maar moet u die zelf starten via de programma-interface. Onder **Dagelijks** kunt u met behulp van de gegevens onder Weekdagen bv. bepalen dat uw computer de tuning alleen op werkdagen, alleen om de dag of alleen in het weekend als er niet wordt gewerkt, uitvoert. Bovendien kunt u wekelijkse en maandelijkse back-ups instellen.

Niet in batterijbedrijf uitvoeren: Om ervoor te zorgen dat een back-upproces bij notebooks niet plotseling wordt onderbroken wanneer de accu van de notebook leeg is, kunt u bepalen dat back-ups enkel mogen worden uitgevoerd wanneer de notebook op het stroomnet is aangesloten.

Volledige back-up uitvoeren

Geef onder **Volledige back-up uitvoeren** op hoe vaak, op welke dagen en op welk tijdstip de betreffende back-upopdracht moet worden uitgevoerd. Vervolgens zal op basis van de door u ingestelde cyclus automatisch een back-up van alle gegevens worden gemaakt, die u bij **Bestanden/vaste schijven/partities selecteren** daarvoor hebt geselecteerd.

> **Opgelet**: De tijdgestuurde back-up werkt niet bij een cd-rom of dvd-rom, omdat hier eventueel bij het vervangen van het medium een handeling van de gebruiker wordt vereist.

In het gedeelte **Oudere archieven verwijderen** kunt u bepalen wat de G DATA software met bestaande back-ups moet doen. De G DATA software archiveert uw gegevens in een apart bestand met de extensie ARC. Bestaande back-ups, die niet worden overschreven, verhogen uiteraard nog de veiligheid van uw gegevens, omdat zelfs als het huidige archief beschadigd zou zijn, een ouder archief beschikbaar is. Daardoor zijn niet alle gegevens verloren. Over het algemeen nemen archieven echter veel ruimte op de gegevensdragers in beslag en dient u er op te letten dat niet een te grote hoeveelheid archiefmateriaal wordt verzameld. Het is raadzaam om bij **Volledige back-ups bewaren** een maximum aantal back-ups aan te geven, dat op uw veilige gegevensdragers opgeslagen dient te worden. Dan wordt steeds het oudste archief door het huidige archief vervangen.

Wanneer u de optie **Deelbackup(s) aanmaken** aanvinkt, voert de software na een eerste volledige back-up de daaropvolgende keren enkel gedeeltelijke back-ups uit. Het back-upproces verloopt daardoor veel sneller, maar een volledige back-up herstellen op basis van deze gedeeltelijke back-ups duurt wel langer. Een bijkomend nadeel van een gedeeltelijke back-up is dat deze in verhouding meer geheugen in beslag neemt, omdat de niet meer benodigde gegevens in de volledige back-up niet direct worden verwijderd. Na de volgende volledige back-up worden de gegevens van de volledige en gedeeltelijke back-up echter weer samengevoegd en is de hoeveelheid gegevens weer gelijk aan die van een volledige back-up.

Gedeeltelijke back-ups uitvoeren

Gedeeltelijke back-ups zijn bedoeld om gegevensbeveiliging sneller te maken. Bij een gedeeltelijke back-up worden niet alle gegevens gebruikt, maar wordt voortgebouwd op een bestaande volledige back-up. Dat houdt in dat alleen de gegevens worden opgeslagen die sinds de vorige volledige back-up zijn gewijzigd of toegevoegd. Op die manier worden uw gegevens ook volledig beveiligd, terwijl het back-upproces aanzienlijk sneller verloopt.

Differentieel/Incrementeel: Bij een differentiële back-up worden alle gegevens opgeslagen die sinds de laatste complete back-up zijn gewijzigd of toegevoegd. Bij een dergelijke back-up wordt dus altijd voortgebouwd op de laatste complete back-up. U bent zo minder

tijd en opslagruimte kwijt dan bij een nieuwe volledige back-up. De incrementele back-up gaat nog een stap verder en slaat in een gedeeltelijke back-up de bestanden op die sinds de laatste gedeeltelijke back-up zijn gewijzigd. Nadeel hiervan is dat bij herstel van de gegevens meerdere archieven nodig zijn.

Opties

In het gedeelte Opties kunt u de algemene back-upopties wijzigen. Normaal gezien hoeft u hier geen wijzigingen aan te brengen omdat de standaardopties van de G DATA software in de meeste gevallen voldoende zijn.

Algemene archiefopties

Bij de algemene archiefopties hebt u volgende instellingsmogelijkheden:

- **Bestandsgrootte van archief begrenzen**: Wanneer u archieven op cd-, dvd-rom of andere beschrijfbare media opslaat, is het belangrijk dat de G DATA software de grootte van de archiefbestanden begrenst. Hier kunt u kiezen uit een aantal standaardgroottes die het achteraf opslaan van archiefgegevens op cd, dvd of blu-ray-discs mogelijk maken. Zodra het archief de hier opgegeven maximale grootte bereikt, wordt het gesplitst en wordt de back-upinformatie over twee of meer archiefbestanden verdeeld.

- **Multisession cd/dvd maken**: wanneer u deze optie selecteert, maakt u back-up-cd's of p-dvd's die meerdere keren kunnen worden beschreven. Daarbij wordt de eerder opgeslagen inhoud niet verwijderd, maar de nieuwe inhoud wordt eraan toegevoegd.

- **Tijdelijke archieven wissen**: Deze optie moet over het algemeen geactiveerd blijven. Tijdelijke archieven hebben na het uitvoeren van een bepaald aantal back-ups heel veel plaats nodig op uw harde schijf. Na hun tijdelijk gebruik hebt u ze eigenlijk niet meer nodig.

- **Bestanden herstellingsprogramma kopiëren**: wanneer u deze functie inschakelt, wordt naast de archiefbestanden op de opslagplaats van uw back-up een programma gezet waarmee u uw gegevens ook zonder geïnstalleerde G DATA software kunt herstellen. Start hiervoor vanaf de cd/dvd-rom het programma *AVKBackup* of *AVKBackup.exe*.

  Het herstelprogramma wordt alleen op cd/dvd-rom meegekopieerd. Bij back-ups op verwisselbare media (USB-stick, externe harde schijf) is dat niet het geval.

  Wanneer u de G DATA software hebt geïnstalleerd op de computer waarop het herstel moet plaatsvinden, voert u het herstel niet uit met het herstelprogramma op de cd/dvd-rom, maar via de functie **Archieven importeren**.

- **Bestanden op virussen controleren voor het archiveren**: Als de module AntiVirus is geïnstalleerd, kunt u uw bestanden op virussen controleren vooraleer ze in het back-uparchief worden opgeslagen.

- **Archief na het aanmaken controleren**: Met deze functie wordt het archief na het aanmaken nog eens op volledigheid en op fouten gecontroleerd.

- **Archief coderen**: Wanneer u uw gearchiveerde bestanden tegen toegang door derden wilt beveiligen, kunt u deze van een wachtwoord voorzien. Het herstellen van de bestanden kan dan alleen nog met dit wachtwoord gebeuren. Onthoud het wachtwoord goed of noteer het op een veilige plaats. Zonder wachtwoord kunnen uw archiefbestanden niet worden hersteld.

- **Integriteitstest bij differentiële back-up**: Met deze functie kan een gedeeltelijke back-up na het aanmaken nog eens worden gecontroleerd op volledigheid en fouten.

- **Integriteitstest bij herstel van harde schijf**: Met deze functie wordt na het herstel nogmaals gecontroleerd of de gegevens op de juiste manier zijn teruggezet. Bij **Map voor tijdelijke bestanden** gaat het om de opslaglocatie voor bestanden die de G DATA software slechts tijdelijk op uw vaste schijf schrijft. Indien er op uw standaardpartitie onvoldoende plaats is, kunt u hier de partitie en de tijdelijke opslagruimte voor deze bestanden wijzigen.

- **Schaduwkopie van Windows gebruiken**: als deze optie niet is ingeschakeld, kan er geen image van de systeempartitie worden gemaakt.

Gebruikersinstellingen

Om tijdgestuurde back-ups te kunnen uitvoeren, moet u hier de optie **Taak uitvoeren als** aanvinken en daar de toegangsgegevens voor uw Windows-gebruikersaccount invoeren. Deze gegevens zijn noodzakelijk, zodat de back-up op basis van de ingestelde tijd kan worden uitgevoerd, ook als u niet als gebruiker bent aangemeld.

Compressie

In het gedeelte Compressie kunt u bepalen of uw archief sterk of zwak moet worden gecomprimeerd.

- **Goede compressie**: De gegevens worden voor back-up sterk gecomprimeerd. Daardoor wordt er bij back-up minder opslagruimte ingenomen, maar duurt de back-up zelf wel langer.
- **Gebalanceerde compressie**: De back-up wordt niet zo sterk gecomprimeerd, waardoor het proces sneller wordt uitgevoerd.
- **Snelle uitvoering**: De gegevens worden niet gecomprimeerd, waardoor de back-up sneller verloopt.

Bestanden uitsluiten

Normaal gesproken slaat de G DATA software bestanden op basis van hun bestandsindeling op. In uw computersysteem bevinden zich overeenkomstige bestandsindelingen, maar ook in delen die automatisch worden beheerd en niet relevant zijn voor een back-up, omdat de desbetreffende bestanden slechts tijdelijk worden opgeslagen (bijv. ter versnelling van de paginaweergave op het internet). Om te voorkomen dat de G DATA software deze bestanden onnodig archiveert, kunt u het betreffende vinkje uitschakelen.

- **Tijdelijke map met bestanden**: Als u deze optie selecteert, worden de tijdelijke mappen, inclusief submappen en bestanden, niet in de back-up opgenomen.
- **Tijdelijke internetmappen met bestanden**: Als u deze optie selecteert, worden de mappen voor de opslag van internetpagina's, inclusief submappen en bestanden, niet in de back-up opgenomen.
- **Thumbs.db**: Wanneer u deze optie kiest, worden de bestanden thumbs.db, die automatisch door Windows Verkenner worden aangemaakt, niet in de back-up opgenomen. Deze bestanden hebben tot doel om bijvoorbeeld de miniatuurweergave voor slideshows te beheren en worden automatisch gemaakt aan de hand van de originele afbeeldingen.
- **Tijdelijke bestanden (Bestandskenmerk)**: Wanneer u deze optie selecteert, worden de bestanden met het door het systeem toegekende bestandskenmerk tijdelijk niet in de back-up opgenomen.
- **Systeembestanden (Bestandskenmerk)**: Wanneer u deze optie selecteert, worden de bestanden met het door het systeem toegekende bestandskenmerk Systeembestand niet in de back-up opgenomen.
- **Bestandstypen uitsluiten**: Met deze functie kunt u zelf bestandsextensies vastleggen die niet in de back-up worden opgenomen. Ga hierbij als volgt te werk: Voer onder **Bestandstype** (bv. *.txt) de bestandsextensie of de bestandsnaam in die u wilt uitsluiten. Klik nu op **OK**. Herhaal dit voor alle andere bestandstypen en bestandsnamen die u wilt uitsluiten, bv. picasa.ini, *.ini, *bak enzovoort. Het sterretje en het vraagteken kunt u hierbij als jokerteken gebruiken. U kunt de jokertekens als volgt gebruiken:

  Het vraagteken (?) neemt de plaats van afzonderlijke tekens in.

  Het sterretje (*) neemt de plaats van complete tekenreeksen in.

  Om bijvoorbeeld alle bestanden met de extensie exe te controleren, voert u *.exe in. Om bijvoorbeeld bestanden met verschillende spreadsheetindelingen te controleren (bv. *.xlr, *.xls), voert u gewoon *.xl? in. Om bijvoorbeeld verschillende soorten bestanden met een bestandsnaam die met dezelfde letters begint te controleren, voert u tekst*.* in.

Huidige standaardopties opnieuw instellen

Als u op deze knop klikt, worden de standaardopties die voor de G DATA software zijn gedefinieerd, opnieuw ingesteld. Als u dus bij het maken van back-ups per ongeluk de verkeerde opties hebt ingesteld en niet weet hoe u dit ongedaan kunt maken, klikt u op de knop **Huidige standaardopties opnieuw instellen**.

Back-up herstellen

Hier kunt u op basis van de back-upgegevens uw originele bestanden na gegevensverlies herstellen. Klik daarvoor op de knop **Herstellen**.

Nu verschijnt een dialoogvenster met alle opgeslagen back-upprocessen voor de betreffende back-upopdracht.

Selecteer hier de gewenste back-up (bv. de laatst uitgevoerde back-up, wanneer u documenten die u kort geleden per ongeluk hebt verwijderd, wilt herstellen) en klik daarna op **Herstellen**.

U kunt nu bepalen op welke manier het herstel moet gebeuren:

- **Complete back-up herstellen**: alle bestanden en mappen die deel uitmaken van deze back-up, worden hersteld.
- **Alleen geselecteerde partities/bestanden herstellen** Hier ziet u een mapweergave van uw back-up, waarin u kunt bepalen welke bestanden, mappen of partities u wilt herstellen. In de mappenstructuur kunt u mappen openen en selecteren door op de (+)-symbolen te klikken. Hun inhoud wordt dan in het bestandsoverzicht weergegeven. De mappen en bestanden waarvoor u een

vinkje plaatst, worden vanuit de back-up hersteld. Als in een map niet alle bestanden worden gecontroleerd, staat bij deze map een grijs vinkje.

Daarna kunt u bepalen of de bestanden in hun oorspronkelijke mappen moeten worden hersteld of niet. Als de bestanden op een andere plaats moeten worden opgeslagen, kunt u eventueel onder **Nieuwe map** een map selecteren waarin u deze wilt opslaan. Voer onder **Wachtwoord** het toegangswachtwoord in als u uw back-up bij het opslaan met een wachtwoord beveiligd hebt gecomprimeerd.

Als u bestanden in de oorspronkelijke mappen wilt herstellen, hebt u de volgende opties om doelgericht enkel gewijzigde bestanden te herstellen:

- **altijd vervangen**: Bij deze instelling worden de bestanden uit de veiligheidskopie altijd als belangrijker beschouwd dan de bestanden die in de oorspronkelijke map staan. Als u hier een vinkje zet, worden eventueel nog aanwezige bestanden vervangen door de bestanden die zich in het archief bevinden.
- **als de grootte is gewijzigd**: Bij deze instelling worden bestaande bestanden in de oorspronkelijke map alleen maar vervangen wanneer het oorspronkelijke bestand werd gewijzigd. Bestanden waarvan de grootte niet werd gewijzigd, worden overgeslagen. Hierdoor kan het herstel van de gegevens sneller worden uitgevoerd.
- **als het tijdstip "Gewijzigd op" in het archief recenter is**: Hier worden bestanden in de oorspronkelijke map altijd door de kopieën uit het archief vervangen wanneer ze recenter zijn dan de bestanden van het archief. Ook hier kan het herstel sneller worden uitgevoerd omdat niet per se alle bestanden hoeven te worden hersteld, maar alleen de gewijzigde gegevens.
- **als het tijdstip "Gewijzigd op" is gewijzigd**: Hier worden bestanden in de oorspronkelijke map altijd vervangen als er op de wijzigingsdatum iets werd veranderd in vergelijking met de gearchiveerde bestanden.

Klik vervolgens op **Bewerking beëindigen** om het herstel volgens uw instellingen uit te voeren.

Acties

In dit onderdeel kunt u onder andere acties voor het onderhoud van uw back-ups instellen.

Hiervoor staan de volgende hulpprogramma's ter beschikking:

Archief achteraf op cd / dvd branden

U kunt back-upbestanden ook later op cd of dvd branden. Selecteer hiervoor in het dialoogvenster een project dat u wilt branden en klik vervolgens op de knop **Volgende**.

Selecteer het station waarop u de back-up wilt branden.

U hebt hier de volgende opties:

- **Controle uitvoeren na het branden**: Als u hier een vinkje zet, worden de gebrande bestanden na het branden nog eens gecontroleerd. We bevelen deze manier van werken aan, ook al duurt het een beetje langer dan branden zonder controle.
- **Bestanden herstellingsprogramma kopiëren**: wanneer u deze functie inschakelt, wordt naast de archiefbestanden op de opslagplaats van uw back-up een programma gezet waarmee u uw gegevens ook zonder geïnstalleerde G DATA software kunt herstellen. Start hiervoor vanaf de cd/dvd-rom het programma *AVKBackup* of *AVKBackup.exe*.

Klik op de knop **Branden** om het branden te starten. Na het branden wordt de back-up-cd/dvd automatisch uitgeworpen.

> **Opmerking**: natuurlijk worden de back-upbestanden na het branden niet van de originele gegevensdrager verwijderd. Het later branden op cd/dvd is een bijkomende veiligheidsmaatregel.

Archieven importeren

Als u archieven en back-ups wilt herstellen die zich niet op een door de G DATA software beheerd station bevinden, gebruikt u de functie **Archieven importeren**. Er gaat dan een dialoogvenster open waarin u de gewenste archiefbestanden met de extensie *ARC* bijv. op een cd, dvd of in een netwerk kunt zoeken. Zodra u het gewenste archief hebt gevonden, vinkt u het aan en klikt u op de knop **OK**. Een infovenster wijst u erop dat het archief succesvol werd geïmporteerd. Wanneer u dit archief nu voor het herstellen van gegevens wilt gebruiken, gaat u naar het gedeelte **Herstellen** van de G DATA software. Selecteer vervolgens de gewenste back-up en start het herstel.

> Opmerking: door de G DATA software gemaakte archiefbestanden hebben de bestandsextensie ARC.

Opstartmedium maken

Om back-ups ook zonder geïnstalleerde G DATA software te kunnen herstellen, kunt u een cd/dvd of USB-stick maken met speciale software waarmee u gegevens kunt herstellen. Als u op die manier back-ups wilt herstellen, start u het opstartmedium en selecteert u het programma *AVKBackup* of *AVKBackup.exe*. Daarna kunt u de gewenste back-ups selecteren en het herstel starten.

> **Opmerking**: het maken van een opstartmedium wordt uitgelegd in het hoofdstuk **Opstartmedium**. Het opstartmedium vervult een dubbele functie in de G DATA software. Hiermee kunt u back-ups herstellen en met de BootScan kunt u uw computer op virussen controleren voordat Windows wordt gestart.

Wachtwoordmanager

Met de Wachtwoordmanager kunt u op een eenvoudige manier wachtwoorden beheren en gemakkelijk als invoegtoepassing in uw browser gebruiken.

De Wachtwoordmanager ondersteunt de volgende browsers in de nieuwste generatie:

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer

Opmerking: afhankelijk van de instellingen van uw browser (bv. privacyinstellingen) kan de werking van de Wachtwoordmanager beperkt zijn.

Maak eerst een wachtwoordsafe aan en installeer daarna de invoegtoepassing voor de browser van uw keuze. U kunt de wachtwoordsafe uiteraard ook installeren voor alle compatibele browsers.

Nieuwe safe aanmaken en invoegtoepassing installeren

Klik op **Wachtwoordsafe**. Er wordt een dialoogvenster geopend waarin u met de optie **Nieuwe safe aanmaken** een nieuwe safe kunt maken.

Voer hiervoor een wachtwoord in, bevestig het, klik op **Safe aanmaken** en de safe wordt gemaakt. De wachtwoordherinnering kan u helpen als u uw wachtwoord vergeten bent.

De safe is aangemaakt en aan de rechterkant van het programmavenster kunt u kiezen in welke browsers u de invoegtoepassing Wachtwoordmanager wilt installeren. U hoeft enkel op de desbetreffende browsernaam te klikken om de invoegtoepassing te installeren.

Als u de browser de volgende keer opent, wordt u mogelijk gevraagd of u de nieuwe invoegtoepassing wilt gebruiken. Bevestig dit voor de G DATA Wachtwoordmanager.

In de taakbalk van de browser vindt u nu het volgende pictogram. Klik op het pictogram als u de Wachtwoordmanager wilt gebruiken.

Voer hiervoor uw wachtwoord in het geopende dialoogvenster in en klik op **Ontgrendelen**. Het gebruik van de browserinvoegtoepassing wordt in het volgende **hoofdstuk** uitgelegd.

Gebruik van de browserinvoegtoepassingen

Als u op het volgende pictogram in de taakbalk van de browser klikt, kunt u de Wachtwoordmanager gebruiken.

Opmerking: Afhankelijk van de privacyinstelling (bv. geschiedenis opslaan) kan de invoegtoepassing mogelijk niet worden gebruikt. In geval van problemen met de invoegtoepassing controleert u best eerst de instellingen van uw browser.

Voer hiervoor uw wachtwoord in het geopende dialoogvenster in en klik op **Ontgrendelen**. Nu zijn de volgende onderdelen beschikbaar:

Favorieten: met deze functie kunt u snel de met een wachtwoord beveiligde websites die u regelmatig gebruikt, oproepen.

Logins: hier kunt u de logins voor met een wachtwoord beveiligde websites beheren.

Contactpersonen: met behulp van de hier ingevoerde contactgegevens kunnen formulieren, zoals leveringsadressen automatisch worden ingevuld.

Notities: hier kunt u bijkomende, met een wachtwoord beveiligde notities opslaan.

Instellingen: Als u de Wachtwoordmanager opnieuw wilt sluiten, klikt u hier op **Vergrendelen**. Als u op Instellingen klikt, kunt u

favorieten, logins, contactpersonen en notities eenvoudig beheren in dialoogvensters. Met de Wachtwoordgenerator kunt u automatisch een veilig wachtwoord laten aanmaken en via het klembord direct gebruiken.

In het beheer van de Wachtwoordmanager kunt u als volgt nieuwe gegevens toevoegen en gegevens bewerken en verwijderen.

Nieuw gegeven: als u hierop klikt, kunt u een nieuw gegeven aanmaken en alle vereiste gegevens in de desbetreffende dialoogvensters voor logins, contactpersonen of notities invoeren.

Gegeven opslaan: als u hierop klikt, wordt het gegeven opgeslagen en verschijnt deze ook in de snelkeuze van de browserinvoegtoepassing.

Gegeven verwijderen: hiermee verwijdert u gegevens die u niet meer nodig hebt.

Tuner

Met de tuner hebt u een tool in handen die uw Windows-systeem aanzienlijk sneller en overzichtelijker maakt: van de automatische herinnering aan Windows Update, via een tijdgestuurde regelmatige defragmentatie tot en met het regelmatig verwijderen van overbodige gegevens in het register en het opruimen van tijdelijke bestanden.

U kunt uw computer handmatig tunen met een druk op een knop of tijdgestuurd regelmatig tuningtaken laten uitvoeren.

Laatste tuningrun: hier ziet u wanneer voor het laatst een tuning van uw computer werd uitgevoerd. Om een nieuwe tuning te starten, selecteert u hier de optie **Tuningrun nu uitvoeren**. Zodra u de tuningrun start, ziet u een voortgangsbalk met de huidige status van de tuning.

Automatische tuningrun: als u de tuning van uw computer wilt automatiseren, kunt u door de optie **Automatische tuningrun inschakelen** te selecteren een overeenkomstige tijdgestuurde tuningtaak maken. Om de automatische tuningrun in te stellen, selecteert u de optie **Meer instellingen**.

Configuratie: In dit gebied kunt u alle modules selecteren die de tuner voor het tuningproces moet gebruiken. Geselecteerde modules worden daarbij dan hetzij via een automatische, tijdgestuurde actie gestart (zie het hoofdstuk Planning) hetzij handmatig. Om een module te activeren, klikt u er tweemaal op met de muis. U kunt hier de volgende tuningonderdelen instellen:

- *Beveiliging*: Diverse functies die automatisch gegevens downloaden van internet zijn alleen van nut voor de aanbieder en niet voor u. Vaak wordt ook via zulke functies de deur wijd opengezet voor schadelijke software. Met deze modules beveiligt u uw systeem en blijft het volledig bijgewerkt.
- *Prestaties*: Tijdelijke bestanden, zoals reservekopieën, logboekbestanden en installatiegegevens, die u niet meer nodig hebt, maken de harde schijf trager en nemen waardevolle opslagruimte in beslag. Bovendien vertragen overbodig geworden processen en koppelingen van gegevens uw systeem aanzienlijk. Met de hier opgesomde modules kunt u uw computer van deze overbodige ballast bevrijden en sneller maken.
- *Privacy*: Hier zijn de modules ondergebracht die uw gegevens beschermen. De sporen die bij het surfen of bij algemeen computergebruik onvrijwillig ontstaan, vertellen veel over uw gebruik en bevatten belangrijke gegevens en wachtwoorden. Hier worden deze sporen gewist.

Herstel: de software maakt bij elke wijziging een herstelpunt. Als een bepaalde tuning-actie tot ongewenste resultaten heeft geleid, kunt u deze actie ongedaan maken en de toestand van het systeem vóór de wijziging herstellen. Lees hiervoor ook het hoofdstuk Herstel.

Browser Cleaner: G DATA Browser Cleaner kan ongewenste programmaonderdelen en aanvullende programma's blokkeren of verwijderen. Deze programma's worden vaak samen met gratis software geïnstalleerd en kunnen browserinstellingen wijzigen of zelfs gegevens bespioneren. Lees hiervoor ook het hoofdstuk Browser Cleaner.

Herstel

In de software wordt bij elke wijziging een herstelpunt gemaakt. Als een bepaalde tuning-actie tot ongewenste resultaten heeft geleid, kunt u deze actie ongedaan maken en de toestand van het systeem vóór de wijziging herstellen.

Alles selecteren: als u alle wijzigingen die door de tuning zijn uitgevoerd wilt afwijzen, selecteert u met deze optie alle herstelpunten en klikt u vervolgens op de knop **Herstellen**.

Herstellen: als u enkel bepaalde wijzigingen die door de tuning zijn uitgevoerd wilt afwijzen, selecteert u met deze optie het gewenste herstelpunt en klikt u vervolgens op de knop **Herstellen**.

Geselecteerde verwijderen: herstelpunten die u niet meer nodig hebt, kunt u met deze knop verwijderen.

Browser Cleaner

G DATA Browser Cleaner kan ongewenste programmaonderdelen en aanvullende programma's blokkeren of verwijderen. Deze programma's worden vaak samen met gratis software geïnstalleerd en kunnen browserinstellingen wijzigen of zelfs gegevens bespioneren. Met Browser Cleaner kunt u deze ongewenste programma's ("PUP" = Potentially Unwanted Programs) laten weergeven in de browsers Internet Explorer, Firefox en Google Chrome. Daarna kunt u zelf bepalen of u deze alleen wilt uitschakelen of volledig wilt verwijderen. Het uitschakelen van uitbreidingen kan op elk ogenblik ongedaan worden gemaakt.

> **Opmerking:** G DATA Browser Cleaner werkt samen met Microsoft Internet Explorer, Mozilla Firefox en Google Chrome en maakt een bijzonder eenvoudig beheer van alle geïnstalleerde browseruitbreidingen mogelijk. Met één muisklik kunnen alle plug-ins in de lijst worden uitgeschakeld of verwijderd om de browser te ontdoen van ongewenste uitbreidingen. Het hulpprogramma geeft optioneel alle als veilig beschouwde plug-ins weer, zodat u de onveilige of ongewenste uitbreidingen snel en eenvoudig kunt onderscheiden. G DATA Browser Cleaner maakt deel uit van de uitgebreide beveiligingsoplossing G DATA Total Security en is altijd beschikbaar voor gebruikers hiervan.

Kinderbeveiliging

Met behulp van de kinderbeveiliging kunt u het surfgedrag en het computergebruik van uw kinderen regelen.

Selecteer een op uw computer aangemelde gebruiker onder **Gebruiker** en stel daar de betreffende beperkingen voor deze gebruiker in. Met de knop **Nieuwe gebruiker aanmaken** kunt u ook direct nieuwe accounts op uw computer aanmaken (bv. voor uw kinderen).

- **Kinderbeveiliging voor deze gebruiker**: Hier kunt u de kinderbeveiliging voor de eerder geselecteerde gebruiker in- of uitschakelen.
- **Verboden inhoud**: In dit gedeelte wordt een dialoogvenster geopend waarin u voor de geselecteerde gebruiker bepaalde internetinhoud kunt blokkeren. Klik op **Bewerken** om de verboden inhoud voor de betreffende gebruiker te bepalen.
- **Toegestane inhoud**: In dit gedeelte wordt een dialoogvenster geopend waarin u voor de geselecteerde gebruiker bepaalde internetinhoud kunt toestaan. Klik op **Bewerken** om de toegestane inhoud voor de betreffende gebruiker te bepalen.
- **Internetgebruikstijd controleren**: hier kunt u instellen hoe lang en op welke tijdstippen de geselecteerde gebruiker internettoegang krijgt. Klik op **Bewerken** om de gebruikstijden voor de betreffende gebruiker te bepalen.
- **Computergebruikstijd controleren**: Hier kunt u instellen hoe lang en op welke tijdstippen de geselecteerde gebruiker de computer mag gebruiken. Klik op **Bewerken** om de gebruikstijden voor de betreffende gebruiker te bepalen.

Instellingen: hier kunt u basisinstellingen voor de werking van het kinderslot wijzigen en aanpassen aan individuele behoeften.

Nieuwe gebruiker aanmaken

Klik op de knop **Nieuwe gebruiker aanmaken**. Er verschijnt een dialoogvenster waarin u de gebruikersnaam en het wachtwoord voor deze gebruiker kunt invoeren.

> **Opmerking**: met het oog op het beveiligingsniveau moet een wachtwoord minimaal acht tekens lang zijn en zowel hoofdletters als kleine letters en cijfers bevatten.

De nieuwe gebruikersnaam wordt weergegeven onder **Gebruiker**. Voor deze gebruiker wordt ook een Windows-gebruikersaccount gemaakt. Dat betekent dat het kinderslot voor die persoon automatisch wordt geactiveerd met de betreffende instellingen wanneer hij of zij zich met de gebruikersnaam aanmeldt bij Windows. Dubbelklik vervolgens met de muis op de instellingen die voor deze gebruiker moeten worden toegepast, dus bijv. het tegenhouden van **Verboden inhoud** of uitsluitend toegang tot **Toegestane inhoud** of bepaal of voor deze gebruiker de **Internetgebruikstijd** of **Computergebruikstijd** moet worden bewaakt.

Verboden inhoud

In dit deel wordt een dialoogvenster geopend waarin u voor de geselecteerde gebruiker bepaalde inhoud van het internet kunt blokkeren. Selecteer de categorieën die u wilt blokkeren door een vinkje te plaatsen. Klik vervolgens op **OK**. De websites die aan de criteria voor blokkering voldoen, zijn nu niet meer toegankelijk voor deze gebruiker.

Als u op de knop **Nieuw** klikt, wordt een dialoogvenster geopend waarin u eigen criteria voor te blokkeren inhoud (ook blacklists genoemd) kunt definiëren. Definieer hiervoor eerst de naam en eventueel een informatietekst voor het individueel aangemaakte filter.

Klik nu op **OK** om naar een volgend venster te gaan. Hier kunt u de inhoud samenvatten die door het filter moet worden onderdrukt.

Voer onder **Filter** een begrip in dat moet worden geblokkeerd en bij **Plaats van de zoekactie** het bereik van een website waarin moet worden gezocht.

U hebt hier de volgende keuzemogelijkheden:

- **URL**: Als u hier het vinkje plaatst, wordt in het webadres naar de te blokkeren tekst gezocht. Als u bijvoorbeeld sites wilt blokkeren als *www.chatcity.no*; *www.crazychat.co.uk*, dan volstaat het dat u als **filter** *chat* invoert, **URL** aanvinkt en vervolgens op de knop **Toevoegen** klikt. Nu worden alle sites geblokkeerd die ergens in hun domeinnaam of het internetadres de lettervolgorde *chat* hebben.
- **Titel**: Als u hier het vinkje plaatst, wordt in de titel van de website naar de te blokkeren tekst gezocht. Dit is de vermelding die u bijvoorbeeld ziet als u een site toevoegt aan de Favorieten. Als u bijvoorbeeld sites wilt blokkeren zoals *Chat City Detroit*; *Teenage Chat 2005*, dan volstaat het dat u als **filter** *chat* invoert, **Titel** aanvinkt en vervolgens op de knop **Toevoegen** klikt. Nu worden alle sites geblokkeerd die ergens in hun titel de lettervolgorde *chat* hebben.
- **Meta**: Zogeheten metatags zijn verborgen teksten op websites die worden gebruikt om deze sites beter, of gewoon vaker, te laten

herkennen door zoekmachines. Zoektermen als *sex* of *chat* worden hier graag gebruikt om het aantal paginahits te vergroten. Als u sites wilt blokkeren waarvoor in de metatag *chat* staat, dan volstaat het dat u **chat** invoert als *filter*, **Meta** aanvinkt en vervolgens op de knop **Toevoegen** klikt. Vervolgens worden alle pagina's geblokkeerd die in de metatags ergens de lettervolgorde *chat* hebben.

- **In de hele tekst**: Als u de leesbare inhoud van een pagina direct wilt controleren op te blokkeren inhoud, dan voert u gewoon het te blokkeren begrip in, bijvoorbeeld *chat*, vinkt u **In de hele tekst** aan en klikt u vervolgens op de knop **Toevoegen**. Nu worden alle pagina's geblokkeerd die in de weergegeven paginatekst, ergens de lettervolgorde *chat* bevatten.

U kunt specifieke sites die onbedoeld binnen het bereik van een filter vallen, opnieuw toelaten door deze bij de optie Uitzonderingen in te voeren. Klik daarvoor op de knop **Uitzonderingen** en voer daar de betreffende pagina in.

> **Opmerking**: zelf aangemaakte filters kunt u in het gedeelte **Eigen filters** vrij bewerken en verwijderen. Lees hiervoor het hoofdstuk **Eigen filters**.

Toegestane inhoud

In dit deel wordt een dialoogvenster geopend waarin u voor de huidige geselecteerde gebruiker bepaalde inhoud van het internet kunt toelaten. Selecteer de categorieën die u wilt vrijgeven door een vinkje te plaatsen. Klik hierna op **OK**. De internetsites die voldoen aan de criteria zijn nu toegankelijk voor deze gebruiker.

Als u op de knop **Nieuw** klikt, wordt een dialoogvenster geopend waarin u eigen criteria voor toegestane inhoud (ook whitelists genoemd) kunt definiëren. Definieer hiervoor eerst de naam en eventueel een informatietekst voor het afzonderlijk aangemaakte filter.

Klik nu op **OK**. Een dialoogvenster verschijnt waarin u de whitelist kunt aanvullen, bijvoorbeeld met websites die geschikt zijn voor kinderen.

Voer daarvoor bij **Filter** in welke onderdelen van domeinnamen vrij toegankelijk moeten zijn. Als u bijvoorbeeld een website met kindvriendelijke inhoud wilt vrijgeven, kunt u hier bijvoorbeeld *http://portal.omroep.nl/zapp* invoeren om toegang te verlenen tot deze website. Voer bij **Beschrijving** in wat er op deze website te vinden is, bijv. *Zapp - kindvriendelijke website* en voer bij **Koppeling naar website** het exacte webadres in. De omschrijving en de koppeling naar de website zijn alleen belangrijk als het kind bijvoorbeeld zelf een site opzoekt waarvoor het geen toestemming heeft. In plaats van een foutmelding verschijnt dan namelijk een HTML-pagina in de browser die alle in de whitelist ingevoerde websites met hun beschrijving toont. Zo kan uw kind direct opnieuw naar een website gaan waarvoor u toestemming hebt gegeven. Als u klaar bent met het invoeren, klik dan op **Toevoegen** om de whitelist bij te werken.

> **Opmerking**: de filter zoekt naar onderdelen in de domeinnaam. Afhankelijk van de vermelding in het filter kunnen de resultaten dus van elkaar verschillen. Meer uitgebreide of meer nauwkeurige beperkingen kunnen hier afhankelijk van de website helpen.

Internetgebruikstijd controleren

Hier kunt u instellen hoe lang en op welke tijden de geselecteerde gebruiker toegang tot het internet krijgt. Vink daarvoor het vakje aan bij **Internetgebruikstijd controleren**. Nu kunt u bepalen hoe lang de gebruiker in totaal per maand op het internet mag, hoe lang per week en hoeveel uur op bepaalde weekdagen. Zo kunnen bijvoorbeeld voor schoolgaande kinderen de weekends anders worden ingesteld dan de werkdagen. U kunt de betreffende periodes daarvoor eenvoudig ingeven bij **Dagen/uu:mm**, waarbij de aanduiding *04/20:05* bijvoorbeeld een internetgebruikstijd van 4 dagen, 20 uur en 5 minuten voorstelt.

> **Opmerking**: in het samenspel van de gegevens voor het internetgebruik telt altijd de kleinste waarde. Wanneer u bijvoorbeeld voor de maand een tijdsbeperking van vier dagen vastlegt, maar tijdens de week vijf dagen toestaat, stelt de software de internetgebruikstijd voor de gebruiker automatisch in op vier dagen.

Als de betreffende gebruiker probeert langer dan de toegestane tijd gebruik te maken van internet, verschijnt een opmerking die hem laat weten dat de toegestane tijd werd overschreden.

Tijden blokkeren

Met de knop **Tijden blokkeren** kunt u een dialoogvenster openen waarin u – naast de beperking van het internetgebruik – speciale periodes per week categorisch kunt blokkeren. Geblokkeerde periodes zijn daarbij rood weergegeven, vrijgegeven periodes zijn groen. Om een periode vrij te geven of te blokkeren, selecteert u die periode gewoon met de muis. Dan verschijnt er naast de cursor een contextmenu, waarin u twee mogelijkheden hebt: **Tijd vrijgeven** en **Tijd blokkeren**. Als de betreffende gebruiker probeert tijdens de geblokkeerde tijden gebruik te maken van Internet, verschijnt er in de browser een informatiescherm dat hem/haar erover informeert dat hij op dit moment geen toegang tot Internet heeft.

Computergebruikstijd controleren

Hier kunt u instellen hoe lang en op welke tijdstippen de geselecteerde gebruiker de computer mag gebruiken. Vink daarvoor het vakje aan bij **Computergebruikstijd controleren**. Nu kunt u bepalen hoe lang de gebruiker de computer in totaal per maand mag gebruiken, hoe lang per week en hoeveel uren op bepaalde weekdagen. Zo kunnen bijvoorbeeld voor schoolgaande kinderen de weekends anders worden ingesteld dan de werkdagen. U kunt de betreffende periodes daarvoor eenvoudig opgeven bij **Dagen/uu:mm**, waarbij de aanduiding *04/20:05* bijvoorbeeld een computergebruikstijd van 4 dagen, 20 uur en 5 minuten voorstelt. Via de knop **Waarschuwing voor het aflopen van de tijd weergeven** kunt u een gebruiker, kort voordat de computer automatisch wordt afgesloten, waarschuwen zodat deze zijn gegevens nog kan opslaan. Als de computer zonder waarschuwing wordt afgesloten, kan dat immers tot gegevensverlies leiden.

> **Opmerking**: in het samenspel van de gegevens over het computergebruik telt altijd de kleinste waarde. Wanneer u bijvoorbeeld voor de maand een tijdsbeperking van vier dagen vastlegt, maar tijdens de week vijf dagen toestaat, stelt de software het computergebruik voor de gebruiker automatisch in op vier dagen.

Tijden blokkeren

Met de knop **Tijden blokkeren** kunt u een dialoogvenster openen waarin u - naast de beperking van het computergebruik - speciale periodes per week categorisch kunt blokkeren. Geblokkeerde periodes zijn daarbij rood weergegeven, vrijgegeven periodes zijn groen. Om een periode vrij te geven of te blokkeren, selecteert u die periode gewoon met de muis. Dan verschijnt er naast de cursor een contextmenu, waarin u twee mogelijkheden hebt: **Tijd vrijgeven** en **Tijd blokkeren**.

Eigen filters

In dit gedeelte kunt u niet alleen de door uzelf samengestelde whitelists (met toegestane inhoud) en blacklists (met verboden inhoud) aanpassen, maar ook handmatig compleet nieuwe lijsten maken.

De onderstaande lijsten kunnen worden onderscheiden:

- **Toegestane inhoud**: Als u voor een van de geselecteerde gebruikers een whitelist kiest, dan kan deze uitsluitend websites bekijken die op deze whitelist staan. U kunt als beheerder de whitelist geheel naar eigen inzicht aanmaken of uit de vooraf gedefinieerde whitelists een passende lijst voor een gebruiker selecteren. Een whitelist leent zich er in het bijzonder voor om kleine kinderen zeer beperkt toegang tot internet te geven, waardoor ze alleen websites kunnen bezoeken met pedagogisch verantwoorde inhoud.

- **Verboden inhoud**: Met een blacklist kunt u geselecteerde websites voor een gebruiker blokkeren. Afgezien van die geblokkeerde websites heeft de gebruiker vrije toegang tot internet. </text><text styleclass="Normal" style="font-weight:bold; font-style:italic;" translate="true">Tip: denk eraan dat u met deze optie wel bepaalde sites kunt blokkeren, maar dat vergelijkbare inhoud ook op andere websites beschikbaar kan zijn. Een blacklist met internetadressen vormt daarom nooit een volledige bescherming tegen ongewenste inhoud.

Met de volgende knoppen kunt u de uitzonderingslijsten bewerken:

- **Verwijderen**: Via de functie **Verwijderen** kunt u met de muis geselecteerde lijsten eenvoudig verwijderen.

- **Nieuw**: Hiermee kunt u een geheel nieuwe blacklist of whitelist maken. De werkwijze is daarbij dezelfde zoals is beschreven in de hoofdstukken **Verboden inhoud** en **Toegestane inhoud** .

- **Bewerken**: hiermee kunt u de inhoud van een bestaande lijst wijzigen.

Instellingen: Logboek

In dit gedeelte kunt u basisinstellingen voor de informatie in logboeken wijzigen. Op die manier is het mogelijk te bepalen of overtredingen tegen toegestane en/of verboden inhoud in een logboek moet worden vastgelegd of niet. Als de inhoud in logboeken wordt vastgelegd, kunt u de logboeken van de verschillende gebruikers bij Logboek inkijken.

Omdat logboekbestanden bij regelmatig gebruik heel groot worden, kunt u bij de kinderbeveiliging onder **Melding weergeven wanneer bestand ____ KB bereikt** instellen dat u ervan op de hoogte wordt gebracht dat het logboekbestand een bepaalde grootte heeft overschreden. U kunt dit bestand dan bij **Logboek**onder **Logboeken verwijderen** handmatig verwijderen.

Codering

De coderingsmodule doet dienst als een bankkluis voor de beveiliging van vertrouwelijke gegevens. Een safe kan bijvoorbeeld worden gebruikt als extra station, zoals een bijkomende partitie van de vaste schijf, en is heel eenvoudig te bedienen.

Om safes te maken en te beheren, beschikt u over de volgende opties:

- **Bijwerken**: Wanneer u intussen safes geopend of gesloten hebt buiten de coderingsmodule, klikt u best op **Bijwerken** om de statusweergave voor de door de coderingsmodule beheerde safes up-to-date te brengen.
- **Openen/Sluiten**: hier kunt u de safes die zich op uw computer en aangesloten opslagmedia bevinden, openen of sluiten. Houd er rekening mee dat u een wachtwoord nodig hebt om de safe te openen. Dat is het wachtwoord dat u bij het aanmaken van de safe hebt opgegeven. Safes kunnen hier zonder wachtwoord worden gesloten.
- **Nieuwe codering maken**: Met deze functie kunt u een nieuwe safe maken. Daarvoor wordt een wizard geopend die u helpt bij het maken van de safe. Lees hiervoor het hoofdstuk **Nieuwe safe maken**.
- **Draagbare safe maken**: Zodra u een safe hebt gemaakt, kunt u van deze safe ook een draagbare safe maken, d.w.z. u kunt de safe zo configureren dat u deze op een USB-stick kunt gebruiken of zelfs via e-mail kunt verzenden. Lees hiervoor het hoofdstuk **Draagbare safe maken**.
- **Verwijderen**: in het safebeheer krijgt u een overzicht van alle safes die zich op uw computer en de aangesloten opslagmedia bevinden. Hier kunt u safes die u niet meer nodig hebt, ook verwijderen. Houd er rekening mee dat u safes hier ook kunt verwijderen zonder dat u daarvoor een wachtwoord nodig hebt. Zorg er daarom voor dat u de inhoud van de safe die u wilt verwijderen echt niet meer nodig hebt.

Nieuwe safe maken

Wanneer u een nieuwe safe wilt maken, wordt u daarbij ondersteund door een interactief dialoogvenster. Klik op de knop **Volgende** om door te gaan.

Bestandslocatie en grootte van de safe

Geef nu aan waar de safe moet worden opgeslagen en hoe groot de safe moet zijn.

> **Opmerking**: de safe is in feite een beveiligd bestand dat zich als een schijfpartitie gedraagt wanneer deze geopend is, d.w.z. dat u via de bestandslocatie een safebestand aanmaakt op de gewenste plaats op uw vaste schijf. Hier worden uw bestanden gecodeerd opgeslagen. Wanneer u de safe hebt geopend en deze gebruikt, kunt u de bestanden en mappen daarin bewerken, verwijderen, kopiëren en verplaatsen, net zoals op een normale vaste schijf of schijfpartitie.

Bestandslocatie

Selecteer hier op welke gegevensdrager (bv. lokale gegevensdrager (C:)) de safe moet worden aangemaakt.

> **Opmerking**: safes die in een beveiligde map zijn gemaakt, zijn alleen zichtbaar op uw computer als de G DATA software op uw computer is geïnstalleerd. Als u de installatie van de software ongedaan maakt, zijn de op die manier aangemaakte datasafes niet meer zichtbaar.

Safegrootte

Selecteer vervolgens een safegrootte door de schuifregelaar op de overeenkomstige plaats te zetten. U hebt daarbij zoveel ruimte als er nog beschikbaar is op de gekozen opslaglocatie. In het algemeen moet er minstens 2 GB vrije ruimte overblijven opdat uw computersysteem op andere gebieden niet wordt afgeremd door gebrek aan opslagruimte.

> **Opmerking**: via de knop links van de schuifregelaar voor de safegrootte kunt u snel een keuze maken. Zo kunt u bijvoorbeeld de grootte van de safe exact bepalen of de safe bijv. zo groot maken dat ze eventueel op een cd, dvd of BluRay kan worden gebrand.

Klik nu op de knop **Volgende**.

Safeparameters

In dit dialoogvenster kunt u de volgende gegevens en instellingen voor de safe opgeven:

- **Safebenaming**: De naam waaronder de safe door de G DATA software wordt beheerd.
- **Beschrijving**: een bijkomende korte beschrijving die bijvoorbeeld informatie over de inhoud van de safe bevat.
- **Bestandssysteem**: hier kunt u bepalen of het virtuele station dat de safe aanmaakt, het bestandssysteem FAT of NTFS gebruikt. In het algemeen moet hier de optie **Automatische selectie** geselecteerd blijven.
- **Schijf voor de safe automatisch selecteren**: de safe verschijnt op uw computer als een vaste schijf. U kunt hier een vaste stationsletter voor de safe opgeven of het systeem automatisch een stationsletter laten kiezen. Hier is doorgaans de automatische selectie aanbevolen.
- **Schijf indelen**: Deze optie is alleen beschikbaar wanneer u het station voor de safe niet automatisch door de software laat kiezen.

Klik nu op de knop **Volgende**.

Safetoegang

Hier kunt u een wachtwoord voor een safe opgeven. Klik daarvoor op de knop **Toevoegen**.

Geef nu in het geopende dialoogvenster het gewenste wachtwoord op onder **Wachtwoord** en **Wachtwoord herhalen**. Het wachtwoord wordt pas aanvaard als beide ingevoerde wachtwoorden identiek zijn. Dit moet bijvoorbeeld voorkomen dat u door een tikfout een wachtwoord opgeeft dat u zelf niet meer kunt herstellen.

Klik op **Toevoegen** om het wachtwoord te activeren en daarna op **Volgende** om de configuratie van de safe af te sluiten.

> **Opmerking**: u kunt bij het aanmaken van een safe ook meerdere verschillende wachtwoorden opgeven en op die manier verschillende rechten definiëren. u kunt bijvoorbeeld een safe aanmaken waarin u bestanden kunt lezen en wijzigen. U kunt ook andere mensen een ander wachtwoord toekennen waarmee ze de inhoud van deze safe alleen kunnen lezen, maar niet wijzigen.

Wanneer u de safe na het aanmaken selecteert en op de knop **Bevoegdheid** klikt, hebt u de volgende instelmogelijkheden:

- **Autostart uitvoeren**: In elke safe bevindt zich een map met de naam Autostart. Als deze optie op Ja ingesteld blijft, worden alle uitvoerbare bestanden die zich in deze map bevinden automatisch gestart bij het openen van de safe.
- **Openen als "Alleen lezen"**: Een gebruiker die zich met de toegangsmethode 'alleen lezen' aanmeldt, kan de bestanden in de safe niet opslaan of wijzigen. Hij kan ze alleen lezen.
- **Openen als wisselmedium**: De G DATA software opent datasafes in de Verkenner als lokale vaste schijven. Wanneer u de safe als verwisselbare schijf in het systeem zichtbaar wilt maken, markeert u deze optie.
- **Gemeenschappelijk gebruik**: Door deze optie aan te duiden kan de safemap gemeenschappelijk gebruikt worden door andere computers in het netwerk. Waarschuwing: Bij deze instelling is de toegang tot de safe mogelijk zonder dat hiervoor een wachtwoord moet worden ingevoerd. Wij bevelen aan om in dit geval een voorzichtige en bewuste keuze te maken met betrekking tot het gemeenschappelijk gebruik van de safe. Het gemeenschappelijk gebruik van de safe voor alle personen in het netwerk is hier zinloos aangezien in dit geval de gegevens voor iedereen toegankelijk zijn.
- **De safe sluiten na het afmelden van de gebruiker**: Deze optie is standaard ingeschakeld, aangezien andere gebruikers de inhoud van de safe kunnen bekijken als de safe ook na afmelding van de gebruiker open blijft staan.
- **Autosafe**: Alle safes met deze eigenschap kunnen met één opdracht worden geopend.

Safeconfiguratie

Bij de laatste stap informeert de safe-aanmaakwizard u over de instellingsparameters. Als u deze instellingen wilt wijzigen, klikt u op de knop **Vorige**. Als u tevreden bent over de instellingen klikt u op **Aanmaken**.

De virtuele en gecodeerde datasafe wordt op de harde schijf van uw computer aangemaakt. Door nogmaals op de knop **Bewerking beëindigen** te klikken, wordt de safe aangemaakt en desgewenst rechtstreeks geopend.

Draagbare safe maken

Zodra u een safe hebt gemaakt, kunt u hiervan ook een draagbare safe maken, d.w.z. u kunt de safe zo configureren dat u deze op een USB-stick kunt gebruiken of zelfs via e-mail kunt verzenden.

Selecteer een gemaakte safe in het overzicht met gegevenssafes en klik daarna op **Draagbare safe maken**. Nu verschijnt een dialoogvenster dat u helpt bij het aanmaken van een draagbare safe. Klik op **Volgende** om dit te starten.

Safeparameters

Net zoals bij het opgeven van de safeparameters voor standaardsafes kunt u hier parameters wijzigen. Voor draagbare safes zijn er echter slechts beperkte instelmogelijkheden:

- **Schijf voor de safe automatisch selecteren**: de geopende safe ziet eruit als een schijfstation. U kunt hier een vaste stationsletter voor de safe opgeven of het systeem automatisch een stationsletter laten kiezen. Hier is doorgaans de automatische selectie aanbevolen.

- **Safe aan gegevensdrager koppelen**: hier kunt u bepalen dat u de draagbare safe bv. uitsluitend met de USB-stick of vaste schijf gebruikt waarop u deze aanmaakt. Wanneer u de safe niet aan de gegevensdrager koppelt, kunt u het safebestand (te herkennen aan de bestandsextensie **tsnxg**) bv. ook als e-mailbijlage verzenden of naar een andere gegevensdrager verplaatsen/kopiëren.

Medium

Hier kunt u bepalen op welk medium u de draagbare safe wilt opslaan. Dat kan bijvoorbeeld een USB-stick, een externe vaste schijf of een cd/dvd zijn.

> **Opmerking**: wanneer u een safe op cd of dvd opslaat, kan deze uiteraard enkel worden geopend en gelezen. Bestanden en mappen in de safe kunnen niet worden gewijzigd op dit soort gegevensdrager.

Safegrootte

Hier krijgt u informatie over de hoeveelheid schijfruimte die de safe nodig heeft op de doelschijf. Als de opslagruimte te groot is, kunt u hier het aanmaken van de draagbare safe afbreken.

> **Opmerking**: Naast de grootte van de safe zelf, komen hier ongeveer 6 MB bijkomende stuurprogrammagegevens bij, zodat u de safe ook kunt openen op een Windows-systeem waarop geen G DATA software is geïnstalleerd.

Voltooien

Klik op **Bewerking beëindigen** om het maken van de draagbare safe af te sluiten. Als u dat wenst, wordt het bestand waarin de draagbare safe zich op het gewenste opslagmedium bevindt nu weergegeven in de bestandsbrowser.

Draagbare safe openen

Als u een draagbare safe wilt openen op een Windows-computer zonder de module G DATA Datasafe, krijgt u toegang tot de gegevens door op de USB-stick, draagbare harde schijf of cd/dvd het programmabestand **start.exe** of **start** in de map **TSNxG_4** te selecteren. Wanneer u hierop klikt, verschijnt een dialoogvenster waarin u de safe kunt openen of (wanneer deze al geopend is) sluiten.

> **Opgelet**: Wanneer G DATA Datasafe voor de eerste keer op een computer wordt gebruikt, worden nu de benodigde stuurprogrammagegevens en programmaonderdelen geladen. Daarna moet u de computer opnieuw opstarten. Nadat u de computer opnieuw hebt opgestart, selecteert u nogmaals **Start** of **Start.exe**.

Geef nu uw wachtwoord op of kies een van de andere toegangsmethoden.

De safe wordt geopend en de inhoud van de safe kan worden gebruikt.

Na het aanmelden bij de safe verschijnt in Windows Verkenner naast het lokale station het symbool van de safe als extra station met een eigen stationsletter. Iedere mobiele-safegebruiker kan gegevens van de safe op de computer overzetten. Bij gebruik van een mobiele safe op een USB-stick of een Flash-geheugenkaart kan de daartoe bevoegde gebruiker de safegegevens van de computer naar de safe kopiëren.

Het sluiten van de mobiele safe gebeurt op dezelfde manier als het openen. Dubbelklik op de stationsletter van de safe of selecteer de relevante opdracht met de rechtermuisknop in het contextmenu.

> **Opgelet**: Het is aan te bevelen de safe te sluiten vóórdat u de mobiele gegevensdrager verwijdert. Open daarvoor de map van

G DATA op de mobiele gegevensdrager en klik op Start.exe. Daarna verschijnt een dialoogvenster waarin u de safe kunt sluiten.

Autostart Manager

Met de Autostart Manager kunt u programma's beheren die automatisch worden gestart wanneer Windows start. Normaal worden deze programma's direct bij het opstarten van het systeem geladen. Wanneer u deze met de Autostart Manager beheert, kunt u deze ook met vertraging of afhankelijk van de belasting van het systeem of de vaste schijf starten. Daardoor start het systeem sneller op en presteert uw computer beter.

Wanneer u de Autostart Manager opent, ziet u aan de linkerkant een lijst met alle autostart-programma's die op uw computer zijn geïnstalleerd. Deze starten normaal gezien zonder vertraging, dus direct bij het starten van Windows. Daardoor start uw computer mogelijk heel langzaam op.

Selecteer met het pijlsymbool de autostart-programma's die u op een ander moment wilt starten en spreid op die manier de startprocedure van Windows. Uw Windows-besturingssysteem zal zo sneller opstarten en sneller gebruiksklaar zijn.

Wanneer u een autostart-programma opnieuw zonder vertraging wilt laten starten, verplaatst u het programma opnieuw van de map **Automatisch starten met vertraging** naar de map **Automatisch starten zonder vertraging**.

Vertraging instellen

Wanneer zich een programma in de map Automatisch starten met vertraging bevindt, kunt u eenvoudig bepalen met hoeveel minuten de start van de software moet worden vertraagd. Klik daarvoor op het programma en selecteer in de kolom Vertraging de gewenste periode.

De volgende opties zijn hier beschikbaar:

- **Niet starten**: Autostart Manager beheert de toepassing, maar deze start niet wanneer het systeem de volgende keer opnieuw wordt opgestart. Ze blijft inactief.
- **1 - 10 minuten**: de toepassing start het hier ingestelde aantal minuten later.
- **Automatische start**: De toepassing wordt afhankelijk van de belasting van de CPU/vaste schijf automatisch gestart. Dat betekent dat een autostart-toepassing pas wordt gestart wanneer de systeembelasting, die ontstaat door het starten van andere autostart-toepassingen of andere processen, opnieuw is gedaald.

Eigenschappen

Wanneer u dubbelklikt op de naam van een programma in de lijsten van de Autostart Manager, krijgt u uitgebreide informatie over de beheerde software.

Apparaatcontrole

Via de apparaatcontrole kunt u voor uw computer bepalen welke opslagmedia zijn toegestaan voor het lezen en/of schrijven van gegevens. U kunt bijvoorbeeld voorkomen dat privégegevens op een USB-stick gelezen of op een cd gebrand worden. Bovendien kunt u bij verwisselbare schijven zoals USB-sticks of externe USB-stations precies bepalen met welke verwisselbare schijf u gegevens kunt downloaden. Zo kunt u bijvoorbeeld uw eigen USB-schijf voor gegevensback-up gebruiken, maar andere vaste schijven geen toegang geven.

In dit overzicht ziet u welk effect de instellingen voor apparaatcontrole voor de betreffende gebruiker hebben. Met de knop "Regels bewerken" kunt u de instellingen voor het apparaat en voor de gebruiker aan uw wensen aanpassen.

> **USB Keyboard Guard:** onze software beschermt u onmiddellijk ook tegen een nieuwe bedreiging: geïnfecteerde USB-sticks die zich bij uw besturingssysteem voordoen als toetsenborden om zo schadelijke software te kunnen binnensmokkelen. De software brengt u daarvan op de hoogte wanneer uw systeem bij het aansluiten van een USB-apparaat ervan uitgaat dat het om een nieuw toetsenbord gaat. Door het invoeren van een pincode kunt u zelf bevestigen of dat daadwerkelijk geval is. De software onthoudt vanzelfsprekend alle reeds goedgekeurde toetsenborden en vraagt u niet opnieuw om bevestiging.

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. U kunt de volgende overkoepelende functies voor de instellingen gebruiken:

Instellingen opslaan: U kunt de uitgevoerde instellingen opslaan in een GDataSettings-bestand. Als u de G DATA software op meerdere computers gebruikt, kunt u zo de instellingen op één computer opgeven, deze opslaan en daarna het Settings-bestand op de andere computers laden.

Instellingen laden: Met deze optie kunt u een GDataSettings-bestand laden dat op deze of een andere computer werd gemaakt.

Instellingen terugzetten: Als u een fout hebt gemaakt bij het instellen van uw G DATA software, kunt u met deze knop alle instellingen van het programma terugzetten naar de standaardinstellingen. Daarbij kunt u bepalen of u alle of slechts bepaalde instellingsgebieden wilt terugzetten. Vink daarvoor de gebieden aan die u wilt terugzetten.

Algemeen

Beveiliging/prestaties

Wanneer u de virusbeveiliging op een langzame computer wilt gebruiken, kunt u het beveiligingsniveau verbeteren om de prestaties en de werksnelheid van de computer te verbeteren. In het schema ziet u welke effecten het optimaliseren van de instellingen heeft.

- **Standaardcomputer (aanbevolen)**: met deze optie biedt de G DATA software optimale beveiliging. Beide antivirusengines van het programma werken in dit geval samen. Bovendien worden alle lees- en schrijfbewerkingen op uw computer op schadelijke codes gecontroleerd.

  Engine: uw G DATA software werkt met twee antivirusengines. Het gebruik van beide engines staat garant voor optimale resultaten bij het voorkomen van virussen.

- **Langzame computer**: om de werksnelheid van langzame computers niet te beïnvloeden, kan de G DATA software ook met slechts één engine werken. Deze beveiliging is de enige optie bij talrijke op de markt verkrijgbare antivirusprogramma's, die van meet af aan slechts met één engine werken. Bij deze optie is de beveiliging nog steeds goed. U kunt bovendien bepalen dat in de Bewaker-modus enkel op malware wordt gecontroleerd wanneer schrijfbewerkingen worden uitgevoerd. Op die manier worden enkel nieuw opgeslagen gegevens gecontroleerd, wat de prestaties ten goede komt.

- **Aangepast**: Hier kunt u bepalen of u beide of slechts één engine wilt gebruiken en instellen of de bewaker bij het lezen en schrijven, enkel bij het schrijven (uitvoeren) of helemaal niet actief (niet aanbevolen) moet worden.

Wachtwoord

U kunt de instellingen van uw G DATA software beveiligen met behulp van een wachtwoord. Op die manier kan een andere gebruiker van uw computer bijvoorbeeld niet de virusbewaker of afwezigheidsscan uitschakelen.

Als u een wachtwoord wilt instellen, voert u dit eerst in onder "Wachtwoord" en daarna onder "Wachtwoord herhalen" om spelfouten te voorkomen. Daarnaast kunt u onder "Geheugensteun voor wachtwoord" een tip voor het wachtwoord opgeven.

Opmerking: de geheugensteun voor het wachtwoord wordt weergegeven wanneer u een verkeerd wachtwoord hebt ingevoerd. Daarom mag de geheugensteun enkel voor u een zinvolle verwijzing naar het wachtwoord zijn.

Opmerking: deze wachtwoordbeveiliging vormt een uitgebreide beveiliging van de software. U bereikt maximale beveiliging door met meerdere gebruikersaccounts te werken. U kunt bijvoorbeeld als beheerder in uw gebruikersaccount de virusbeveiliging beheren. Andere gebruikers (bv. kinderen, vrienden of familie) kunnen hier via hun gebruikersaccounts met beperkte rechten geen wijzigingen aanbrengen.

Opmerking: wanneer u bijvoorbeeld na het maken van verschillende gebruikersaccounts geen wachtwoord meer nodig hebt voor de G DATA software, kunt u met de knop "Wachtwoord verwijderen" de verplichting om een wachtwoord in te voeren opnieuw opheffen.

AntiVirus

Realtimebeveiliging

De realtimebeveiliging van de virusbewaker scant uw computer doorlopend op virussen en controleert schrijf- en leesprocessen. Zodra een programma schadelijke functies probeert uit te voeren of schadelijke bestanden probeert te verspreiden, wordt dat door de bewaker verhinderd. De virusbewaker is uw belangrijkste bescherming! Schakel deze nooit uit!

U hebt hier de volgende opties:

- **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**: Bepaal hier of archiefbestanden (zoals bestanden met de extensies RAR, ZIP of PST) anders moeten worden behandeld 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 **Quarantaine** niet meer kan worden gebruikt.
- **Gedragscontrole**: 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.
- **AntiRansomware**: Beveiliging tegen versleutelingstrojans.
- **Exploit Protection**: een zogenaamde exploit misbruikt de zwakke plekken in populaire gebruikersprogramma's en kan zo in het ergste geval de controle over uw computer overnemen. Exploits kunnen zelfs toeslaan als toepassingen (bv. PDF-viewer, browser) regelmatig worden bijgewerkt. Exploit Protection biedt bescherming tegen dergelijke aanvallen en beschermt ook proactief tegen nog onbekende aanvallen.

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. Kies nu of u een station, een map, een bestand of een bestandstype wilt uitsluiten.
4. Selecteer vervolgens daaronder de map 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.

   Opmerking: U kunt de jokertekens als volgt gebruiken:

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

   Om bijvoorbeeld alle bestanden met de bestandsextensie .sav te beveiligen, voert u *.sav in. Om een aantal bijzondere bestanden met opeenvolgende bestandsnamen te beveiligen (bv. 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.

Geavanceerd

Bepaal bovendien door het klikken op de knop **geavanceerd** welke bijkomende 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.

- **Kritieke mappen grondig controleren**: Met deze functie kunt u bijzonder kritieke mappen, zoals in het netwerk vrijgegeven mappen, persoonlijke gegevens of cloudservices (zoals Microsoft Dropbox OneDrive, Google Drive enz.), uiterst grondig controleren. Nadat u de mappen in het dialoogvenster hebt geselecteerd, worden deze dan, onafhankelijk van de instellingen die u voor alle andere bestanden en mappen gebruikt, altijd gecontroleerd in de modus **Bij het lezen en schrijven controleren**. Als u de modus **Bij het lezen en schrijven controleren** voor alle bestanden hebt geselecteerd, is de instelmogelijkheid voor kritieke mappen gedeactiveerd (grijs).

- **Netwerktoegangen controleren**: Wanneer voor uw computer een netwerkverbinding met onbeveiligde computers bestaat (bijv. vreemde notebooks), is het nuttig om ook de netwerktoegangen 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**: Het controleren van gecomprimeerde bestanden in archieven (te herkennen aan bestandsextensies als ZIP, RAR of PST) is heel tijdrovend en kan meestal worden weggelaten als de virusbewaker algemeen op het systeem actief is. Om de snelheid van de viruscontrole te verhogen, kunt u de grootte van de archiefbestanden die worden doorzocht beperken tot een bepaald aantal kilobytes.

- **E-mailarchieven controleren**: Aangezien de software de inkomende 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 wel een aantal minuten duren.

- **Systeemgebieden bij het starten van het systeem controleren**: Systeemgebieden (bv. bootsectoren) van uw computer hoeven doorgaans niet te worden uitgesloten van de viruscontrole. U kunt hier vastleggen of u deze bij het starten van het systeem of bij het wisselen van medium (bv. nieuwe cd-rom) wilt controleren. Normaal gezien moet u minstens een van beide functies geactiveerd hebben.

- **Systeemgebieden bij wisselen van medium controleren**: Systeemgebieden (bv. bootsectoren) van uw computer hoeven doorgaans niet te worden uitgesloten van de viruscontrole. U kunt hier vastleggen of u deze bij het starten van het systeem of bij het wisselen van medium (nieuwe cd-rom enz.) wilt controleren. Normaal gezien moet u minstens een van beide functies geactiveerd hebben.

- **Op telefoonkiezers / spyware / adware / riskware controleren**: Met de software kunt u uw systeem ook op dialers en andere schadelijke programma's 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 volledige getypte teksten op (en op die manier ook uw wachtwoorden) en sturen deze via internet door aan onbekenden.

- **Alleen nieuwe of gewijzigde bestanden controleren**: Als u deze functie inschakelt, worden bij de controle de bestanden overgeslagen 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 machine/motor), dus twee viruscontroleprogramma's die op elkaar zijn afgestemd. 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.
- **Geïnfecteerde archieven**: Bepaal hier of archiefbestanden (zoals bestanden met de extensies RAR, ZIP of PST) anders moeten worden behandeld 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 terugzetten uit de **Quarantaine** niet meer kan worden gebruikt.
- **Bij zware systeemlast 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. Kies nu of u een station, een map, een bestand of een bestandstype wilt uitsluiten.
4. Selecteer vervolgens daaronder de map 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.

   Opmerking: U kunt de jokertekens als volgt gebruiken:

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

   Om bijvoorbeeld alle bestanden met de bestandsextensie .sav te beveiligen, voert u *.sav in. Om een aantal bijzondere bestanden met opeenvolgende bestandsnamen te beveiligen (bv. 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 door de 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.

Geavanceerd

Door op de knop "Geavanceerd" te klikken, kunt u gevorderde instellingen voor viruscontrole bepalen.

Meestal volstaat het om de opgegeven standaardinstellingen te gebruiken.

- **Bestandstypen**: Hier kunt u vastleggen welke bestandstypen door de software op virussen moeten worden gecontroleerd. De optie Alleen programmabestanden en documenten selecteren biedt 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**: Het controleren van gecomprimeerde bestanden in archieven (te herkennen aan bestandsextensies als ZIP, RAR of PST) is heel tijdrovend en kan meestal worden weggelaten als de virusbewaker algemeen op het systeem actief is. Om de snelheid van de viruscontrole te verhogen, kunt u de grootte van de archiefbestanden die worden doorzocht beperken tot een bepaald aantal kilobytes.
- **E-mailarchieven controleren**: Hier kunt u aangeven of ook uw e-mailarchief op infecties moet worden gecontroleerd.
- **Systeemgebieden controleren**: Systeemgebieden (bv. bootsectoren) van uw computer hoeven doorgaans niet te worden uitgesloten van de viruscontrole.
- **Op telefoonkiezers / spyware / adware / riskware controleren**: Met deze functie kunt u uw systeem ook controleren op dialers en andere schadelijke software. 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 volledige getypte teksten op (en op die manier ook uw wachtwoorden) en sturen deze via internet door aan onbekenden.
- **Op RootKits controleren**: Rootkits proberen gebruikelijke virusherkenningsmethodes 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 bij de controle de bestanden overgeslagen 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.
- **Viruscontrole voor verwisselbare schijf aanbieden**: Als u dit vakje aanvinkt, wordt u bij het aansluiten van een verwisselbaar opslagmedium (USB-stick, externe harde schijf enz.) op uw computer gevraagd of dit apparaat op virussen moet worden gecontroleerd.

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. Voer bij de opties de toegangsgegevens (gebruikersnaam en wachtwoord) in die u bij de online aanmelding van de software via e-mail hebt ontvangen. Met behulp van deze gegevens herkent de G DATA updateserver u en kan het bijwerken nu volledig automatisch verlopen.

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

Toegangen beheren: met deze optie hebt u de mogelijkheid zelf te bepalen, welke internetverbindingen mogen worden gebruikt om programma-updates en upgrades op te halen. Dit is bijzonder nuttig als u tijdelijk via een netwerk bent verbinden waar de gegevensoverdracht moet worden betaald, zoals bijvoorbeeld bij bepaalde mobiele telefoonkosten zonder echte vast tarief voor gegevensoverdracht.

Virushandtekeningen importeren/exporteren: bij computers die slechts zelden of helemaal niet met internet verbonden zijn of waarbij het gegevensvolume voor downloads beperkt is, kunt u de virushandtekeningen ook via een gegevensdrager (bv. USB-stick) bijwerken. Dit noemt men een **offline-update**. Daarvoor moet u op een computer die met internet verbonden is en die over de nodige rechten beschikt, de virushandtekeningen naar de gegevensdrager exporteren. Daarna importeert u deze met de functie "Importeren van" op de computer zonder internetverbinding. Het systeem op deze computer wordt dan ook beschermd met de nieuwste virushandtekeningen. In tegenstelling tot regelmatige updates van de virushandtekeningen via internet, is de gebruiker in dit geval verantwoordelijk en moet hij de virushandtekeningen zelf zo vaak mogelijk bijwerken.

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: Wanneer u deze optie aanvinkt, wordt elke update van de virushandtekeningen geregistreerd in het logboek, dat u bij de extra functies van de G DATA software (in het **SecurityCenter** onder **Logboeken**) kunt raadplegen. Naast deze gegevens vindt u in het logboek bijvoorbeeld informatie over gevonden virussen en andere acties die door het programma zijn uitgevoerd.

Licentie activeren

Als u de G DATA software nog niet hebt geregistreerd, kunt u dat nu doen en uw registratienummer en klantgegevens invoeren. Afhankelijk van het type product vindt u het registratienummer bijvoorbeeld op de achterkant van de gebruikershandleiding, in de bevestigingsmail bij de softwaredownload 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 verlaten.

> **Opgelet**: Voor uw administratie en een eventuele nieuwe installatie 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 uw licentie niet activeren?** 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 virushandtekeningen, controleert u eerst of u via een internetbrowser (bv. Internet Explorer) verbinding met internet kunt maken. 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 een proxyserver gebruikt, 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

Wanneer de webbeveiliging actief is, wordt de internetinhoud al bij het surfen op eventuele schadelijke software gecontroleerd. Hier zijn de volgende instellingen beschikbaar.

- **Internetinhoud (HTTP) controleren**: In de webbeveiligingsopties kunt u bepalen dat alle HTTP-webinhoud al bij het surfen op virussen gecontroleerd dient te worden. Geïnfecteerde webinhoud wordt dan überhaupt niet uitgevoerd en de bijbehorende pagina's worden niet weergegeven. Vink hiervoor de optie **Internetinhoud (HTTP) controleren** aan.

  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. Lees hiervoor ook het hoofdstuk **Uitzonderingen vastleggen**. Met de knop **Geavanceerd** kunt u extra opties voor de behandeling van internetinhoud instellen.

- **Phishingbeveiliging**: met behulp van phishing proberen oplichters via internet klanten van een bepaalde bank of winkel naar een vervalste website te lokken om daar hun gegevens te stelen. Het activeren van de phishingbeveiliging: wordt sterk aanbevolen.

- **Adressen van geïnfecteerde internetpagina's inzenden**: Via deze functie kunt u, uiteraard anoniem, automatisch internetpagina's melden die door de software als gevaarlijk worden bestempeld. Zo helpt u mee aan de veiligheid voor alle gebruikers.

- **BankGuard-browserbeveiliging**: Banktrojanen vormen een steeds grotere bedreiging. Elk uur ontwikkelen cybercriminelen nieuwe malwarevarianten (bv. ZeuS, SpyEye) om uw geld te stelen. Banken beveiligen het gegevensverkeer op internet, maar de gegevens worden gedecodeerd in de browser en daar slaan banktrojanen toe. De toonaangevende technologie van G DATA BankGuard beveiligt uw banktransacties vanaf het begin en biedt meteen beveiliging op de plaatsen waar de aanval plaatsvindt. Door de gebruikte netwerkbibliotheken in realtime te controleren, zorgt G DATA BankGuard ervoor dat uw internetbrowser niet door een banktrojaan wordt gemanipuleerd. We raden u aan om de beveiliging van G DATA BankGuard ingeschakeld te laten.

  Info: Naast de Man-in-the-Middle-methode waarbij de aanvaller de communicatie tussen de gebruiker en de doelcomputer beïnvloedt, is er ook de aanvalmethode Man-in-the-Browser (MITB). Bij deze methode infecteert de aanvaller de browser zelf en krijgt deze toegang tot de gegevens voordat deze worden gecodeerd. De module BankGuard beveiligt u ook tegen deze soort aanvallen, door de zogenaamde digitale vingerafdruk van een bestand of een deel van een internetpagina met een database op internet wordt vergeleken. Op deze wijze wordt onmiddellijk een bedrog ontdekt en wisselt de G DATA software de frauduleuze gegevensverbinding automatisch om voor het origineel.

- **Keyloggerbeveiliging**: de keyloggerbeveiliging controleert ook onafhankelijk van virushandtekeningen, of de toetsenbordinvoer op uw systeem wordt bespioneerd. Op die manier kunnen aanvallers uw wachtwoordinvoer registreren. Deze functie moet altijd ingeschakeld blijven.

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 venster Whitelist 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**.

Geavanceerd

Hier kunt u bepalen 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 op normale wijze overgedragen naar de internetbrowser.

- **Bericht weergeven bij het scannen van downloads**: Activeer deze functie om een bericht te krijgen wanneer er een download wordt gescand.

- **Groottebeperking 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.

> **Opgelet**: Microsoft Outlook controleert e-mails door middel van een plug-in. Deze biedt dezelfde bescherming als de beveiliging voor POP3/IMAP in de antivirusopties. 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

Voor de virusbeveiliging van inkomende e-mails beschikt u over de volgende opties:

- **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 deze optie te activeren worden alle e-mails die tijdens uw werk op de computer worden ontvangen, op virussen 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

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. Om uitgaande e-mails op virussen te controleren, vinkt u de optie **E-mails vóór het verzenden controleren** aan.

Scanopties

Hier kunt u basisopties van de viruscontrole in- of uitschakelen:

- **Engines gebruiken**: de software werkt met twee antivirusengines, twee analysesystemen die op elkaar zijn afgestemd. 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 op internet en is daardoor in staat op massamailings te reageren voordat de betreffende virushandtekeningen beschikbaar zijn. OutbreakShield zoekt daarvoor op internet naar een opvallende stijging 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 virushandtekeningen. OutbreakShield is geïntegreerd in de e-mailvirusblokkering.

Versleutelde verbindingen (SSL)

Heel wat e-mailproviders (bv. GMX, WEB.DE, T-Online en Freenet) zijn intussen naar SSL-versleuteling overgeschakeld. Daardoor zijn e-mails en e-mailaccounts veel veiliger geworden. Toch blijft het belangrijk uw e-mails te beveiligen met antivirussoftware. G DATA biedt hiervoor de module **Versleutelde verbindingen (SSL)** aan. U hebt ook de mogelijkheid om met SSL versleutelde e-mails op virussen en malware te controleren.

Om ervoor te zorgen dat de G DATA software de met SSL versleutelde e-mails kan controleren, moet een certificaat van de G DATA software in de e-mailsoftware geïmporteerd worden. Op die manier kan de G DATA software de inkomende e-mails controleren.

Alle e-mailprogramma's die certificaten kunnen importeren of die toegang hebben tot het certificaatarchief van Windows worden ondersteund, waaronder:

- Outlook 2003 of hoger
- Thunderbird
- The Bat

- Pegasusmail

Als het certificaat van G DATA niet automatisch werd geïnstalleerd, gaat u als volgt te werk:

1. Bij de installatie van het certificaat mag uw e-mailprogramma niet actief zijn. Sluit daarom alle e-mailprogramma's voordat u het certificaat aanmaakt en installeert.
2. Vink de optie SSL-verbindingen controleren in de G DATA software aan.
3. Klik op de knop Certificaat exporteren. De G DATA software maakt nu een certificaat aan. Dit bestand heet GDataRootCertificate.crt.
4. Open nu het bestand GDataRootCertificate.crt. Er verschijnt een dialoogvenster waarin u het certificaat op uw computer kunt installeren.
5. Klik in het dialoogvenster op de knop **Certificaat installeren** en volg de instructies in de installatiewizard.

Klaar. Outlook en alle andere e-mailprogramma's die toegang hebben tot het certificaatarchief van Windows beschikken nu over het vereiste certificaat om ook met SSL versleutelde e-mails op virussen en andere malware te controleren.

> **Opmerking**: als u **Thunderbird (portable)** gebruikt en het certificaat niet automatisch is geïmporteerd, moet u dit achteraf importeren en de vertrouwensinstellingen van het aangemaakte G DATA certificaat beheren. Selecteer daarvoor in Thunderbird (portable) onder **Opties > Geavanceerd > Certificaten** de knop **Certificaten**. Als u hierop klikt, verschijnen er verschillende tabbladen. Selecteer het tabblad **Organisaties** en daarna de knop **Importeren**. Nu kunt u het certificaat **G DATA Mail Scanner Root** selecteren.
>
> Als u nu de volgende opties aanvinkt en op OK klikt, wordt uw Thunderbird portable door G DATA beveiligd:
>
> - **Vertrouw dit certificaat om websites te identificeren.**
> - **Vertrouw dit certificaat om e-mailgebruikers te identificeren.**
> - **Vertrouw dit certificaat om softwareontwikkelaars te identificeren**.
>
> Andere e-mailprogramma's hebben vergelijkbare functies voor het importeren van certificaten. In geval van twijfel raadpleegt u de instructies in de helpdocumentatie van het door u gebruikte e-mailprogramma.

Geavanceerd

Als u niet de standaardpoort gebruikt voor uw e-mailprogramma, dan 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.

> **Opgelet**: Microsoft Outlook wordt door een speciale plug-in beveiligd. Hiermee kunt u direct in Outlook mappen en e-mails controleren. Om in Outlook een e-mail of een map op virussen te controleren, klikt u gewoon op het G DATA symbool. De op dat moment geselecteerde e-mailmap wordt dan op virussen gecontroleerd.

Omdat de software de inkomende e-mails bewerkt voordat deze het e-mailprogramma bereiken, kan het bij grote hoeveelheden e-mails of een trage verbinding gebeuren dat het e-mailprogramma een foutmelding geeft. De reden daarvoor is dat het programma de e-mailgegevens niet onmiddellijk ontvangt, omdat ze door de software eerst op virussen worden 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 aan het e-mailprogramma doorgegeven.

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.

Geplande 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.

In de volgende hoofdstukken wordt uitgelegd hoe u individuele viruscontroles uitvoert.

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 (maandelijkse 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 een taak genoemd.

Omvang van de analyse

Bepaal hier of de virusscan op de lokale harde schijven wordt uitgevoerd, of het geheugen en autostart moeten worden getest of dat 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 op de (+)-symbolen te klikken. 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.

Planning

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 opstarten van het systeem** selecteert, moet u geen tijdsinstellingen opgeven 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 stroomnetis aangesloten.

Scaninstellingen

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 optimaal op elkaar zijn afgestemd. 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.
- **Geïnfecteerde archieven**: Bepaal hier of archiefbestanden (zoals bestanden met de extensies RAR, ZIP of PST) anders moeten worden behandeld 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.

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**: Het controleren van gecomprimeerde bestanden in archieven (te herkennen aan bestandsextensies als ZIP, RAR of PST) is heel tijdrovend en kan meestal worden weggelaten als de virusbewaker algemeen op het systeem actief is. 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 (bv. bootsectoren) van uw computer hoeven doorgaans niet te worden

uitgesloten van de viruscontrole.

- **Op telefoonkiezers / 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 virusherkenningsmethodes 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.

AntiSpam

Spamfilter

Via het spamfilter beschikt u over uitgebreide instelmogelijkheden om berichten met ongewenste inhoud of van ongewenste afzenders (bijvoorbeeld verzenders van massamailings) effectief te blokkeren. Het programma controleert e-mailberichten op allerlei kenmerken die typerend zijn voor spam. Aan de hand van de desbetreffende kenmerken wordt een waarde berekend, die de waarschijnlijkheid op spam weergeeft. Met de knop **Spamfilter gebruiken** schakelt u de spamfilter in of uit.

Om de verschillende filtertypes van de spamfilter in of uit te schakelen, zet u al dan niet een vinkje bij het betreffende item. Als u bij de verschillende filters wijzigingen wilt aanbrengen, klik dan op het betreffende item. Er verschijnt dan een dialoogvenster waarin u de parameters kunt wijzigen. De volgende instelmogelijkheden zijn beschikbaar:

- **Spam-OutbreakShield**: met OutbreakShield kunnen schadelijke bestanden in massaal verzonden spam-mails al worden herkend en bestreden voordat de daarvoor bijgewerkte virusdefinities 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. Als u een proxyserver gebruikt, klikt u op de knop **Internetinstellingen** en brengt u de relevante wijzigingen aan. U dient deze instelling alleen te wijzigen als OutbreakShield niet werkt.

- **Whitelist gebruiken**: Met de Witte lijst kunt u adressen van afzenders of domeinen uitzonderen van een spamverdenking. Typ daarvoor in het veld **Adressen/domeinen** het e-mailadres (bijvoorbeeld *newsletter@infopag.nl*) of domein (bijvoorbeeld *infopag.nl*) dat u van spamverdenking wilt uitsluiten. De G DATA software zal e-mails van deze afzender of dit afzenderdomein dan niet als spam behandelen.

  Met de knop **Importeren** kunt u ook kant-en-klare lijsten met e-mailadressen of domeinen aan de whitelist toevoegen. De adressen en domeinen moeten in een dergelijke lijst op aparte regels onder elkaar zijn ingevoerd. Als formaat wordt hierbij een eenvoudig txt-bestand gebruikt, zoals dat bijvoorbeeld in Windows Kladblok kan worden aangemaakt. Met de knop **Exporteren** kunt u een dergelijke whitelist ook als tekstbestand exporteren.

- **Blacklist gebruiken**: Met de blacklist kunt u adressen van bepaalde afzenders of domeinen identificeren als verzenders van spam. Typ daarvoor in het veld **Adressen/domeinen** het e-mailadres (bijvoorbeeld *newsletter@megaspam.nl*) of domein (bijvoorbeeld *megaspam.nl*) dat u wilt aanmerken als spam. De G DATA software zal e-mails van deze afzender of dit afzenderdomein voortaan beschouwen als e-mails met een zeer hoge spamwaarschijnlijkheid. Met de knop **Importeren** kunt u ook kant-en-klare lijsten met e-mailadressen of domeinen aan de blacklist toevoegen. De adressen en domeinen moeten in een dergelijke lijst op aparte regels onder elkaar zijn ingevoerd. Als formaat wordt hierbij een eenvoudig txt-bestand gebruikt, zoals dat bijvoorbeeld in Windows Kladblok kan worden aangemaakt. Met de knop **Exporteren** kunt u een dergelijke blacklist ook als tekstbestand exporteren.

- **Real-time blacklists (standaardinstelling) gebruiken**: Op internet zijn lijsten te vinden met IP-adressen van servers waarvan bekend is dat ze worden gebruikt om spam te verzenden. Via aanvragen aan de real-time blacklists achterhaalt de G DATA software of de verzendende server op deze lijsten staat. Is dat het geval, neemt de spamwaarschijnlijkheid toe. Normaal gesproken kunt u hier het beste de standaardinstelling gebruiken, maar u kunt ook zelf adreslijsten aanleggen onder Zwarte lijst 1, 2 en 3.

- **Trefwoorden (e-mailtekst) gebruiken**: Via de lijst met trefwoorden kunt u e-mailberichten ook aan de hand van de in de e-mailtekst gebruikte woorden aanmerken als spam. Als minimum een van de woorden in de e-mail op deze lijst staat, dan wordt de kans op spam verhoogd. Indien gewenst kunt u de lijst aanpassen via de knoppen **Toevoegen**, **Wijzigen** en **Verwijderen**. Met de knop **Importeren** kunt u ook kant-en-klare lijsten met trefwoorden in uw lijst invoegen. De vermeldingen moeten in een dergelijke

lijst zijn ingevoerd op aparte regels, onder elkaar. Als formaat wordt hierbij een eenvoudig txt-bestand gebruikt, zoals dat bijvoorbeeld in Windows Kladblok kan worden aangemaakt. Met de knop **Exporteren** kunt u een dergelijke lijst met trefwoorden ook als tekstbestand exporteren. Als u de optie **Alleen volledige woorden zoeken** aanvinkt, doorzoekt de G DATA software de onderwerpregel van een e-mail alleen op complete woorden.

- **Trefwoorden (onderwerp) gebruiken**: Via de lijst met trefwoorden kunt u e-mailberichten ook aan de hand van de in de onderwerpregel gebruikte woorden onder spamverdenking plaatsen. Als minimaal een van de woorden in de onderwerpregel staat, stijgt de spamwaarschijnlijkheid.

- **Inhoudsfilter gebruiken**: Een inhoudsfilter is een zelflerende filter die op basis van de in de e-mail gebruikte woorden de spamwaarschijnlijkheid berekent. Dit filter werkt niet alleen op basis van vaststaande woordenlijsten, maar leert bij elk nieuw binnengekomen e-mailbericht nieuwe woorden. Via de knop **Tabelinhoud opvragen** kunt u de woordenlijsten weergeven die het inhoudsfilter gebruikt om e-mailberichten te herkennen als spam. Met de knop **Tabellen terugzetten** verwijdert u alle geleerde woorden uit de tabel en begint het leerproces van het zelflerende inhoudsfilter opnieuw.

Reactie

Hier kunt u opgeven hoe het spamfilter moet omgaan met e-mails die mogelijkerwijs spam bevatten. Er zijn drie gradaties die worden beïnvloed door de mate waarin de G DATA software het waarschijnlijk acht dat het bij het betreffende e-mailbericht om spam gaat.

- **Spamverdenking**: hier wordt bepaald wat er met e-mailberichten moet gebeuren waarin de G DATA software spamelementen vindt. Hierbij hoeft het niet altijd om spam te gaan. Het kunnen ook e-mails zijn die de ontvanger wel wenst te ontvangen, zoals nieuwsbrieven of mailings. Hier is het aan te bevelen om de ontvanger te wijzen op de spamverdenking.

- **Hoge spamwaarschijnlijkheid**: hier vindt u de e-mails die veel kenmerken van spam bevatten en slechts in zeer zeldzame gevallen door de ontvanger gewenst zijn.

- **Zeer hoge spamwaarschijnlijkheid**: hier vindt u de e-mails die aan alle spamcriteria voldoen. Het gaat hierbij vrijwel nooit om gewenste e-mailberichten en in de meeste gevallen is het aan te raden dergelijke e-mailberichten te weigeren.

U kunt voor elk van deze drie gradaties zelf bepalen hoe de reactie moet zijn. Klik daarvoor op de knop **Wijzigen** en bepaal hoe de G DATA software moet reageren. Met de optie **E-mail weigeren** kunt u ervoor zorgen dat de e-mail niet eens in uw postvak terechtkomt. Met de optie **Spamwaarschuwing in het onderwerp en tekst van de e-mail invoegen** kunt u als spam herkende e-mails ook als zodanig kenmerken, zodat u ze gemakkelijker kunt herkennen. Als u **Microsoft Outlook** gebruikt (pas op: niet te verwarren met Outlook Express of Windows Mail), hebt u ook de mogelijkheid om e-mails met spamverdenking naar een zelf te bepalen map in uw postvak te verplaatsen (**E-mail in map plaatsen**). U kunt deze map direct in de G DATA software instellen door de betreffende map te definiëren onder **Mapnaam**.

> **Opmerking**: ook als u Outlook niet gebruikt, kunt u als spam herkende e-mails naar een aparte map laten verplaatsen. Voeg daarvoor een waarschuwing toe aan de onderwerpregel (bijvoorbeeld "*[Spam]*") en stel in uw e-mailprogramma een regel in die e-mails met deze tekst in het onderwerp naar een andere map verplaatst.

Pro-instellingen

Hier kunt u de spamherkenning door de G DATA software tot in het kleinste detail wijzigen en aan uw e-mailverkeer aanpassen. Toch is het over het algemeen aan te raden de standaardinstellingen te gebruiken. Breng onder Pro-instellingen alleen wijzigingen aan als u bekend bent met de materie en precies weet wat u doet.

Overige filters

De volgende filters zijn hier standaard ingesteld en kunnen indien nodig worden uitgeschakeld door het vinkje te verwijderen.

- **HTML-scripts uitschakelen**

- **Filteren op gevaarlijke bijlagen**

Daarnaast kunt u via de knop **Nieuw** nieuwe filterregels instellen en via de knop **Bewerken** bestaande filters bewerken. De gemaakte filters worden in de lijst weergegeven en kunnen via de bijbehorende vakjes links worden in- of uitgeschakeld. Indien er een vinkje in het vakje staat, is de desbetreffende filter actief. Indien er geen vinkje in het vakje staat, is de desbetreffende filter niet actief. Als u een filter definitief wilt verwijderen, selecteert u de filter met de muis en klikt u op de knop **Verwijderen**.

De filtermogelijkheden die hier beschikbaar zijn, zijn extra filters die de eigenlijke spamfilter van de G DATA software ondersteunen en die uw individuele instellingen vergemakkelijken. Via de eigenlijke spamfilter beschikt u over uitgebreide instelmogelijkheden om berichten met ongewenste inhoud of van ongewenste afzenders (bijvoorbeeld afzenders van massamailings) effectief te blokkeren. Het programma controleert e-mailberichten op allerlei kenmerken die typerend zijn voor spam. Aan de hand van de desbetreffende

kenmerken wordt een waarde berekend, die de waarschijnlijkheid op spam weergeeft. Hiervoor beschikt u over verschillende tabbladen waarop de relevante instelmogelijkheden per onderwerp worden opgesomd.

Als u een nieuwe filter aanmaakt, wordt een keuzevenster geopend waarin u het basisfiltertype kunt vastleggen. Alle overige gegevens voor de in te stellen filter kunt u vervolgens in het wizardvenster voor het filtertype opgeven. Op deze manier kunt u eenvoudig filters samenstellen tegen elke mogelijke dreiging.

- **HTML-scripts uitschakelen**: Deze filter schakelt scripts in het HTML-gedeelte van een e-mail uit. Scripts die nuttig kunnen zijn op een internetsite, zijn eerder storend als ze in een HTML-bericht zijn opgenomen. HTML-scripts worden soms ook gebruikt om computers te infecteren aangezien scripts alleen al door weergave in het voorbeeldvenster van een e-mailbericht actief kunnen worden en niet pas door het openen van een geïnfecteerde bijlage.

- **Filteren op gevaarlijke bijlagen**: U kunt e-mailbijlagen (= attachments) op vele manieren filteren. De meeste e-mailvirussen verspreiden zich via dergelijke attachments, die in de meeste gevallen meer of minder goed verborgen uitvoerbare bestanden bevatten. Daarbij kan het gaan om een klassiek .exe-bestand dat een schadelijk programma bevat, maar ook om VB-scripts die in bepaalde gevallen zelfs zijn verstopt in op het eerste gezicht veilige, grafische bestanden, filmbestanden of geluidsbestanden. Over het algemeen moet men zeer voorzichtig zijn bij het openen van bijgevoegde bestanden waar niet uitdrukkelijk om is gevraagd. Informeer in twijfelgevallen eerst bij de afzender of het e-mailbericht inderdaad door hem of haar is verzonden.

  Onder **Bestandsextensies** kunt u de bestandsextensies weergeven waarvoor u de betreffende filter wilt gebruiken. Hierbij kunt u bijvoorbeeld alle uitvoerbare bestanden (bijvoorbeeld .exe- en .com-bestanden) in een filter samenbrengen. U kunt ook andere formaten filteren (bijvoorbeeld mpeg, avi, mp3, jpeg, gif enz.), als die vanwege hun omvang de e-mailserver te zwaar belasten. Uiteraard kunt u ook willekeurige archiefbestanden filteren (bijvoorbeeld zip, rar of cab). Scheid alle bestandsextensies binnen een filtergroep door een puntkomma.

  Met de functie **Ook bijlagen in ingesloten e-mails filteren** zorgt u ervoor dat het filteren van de onder **Bestandsextensies** geselecteerde bijlagensoorten ook plaatsvindt in e-mailberichten die zelf onderdeel zijn van een ander e-mailbericht. Deze optie moet normaal gesproken geactiveerd zijn.

  Met de optie **Bijlagen alleen andere naam geven** worden de te filteren bijlagen niet automatisch verwijderd, maar alleen een andere naam gegeven. Dat is bijvoorbeeld zinvol bij uitvoerbare bestanden (zoals EXE en COM) en bij Microsoft Office-bestanden die mogelijk uitvoerbare scripts en macro's kunnen bevatten. Door de naam van een bijlage te wijzigen kan deze niet per ongeluk en ondoordacht worden geopend. De bijlage moet door de ontvanger namelijk eerst worden opgeslagen en desgewenst moet de naam opnieuw worden gewijzigd voordat deze kan worden gebruikt. Als er geen vinkje staat bij **Bijlagen alleen andere naam geven**, worden de betreffende bijlagen meteen verwijderd.

  Onder **Achtervoegsel** voert u de tekenreeks in waarmee u de feitelijke extensie wilt uitbreiden. Op die manier is het niet langer mogelijk om een uitvoerbaar bestand te activeren door erop te klikken (bijvoorbeeld *.exe_danger). Bij **Melding in de tekst van de e-mail invoegen** kunt u de ontvanger van het gefilterde e-mailbericht laten weten dat een bijlage op grond van een filterregel is verwijderd of een andere naam is gegeven.

- **Inhoudsfilter**: Met het inhoudsfilter kunt u e-mails met bepaalde onderwerpen of teksten eenvoudig blokkeren.

  Voer hiervoor bij **Zoekcriterium** gewoon de trefwoorden en uitdrukkingen in waarop de G DATA software moet reageren. Hierbij kunt u tekst op een willekeurige manier combineren met de logische operators EN en OF.

  Geef bij **Zoekbereik** aan in welke onderdelen van een e-mail naar deze woorden moet worden gezocht. Met **Koptekst** wordt het gedeelte van een e-mail aangeduid dat onder meer de e-mailadressen van de afzender en geadresseerde, het onderwerp en informatie over de gebruikte programma's, protocollen en verzenddatum bevat. Als u kiest voor het onderdeel **Onderwerp**, wordt enkel de inhoud van de onderwerpregel gecontroleerd en geen verdere tekstinformatie uit de koptekst. Bij **E-mailtekst** kunt u bovendien kiezen of het zoekbereik beperkt is tot pure tekstberichten of ook de tekst in HTML-berichten (HTML-tekst) moet worden doorzocht.

  Bij **Ingesloten e-mails** kunt u aangeven of de inhoudsfilter ook e-mails moet doorzoeken die als bijlage bij de ontvangen e-mail zijn gevoegd.
  Onder **Reactie** kunt u instellen wat er moet gebeuren met e-mails die door de G DATA software als spam worden herkend. Onder **E-mail weigeren** wordt de betreffende e-mail zelfs niet ontvangen door uw e-mailprogramma.

  Wanneer u **Waarschuwing in onderwerp en tekst van de e-mail invoegen** aanvinkt, kunt u de eigenlijke tekst van de onderwerpregel laten voorafgaan door een waarschuwing (Voorvoegsel op onderwerpregel), bv. *Spam* of *Waarschuwing*.
  Desgewenst kunt u ook tekst invoeren die bij verdenking van spam voorafgaat aan de eigenlijke e-mailtekst (Melding in de tekst).

  Als u *Microsoft Outlook* gebruikt (**let op**: niet te verwarren met Outlook Express of Outlook Mail), hebt u de mogelijkheid om e-mails met spamverdenking naar een zelf te bepalen map in uw postvak te verplaatsen (**E-mail in map plaatsen**). U kunt deze map direct in de G DATA software instellen door de betreffende map te definiëren onder **Mapnaam**.

- **Afzender filteren**: Met de afzenderfilter kunt u e-mails die afkomstig zijn van bepaalde afzenders eenvoudig blokkeren. Voer hiervoor gewoon onder **Afzenders/domeinen** de e-mailadressen of domeinnamen in waarop de G DATA software moet reageren. Meerdere vermeldingen moeten worden gescheiden door een puntkomma.

  Onder **Reactie** kunt u instellen wat er moet gebeuren met e-mails die door de G DATA software als spam worden herkend.

  Onder **E-mail weigeren** wordt de betreffende e-mail zelfs niet ontvangen door uw e-mailprogramma.

  Wanneer u **Waarschuwing in onderwerp en tekst van de e-mail invoegen** aanvinkt, kunt u de eigenlijke tekst van de onderwerpregel laten voorafgaan door een waarschuwing (Voorvoegsel op onderwerpregel), bv. *Spam* of *Waarschuwing*. Desgewenst kunt u ook tekst invoeren die bij verdenking van spam voorafgaat aan de eigenlijke e-mailtekst (Melding in de tekst).

  Als u *Microsoft Outlook* gebruikt (**let op**: niet te verwarren met Outlook Express of Windows Mail), hebt u de mogelijkheid om e-mails met spamverdenking naar een zelf te bepalen map in uw postvak te verplaatsen (**E-mail in map plaatsen**). U kunt deze map direct in de G DATA software instellen door de betreffende map te definiëren onder **Mapnaam**.

- **Talenfilter**: Met het talenfilter kunt u automatisch e-mails in een bepaalde taal als spam definiëren. Als u bijvoorbeeld in de regel geen e-mailcontact hebt met Engelstalige personen, dan kunt u door Engels te definiëren als spamtaal al heel veel spam uitfilteren. Als u hier de talen selecteert waarin u normaal gesproken geen e-mails krijgt, verhoogt de G DATA software de spambeoordeling van deze e-mails aanzienlijk.

  Onder **Reactie** kunt u instellen wat er moet gebeuren met e-mails die door de G DATA software als spam worden herkend.

  Onder **E-mail weigeren** wordt de betreffende e-mail zelfs niet ontvangen door uw e-mailprogramma.

  Wanneer u **Waarschuwing in onderwerp en tekst van de e-mail invoegen** aanvinkt, kunt u de eigenlijke tekst van de onderwerpregel laten voorafgaan door een waarschuwing (Voorvoegsel op onderwerpregel), bv. *Spam* of *Waarschuwing*. Desgewenst kunt u ook tekst invoeren die bij verdenking van spam voorafgaat aan de eigenlijke e-mailtekst (Melding in de tekst).

  Als u *Microsoft Outlook* gebruikt (**let op**: niet te verwarren met Outlook Express of Windows Mail), hebt u de mogelijkheid om e-mails met spamverdenking naar een zelf te bepalen map in uw postvak te verplaatsen (**E-mail in map plaatsen**). U kunt deze map direct in de G DATA software instellen door de betreffende map bij **Mapnaam** te definiëren.

Diversen

In dit gedeelte kunt u overige instellingen opgeven.

- **Ongelezen e-mails in Postvak IN bij starten van het programma controleren**: *Alleen voor Microsoft Outlook*: Met deze optie worden e-mails op spam gecontroleerd. Zodra u Outlook opent, worden alle ongelezen e-mails in de map Postvak IN en de onderliggende mappen door de G DATA software gecontroleerd.

- **Andere e-mailprogramma's (gebruik van POP3)**: E-mails die via POP3 binnenkomen, kunnen om technische redenen niet rechtstreeks worden verwijderd. Wanneer een filter e-mails moet weigeren, worden deze van een standaard vervangende tekst voorzien. De vervangende tekst bij geweigerde e-mails luidt: **Het bericht is geweigerd**. U kunt de tekst voor deze berichtfuncties ook individueel instellen. In de vrij te definiëren tekst voor het **onderwerp** en de **e-mailtekst** zijn de volgende jokertekens (procentteken met aansluitend een kleine letter) beschikbaar:

  %s Afzender

  %u Onderwerp

U kunt in uw e-mailprogramma een regel definiëren die e-mails met de hier ingestelde vervangende tekst automatisch verwijdert.

Firewall

Automatisch systeem

Als u zich niet verder met de firewall wilt bezighouden, kunt u de instelling op Automatisch systeem laten staan. In veel gevallen is het voldoende de firewall in de modus Automatische piloot te gebruiken. U kunt de G DATA firewall echter ook volledig op uw behoeften afstemmen via allerlei aanvullende opties.

De firewall-instellingen zijn ondergebracht in twee basisgedeelten, die u afzonderlijk kunt configureren:

Automatische piloot

Hier kunt u aangeven of de firewall zelfstandig en zelflerend werkt, waarbij de gebruiker niet wordt gevraagd of aanvragen van internet

moeten worden geblokkeerd, of als de gebruiker in twijfelgevallen wordt geraadpleegd.

- **Modus Automatische piloot**: Hier werkt de firewall volkomen autonoom en houdt automatisch de gevaren voor uw thuis-pc tegen. Deze instelling biedt een praktische en volledige beveiliging en is in de meeste gevallen aan te bevelen.
- **Handmatige regelaanmaak**: Via de handmatige regelaanmaak kunt u de firewall volledig op uw wensen afstemmen.
- **Autopiloot-modus aanbieden, als een toepassing in volledige schermweergave wordt gestart**: Vooral bij computerspelletjes (en andere toepassingen in volledige schermweergave) kan het vervelend zijn wanneer de firewall u voortdurend met vragen bestookt en zo het verloop van het spel of de weergave stoort. Om ongestoord speelgenot te garanderen zonder de beveiliging te verwaarlozen, is de automatische piloot een nuttige instelling, aangezien hij vragen van de firewall onderdrukt. Als u de automatische piloot niet als standaardinstelling gebruikt, kunt u er via deze functie voor zorgen dat hij altijd wordt aangeboden als u een programma in volledige schermweergave gebruikt.

Door gebruiker gedefinieerde beveiligingsinstellingen

Tijdens het dagelijkse gebruik van de computer leert de firewall automatisch welke programma's u gebruikt om toegang te krijgen tot internet en welke programma's een veiligheidsrisico vormen. Het voordeel van het gebruik van vooraf gedefinieerde beveiligingsniveaus is dat u de firewall ook zonder administratieve rompslomp en kennis van netwerkbeveiliging aan uw eigen behoeften kunt aanpassen. Bepaal gewoon met de schuifregelaar welk beveiligingsniveau u wenst. U heeft de keuze uit de volgende veiligheidsniveaus:

- **Hoogste beveiliging**: De regels voor de firewall worden volgens zeer nauwgezette richtlijnen bepaald. Hiervoor moet u op de hoogte zijn van specifieke netwerkbegrippen (TCP, UDP, poorten, enz.). De firewall ontdekt zelfs de kleinste afwijking en zal tijdens de leerfase zeer veel informatie vragen.
- **Hoge beveiliging**: De regels voor de firewall worden volgens zeer nauwgezette richtlijnen bepaald. Hiervoor moet u op de hoogte zijn van specifieke netwerkbegrippen (TCP, UDP, poorten, enz.). De firewall zal tijdens de leerfase regelmatig om informatie vragen als dat gezien de omstandigheden nodig is.
- **Normale beveiliging**: De regels voor de firewall worden alleen vastgelegd op gebruikersniveau. Wizards zorgen ervoor dat u geen netwerkspecifieke details te zien krijgt. Tijdens de leerfase krijgt u zo weinig mogelijk vragen.
- **Lage beveiliging**: De regels voor de firewall worden alleen vastgelegd op gebruikersniveau. Wizards zorgen ervoor dat u geen netwerkspecifieke details te zien krijgt. Tijdens de leerfase wordt u zelden iets gevraagd. Ook op dit beveiligingsniveau heeft u de hoogst mogelijke beveiliging bij binnenkomende verzoeken voor het maken van een verbinding.
- **Firewall uitgeschakeld**: U kunt de firewall desgewenst ook uitschakelen. Uw computer blijft dan verbonden met internet en andere netwerken, maar wordt dan niet langer door de firewall beschermd tegen aanvallen of spionage.

Als u de firewall meer op uw behoeften wilt afstemmen, vink dan de optie **Door gebruiker gedefinieerde beveiligingsinstellingen** aan. Bedenk daarbij echter wel dat u voor deze instellingen minimaal over een basiskennis van netwerkbeveiliging moet beschikken.

Vragen

Hier stelt u in wanneer, hoe en of de firewall de gebruiker een vraag dient te stellen op het moment dat een programma een verbinding met het internet of netwerk wilt maken.

Regel maken

Als de firewall een verbinding met het netwerk vaststelt, verschijnt een informatievenster waarin u kunt bepalen hoe verder moet worden omgegaan met de betreffende toepassing. Hier kunt u bepalen wat u precies met het toestaan of verbieden van een netwerktoegang wilt bereiken:

- **Per toepassing**: Hiermee wordt de toegang tot het netwerk voor de huidige toepassing via elke willekeurige poort of met elk willekeurig overdrachtsprotocol (bv. TCP of UDP) altijd toegestaan of geweigerd.
- **Per protocol/poort/toepassing**: De toepassing die toegang tot het netwerk vraagt, krijgt alleen toestemming om met het gevraagde overdrachtsprotocol en uitsluitend via de gevraagde poort online te gaan. Als dezelfde toepassing toestemming vraagt om via een andere poort of met een ander protocol verbinding met het netwerk te maken, verschijnt de vraag opnieuw en kan een nieuwe regel worden opgesteld.
- **Per toepassing, indien er ten minste x vragen zijn**: Er zijn toepassingen (bv. Microsoft Outlook), die bij een netwerkverzoek meteen meerdere poorten proberen resp. tegelijkertijd verschillende protocollen gebruiken. Aangezien dit bijvoorbeeld bij de instelling Per &Protocol/Poort/Toepassing meerdere vragen met zich mee zou brengen, kan hier ook worden ingesteld dat toepassingen een algemene vrijgave of weigering voor het netwerkgebruik krijgen, zodra de gebruiker u de verbinding toestaat of weigert.

Onbekende servertoepassingen

Toepassingen die nog niet via een regel in de firewall worden beheerd, kunnen verschillend worden behandeld. Het tijdstip van het verzoek staat daarbij in een bepaalde speelruimte binnen de beslissingsbevoegdheid. Als de servertoepassing Op ontvangst gaat, wil dat zeggen dat ze quasi op stand-by een verbindingsverzoek verwacht. Als dat niet het geval is, volgt de vraag pas als het eigenlijke verbindingsverzoek wordt ingediend.

Controle op onbeveiligde netwerken

Natuurlijk kan een firewall alleen probleemloos functioneren als alle netwerken waarvoor de te beveiligen computer toegang heeft ook door deze firewall herkend en bewaakt worden. Zorg er daarom voor dat deze controle op onbeveiligde netwerken altijd geactiveerd is.

Herhaalde toepassingsvragen

U kunt steeds terugkerende verbindingsverzoeken van een toepassing bundelen. Op die manier verschijnt bij verbindingsaanvragen waarvoor u nog geen regel hebt opgegeven, niet elke keer een vraag, maar bijvoorbeeld slechts om de 20 seconden of met een andere door u te bepalen frequentie.

Controle op verwijzingen

Bij de controle op verwijzingen wordt voor toepassingen die van de firewall al toegang tot het netwerk hebben gekregen, een controlesom gemaakt op basis van de bestandsgrootte en andere criteria. Wanneer de checksum van een programma plotseling afwijkingen vertoont, is het mogelijk dat het programma door een schadelijk programma is gewijzigd. In dat geval slaat de firewall alarm.

Controle op verwijzingen voor geladen modules: hier worden niet alleen de toepassingen bewaakt, maar ook de modules die door de toepassingen worden gebruikt (bv. DLL's). Aangezien deze vaak worden gewijzigd en ook nieuwe modules worden gedownload, kan een consequente controle op gewijzigde en onbekende verwijzingen bij modules een aanzienlijke administratieve rompslomp tot gevolg hebben. Elke gewijzigde module zou dan namelijk een veiligheidsvraag van de firewall met zich meebrengen. De modulecontrole mag daarom enkel bij heel hoge veiligheidseisen op deze manier worden gebruikt.

Diversen

Hier beschikt u over nog meer instelmogelijkheden.

Standaardinstelling voor de wizard Regels

Hier kunt u bepalen of u de nieuwe regels wilt maken via de Wizard Regels of in de uitgebreide bewerkingsmodus.. Gebruikers die onbekend zijn met netwerkbeveiliging raden wij de wizard Regels aan.

Controles bij de start van het programma

Hier kunt u aangeven of de firewall, telkens wanneer het programma wordt gestart, naar onbekende servertoepassingen moet zoeken. Deze zoekfunctie moet altijd ingeschakeld zijn, behalve als u in een gesloten netwerk werkt.

Verbindingslogboeken opslaan

Hier kunt u bepalen hoe lang de firewall verbindingsgegevens moet bewaren. U kunt de gegevens van één uur tot 60 uur bewaren en controleren in het gedeelte Logboeken.

Tuner

Algemeen

Hier kunt u de volgende instellingen opgeven:

- **Herstelgegevens verwijderen**: Hier kunt u bepalen wanneer herstelgegevens (die de G DATA software bij wijzigingen maakt) moeten worden verwijderd.
- **Oude gegevens verwijderen**: Hier kunt u bepalen wanneer oude gegevens (zoals oude TEMP-mappen) moeten worden verwijderd.
- **Bureaubladsnelkoppelingen verwijderen**: Hier kunt u bepalen na hoeveel dagen ongebruikte bureaubladsnelkoppelingen

moeten worden verwijderd.

- **Bij Microsoft Update ook Office-updates zoeken**: Hier kunt u bepalen of de tuner bij het zoeken naar de laatste Windows-updates ook automatisch naar Office-updates moet zoeken op het internet. Een update van beide onderdelen bespaart tijd en houdt de computer ook veiligheidstechnisch up-to-date. Het zoeken naar Office-updates werkt natuurlijk alleen als Microsoft Office op de desbetreffende computer is geïnstalleerd.

- **Geen gedetailleerde logboekbestanden over verwijderde elementen maken**: De tuner is zo ontworpen dat deze alle informatie over doorgevoerde wijzigingen bijhoudt. Als u een logboekbestand over de door de tuner verwijderde elementen als veiligheidsrisico beschouwt, kunt u ervoor zorgen dat een dergelijk verwijderingslogboek niet wordt gemaakt.

- **Tijdelijke bestanden permanent verwijderen**: Met deze functie sluit u de webbestanden (zoals cookies en tijdelijke internetgegevens) uit van de herstelfunctie van de tuner. U kunt deze bestanden dan niet meer herstellen. Als u deze functie inschakelt, wordt het aantal bestanden dat de tuner in het gedeelte Herstellen moet beheren, aanzienlijk kleiner. Dit levert prestatievoordelen op.

- **Computer automatisch opnieuw starten door de service niet toestaan**: bij geplande tuningprocessen is het mogelijk dat de tuner de computer opnieuw start. Met deze optie voorkomt u dat dat gebeurt. Omdat de Tuner de computer alleen ongevraagd opnieuw zou opstarten als er geen gebruiker is aangemeld, is het in de meeste gevallen zeker aan te raden om deze optie niet te activeren.

- **Herstel van individuele herstelpunten toestaan**: zonder deze functie kan de G DATA software geen herstel meer uitvoeren.

- **Bij het defragmenteren geen rekening houden met het stationstype**: omdat de meeste fabrikanten afraden om hun SSD's te defragmenteren, is defragmenteren standaard uitgesloten voor dit type harde schijf in G DATA Tuner. Als het type van de stations van de G DATA software niet automatisch kan worden bepaald, maar u zeker bent dat er zich geen SSD-stations in uw computer bevinden, kunt u deze optie aangevinkt laten. De tuner start in dat geval bij elke uitvoering met het defragmenteren van alle harde schijven die zich in het systeem bevinden.

Configuratie

In dit gebied kunt u alle modules selecteren die de tuner voor het tuningproces moet gebruiken. Geselecteerde modules worden daarbij dan hetzij via een automatische, tijdgestuurde actie gestart (zie het hoofdstuk **Planning**) hetzij handmatig. Om een module te activeren, klikt u er tweemaal op met de muis. U kunt hier de volgende tuningonderdelen instellen:

- *Beveiliging*: Diverse functies die automatisch gegevens downloaden van internet zijn alleen van nut voor de aanbieder en niet voor u. Vaak wordt ook via zulke functies de deur wijd opengezet voor schadelijke software. Met deze modules beveiligt u uw systeem en blijft het volledig bijgewerkt.

- *Prestaties*: Tijdelijke bestanden, zoals reservekopieën, logboekbestanden en installatiegegevens, die u niet meer nodig hebt, maken de harde schijf trager en nemen waardevolle opslagruimte in beslag. Bovendien vertragen overbodig geworden processen en koppelingen van gegevens uw systeem aanzienlijk. Met de hier opgesomde modules kunt u uw computer van deze overbodige ballast bevrijden en sneller maken.

- *Privacy*: Hier zijn de modules ondergebracht die uw gegevens beschermen. De sporen die bij het surfen of bij algemeen computergebruik onvrijwillig ontstaan, vertellen veel over uw gebruik en bevatten belangrijke gegevens en wachtwoorden. Hier worden deze sporen gewist.

Mapbeveiliging

Via dit tabblad kunt u bepaalde mappen (bv. ook uw Windows-partities) uitsluiten van de automatische verwijdering van oude bestanden.

Klik hiervoor op het symbool **Toevoegen** en selecteer de betreffende map of het gewenste station.

Om een uitzonderingsmap weer vrij te geven, selecteert u de map in de lijst en klikt u op de knop **Verwijderen**.

Bestandsbeveiliging

Met de bestandsbeveiliging kunt u bepaalde bestanden beschermen tegen het verwijderen door de tuner, bijvoorbeeld scores van computerspelletjes of soortgelijke bestanden met ongebruikelijke bestandsextensies, die ook als back-upbestanden of tijdelijke bestanden kunnen worden geïnterpreteerd.

Om bepaalde bestanden te beveiligen klikt u op de knop **Toevoegen** en voert u de betreffende bestandsnaam in. U kunt hier ook met jokertekens werken.

U kunt de jokertekens als volgt gebruiken:

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

Om bijvoorbeeld alle bestanden met de bestandsextensie .sav te beveiligen, voert u dus *.sav in. Om bijvoorbeeld verschillende soorten bestanden met een bestandsnaam die met dezelfde letters begint te beveiligen, voert u bijvoorbeeld tekst*.* in.

Selecteer nu nog de map waarin de bestanden moeten worden beveiligd door op de knop Uitgebreid te klikken. Kies hier nu de opslagplaats waar de bestanden die u wilt beveiligen zich bevinden. De tuner beveiligt nu de overeenkomstig gedefinieerde bestanden alleen in deze map (bijv. scores in de desbestreffende speelmap).

Om een bestandsbeveiliging weer vrij te geven, selecteert u de map in de weergegeven lijst en klikt u op de knop **Verwijderen**.

Planning

Op het tabblad **Planning** kunt u instellen wanneer en met welke frequentie het automatische tuningproces moet worden uitgevoerd.

Onder **Dagelijks** kunt u met behulp van de gegevens onder Weekdagen bv. bepalen dat uw computer de tuning alleen op werkdagen, alleen om de dag of alleen in het weekend als er niet wordt gewerkt uitvoert. Om onder **Tijdstip** dag- en tijdinstellingen te wijzigen, selecteert u het element dat u wilt wijzigen (bijv. dag, uur, maand, jaar) met de muis en gebruikt u de pijltjestoetsen, of de kleine pijlsymbolen rechts van het invoerveld, om in het betreffende element chronologisch te bewegen.

Als u de automatische tuning niet wilt inschakelen, verwijdert u het vinkje bij de optie **Ingeschakeld** voor de automatische tuningrun.

Apparaatcontrole

Via de apparaatcontrole kunt u voor uw computer bepalen welke opslagmedia zijn toegestaan voor het lezen en/of schrijven van gegevens. U kunt bijvoorbeeld voorkomen dat privégegevens op een USB-stick gelezen of op een cd gebrand worden. Bovendien kunt u bij verwisselbare schijven zoals USB-sticks of externe USB-stations precies bepalen met welke verwisselbare schijf u gegevens kunt downloaden. Zo kunt u bijvoorbeeld uw eigen USB-schijf voor gegevensback-up gebruiken, maar andere vaste schijven geen toegang geven.

Om de apparaatcontrole te gebruiken, vinkt u **Apparaatcontrole inschakelen** aan en selecteert u vervolgens voor welke apparaten u beperkingen wilt vastleggen:

- **Verwisselbare schijven (bv. USB-sticks)**
- **Cd-/dvd-stations**
- **Diskettestations**

U kunt nu regels voor de afzonderlijke opslagmedia opgeven.

Algemene regel

Hier kunt u bepalen of het betreffende apparaat helemaal niet mag worden gebruikt (**Toegang blokkeren**), of alleen gegevens ervan mogen worden gedownload, zonder dat er bestanden op kunnen worden opgeslagen (**Leestoegang**) of er geen beperkingen voor dit apparaat gelden (**Volledige toegang**). Deze regel geldt dan voor alle gebruikers van uw computer.

Gebruikersspecifieke regels

Als u wilt dat bepaalde gebruikers slechts beperkte rechten voor opslagmedia krijgen, dan kunt u in dit gedeelte eerst de gebruikersnaam van de op uw computer aangemaakte gebruiker selecteren en daarna de toegang tot het betreffende opslagmedium

zoals beschreven onder **Algemene regel** beperken. Op die manier kunt u zich bijvoorbeeld als beheerder en eigenaar van de computer volledige toegang geven, terwijl andere gebruikers slechts beperkte rechten hebben.

Selecteer hier de gebruiker. Wanneer u op OK klikt, wordt een nieuw dialoogvenster geopend, waarin u kunt bepalen welke soort toegang deze gebruiker krijgt en of de rechten voor deze gebruiker tot een bepaalde tijd (bv. twee weken) beperkt zijn (**Geldigheid**).

> **Opmerking**: de gebruikersspecifieke regels heffen de algemene regels op. Wanneer u dus algemeen bepaalt dat de toegang tot USB-sticks niet is toegestaan, kunt u een bepaalde gebruiker toch toestemming hiervoor geven via een gebruikersspecifieke regel. Wanneer een gebruiker via de apparaatcontrole bepaalde toegangsbeperkingen heeft gekregen die in tijd beperkt zijn, dan gelden na afloop van deze beperking opnieuw de algemene regels voor deze gebruiker.

Apparaatspecifieke regels

Bij het gebruik van verwisselbare schijven zoals USB-sticks of externe vaste schijven, kunt u ook bepalen dat enkel bepaalde verwisselbare schijven toegang krijgen tot uw computer. Verbind daarvoor de verwisselbare schijf met uw computer en klik daarna op **Toevoegen**. In het geopende dialoogvenster kunt u de gewenste verwisselbare schijf selecteren. Wanneer u op OK klikt, wordt een nieuw dialoogvenster geopend, waarin u kunt bepalen welke soort toegang deze gebruiker krijgt en of de rechten voor deze gegevensdrager tot een bepaalde tijd (bv. twee weken) beperkt zijn (**Geldigheid**) en of elke gebruiker deze gegevensdrager met zijn gebruikerstoegang mag gebruiken of niet.

Back-up

In dit gedeelte kunt u algemene instellingen voor de werking van de back-upmodule bepalen.

- **Map voor tijdelijke bestanden**: Bepaal hier waar tussentijds opgeslagen gegevens door de back-upmodule moeten worden opgeslagen. Deze bestanden ontstaan bij het aanmaken en bij het herstellen van een back-up en worden na het betreffende proces ook weer automatisch verwijderd. Toch moet u voldoende schijfruimte beschikbaar hebben, omdat de snelheid van de back-up en het herstel anders wordt beperkt. Deze instelling mag enkel worden gewijzigd wanneer in de geselecteerde map voor tijdelijke bestanden te weinig schijfruimte beschikbaar is.

- **Controle bron-/doelstation op dezelfde harde schijf**: Normaal waarschuwt de back-upmodule de gebruiker telkens wanneer hij een back-up wil aanmaken op de gegevensdrager waarop zich ook de oorspronkelijke bestanden bevinden. Dat gebeurt omdat bij een uitval/verlies van deze gegevensdrager de back-up automatisch ook niet meer beschikbaar is. Als u om de een of andere reden toch regelmatig back-ups op de oorspronkelijke gegevensdrager wilt uitvoeren, kunt u deze waarschuwing hier uitschakelen.

Logboeken

Voor de afzonderlijke modules zijn er logboekfuncties beschikbaar waarmee u op elk moment een overzicht krijgt van de acties die de G DATA software voor uw beveiliging uitvoert.

Virusbeveiligingslogboeken

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.

Firewall-logboeken

Het gedeelte Logboeken biedt voor elke actie van de firewall een omvangrijk logbestand. Hier kunt u aparte acties openen door erop te dubbelklikken en deze eventueel afdrukken of als tekstbestand opslaan. Lees hiervoor ook het hoofdstuk **Instellingen: Diversen**.

Back-uplogboeken

Het gebied Logboeken biedt voor elke actie en elke back-uptaak een omvangrijk logbestand. Hier kunt u aparte acties openen door erop te dubbelklikken en deze eventueel afdrukken of als tekstbestand opslaan. Lees hiervoor ook het hoofdstuk **Back-up maken en herstellen**.

Spambeveiliginglogboeken

Het gedeelte Logboeken biedt een omvangrijk logbestand voor elke actie. Hier kunt u aparte acties openen door erop te dubbelklikken en deze eventueel afdrukken of als tekstbestand opslaan.

Kinderbeveiligingslogboeken

In het onderdeel Logboek krijgt u als administrator een overzicht te zien van alle pogingen van andere gebruikers om geblokkeerde inhoud te openen. Bovenaan kunt u uit de lijst de gebruiker selecteren waarvan u het logboek wilt bekijken. Lees hiertoe het hoofdstuk **Instellingen: Logboek**.

> **Opmerking**: u kunt deze logboeken natuurlijk ook verwijderen met de knop **Logboeken verwijderen**.

Apparaatcontrolelogboeken

Het gedeelte Logboeken biedt een omvangrijk logbestand voor elke actie van het apparaatbeheer. Lees hierover ook het volgende hoofdstuk: **Instellingen: Apparaatcontrole**

FAQ: BootScan

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 is geïnfecteerd, raden wij u aan een BootScan uit te voeren voordat u de software installeert.

> **BootScan**: Als u uw computer aanzet, start uw Windows-besturingssysteem doorgaans automatisch. Dit proces wordt booten genoemd. U kunt echter ook andere besturingssystemen en programma's automatisch laten starten.
>
> Om uw computer al vóór het opstarten van Windows op virussen te controleren, heeft G DATA naast de Windows-versie nog een speciale opstartversie voor u beschikbaar.

Voorwaarden

Met de BootScan kunt u virussen bestrijden die zich al voor de installatie van uw antivirussoftware op uw computer hebben genesteld.

Hiervoor is een speciale programmaversie van de software beschikbaar die al vóór het opstarten van Windows kan worden uitgevoerd.

Opstarten vanaf cd/dvd-rom: Als uw computer niet vanaf de cd/dvd-rom opstart, voert u vooraf de volgende stappen uit:

1. Schakel uw computer uit.

2. Start uw computer opnieuw op. Normaal gesproken komt u in de BIOS-instelling als u bij het opstarten (booten) van de computer op de DEL-toets (of naargelang het systeem ook F2 of F10) drukt.

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**. Dti betekent dat het cd/dvd-rom-station het **1st Boot Device** wordt en de harde-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.

   Hoe breek ik een BootScan af? Als na het opnieuw opstarten van uw computer niet de gebruikelijke Windows-omgeving wordt weergegeven, maar de interface van de G DATA BootScan-software, hoeft u zich geen zorgen te maken.

   Als u geen BootScan hebt gepland, selecteert u de optie **Microsoft Windows** met de pijltoetsen en klikt u vervolgens op **Return**. Nu start Windows normaal op zonder voorafgaande BootScan.

   Opstarten vanaf USB-stick: Als u een USB-stick als opstartmedium wilt gebruiken, kunt u deze ook als 1ste opstartapparaat selecteren.

FAQ: Programmafuncties

Security-symbool

De G DATA software beveiligt uw computer permanent 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 de beveiliging op uw computer actief is.

Als de bewaker uitgeschakeld is of zich andere problemen voordoen, geeft het G DATA symbool een waarschuwing weer. U kunt dan best zo snel mogelijk de G DATA software starten en de instellingen controleren.

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 eventueel 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 u een versie van de G DATA software met geïntegreerde firewall gebruikt, kunt u de firewall desgewenst 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. Net zoals de firewall is de automatische piloot beschikbaar in bepaalde versies van de G DATA software.
- **Virushandtekeningen bijwerken**: 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 **Virushandtekeningen bijwerken** starten. De redenen voor een virusupdate leest u in het hoofdstuk: Viruscontrole
- **Statistieken**: Hier kunt u een statistisch overzicht van de controles van de virusbewaker weergeven en informatie over afwezigheidsscans, meldingen van de webfilter en andere parameters raadplegen.

Viruscontrole uitvoeren

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.

Als er tijdens een viruscontrole virussen of andere schadelijke software worden ontdekt, 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 in 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 systeemlast 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 (voor zover u in de instellingen onder **Instellingen: Handmatige viruscontrole** voor geïnfecteerde bestanden en archieven niets anders hebt geconfigureerd) en desinfecteert de aangetaste bestanden, d.w.z. dat de bestanden worden gerepareerd zodat deze weer zonder beperkingen kunnen worden gebruikt en geen gevaar meer vormen voor de computer.

Bestanden die niet kunnen worden gedesinfecteerd, worden in quarantaine geplaatst, d.w.z. ze worden gecodeerd in een extra beveiligde map 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 afzonderlijk 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. **Opgelet**: 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 logboekinvoer 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. Lees hierover ook het hoofdstuk: **Bestanden in 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: **Bestanden in 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.

Door op de knop **Acties uitvoeren** te klikken, reageert de G DATA software op elk gevonden virus zoals u dat hebt gedefinieerd.

Uw systeem werd op virussen gecontroleerd. Als u toch een instelling met de optie **Registratie in logboek** hebt gebruikt, is het mogelijk dat uw computer niet virusvrij is.

Virusalarm

Wanneer de G DATA software een virus of ander schadelijk programma op uw computer aantreft, verschijnt een opmerkingenvenster aan de zijkant van het scherm.

U kunt nu op de volgende manieren met het geïnfecteerde bestand omgaan.

- **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**: 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: Bestanden in quarantaine
- **Geïnfecteerd 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.

> **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 doorgaans gegevens van uw e-mailpostvak in Outlook.

Firewallalarm

Normaal gesproken vraagt de firewall in de modus Handmatige regelaanmaak of onbekende programma's en processen verbinding mogen maken met het netwerk. Daarvoor wordt een informatievenster geopend waarin details over de betreffende toepassing staan. U kunt hier een toepassing eenmalig of onbeperkt toegang tot het netwerk verlenen of weigeren. Zodra u een programma onbeperkt toegang geeft of weigert, wordt dit opgenomen als regel in de regelset voor het betreffende netwerk en wordt deze vraag niet opnieuw gesteld.

U beschikt hier over de volgende knoppen:

- **Altijd toestaan**: Via deze knop maakt u voor de bovengenoemde toepassing (bijvoorbeeld Opera.exe of Explorer.exe of iTunes.exe) een regel die deze toepassing binnen het genoemde netwerk altijd toegang tot het netwerk of internet geeft. Deze regel vindt u vervolgens ook als Op verzoek aangemaakte regel in het onderdeel Regelsets.
- **Tijdelijk toestaan**: Via deze knop geeft u de betreffende toepassing slechts eenmalig toegang tot het netwerk. Bij een volgende toegangspoging van dit programma, stelt de firewall u opnieuw de vraag of u toegang wilt verlenen of weigeren.
- **Altijd weigeren**: Via deze knop maakt u voor de bovengenoemde toepassing (bijvoorbeeld dialer.exe of spam.exe of trojan.exe) een regel die deze toepassing binnen het genoemde netwerk altijd toegang tot het netwerk of internet weigert. Deze regel vindt u vervolgens ook als Op verzoek aangemaakte regel in het onderdeel Regelsets.
- **Tijdelijk weigeren**: Met deze knop weigert u de betreffende toepassing slechts eenmalig toegang tot het netwerk. Bij een volgende toegangspoging van dit programma, stelt de firewall u opnieuw de vraag of u toegang wilt verlenen of weigeren.

Verder krijgt u informatie over het protocol, de poort en het IP-adres waarmee de betreffende toepassing verbinding wilt maken.

Melding not-a-virus

Bij bestanden die als not-a-virus zijn gemeld, 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.

Deïnstallatie

Als u de G DATA software van uw computer wilt verwijderen, doet u dat het best via het configuratiescherm van uw besturingssysteem. De deïnstallatie wordt dan volledig automatisch uitgevoerd.

Als u tijdens de deïnstallatie nog bestanden in quarantaine van de G DATA software hebt staan, krijgt u de vraag of u deze bestanden wilt verwijderen. Als u deze bestanden niet verwijdert, worden ze gecodeerd opgeslagen in een speciale G DATA map op uw computer zodat ze geen verdere schade kunnen aanrichten. U kunt pas opnieuw over deze bestanden beschikken 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.

FAQ: Licentievragen

Meervoudige licenties

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 registratie op de G DATA UpdateServer hebt gekregen. Herhaal deze procedure voor elke volgende computer.

Gebruik de toegangsgegevens (gebruikersnaam en wachtwoord) die u na de eerste registratie hebt ontvangen voor de internetupdate voor al uw computers. Ga hierbij als volgt te werk:

1. Start de G DATA software.
2. Klik in het **SecurityCenter** op **Virushandtekening 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. U ontvangt de factuur een van de daaropvolgende dagen via e-mail als PDF.

> **Opmerking**: dit dialoogvenster verschijnt alleen na afloop van het eerste jaar. Daarna wordt uw G DATA licentie elk jaar automatisch verlengd. U kunt deze verlengingsservice op elk moment zonder opgave 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.

> **Opmerking**: 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.

Copyright

Copyright © 2017 G DATA Software AG
Engine: De virusscan-engine en de spywarescan-engines zijn op BitDefender-technologieën gebaseerd © 1997-2017 BitDefender SRL.
OutbreakShield: © 2017 Commtouch Software Ltd.
[G DATA - 31/07/2017, 11:12]