

AVG 8.0 Anti-Virus Edition

User Manual

Document revision 80.3 (10.3.2008)

Copyright AVG Technologies CZ, s.r.o. All rights reserved. All other trademarks are the property of their respective owners.

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz).

This product uses compression library zlib, Copyright (c) 1995-2002 Jean-loup Gailly and Mark Adler.



Contents

1. Inleiding
2. AVG installatievereisten
2.1 Ondersteunde besturingssystemen ······7
2.2 Minimale hardware eisen ······7
3. AVG installatieopties
4. AVG installatieprocedure 9
4.1 Start van installatie ······9
4.2 Licentieovereenkomst
4.3 Systeemstatus controleren 10
4.4 Installatietype selecteren
4.5 AVG aanpassen ······11
4.6 Aangepaste installatie - Doelmap13
4.7 Aangepaste installatie - Onderdelen selecteren
4.8 Aangepaste installatie - E-mail scannen
4.9 AVG Werkbalk Beveiliging
4.10 Overzicht van installatie ······17
4.11 Installeren ······1/
4.12 Installatie voltooid ······1/
5. De AVG-wizard Basisconfiguratie 19
5.1 AVG Essentiële configuratie
5.2 AVG Taakplanning ······20
5.3 Rapportage van websites met exploits ······20
5.4 Yahoo! Zoekmachine
5.5 AVG bijwerken ······22
5.6 AVG-configuratie voltooid ······22
6. Na de installatie 24
6.1 Het product registreren ······24
6.2 Toegang tot gebruikersinterface ······24
6.3 Volledige computerscan
6.4 Eicar-test ······24
6.5 AVG standaardconfiguratie25



	🚽 A
	Tough on threats.
7. AVG gebruikersinterface ·····	26
7.1 Systeemmenu ······	27
7.1.1 Bestand ·····	
7.1.2 Onderdelen ·····	
7.1.3 Historie	
7.1.4 Hulpmiddelen ·····	
7.1.5 Help ·····	
7.2 Info Beveiligingsstatus ·····	
7.3 Snelkoppelingen ·····	
7.4 Overzicht van onderdelen ·····	
7.5 Statistieken ·····	
7.6 Systeemvakpictogram ·····	
8. AVG onderdelen	35
8.1 Anti-Virus ·····	
8.1.1 Anti-Virus Principes ·····	35
8.1.2 Anti-virus interface ·····	
8.2 Anti-Spyware ·····	
8.2.1 Anti-Spyware Principes ·····	
8.2.2 Anti-Spyware interface ·····	
8.3 Anti-Rootkit ·····	
8.3.1 Anti-Rootkit principes ·····	
8.3.2 Anti-Rootkit interface ·····	
8.4 Firewall	
8.4.1 Firewallprofielen ·····	
8.5 Licentie ·····	43
8.6 LinkScanner ·····	45
8.6.1 AVG Search Shield	
8.6.2 AVG Active Surf-Shield ·····	
8.7 Web Shield ·····	
8.7.1 Web Shield principes ·····	
8.7.2 Web Shield interface ·····	
8.8 Resident Shield ·····	50
8.8.1 Resident Shield Principes ·····	
8.8.2 Resident Shield interface ·····	
8.8.3 Resident Shield detectie	
8.9 Updatebeheer ······	53



	Т	fough on three
	8 9 1 Undatebabeer principes	53
	8 9 2 Undatebeneer interface	53
8	3 10 AVG Werkhalk Beveiliging	56
•		EO
9.7	AVG Geavanceerde instellingen	59
9).1 Weergave ·····	59
9	9.2 Onderhoud ·····	61
	9.2.1 Quarantaine ·····	61
9	9.3 PUP-uitzonderingen ·····	63
9	9.4 Web Shield ·····	65
	9.4.1 Webbescherming	65
	9.4.2 Instant Messaging	65
9).5 LinkScanner ·····	69
9).6 Scans	70
	9.6.1 De hele computer scannen ·····	70
	9.6.2 Shell-extensie scannen	70 70
~	9.6.3 Bepaalde mappen of bestanden scannen ·····	75
9	9.7 Schema's	75
	9.7.1 Geplande scan	75
	9.7.2 Updateschema virusdatabase	75
	9.7.3 Opualeschema programma	75
c	9.7.4 Anti-Spani updateschema	
2		87
	9.8.2 Mailfiltering	87
	9.8.3 Logboeken en resultaten	87
	9.8.4 Servers	87
ç).9 Resident Shield	95
-	9.9.1 Geavanceerde instellingen	95
	9.9.2 Uitzonderingen	95
9).10 Update	99
	9.10.1 Proxy	99
	9.10.2 Inbellen ·····	99
	9.10.3 URL	99
9	9.11 Extern beheer	105
10	. AVG scannen ·····	107
		107
1	U.1 Scaninterface ·····	10/



	A
	Tough on threats.
10.2 Vooraf ingestelde scans ·····	
10.2.1 De hele computer scannen ·····	
10.2.2 Bepaalde mappen of bestanden scannen	
10.3 Scannen in Windows Verkenner ·····	
10.4 Scannen vanaf opdrachtregel	
10.5 Scans plannen ·····	
10.5.1 Schema-instellingen ·····	
10.5.2 Hoe er gescand moet worden ·····	
10.5.3 Wat er gescand moet worden	
10.6 Overzicht scanresultaten ·····	
10.7 Details scanresultaten ·····	
10.7.1 Tabblad Overzicht resultaten	
10.7.2 Tabblad Infecties	
10.7.3 Tabblad Spyware	
10.7.4 Tabblad Waarschuwingen ·····	
10.7.5 Tabblad Informatie ·····	
10.8 Quarantaine ·····	
11. AVG Updates	136
11.1 Updateniveaus	
11.2 Soorten updates ······	
11.3 Updateprocedure ·····	
12. Gebeurtenishistorie	138
13. Veelgestelde vragen en technische ondersteuning	140



1. Inleiding

In deze gebruikershandleiding staat uitgebreide informatie voor AVG 8.0 Anti-Virus

Gefeliciteerd met uw aankoop van AVG 8.0 Anti-Virus !

AVG 8.0 Anti-Virus is één van een hele reeks onderscheiden AVG producten die zijn ontwikkeld om uw gemoedsrust te bevorderen en uw pc volledig te beschermen. Net als alle AVG producten is **AVG 8.0 Anti-Virus** volledig opnieuw ontwikkeld, vanaf de basis, om u de geroemde en veelgeprezen beveiliging van te kunnen bieden, op een nieuwe, efficiëntere en meer gebruikersvriendelijke manier.

Uw nieuwe **AVG 8.0 Anti-Virus** product heeft een gestrooomlijnde interface in combinatie met scanfuncties die agressiever en sneller zjin. Om het u gemakkelijk te maken zijn meer beveiligingsfuncties geautomatiseerd, en zijn nieuwe, 'intelligente' gebruikersopties toegevoegd, zodat u onze beveiligingsfuncties aan uw wensen kunt aanpassen. Geen compromissen meer tussen veiligheid en gemak!

AVG is ontwikkeld om de omgeving waarin uw computer en netwerk moeten functioneren, te beschermen. Geniet van de volledige bescherming van AVG.



2. AVG installatievereisten

2.1. Ondersteunde besturingssystemen

AVG 8.0 Anti-Virus is ontworpen om werkstations met de volgende besturingssystemen te beschermen:

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows 2000 Server SP4 + Update Rollup 1
- Windows XP Home SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Server 2003 (x86, x64 en Itanium) SP1
- Windows Vista (x86 en x64, alle edities)

(en mogelijk hogere servicepacks voor bepaalde besturingssystemen)

2.2. Minimale hardware eisen

Voor **AVG 8.0 Anti-Virus** zijn de volgende minimale hardware eisen van toepassing:

- Intel Pentium CPU 300 MHz
- 70 MB vrije schijfruimte (voor de installatie)
- 64 MB RAM-geheugen



3. AVG installatieopties

AVG kan geïnstalleerd worden met het installatiebestand op uw installatie-cd. U kunt het nieuwste installatiebestand echter ook downloaden vanaf de <u>AVG website www.</u> <u>avg.com</u>.

Voordat u AVG installeert, raden wij u sterk aan de website van AVG te bezoeken om na te gaan of er een nieuw installatiebestand is. Zo weet u zeker dat u de nieuwste versie installeert van AVG 8.0 Anti-Virus .

Tijdens het installatieproces wordt u om uw licentie/verkoop-nummer gevraagd. Zorg ervoor dat u het bij de hand hebt voordat u met de installatie begint. Het verkoopnummer staat op de cd-hoes. Als u uw exemplaar van AVG online hebt aangeschaft, hebt u het licentienummer per e-mail ontvangen.



4. AVG installatieprocedure

Voor installatie van AVG op uw computer dient u te beschikken over het nieuwste installatiebestand. U kunt het installatiebestand gebruiken dat op de cd staat die onderdeel uitmaakt van de editie in de doos, maar dat bestand kan verouderd zijn. We raden u daarom aan het nieuwste installatiebestand online op te vragen. U kunt het bestand downloaden van de <u>website van AVG</u> (<u>www.avg.com</u>) / sectie **Downloads**.

Als u het installatiebestand hebt gedownload en opgeslagen op uw vaste schijf, kunt u de installatieprocedure starten. De installatieprocedure bestaat uit een reeks dialoogvensters met steeds een korte beschrijving bij elke stap. Hieronder volgt een toelichting op de dialoogvensters:

🞽 AVG 8.0 build 81 (27/2/2008) 🛛 🔀		
	Welkom	
🕌 AVG	Welkom bij het installatieprogramma AVG. Met dit programma installeert u AVG op de computer. Klik op Volgende om verder te gaan met de installatie of op Afsluiten om nu te stoppen.	
	WAARSCHUWING: dit programma is auteursrechtelijk beschermd en valt onder internationale verdragen. Het zonder toestemming reproduceren of distribueren van dit programma, of een gedeelte daarvan, kan leiden tot strenge civiel- en strafrechtelijke boetes. Overtredingen zullen met alle beschikbare juridische middelen worden bestreden.	
	Baadpleeg voordat u begint met het installatieproces, de sectie <u>FAQ [Veelgestelde vragen]</u> , waar u adviezen en aanbevelingen vindt zodat u het programma kunt installeren in overeenstemming met uw behoeften en vereisten.	
	Kies de taal voor de installatie	
	V <u>o</u> lgende >	

4.1. Start van installatie

Bij de start van de installatieprocedure wordt het venster **Welkom** weergegeven. In dat venster kiest u de taal die u wilt gebruiken voor de installatieprocedure. In het onderste deel van het venster staat de optie **Kies taal voor de installatie**; daar selecteert u de gewenste taal in het vervolgkeuzemenu. Klik daarna op de knop **Volgende** om de keuze te bevestigen en verder te gaan naar het volgende dialoogvenster.

Let op: u selecteert hier alleen een taal voor de installatieprocedure. U kiest nog geen taal voor de AVG toepassing zelf - dat gebeurt in een later stadium van de installatieprocedure!



4.2. Licentieovereenkomst

In het dialoogvenster *Licentieovereenkomst* staat de volledige tekst van de AVG Licentieovereenkomst. Lees de verklaring zorgvuldig door en bevestig dat u die heeft gelezen en begrepen en dat u de voorwaarden accepteert door te klikken op de knop *Accepteren*. Als u niet instemt met de licentieverklaring, klikt u op de knop *Afwijzen*, dan wordt de installatieprocedure meteen afgebroken.

4.3. Systeemstatus controleren



Nadat u zich akkoord hebt verklaard met de licentieverklaring, wordt u omgeleid naar het dialoogvenster **Systeemstatus controleren**. U hoeft in dit dialoogvenster niets te doen; uw systeem wordt gecontroleerd voordat u kunt beginnen met de installatie van AVG. Wacht tot het proces is voltooid, daarna wordt automatisch het volgende dialoogvenster geopend.



4.4. Installatietype selecteren



In het dialoogvenster **Installatietype selecteren** kunt u kiezen uit twee typen installatie: **standaard** en **aangepaste** installatie.

We raden de meeste gebruikers aan de **standaardinstallatie** te gebruiken, waarbij AVG in een automatische modus wordt geïnstalleerd met vooraf door de leverancier ingestelde instellingen. Die configuratie combineert maximale bescherming met een efficiënt gebruik van o.a. werkgeheugen. Als het in de toekomst nodig mocht blijken om de configuratie aan te passen, kunt u dat altijd vanuit de AVG toepassing doen.

Een aangepaste installatie is alleen aanbevolen voor ervaren gebruikers die een goede reden hebben om AVG te installeren met afwijkende instellingen, bijvoorbeeld om aan specifieke systeemeisen te voldoen.

4.5. AVG aanpassen

In het dialoogvenster **AVG aanpassen** vult u uw registratiegegevens in. Geef uw naam (in het veld **gebruikersnaam**) en de naam van uw organisatie (in het veld **Bedrijfsnaam**) op.

Voer vervolgens uw licentienummer/verkoopnummer in in het veld *Licentie-/ verkoopnummer*. Het verkoopnummer staat op de cd-hoes in de AVG-doos. Het licentienummer staat in de bevestiging die u via e-mail hebt ontvangen na aankoop van AVG online. U moet dat nummer precies zo typen als het wordt weergegeven. Als



u beschikt over de digitale versie van het licentienummer (in de e-mail), is het raadzaam het nummer over te nemen met kopiëren-en-plakken.

🛃 AVG 8.0 build 81 (27/2/2008)		
	AVG aanpassen	
📕 AVG	Gebr <u>u</u> ikersnaam:	
	Bedrijfsnaam:	
	Licentie-/ verkoopnummer:	
	U vindt uw licentie-/verkoopnummer:	
	 in het e-mailbericht dat naar uw e-mailadres is verzonden op de productregistratiekaart, of op het label op de verpakking 	
	[Volgende >	

Klik op de knop **Volgende** om verder te gaan met de installatieprocedure.

Als u bij de vorige stap hebt gekozen voor een standaardinstallatie, wordt het dialoogvenster **Overzicht van installatie** geopend. Als u hebt gekozen voor een aangepaste installatie, wordt het dialoogvenster **Doelmap** geopend.



4.6. Aangepaste installatie - Doelmap

🛃 AVG 8.0 build 81 (27/2/2008) 🛛 🛛 🔀	
	Doelmap
📕 🕌 AVG	Selecteer de map waarin u AVG wilt installeren. Klik op Bladeren om een andere map te selecteren.
	U kunt het beste de standaardmap gebruiken.

In het dialoogvenster **Doelmap** kunt u opgeven in welke map AVG moet worden geïnstalleerd. Standaard wordt AVG geïnstalleerd in de map Program Files op station C:. Als u de voorkeur geeft aan een andere locatie, klikt u op de knop **Bladeren** om de mapstructuur weer te geven, en selecteert u de map van uw keuze. Klik op de knop **Volgende** om uw keuze te bevestigen.



4.7. Aangepaste installatie - Onderdelen selecteren

🛃 AVG 8.0 build 81 (27/2/2008) 🛛 🔀		
	Onderdelen selecteren	
🚔 AVG	Selecteer de onderdelen die u wilt installeren. Alleen de geselecteerde onderdelen worden geïnstalleerd. Onderdelen die niet zijn geselecteerd, worden niet geïnstalleerd of verwijderd.	
	AVG voor Windows AVG Firewall Web Shield Beheer op afstand (AVG-Admin) Extra geinstalleerde talen E-mailscanner E-mailscanner	
	< Ierug Volgende > Afsluiten	

In het dialoogvenster**Onderdelen selecteren** staat een overzicht van alle AVG onderdelen die kunnen worden geïnstalleerd. Als de standaardinstellingen niet voldoen, kunt u onderdelen toevoegen of verwijderen.

U kunt echter alleen kiezen uit onderdelen die deel uitmaken van de door u gekochte AVG Edition. Alleen die onderdelen worden voor installatie weergegeven in het dialoogvenster Onderdelen selecteren!

U kunt ook opgeven in welke taal (talen) AVG moet worden geïnstalleerd. Schakel het selectievakje **Extra geïnstalleerde talen** in en selecteer daarna de gewenste talen in het menu.

Klik op de knop **Volgende** om verder te gaan.

4.8. Aangepaste installatie - E-mail scannen

Bij een **standaardinstallatie** van AVG zal het installatieprogramma vaststellen wat uw standaard e-mailclient is en automatisch de bijbehorende invoegtoepassing voor het scannen van e-mail installeren. Er zijn invoegtoepassingen voor de ondersteuning van de meest gebruikte e-mailclients: MS Outlook, MS Exchange, The BAT!, Qualcomm Eudora, enz.

Bij een Aangepaste installatie kunt u de Persoonlijke E-mailscanner installeren,



een uitgebreid hulpprogramma voor het scannen van e-mail dat garant staat voor virusvrije e-mail, welke e-mailclient u ook gebruikt.

🛃 AVG 8.0 build 81 (27/2/2008) 🛛 🛛 🔀		
	E-mail scannen	
AVG	Het installatieprogramma heeft gedetecteerd dat het standaard e- -mailprogramma niet is ingesteld of niet wordt ondersteund door AVG. Selecteer Persoonlijke e-mailscanner als u Persoonlijke e- -mailscanner wilt installeren of Geavanceerde configuratie als u de e-mailscanfunctie handmatig wilt instellen.	
	C Persoonlijke e-mailscanner (aanbevolen) Installeett Persoonlijke e-mailscanner voor het controleren van e-mailberichten.	
	 Geavanceerde configuratie De e-mailscanfunctie kan handmatig worden geconfigureerd in het volgende dialoogvenster. 	
	< Ierug Volgende > Afsluiten	

In het dialoogvenster **E-mail scannen** kunt u ervoor kiezen om **Persoonlijke emailscanner** zo te installeren dat uw e-mail automatisch wordt beveiligd, maar u kunt ook een geavanceerde configuratie opgeven voor het scannen van e-mail. Het is raadzaam om **Persoonlijke E-mailscanner** in de automatische modus te installeren.

Maar als u een goede reden hebt om E-mailscanner handmatig in te stellen, kan dat ook. Selecteer in het dialoogvenster *E-mail scannen* de optie *Geavanceerde configuratie* en ga verder naar het dialoogvenster *E-mail scannen - Invoegtoepassing selecteren*. In dat dialoogvenster kunt u de specifieke invoegtoepassingen selecteren die moeten worden geïnstalleerd:



🛃 AVG 8.0 build 81 (27/2/2	2008)
	E-mailscanner
📕 AVG	Selecteer de e-mailinvoegtoepassingen die u wilt installeren.
	 Invoegtoepassing voor The Bat! Invoegtoepassing voor Microsoft Outlook Persoonlijke e-mailscanner (voor alle andere e-mail program)
	< Ierug (Volgende >) Afsluiten

Klik op de knop **Volgende** om uw keuze te bevestigen.

4.9. AVG Werkbalk Beveiliging

🕌 AVG 8.0 build 81 (27/2/2008) 🛛 🔀		
	AVG Werkbalk Beveiliging	
AVG	De nieuwe AVG Werkbalk Beveiliging is een fantastisch hulpmiddel voor bescherming tegen de nieuwste bedreigingen van internet wanneer u online bent. Als u de werkbalk installeert, wordt u beschermd tegen nevendownloads, vergiftigde websites en zwendel met phishing en andere fraude. U kunt nu vertrouwd zoeken en surfen, in de wetenschap dat de LinkScanner®- technologie van AVG paraat is steeds als u op een koppeling klikt.	
	✓ Ja, ik wil de AVG Werkbalk Beveiliging installeren Meer informatie	
	< <u>I</u> erug <u>Volgende</u> > <u>A</u> fsluiten	

In het dialoogvenster **AVG Werkbalk Beveiliging** bepaalt u of u de <u>AVG Werkbalk</u> <u>Beveiliging</u> van **AVG 8.0 Anti-Virus** wilt installeren. De <u>AVG Werkbalk</u> <u>Beveiliging</u> werkt in uw browser samen met de technologie van AVG 8.0 en AVG XPL



om u een uitgebreide bescherming te bieden tegen online bedreigingen als u surft op internet.

4.10.Overzicht van installatie

🛃 AVG 8.0 build 81 (27/2/2008) 🛛 🛛 🔀		
	Overzicht van installatie	
AVG 📲	Controleer de onderstaande informatie en bevestig de juistheid daarvan. Klik op Voltooien om de installatie af te ronden of klik op Terug om instellingen te wijzigen.	
	Doelmap voor bestanden van AVG: C:\Program Files\AVG\AVG8 Licentie: Licentie voor gebruiker: AVG Bedrijfsnaam: AVG Licentietype: volledig	
	< Ierug Voltooien Afsluiten	

In het dialoogvenster **Overzicht van installatie** staat een overzicht van alle parameters van de installatieprocedure. Controleer of de gegevens juist zijn. Als dat het geval is, klikt u op de knop **Voltooien** om verder te gaan. In het andere geval klikt u op de knop **Terug** om naar het vorige dialoogvenster te gaan en de gegevens aan te passen.

4.11.Installeren

In het dialoogvenster **Installeren** wordt de voortgang van de installatieprocedure weergegeven, u hoeft zelf niets te doen. Wacht tot de installatie is voltooid, op dat moment wordt het dialoogvenster**Installatie voltooid** geopend.

4.12.Installatie voltooid

Het dialoogvenster **Installatie voltooid** is de laatste stap van de installatieprocedure van AVG. AVG is nu op uw computer geïnstalleerd en volledig functioneel. Het programma wordt volledig automatisch op de achtergrond uitgevoerd.

Meteen na de installatie wordt automatisch de <u>AVG-wizard Basisconfiguratie</u> gestart, die u in een paar stappen zal leiden door de **AVG 8.0 Anti-Virus** elementaire



configuratie. Hoewel u de configuratie van AVG op elk gewenst moment kunt oproepen als AVG wordt uitgevoerd, raden we met klem aan van de wizard gebruik te maken en met hulp van de wizard een basisconfiguratie in te stellen.



5. De AVG-wizard Basisconfiguratie

Wanneer u AVG voor de eerste keer op uw computer installeert, wordt de **wizard AVG Basisconfiguratie** gestart om u te helpen met de begininstellingen van **AVG 8.0 Anti-Virus**. Hoewel u alle voorgestelde parameters ook op een later tijdstip kunt instellen, is het toch raadzaam om de rondleiding van de wizard te volgen, zodat u de beveiliging van uw computer op eenvoudige wijze onmiddellijk kunt instellen. Voer de stappen uit die in de vensters van de wizard worden beschreven:

5.1. AVG Essentiële configuratie



In het welkomstvenster van de **wizard AVG Basisconfiguratie** wordt een kort overzicht weergegeven van de status van AVG op uw computer. Daarnaast wordt er een aantal stappen weergegeven, die moeten worden gevolgd om de beveiliging van uw computer te voltooien. Klik op de knop **Volgende**om door te gaan.



5.2. AVG Taakplanning

🛃 AVG Wizard Eerste uitvoering	$\overline{\mathbf{X}}$
Stap 2 van 7: AVG takenplanning De regelmatige updates en dagelijkse scans plannen	
Update Hoe vaak wilt u updates uitvoeren voor AVG? ⊙ om de 4 uur ⊙ Dagelijks	
Scannen Stel uw voorkeurtijd in voor het scannen: 12:00 😨 V Dagelijks scannen inschakelen (aanbevolen)	
Help	< Terug Volgende >

Geef in het dialoogvenster**AVG Taakplanning** een interval op, waarmee moet worden gecontroleerd op de beschikbaarheid van updatebestanden, en leg vast op welk moment de <u>geplande scan</u> moet worden gestart. Het is raadzaam de standaardinstellingen aan te houden. Klik op de knop **Volgende** om door te gaan.

5.3. Rapportage van websites met exploits

😹 AVG Wizard Eerste uitvoering	×
Stap 3 van 7: rapportage van websites met exploits aan AVG Rapportage van websites met exploits aan AVG toestaan	Č.
Help ons nieuwe bedreigingen te herkennen:	
Als u ons toestaat om automatisch een geringe hoeveelheid informatie in te z kwaadaardige websites die u online tegenkomt, kunnen wij alle gebruikers ee bieden.	zamelen over en betere bescherming
We respecteren uw privacy	
Ja, Ik wil rapportage van websites met exploits naar AVG in	schakelen.
Verklaring van privacybeleid	
Help	< Terug



In het dialoogvenster **Rapportage van websites met exploits naar AVG** geeft u op of u de optie rapportage van exploits en kwaadaardige sites die door gebruikers zijn gevonden met behulp van de functies **AVG Active Surf-Shield / AVG Search Shield** van het onderdeel <u>LinkScanner</u> wilt inschakelen om gegevens te verzenden naar de database waarin gegevens worden verzameld over kwaadaardige praktijken op internet. Het is raadzaam de standaardinstelling aan te houden zodat rapportage is ingeschakeld. Klik op de knop **Volgende** om door te gaan.

5.4. Yahoo! Zoekmachine

🕌 AVG Wizard Eerste uitvoering	
Stap 4 van 7: Yahoo! Zoekmachine De standaard zoekprovider instellen	
Yahoo! Search	
Uw standaard zoekprovider is de zoekmachine die u gewoonlijk gebruik	t om te zoeken op internet.
🔲 Ja, ik wil Yahoo! instellen als mijn standaard zoekprovi	der.
Help	< Terug Volgende >

In het dialoogvenster **Yahoo! Zoekmachine** kunt u het selectievakje inschakelen om aan te geven dat u Yahoo! wilt gebruiken als standaardzoekmachine.



5.5. AVG bijwerken

😹 AVG Wizard Eerste uitvoering	$\overline{\mathbf{X}}$
Stap 5 van 7: AVG Update Wilt u nu updates bijwerken?	
Er verschijnen iedere dag nieuwe virusdreigingen. Het onderzoeksteam va dag om u te beschermen tegen de nieuwste dreigingen. Voer de update regelmatig uit voor: • up-to-date bescherming • de nieuwste programmafuncties Klik op Volgende om te kijken of er nieuwe updates zijn, klik op Oversla naar de volgende pagina te gaan.	an AVG werkt 24 uur per H an om zonder bij te werken
Help	< Terug Volgende >

In het venster **AVG Update** wordt er automatisch gecontroleerd of er nieuwe <u>AVG</u> <u>updates</u> beschikbaar zijn, zodat deze kunnen worden gedownload. Klik op de knop **Volgende** als u de recentste updatebestanden wilt downloaden en de update wilt uitvoeren.

5.6. AVG-configuratie voltooid

<table-of-contents> AVG Wizard Eerst</table-of-contents>	🛃 AVG Wizard Eerste uitvoering 🛛 🛛 🔀		
De configuratie van Alle stappen van de	AVG is voltooid configuratie van AVG zijn uitgevoerd.	Ó.	
SÖ	AVG Wizard Eerste uitvoering is voltooid! AVG is geconfigureerd en uw computer wordt nu beschermd. Klik op Voltooien om de AVG Wizard Eerste uitvoering af te slu	iten.	
Help		Voltooien	



AVG 8.0 Anti-Virus is nu geconfigureerd; klik op de knop **Voltooien** om met AVG aan de slag te gaan.



6. Na de installatie

6.1. Het product registreren

Registreer na het voltooien van de installatie van **AVG 8.0 Anti-Virus** uw product online op de <u>website van AVG</u>, pagina**Registratie** (*Volg de instructies op de pagina*). Na de registratie krijgt u volledige toegang tot uw gebruikersaccount bij AVG, de AVG Update nieuwsbrief en andere services die alleen beschibaar zijn voor geregistreerde gebruikers.

6.2. Toegang tot gebruikersinterface

U kunt de **AVG gebruikersinterface** op meerdere manieren openen:

- Dubbelklik op het pictogram van AVG in het systeemvak
- Dubbelklik op het pictogram van AVG op het bureaublad
- Kies Start/Alle Programma's/AVG 8.0/AVG Gebruikersinterface

6.3. Volledige computerscan

Het risico bestaat dat er een computervirus naar uw computer is overgebracht voordat u **AVG 8.0 Anti-Virus** hebt geïnstalleerd. Voer daarom een volledige <u>scan</u> <u>van de computer</u> uit om zeker te weten dat uw pc niet geïnfecteerd is.

Zie voor instructies voor het uitvoeren van een <u>scan van uw computer</u> het hoofdstuk <u>AVG scannen</u>.

6.4. Eicar-test

Om te controleren of **AVG 8.0 Anti-Virus** juist is geïnstalleerd, kunt u de Eicar-test uitvoeren.

De Eicar-test is een standaardmethode die absoluut veilig is, waarmee u kunt testen of uw antivirussysteem goed functioneert. U kunt het Eicar-virus doorgeven omdat het geen echt virus betreft en omdat het geen viruscodefragmenten bevat. De meeste producten reageren op deze test alsof het een echt virus betreft (*het bestand heeft meestal een duidelijke naam, zoals "EICAR-AV-Test"*). U kunt het Eicar-virus downloaden vanaf de Eicar-website op <u>www.eicar.com</u>}. U vindt hier ook de benodigde informatie voor het uitvoeren van de Eicar-test.



Download het bestand *eicar.com* en sla het op naar uw lokale vaste schijf. Het onderdeel <u>Resident shield</u> geeft onmiddellijk een waarschuwing weer nadat u de download van het testbestand hebt bevestigd. Deze waarschuwing van <u>Resident</u> <u>shield</u> toont aan dat AVG goed op uw computer is geïnstalleerd.

😹 Web Shield waarschuwing 🛛 🛛 🔯			
Opgeroepen bestand is geïnfecteerd			<u>75</u>
	Bedreiging	gedetecteerd!	
	Bestandsnaam:	www.eicar.org/download/eicar.com	
	Bedreiging naam:	Virus herkend EICAR_Test Meer informatie over deze Bedreiging .	
Dit dialoogvenster niet meer weergeven.			
Ok Ielp			
Details weergeven			

Als het Eicar-testbestand niet als virus door AVG wordt gedetecteerd, moet u uw programmaconfiguratie opnieuw controleren.

6.5. AVG standaardconfiguratie

De standaardconfiguratie (*dat wil zeggen de manier waarop de toepassing functioneert meteen na installatie*) van **AVG 8.0 Anti-Virus** is het werk van de leverancier van de software: alle onderdelen en functies zijn zo ingesteld dat de toepassing optimaal presteert.

Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen! Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers.

U kunt een paar minder belangrijke instellingen van <u>AVG onderdelen</u> meteen in de gebruikersinterface van de onderdelen wijzigen. Als u de AVG configuratie beter op uw wensen wilt laten aansluiten, gaat u naar <u>Geavanceerde instellingen AVG</u>: selecteer in het systeemmenu de optie **Extra/Geavanceerde instellingen** en bewerk de configuratie van AVG in het dialoogvenster <u>Geavanceerde instellingen</u> AVG dat dan wordt geopend.



7. AVG gebruikersinterface

AVG 8.0 Anti-Virus open met het hoofdvenster:



Het hoofdvenster is onderverdeeld in een aantal secties:

- Systeemmenu (de menubalk boven in het venster), het standaardmenu voor het navigeren naar alle onderdelen, services en functies van AVG - <u>details >></u>
- Info Beveiligingsstatus (bovenste deel van het venster), informatie over de huidige status van AVG - <u>details >></u>
- Snelkoppelingen (linker deelvenster), koppelingen naar de belangrijkste en meest gebruikte AVG-functies - <u>details >></u>
- Onderdelenoverzicht (centrale deel van het venster), overzicht van alle geïnstalleerde onderdelen van AVG - <u>details >></u>



- Statistieken (links onder in het venster), alle statistische gegevens over de uitvoering van de programma's <u>details >></u>
 - **Pictogram systeemvak** (rechts onder in het bureaublad van Windows, in het systeemvak), indicatie van de huidige status van AVG <u>details >></u>

7.1. Systeemmenu

Het **Systeemmenu** is de standaard navigatiestructuur die in alle Windowstoepassingen wordt gebruikt. Hij is horizontaal langs de bovenrand van het **AVG 8.0 Anti-Virus** hoofdvenster geplaatst. Met behulp van het systeemmenu heeft u toegang tot de AVG onderdelen, functies en services.

Het systeemmenu is onderverdeeld in vijf secties:

7.1.1. Bestand

 Afsluiten - afsluiten van de gebruikersinterface van AVG 8.0 Anti-Virus . De AVG toepassing zal echter op de achtergrond actief blijven en uw computer is nog steeds beschermd!

7.1.2. Onderdelen

Het systeemmenu-item <u>Onderdelen</u> heeft koppelingen naar alle geïnstalleerde AVGonderdelen:

- **Systeemoverzicht** Weergeven van het standaard dialoogvenster met het overzicht van alle geïnstalleerde onderdelen en hun status
- Anti-Virus openen van de standaardpagina van het onderdeel Anti-Virus
- Anti-Rootkit openen van de standaardpagina van het onderdeel <u>Anti-</u> <u>Rootkit</u>
- Anti-Spyware openen van de standaardpagina van het onderdeel <u>Anti-</u> <u>Spyware</u>
- •
- •
- •
- E-mailscanner openen van de standaardpagina van het onderdeel E-



mailscanner

- Licentie openen van de standaardpagina van het onderdeel Licentie
- *LinkScanner* openen van de standaardpagina van het onderdeel *LinkScanner*
- Web Shield openen van de standaardpagina van het onderdeel Web Shield
- **Resident Shield** openen van de standaardpagina van het onderdeel <u>Resident Shield</u>
- **Updatebeheer** openen van de standaardpagina van het onderdeel <u>Updatebeheer</u>

7.1.3. Historie

- <u>Scanresultaten</u> de AVG scaninterface wordt geopend, in het bijzonder het <u>Overzicht scanresultaten</u>
- <u>Resident Shielddetectie</u> er wordt een overzicht geopend met bedreigingen die zijn gedetetceerd door <u>Resident Shield</u>
- *E-mailscannerdetectie* er wordt een overzicht geopend met bijlagen bij emailberichten die als gevaarlijk zijn gedetecteerd door het onderdeel *Emailscanner*
- <u>Quarantaine</u> de interface van de<u>Quarantaine</u> wordt geopend, waar AVG alle gedetecteerde infecties opslaat die om de een of andere reden niet automatisch kunnen worden hersteld. In de quarantaine worden de geïnfecteerde bestanden geïsoleerd, zodat uw computer veilig blijft, terwijl het opslaan van de bestanden eventueel herstel van de bestanden in de toekomst mogelijk maakt.
- <u>Gebeurtenishistorie Logboek</u> het dialoogvenster wordt geopend met de geschiedenis van alle vastgelegde acties van AVG 8.0 Anti-Virus .

7.1.4. Hulpmiddelen

- <u>Computer scannen</u> de <u>AVG Scaninterface</u> wordt geopend en een scan van de volledige computer wordt gestart
- <u>Scan geselecteerde map</u> de <u>AVG Scaninterface</u> wordt geopend, zodat u in de bestandsstructuur van uw computer mappen en bestanden kunt selecteren



die moeten worden gescand

- <u>Update</u> automatisch de updateprocedure starten van AVG 8.0 Anti-Virus
- **Bijwerken vanuit directory** de updateprocedure wordt gestart aan de hand van updatebestanden in een bepaalde map op de lokale vaste schijf . Deze optie wordt echter alleen aanbevolen als noodprocedure, bijvoorbeeld onder omstandigheden waarbij er geen verbinding is met internet (*uw computer is bijvoorbeeld geïnfecteerd en afgesloten van internet; uw computer is aangesloten op een netwerk zonder verbinding met internet, enz.*). Selecteer in het venster dat wordt geopend, de map waarin u eerder het updatebestand hebt opgeslagen, en start de updateprocedure.
- **<u>Bestand scannen</u>** u kunt in de bestandsstructuur van de computer een enkel bestand selecteren dat u wilt scannen
- <u>Geavanceerde instellingen</u> het dialoogvenster <u>AVG Geavanceerde</u> <u>instellingen</u> wordt geopend voor het wijzigen van de**AVG 8.0 Anti-Virus** configuratie. Over het algemeen is het raadzaam de standaardinstellingen aan te houden, zoals die zijn ingesteld door de leverancier van de software.

•

7.1.5. Help

- Inhoud de Help-bestanden van AVG worden geopend
- **Online Help** de website van <u>AVG</u> wordt geopend op de pagina voor klantenservice
- Uw AVG-web de introductiepagina van AVG (bij www.avg.com) wordt geopend
- Info virussen & bedreigingen de online <u>Virusencyclopedie</u> wordt geopend, waarin u gedetaileerde informatie kunt zoeken over bekende virussen
- <u>Activeren</u> het dialoogvenster **AVG activeren** wordt geopend met de gegevens die u heeft opgegeven in het dialoogvenster <u>AVG aanpassen</u> van de <u>installatieprocedure</u>. In dit dialoogvenster kunt u uw licentienummer invoeren ter vervanging van ofwel het verkoopnummer (*het nummer waarmee u AVG heeft geïnstalleerd*), ofwel het oude licentienummer (*bijvoorbeeld bij het upgraden naar een nieuw product van AVG*).
- *Nu registreren* er wordt een verbinding tot stand gebracht met de



registratiewebsite <u>www.avg.com</u>. Voer uw registratiegegevens in; alleen klanten die hun AVG product registreren komen in aanmerking voor gratis technische ondersteuning

• **Info over AVG** - het dialoogvenster **Info** wordt geopend met vijf tabbladen met gegevens over de programmanaam, versie van programma en virusdatabase, systeeminformatie, licentieverklaring en contactgegevens van **AVG Technologies CZ**.

7.2. Info Beveiligingsstatus

De sectie **Info Beveiligingsstatus** bevindt zich in het bovenste deel van het hoofdvenster van AVG. In deze sectie staat altijd informatie over de huidige beveiligingsstatus van **AVG 8.0 Anti-Virus**. Hieronder volgt een overzicht van de pictogrammen die in deze sectie kunnen worden weergegeven, en hun betekenis:

Het groene pictogram duidt erop dat AVG volledig functioneert. Uw computer is volledig beveiligd, de bestanden zijn bijgewerkt en alle geïnstalleerde onderdelen werken correct.

Het oranje pictogram is een waarschuwing dat een of meer onderdelen onjuist zijn geconfigureerd en dat u de desbetreffende eigenschappen/ instellingen moet controleren. Er is geen wezenlijk probleem opgetreden in AVG; waarschijnlijk hebt u gewoon om de een of andere reden een onderdeel uitgeschakeld. U wordt nog steeds beschermd door AVG. Neem echter wel even de tijd om de instellingen van het problematische onderdeel te controleren! De naam van het onderdeel wordt gemeld in de sectie **Info Beveiligingsstatus**.

Een rood pictogram geeft aan dat er een kritieke situatie is! Een of meer onderdelen functioneren niet correct en AVG kan uw computer niet beschermen. Besteed onmiddellijk aandacht aan het probleem en probeer het te verhelpen Als het u niet lukt de fout zelf te herstellen, neem dan contact op met het team van de <u>Technische ondersteuning van AVG</u>.

We raden u nadrukkelijk aan de sectie **Info Beveiligingsstatus** goed in de gaten te houden en in het geval van een probleem, daar meteen aandacht aan te besteden en te proberen het probleem op te lossen. Uw computer loopt anders gevaar!



Opmerking: *u* kunt ook, wanneer *u* maar wilt, statusinformatie over AVG opvragen via het <u>systeemvakpictogram</u>.

7.3. Snelkoppelingen

Met behulp van snelkoppelingen (in het linker deelvenster van de <u>AVG</u> <u>gebruikersinterface</u>) kunt u snel de belangrijkste en meest gebruikte functies van AVG oproepen:

	0verzicht
Overzicht	Q Computerscanner
Computerscanner	📝 Nu bijwerken
📝 Nu bijwerken	Update wordt uitgevoerd

- Overzicht klik op deze snelkoppeling om vanuit een geopend dialoogvenster van AVG terug te keren naar het Overzicht van alle geïnstalleerde onderdelen
 zie het hoofdstuk Overzicht van onderdelen >>
- Computerscanner klik op deze snelkoppeling om de scaninterface van AVG op te roepen, waarin u direct scans kunt uitvoeren, plannen en schemainstellingen kunt wijzigen - zie het hoofdstuk <u>AVG tests >></u>
- Nu bijwerken klik op deze snelkoppeling om de interface voor updates te openen en meteen een updateprocedure voor AVG te starten - zie het hoofdstuk <u>AVG updates</u> >>

Deze snelkoppelingen zijn te allen tijde beschikbaar in de gebruikersinterface. Zodra u op een snelkoppeling klikt om een bepaalde procedure uit te voeren, wordt weliswaar een nieuw dialoogvenster geopend, maar de snelkoppelingen blijven niettemin beschikbaar. Bovendien wordt de uitgevoerde procedure grafisch weergegeven - *zie afbeelding 2*



7.4. Overzicht van onderdelen

De sectie **Overzicht van onderdelen** staat in het middelste gedeelte van de <u>AVG</u> <u>gebruikersinterface</u>. De sectie is onderverdeeld in twee gedeelten:

- Een overzicht van alle geïnstalleerde onderdelen dat bestaat uit een deelvenster met het pictogram van het onderdeel en de informatie of het desbetreffende onderdeel actief is of niet.
- Beschrijving van een geselecteerd onderdeel

In de **AVG 8.0 Anti-Virus** bevat het **Overzicht van onderdelen** informatie over de volgende onderdelen:

- Anti-Virus biedt uw computer bescherming tegen virussen die uw computer proberen binnen te dringen - <u>details >></u>
- Anti-Spyware scant toepassingen op de achtergrond terwijl u die uitvoert details >>

٠

 Anti-Rootkit detecteert programma's en technologieën die proberen malware te camoufleren - <u>details >></u>

٠



- *E-mailscanner* controleert alle binnenkomende en uitgaande e-mail op virussen - details >>
- Licentie biedt de volledige tekst van de AVG licentieverklaring details >>
- LinkScanner controleert zoekresultaten die in uw browser worden weergegeven - <u>details >></u>
- Web Shield scant alle gegevens die door een webbrowser worden gedownload - <u>details >></u>
- Resident Shield wordt op de achtergrond uitgevoerd en scant bestanden als ze worden gekopieerd, geopend of opgeslagen - <u>details >></u>
- Updatebeheer beheert alle AVG updates details >>

Klik op het pictogram van een onderdeel om het in het overzicht van onderdelen te selecteren. Dan wordt in het onderste deel van de gebruikersinterface ook de beschrijving van de basisfunctionaliteit van het onderdeel weergegeven. Dubbelklik op een pictogram om de interface van het onderdeel, met een lijst elementaire statistische gegevens, te openen.

7.5. Statistieken

De sectie**Statistieken** bevindt zich links onder in de <u>AVG gebruikersinterface</u>. Er staat een lijst met informatie over het functioneren van het programma.

- Laatste scan de datum waarop de laatst scan is uitgevoerd
- *Laatste update* de datum waarop de laatste update is uitgevoerd
- *Virus DB* informatie over de huidige geïnstalleerde versie van de virusdatabase
- **AVG-versie** informatie over de geïnstalleerde AVG-versie (een nummer met de opmaak 8.0.xx, waarbij 8.0 de productversie is en xx voor het typenummer staat)
- Vervaldatum licentie de vervaldatum van uw AVG-licentie



7.6. Systeemvakpictogram

Het systeemvakpictogram (op de taakbalk van Windows) geeft een indicatie van de huidige status van **AVG 8.0 Anti-Virus**. Het pictogram wordt steeds weergegeven in het systeemvak, ongeacht of het hoofdvenster van AVG is geopend of gesloten.

Als alle kleuren worden gebruikt voor weergave **a**, geeft het **systeemvakpictogram** aan dat alle AVG-onderdelen actief zijn en geheel naar behoren werken. Een grijs gekleurd pictogram met een uitroepteken **a** duidt op een probleem (niet-actief onderdeel, foutstatus, enz.) Dubbelklik op het **systeemvakpictogram** om het hoofdvenster te openen en een onderdeel aan te passen.

U kunt door op het **systeemvakpictogram** te dubbelklikken op elk gewenst moment snel het hoofdvenster van AVG openen.

Als u met de rechtermuisknop op het **systeemvakpictogram** klikt, opent u een snelmenu met de volgende twee opties:

- AVG gebruikersinterface openen klik op de optie als u de <u>AVG</u> gebruikersinterface wilt openen
- Update Onmiddellijk starten van een update
- **Afsluiten** klik op de optie om AVG af te sluiten (*u sluit alleen de gebruikersinterface af, AVG blijft op de achtergrond actief en uw computer wordt nog steeds volledig beschermd!)*



8. AVG onderdelen

8.1. Anti-Virus

8.1.1. Anti-Virus Principes

De scan-engine van de antivirussoftware scant alle bestanden en alle activiteiten waarbij bestanden betrokken zijn (openen/sluiten van bestanden, enz.) op bekende virussen. Elk gedetecteerd virus wordt geblokkeerd, zodat het geen activiteit kan ontwikkelen, en wordt daarna schoongemaakt of in quarantaine geplaatst. De meeste antivirusprogramma's gebruiken ook heuristische analyse, waar bij bestanden worden gescand op typische kenmerken van virussen, zogenaamde virale handtekeningen. Dat betekent dat de virusscanner een nieuw, nog onbekend virus kan detecteren, als dat virus bepaalde typerende kenmerken heeft van bestaande virussen.

De belangrijste functie van bescherming tegen virussen is het verhinderen van activiteit van bekende virussen!

Omdat bij het gebruik van slechts één technologie een bepaald virus misschien over het hoofd kan worden gezien of niet wordt herkend, zijn in **Anti-Virus** diverse technologieën gecombineerd om te garanderen dat uw computer wordt beschermd:

- Scannen hiermee wordt naar tekenreeksen gezocht die kenmerkend voor een bepaald virus zijn
- Heuristische analyse dynamische emulatie van de instructies van gescande object en in een virtuele computeromgeving
- Algemene detectie detectie van instructies die kenmerkend zijn voor een bepaald virus of een bepaalde groep virussen

AVG kan bovendien uitvoerbare toepassingen en DLL-bibliotheken analyseren en detecteren die mogelijk ongewenst zijn binnen het systeem. Dergelijke bedreigingen noemen we potentieel ongewenste programma's (verschillende typen spyware, adware, enz.). Daarnaast scant AVG uw systeemregister op verdachte sleutels, tijdelijke internetbestanden en zogeheten tracking-cookies. U kunt hierbij instellen dat alle mogelijk schadelijke items op dezelfde wijze moeten worden afgehandeld als andere infecties.



8.1.2. Anti-virus interface

🕌 AVG Enterprise		
Bestand Onderdelen Historie Extr	a <u>H</u> elp	
🕌 AVG	U bent beschermd. Alle beveiligingsfuncties zijn	n up-to-date en functioneren correct.
Overzicht Anti-Virus Computerscanner	Anti-Virus Onderdeel Anti-Virus detecteert v bestanden of DLL-biblioth bovendien de interne viru. Anti-Virus up-to-date hou	russen, wormen en Trojaanse paarden, en bovendien uitvoerbare eken die mogelijk ongewenst zijn in uw systeem. Anti-Virus bevat sdatabase en om die reden is het cruciaal dat u het onderdeel dt voor een optimale bescherming.
📝 Nu bijwerken	Anti-Virus-component is actief.	
	Infecties in database: Laatste update database: Databaseversie:	1182357 dinsdag 26 februari 2008, 20:50 269.21.1/1300
Statistieken Laatste scan: Nog niet gescand Update: 3-3:08, 22:22 Virusdatabase: 263:21:1/1300 AVG versie: 8:0.81 Vervaldatum licentie: 1-6:2008		Terug

De interface van het onderdeel **Anti-Virus** biedt elementaire informatie over de functionaliteit van het onderdeel, de huidige status (*Anti-Virus-component is actief.*), en een beknopt overzicht met **Anti-Virus**-statistieken:

- **Infecties in database** het aantal in de meest actuele versie van de virusdatabase gedefinieerde virussen
- **Laatste update database** de datum en het tijdstip waarop de virusdatabase voor het laatst is bijgewerkt
- Databaseversie het nummer van de laatste databaseversie; dit nummer wordt bij iedere nieuwe versie één hoger

Het dialoogvenster van dit onderdeel heeft maar één knop (**Terug**) - klik op deze knop om terug te keren naar de standaard <u>AVG gebruikersinterface</u> (Overzicht van onderdelen).

Opmerking: De leverancier van heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als de noodzaak voor wijziging van de configuratie van AVG zich voordoet, selecteert u in het systeemmenu de optie **Bestand/Geavanceerde**


instellingen en wijzigt u de AVG-configuratie in het dialoogvenster <u>Geavanceerde</u> <u>instellingen AVG</u> dat dan wordt geopend.

8.2. Anti-Spyware

8.2.1. Anti-Spyware Principes

Spyware wordt meestal gedefinieerd als een soort malware: software die informatie op een computer verzamelt zonder medeweten of toestemming van de gebruiker. Sommige spywaretoepassingen worden opzettelijk geïnstalleerd en bevatten vaak reclame, pop-ups of andere soorten ongewenste software.

Spyware en malware worden voornamelijk verspreid via websites met een inhoud die mogelijk gevaarlijk is. Daarnaast wordt dergelijke software ook verspreid via emailberichten en via wormen en virussen. De meest geschikte beveiligingsmethode is een achtergrondscanner die altijd is ingeschakeld, zoals **Anti-Spyware**. Dit onderdeel werkt als een resident shield en scant uw toepassingen op de achtergrond wanneer deze worden uitgevoerd.

Het is echter mogelijk dat uw computer reeds malware bevatte op het moment dat u AVG op de computer hebt geïnstalleerd, of dat u **AVG 8.0 Anti-Virus** niet regelmatig hebt bijgewerkt met de recentste database- en <u>programma-updates</u>. AVG is daarom voorzien van een scanfunctie waarmee u uw computer op malware/spyware kunt scannen. Die detecteert ook slapende en niet-actieve malware, dat wil zeggen malware die al wel is gedownload, maar nog niet is geactiveerd.



8.2.2. Anti-Spyware interface

讃 AVG Enterprise					
Bestand Onderdelen Historie Extra	Help				
📕 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.				
Overzicht Anti-Spyware Computerscanner	Anti-Spyware Onderdeel Image: Spyware biedt bescherming tegen alle soorten malware (kwaadaardige software), bijv. spyware die heimelijk gegevens verzamelt van uw computer, en adware die ongewenste reclame op uw computer weergeeft. Voor 100 procent bescherming dient u steeds de Anti-Spyware-component up-to-date te houden.				
📝 Nu bijwerken	Anti-Spyware-component is actief.				
	Spywaredefinities: 86857 Laatste update database: dinsdag 26 februari 2008, 20:50 Databaseversie: 269.21.1/1300				
Statistieken Laatste scan: Nog niet gescand Update: 3:3-08, 22:22 Vrusdatabase: 269 21.1/1300 AVG versie: 8:0.81 Vervaldatum licentie: 1-6:2008 Melding weergeven	Terug				

De interface van het onderdeel **Anti-Spyware** biedt een beknopt overzicht van de functionaliteit van het onderdeel, de huidige status (*Anti-Spyware-component is actief.*) en een paar **Anti-Spyware**-statistieken:

- **Spyware in database** het totale aantal spywaremonsters dat in de nieuwste versie van de spywaredatabase is gedefinieerd
- *Laatste update database* de datum en het tijdstip waarop de virusdatabase voor het laatst is bijgewerkt
- Databaseversie het nummer van de laatste spywaredatabaseversie; dit nummer wordt bij iedere nieuwe versie één hoger

Het dialoogvenster van dit onderdeel heeft maar één knop (**Terug**) - klik op deze knop om terug te keren naar de standaard <u>AVG gebruikersinterface</u> (Overzicht van onderdelen).

Opmerking: De leverancier van heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als de noodzaak voor wijziging van de configuratie van AVG zich voordoet, selecteert u in het systeemmenu de optie **Bestand/Geavanceerde**



instellingen en wijzigt u de AVG-configuratie in het dialoogvenster <u>Geavanceerde</u> <u>instellingen AVG</u> dat dan wordt geopend.

8.3. Anti-Rootkit

8.3.1. Anti-Rootkit principes

Anti-Rootkit is een speciaal ontwikkeld hulpmiddel voor het detecteren en effectief verwijderen van gevaarlijke rootkits, programma's en technologie die de aanwezigheid van schadelijke software op een computer kunnen camoufleren.

Een rootkit is een programma dat is ontwikkeld om de controle over een computersysteem over te nemen zonder toestemming van de eigenaren en rechtmatige beheerders van het systeem. Toegang tot de hardware is zelden vereist omdat een rootkit is bedoeld om de controle over het besturingssysteem dat op de hardware draait, over te nemen. Gewoonlijk proberen rootkits hun aanwezigheid te verbergen door het ondermijnen of ontwijken van de standaard beveiligingsmechanismen van het besturingssysteem. Vaak zijn het bovendien Trojaanse paarden die gebruikers in de waan laten dat ze veilig met hun systeem kunnen werken. De technieken die worden gebruikt om dit te bereiken omvatten bijvoorbeeld het voor bewakingsprogramma's verbergen van processen die worden uitgevoerd, of het verbergen van bestanden of systeemgegevens voor het besturingssysteem.



8.3.2. Anti-Rootkit interface

🕌 AVG Enterprise						
jestand Onderdelen Historie Extra Help						
🕌 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.					
Overzicht Anti-Rootkit Computerscanner Nu biiwerken	Anti-Rootkit Onderdeel Image: State of the s					
E. In phromon	Anti-Rootkit-component is actief.					
	Laatste controle op rootkits: Nog niet gescand					
	Anti-Rootkit instellingen					
Statistieken Laatste scan: Nog niet gescand Update: 3:3-06, 22:22 Virusdatabase: 256 21.1/1300 AVG versie: 8.0.81	De standaard scanprocedure detecteert en verwijdert rootkits niet, daarom dient u dat onderdeel handmatig uit te voeren om zeker te weten dat er geen bestaande rootkits op uw systeem aanwezig zijn. Vitoepassingen scannen Snelle rootkitscan Volledige rootkitscan V stuurprogramma's scannen					
Vervaldatum licentie: 1-6-2008	Zoeken naar rootkits Terug					

De gebruikersinterface van **Anti-Rootkit** biedt een korte beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status van het onderdeel (*Anti-Rootkit-component is actief.*) en biedt bovendien informatie over de laatste keer dat de **Anti-Rootkit**-test is uitgevoerd.

In het onderste deel van het dialoogvenster staan de **Anti-Rootkit instellingen** waar u een aantal elementaire parameters kunt instellen voor het scannen op de aanwezigheid van rootkits. Schakel eerst de selectievakjes in van de objecten die moeten worden gescand:

- Toepassingen scannen
- DLL-bibliotheken scannen
- Stuurprogramma's scannen

Vervolgens kunt u de scanmodus kiezen:

- **Snelle rootkitscan** alleen de systeemmap wordt gescand (*meestal: c:* *Windows*)
- Volledige rootkitscan alle toegankelijke schijven worden gescand met



uitzondering van A: en B:

Knoppen beschikbaar:

- Zoeken naar rootkits aangezien de rootkitscan geen geïntegreerd onderdeel is van <u>Volledige computer scannen</u>, kunt u rechtstreeks vanuit de Anti-rootkit-interface rootkitscans uitvoeren als u op deze knop klikt.
- Annuleren klik op deze knop om het dialoogvenster te sluiten en terug te keren naar de standaard <u>AVG-gebrukersinterface</u> (het overzicht van onderdelen)

8.4. Firewall

8.4.1. Firewallprofielen

Met *Firewall* kunt u specifieke regels voor het beveiligingsniveau definiëren afhankelijk van de vraag of de computer zich in een domein bevindt, een zelfstandige computer is of zelfs een notebook. Voor deze opties zijn verschillende beveiligingsniveaus vereist. De niveaus worden bepaald door de desbetreffende profielen. Kortom, een *Firewall-profiel* is een specifieke configuratie van het onderdeel *Firewall*, u kunt een aantal van dergelijke vooraf gedefinieerde configuraties gebruiken.

Beschikbare profielen

- Alles toestaan een <u>Firewall</u>-systeemprofiel dat vooraf is ingesteld door de fabrikant en altijd beschikbaar is. Als dit profiel wordt geactiveerd, wordt al het netwerkverkeer toegestaan en worden geen beveiligingsregels toegepast, alsof <u>Firewall</u> is uitgeschakeld. U kunt dit systeemprofiel niet dupliceren of verwijderen en u kunt de instellingen niet wijzigen.
- **Blokkeer alles** een <u>Firewall</u>-systeemprofiel dat vooraf is ingesteld door de fabrikant en altijd beschikbaar is. Als dit profiel wordt geactiveerd, wordt al het netwerkverkeer geblokkeerd en is de computer vanuit netwerken van buitenaf niet toegankelijk en kan hij evenmin met de buitenwereld communiceren. U kunt dit systeemprofiel niet dupliceren of verwijderen en u kunt de instellingen niet wijzigen.
- **Aangepaste profielen** profielen gegenereerd met behulp van de **Wizard Firewallconfiguratie**. U kunt met de wizard maximaal drie aangepaste profielen genereren:



- Standalone computer geschikt voor doorsnee desktop computers thuis met een directe verbinding met internet.
- Computer in een domain geschikt voor computers in een lokaal netwerk, bijvoorbeeld het netwerk van een school of een bedrijfsnetwerk. Er wordt van uitgegaan dat het netwerk wordt beveiligd met aanvullende maatregelen, zodat een minder hoog beveiligingsniveau vereist is dan bij standalone computers.
- Klein thuis- of kantoornetwerk geschikt voor computers in een klein netwerk, bijvoorbeeld thuis of in een klein bedrijf, waar slechts een paar computers met elkaar verbonden zijn, zonder "centrale" beheerder.
- Mobiele computer geschikt voor notebooks. Er wordt van uitgegaan dat de computer die wordt meegenomen op reis, vanaf verschillende onbekende en als gevolg daarvan in hoge mate risicovolle locaties (internetcafé, hotelkamer, enz.) verbinding moet maken met internet, daarom wordt het hoogste beveiligingsniveau ingesteld.

Profiel omschakelen

Via de functie Profiel omschakelen kan de *Firewall* automatisch omschakelen naar het gedefinieerde profiel wanneer u een bepaalde netwerkadapter gebruikt of wanneer u bent verbonden met een bepaald type netwerk. Als aan een netwerkgebied nog geen profiel is toegewezen, zal *Firewall* bij de eerstvolgende keer dat een verbinding tot stand wordt gebracht met dat gebied, een dialoogvenster openen met de vraag een profiel toe te wijzen.

U kunt profielen toewijzen aan alle lokale netwerkinterfaces en -gebieden en nadere instellingen opgeven in het dialoogvenster **Profielen van gebieden en adapters**; in dat dialoogvenster kunt u de functie ook uitschakelen als u er geen gebruik van wilt maken.*dan zal voor alle typen verbindingen het standaardprofiel worden gebruikt*).

Gewoonlijk vinden gebruikers met een notebook die afhankelijk zijn van veel verschillende verbindingen, dit een handige functie. Als u een desktop computer hebt en steeds van dezelfde verbinding gebruikmaakt (*bijvoorbeeld een kabelverbinding met internet*), hoeft u geen aandacht te schenken aan het omschakelen van profielen, omdat u de functie waarschijnlijk nooit gebruikt.



8.5. Licentie

🛃 AVG Enterprise					
Bestand Onderdelen Historie Extra	Help				
📕 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.				
Overzicht Eicentie Computerscanner	Licentie Onderdeel Het onderdeel Licentie beheert uw huidige licentiestatus. Uw licentienummer geeft aan welke specifieke versie van AVG u hebt. Wees nauwkeurig bij het invoeren en activeren van uw licentie, omdat de software anders niet correct wordt bijgewerkt en wij niet in staat zijn u technische ondersteuning te bieden.				
🕅 Nu bijwerken	Licentie-component is actief. Het geïnstalleerde product is AVG Enterprise.				
Update wordt uitgevoerd	Licentienummer: XXX-XXXXX-XXXXX-XXXXX-XXXXX Licentietype: Volledig Vervaldatum licentie: zondag 1 juni 2008 Aantal exemplaren: 10				
Statistieken Laatste scan: Nog niet gescand Update: 3-3-08, 22-22 Virusdatabase: 289-21.1/1300 AVG versie: 8-0.81 Vervaldatum licentie: 1-6-2008 XMelding weergeven	Licentieacties Licentienummer kopiëren Opnieuw activeren Registreren Terug				

Op het scherm van het onderdeel *Licentie* staat een korte tekst met een beschrijving van de functionaliteit van het onderdeel, informatie over de huidige status (*Licentie-component is actief.*) en de volgende informatie:

- Licentienummer de exacte vorm van het licentienummer. Als u uw licentienummer invoert, dient u het heel nauwkeurig zo te typen als het wordt weergegeven. Om het u gemakkelijk te maken heeft het dialoogvenster Licentie een knop Licentienummer kopiëren : Klik op die knop om het licentienummer naar het klembord van Windows te kopiëren, dan kunt u het daarna plakken waar u maar wilt (CTRL+V).
- *Licentietype* specificatie van de productversie bij uw licentienummer.
- **Vervaldatum licentie** de datum waarop de licentie zijn geldigheid verliest. Als u na die datum AVG wilt blijven gebruiken, zult u de licentie moeten vernieuwen. U kunt de <u>licentie online vernieuwen</u> op de website van AVG.
- **Aantal exemplaren** Het aantal werkstations waarop u AVG mag installeren.

Knoppen



- Licentienummer kopiëren klik op de knop om het licentienummer dat nu wordt gebruikt naar het klembord van Windows te kopiëren (*net als met CTRL* +C), zodat u het kunt plakken waar u het nodig hebt
 - **Opnieuw activeren** het dialoogvenster **AVG activeren** wordt geopend met de gegevens die u hebt opgegeven in het dialoogvenster <u>AVG aanpassen</u> van de <u>installatieprocedure</u>. In dit dialoogvenster kunt u uw licentienummer invoeren ter vervanging van ofwel het verkoopnummer (*het nummer waarmee u AVG hebt geïnstalleerd*), ofwel het oude licentienummer (*bijvoorbeeld bij het upgraden naar een nieuw product van AVG*).
 - **Registreren** er wordt een verbinding tot stand gebracht met de registratiewebsite <u>www.avg.com</u>. Voer uw registratiegegevens in; alleen klanten die hun AVG product registreren komen in aanmerking voor gratis technische ondersteuning
 - Annuleren klik op deze knop om het dialoogvenster te sluiten en terug te keren naar de standaard <u>AVG-gebrukersinterface</u> (het overzicht van onderdelen)



8.6. LinkScanner

Het onderdeel *LinkScanner* bestaat uit twee programmafuncties die u in en uit kunt schakelen op de interface van het **Onderdeel LinkScanner**:



- <u>AVG Search Shield</u> inschakelen (*standaard ingeschakeld*): pictogrammen met een indicatie bij de resultaten van zoekopdrachten met Google, Yahoo en MSN, die wordt verkregen door vooraf de inhoud van sites die door de zoekmachine worden geretourneerd, te controleren. De functie ondersteunt de browsers Internet Explorer en Firefox.
- **AVG Active Surf-Shield** inschakelen (standaard ingeschakeld): actieve (real-time) bescherming tegen websites met exploits op het moment dat ze worden geadresseerd. Als zodanig bekend staande kwaadaardige sites en de inhoud met exploits worden geblokkeerd op het moment dat de gebruiker ze adresseert in de browser (of met een andere toepassing die HTTP gebruikt).
- Rapportage van websites met exploits schakel dit selectievakje in voor rapportage van exploits en kwaadaardige sites waarmee gebruikers via Safe Surf of Safe Search zijn geconfronteerd, naar de database waarin gegevens worden verzameld over kwaadaardige praktijken op internet.



8.6.1. AVG Search Shield

Als u op internet zoekt, terwijl **AVG Search-Shield** is ingeschakeld, worden alle zoekresultaten van de belangrijkste zoekmachines zoals Yahoo!, Google en MSN, enz. beoordeeld op gevaarlijke of verdachte koppelingen. De <u>AVG Werkbalk Beveiliging</u> controleert deze koppelingen, markeert de slechte koppelingen en waarschuwt u zo voordat u op een gevaarlijke of verdachte koppeling klikt, zodat u zeker weet dat u alleen naar veilige websites gaat.

Terwijl een koppeling op de pagina met resultaten wordt beoordeeld, wordt bij die koppeling een pictogram weergegeven om aan te geven dat de beoordeling wordt uitgevoerd. Zodra de beoordeling is voltooid, wordt een pictogram ter aanduiding van de gevonden informatie weergegeven:

Werkbalk Beveiliging wordt dit pictogram niet weergegeven!).

De gekoppelde pagina bevat geen bedreigingen, maar is enigszins verdacht (twijfelachtige oorsprong of strekking en daarom niet geschikt voor e-shopping en dergelijke).

De gekoppelde pagina is wellicht veilig, maar bevat koppelingen naar pagina's die zonder meer gevaarlijk zijn, of gevaarlijke code bevatten, ook al vormen ze op het moment geen bedreiging.

De gekoppelde pagina bevat actieve bedreigingen! U krijgt voor uw eigen bescherming geen toestemming de pagina te bezoeken.

🥙 De gekoppelde pagina is niet toegankelijk en is daarom niet gescand.

Als u de muisaanwijzer op een pictogram plaatst, worden details van de desbetreffende koppeling weergegeven. Die extra informatie betreft details van de dreiging (als die er is), het IP-adres van de pagina en het tijdstip waarop de pagina door AVG is gescand:





8.6.2. AVG Active Surf-Shield

Dit krachtige schild blokkeert de kwaadaardige inhoud van webpagina's die u probeert te openen en voorkomt dat die naar uw computer wordt gedownload. Als de functie is ingeschakeld, wordt automatisch verhinderd dat een webpagina wordt geopend als u op een koppeling klikt of de URL typt van een gevaarlijke site, en zo wordt voorkomen dat u per ongeluk geïnfecteerd raakt. Het is belangrijk te weten dat webpagina's met een exploit uw computer kunnen infecteren, alleen al als u de desbetreffende site bezoekt; om die reden zal de <u>AVG Werkbalk Beveiliging</u> verhinderen dat uw webbrowser gevaarlijke webpagina's met exploits of andere serieuze bedreigingen weergeeft.

Als u wordt geconfronteerd met een kwaadaardige website, wordt u door de <u>AVG</u> <u>Werkbalk Beveiliging</u> gewaarschuwd met een scherm als het volgende:



Als u de geïnfecteerde pagina toch wilt bezoeken, kunt u op de desbetreffende koppeling op het scherm klikken, **maar het is niet raadzaam dat te doen!**

8.7. Web Shield



8.7.1. Web Shield principes

Web Shield is een interne vorm van real-time bescherming; het onderdeel scant de inhoud van bezochte webpagina's (en de bestanden die in die pagina's zijn opgenomen) nog voordat ze in de webbrowser worden weergegeven of worden gedownload naar uw computer.

Als Web Shield detecteert dat de pagina die u wilt gaan bezoeken, bijvoorbeeld een gevaarlijk Javascript bevat, wordt weergave van die pagina verhinderd. Bovendien herkent Web Shield malware op pagina's en verhindert het onmiddellijk dat de malware wordt gedownload, zodat de malware uw computer nooit bereikt.

8.7.2. Web Shield interface

🕌 AVG Enterprise						
Bestand Onderdelen Historie Extra	Help					
AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.					
	Web Shield Onderdeel					
Overzicht	Web Shield beschernt u tegen het per ongeluk downloaden van geinfecteerde bestanden en het uitvierden und gelificationale bestanden uit gureneb nichter					
Web Shield						
Computerscanner						
📝 Nu bijwerken	🖉 Web Shield is actief en volledig functioneel.					
	V Inschakelen Web Shield Web Expresberichten					
	Basisinstellingen web					
	Webbescherming					
	Scannen op bedreigingen door mogelijk ongewenste programma's en spyware					
Statistieken	Heuristische analyse gebruiken					
Laatste scan: Nog niet gescand Update: N/A Virusdatabase: 269.21.4/1313 AVG versie: 8.0.85	Maximale grootte te scannen bestand 200 kB					
Vervaldatum licentie: 1-6-2008	Wijzigingen opstaan Annuleren					

De interface van het onderdeel **Web Shield** beschrijft wat dit type bescherming doet. Bovendien vindt u er informatie over de huidige status van het onderdeel (*Web Shield is actief en volledig functioneel.*). In het onderste deel van het dialoogvenster staan de elementaire bewerkingsopties voor het functioneren van het onderdeel.

Basisconfiguratie van het onderdeel

Om te beginnen is er een optie waarmee u Web Shield kunt in- en uitschakelen met



behulp van het selectievakje **Web Shield inschakelen**. De optie is standaard ingeschakeld, zodat het onderdeel **Web Shield** actief is. We raden u aan om het onderdeel niet uit te schakelen, tenzij u een goede reden hebt om dat wel te doen. Als het selectievakje is ingeschakeld en **Web Shield** dus actief is, zijn er twee tabbladen met aanvullende opties voor configuratie:

- **Web** u kunt u de configuratie van het onderdeel aanpassen met betrekking tot het scannen van de inhoud van websites. U kunt de volgende basisopties aanpassen:
 - Webbescherming met deze optie geeft u op of Web Shield de inhoud van webpagina's moet scannen. Ervan uitgaande dat deze optie is ingeschakeld (*standaard*), kunt u nog de volgende functies in- en uitschakelen:
 - Archiefbestanden controleren de inhoud van archieven scannen die zijn inbegrepen op de webpagina die u wilt weergeven
 - Potentieel ongewenste programma's scannen potentieel ongewenste programma's scannen (spyware of adware in de vorm van uitvoerbare bestanden) die zijn ingesloten op de webpagina die u wilt weergeven
 - Heuristische methode gebruiken de inhoud scannen van een weer te geven pagina met behulp van de methode voor heuristische analyse (dynamische emulatie van de instructies van gescande object en in een virtuele computeromgeving - zie het hoofdstuk <u>Antivirus principes</u>)
 - Maximale grootte te scannen bestand Als er bestanden zijn inbegrepen op een weer te geven pagina, kunt u de inhoud daarvan ook scannen voordat ze naar uw computer wrden gedownload. Het scannen van grote bestanden neemt echter soms veel tijd in beslag, wat het downloaden van de webpagina aanzienlijk kan vertragen. Met behulp van de schuifbalk kunt u de maximale grootte opgeven van bestanden die moeten worden gescand met Web Shield. Zelfs als het gedownloade bestand groter is dan u hebt opgegeven, en dus niet wordt gescand met Web Shield, wordt u nog steeds beschermd: in het geval dat het bestand is geïnfecteerd, zal dat onmiddellijk worden gedetecteerd door <u>Resident Shield</u>.
- **Expresberichten** de instellingen voor het onderdeel opgeven die betrekking hebben op het scannen van expresberichten (*bijv. ICQ, Skype, MSN Messenger, ...*).



 Bescherming expresberichten - schakel dit selectievakje in als u wilt dat Web Shield controleert of de online communicatie virusvrij is. Als de optie is ingeschakeld, kunt u nog opgeven welke toepassing voor expresberichten u wilt controleren - op dit moment ondersteunt AVG 8.0 Anti-Virus de toepassingen ICQ en MSN.

Opmerking: De leverancier van heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als de noodzaak voor wijziging van de configuratie van AVG zich voordoet, selecteert u in het systeemmenu de optie **Bestand/Geavanceerde instellingen** en wijzigt u de AVG-configuratie in het dialoogvenster <u>Geavanceerde instellingen AVG</u> dat dan wordt geopend.

Knoppen

De interface van **Web Shield** heeft de volgende knoppen:

- **Wijzigingen opslaan** klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
- **Annuleren** klik op deze knop om terug te keren naar de standaard <u>AVG-</u> <u>gebruikersinterface</u> (*het overzicht van onderdelen*)

8.8. Resident Shield

8.8.1. Resident Shield Principes

Resident Shield scant bestanden als ze worden gekopieerd, geopend of opgeslagen. Als **Resident Shield** een virus ontdekt in een bestand dat wordt geadresseerd, breekt het de bewerking die op dat moment wordt uitgevoerd, af en verhindert het dat het virus zichzelf activeert. **Resident Shield** wordt tijdens het opstarten van het systeem in het geheugen geladen en biedt ook essentiële bescherming voor de systeemgebieden van de computer



8.8.2. Resident Shield interface

🕌 AVG Enterprise						
Bestand Onderdelen Historie Extra	Help					
🛃 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.					
	Resident Shield Onderdeel					
Overzicht						
	Resident Shield scant bestanden als ze worden gekopieerd, geopend en opgeslagen en voorkomt activering als een bedreiging wordt gevonden. Het biedt ook essentiële bescherming					
Resident Shield	voor de systeemgebieden van de computer.					
Computerscanner						
🕅 Nu bijwerken	Resident Shield is actief en volledig functioneel.					
	Resident Shield is uitgevoerd gedurende: 3 min. 15 seconde (n) Gevonden en geblokkeerde bedreigingen: 0 Selecteer Extra / Geavanceerde instellingen in het systeemmenu voor meer gedetailleerde instellingen.					
Statistieken Laatste scan: Nog niet gescand Update: N/A Virusdatabase: 259.21.4/1313 AVG versie: 8.0.85 Vervaldatum licentie: 1-6-2008	Resident Shield instellingen \Resident Shield actief \Other Alle bedreigingen automatisch verwijderen \Other Cookies detecteren \Other Vragen voor het verwijderen van bedreigingen Uitzonderingen beheren \Other Vijzigingen opslaan Annuleren \Other \Other					
XMelding weergeven						

Behalve een overzicht van de belangrijkste statistische gegevens en informatie over de huidige status van het onderdeel (*Resident Shield is actief en volledig functioneel*) heeft de interface van **Resident Shield** ook een paar opties voor het instellen van elementaire parameters voor het onderdeel. Het gaat om de volgende statistieken:

- **Resident Shield is actief geweest voor** het tijdsverloop sinds de laatste keer dat het onderdeel is gestart
- **Gedetecteerde en geblokkeerde bedreigingen** het aantal gedetecteerde infecties waarvan uitvoering/openen is verhinderd

Basisconfiguratie van het onderdeel

Onder in het dialoogvenster is een gedeelte **Resident Shield instellingen**, waar u een paar basisinstellingen kunt opgeven voor het functioneren van het onderdeel (voor gedetailleerde configuratie kiest u, net als voor alle andere onderdelen de optie Bestand/Geavanceerde instellingen in het systeemmenu).

Met de optie **Resident Shield is actief** kunt u de bescherming door Resident Shield gemakkelijk in- en uitschakelen. Standaard is het onderdeel ingeschakeld. Als



Resident Shield is ingeschakeld, kunt u nog nader specificeren hoe gedetecteerde infecties moeten worden verwijderd:

- o automatisch (Alle bedreigingen automatisch verwijderen)
- o of na bevestiging door de gebruiker (*Vragen voor het verwijderen van bedreigingen*)

Deze keuze heeft geen invloed op de mate van bescherming en komt alleen maar tegemoet aan uw voorkeur.

In beide gevallen kunt u kiezen voor **Cookies automatisch verwijderen.** Onder bepaalde omstandigheden kunt u deze optie inschakelen voor een maximale bescherming; standaard is de functie uitgeschakeld. (*Cookies zijn pakketjes tekst die door een server naar een webbrowser worden gestuurd, die steeds onveranderd door de webbrowser worden teruggestuurd op het moment dat de browser de server adresseert. HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*).

Opmerking: De leverancier van heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als de noodzaak voor wijziging van de configuratie van AVG zich voordoet, selecteert u in het systeemmenu de optie **Bestand/Geavanceerde instellingen** en wijzigt u de AVG-configuratie in het dialoogvenster <u>Geavanceerde</u> **instellingen** AVG dat dan wordt geopend.

Knoppen

De interface van **Resident Shield** heeft de volgende knoppen:

- Uitzonderingen beheren als u op deze knop klikt, wordt het dialoogvenster <u>Uitsluitingen voor directory met Resident Shield</u> geopend, waarin u mappen kunt opgeven die niet door <u>Resident Shield</u> moeten worden gescand
- *Wijzigingen opslaan* klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
- Annuleren klik op deze knop om het dialoogvenster te sluiten zonder wijzigingen op te slaan, en terug te keren naar de standaard <u>AVG-</u> <u>gebrukersinterface</u> (het overzicht van onderdelen)



8.8.3. Resident Shield detectie

🛃 AVG Enterprise						
Bestand Onderdelen Historie Extra	Нер					
🕌 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.					
	Resident Shield detectie					
🗊 Overzicht	Infectie Object					
Q Computerscanner	Wirus herkend EICAR_Test C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\Tijdelijke map 1 voor eicar_com.zip\eicar.com Wirus herkend EICAR_Test C:\Documents and Settings\AdministratoriLocal Settings\Temp\Tijdelijke map 1 voor eicar_cor					
📝 Nu bij w erken						
Statistieken Laatste scan: Nog niet gescand Update: 3-3-08, 22:38 Virusdatabase: 283 21, 1/1300 AVG versie: 8.0.81 Vervaldatum licentie: 1-6-2008						
XMelding weergeven						

In het dialoogvenster **Resident Shield-detectie** staat een overzicht van objecten die door <u>Resident Shield</u> zijn gedetecteerd, beoordeeld en aangemerkt als gevaarlijk en vervolgens zijn hersteld of verplaatst naar de <u>Quarantaine</u>. Bij elk object wordt de volgende informatie weergegeven:

- **Infectie** beschrijving (indien mogelijk de naam) van het gedetecteerde object
- Object locatie van het object
- Resultaat de bewerking die met het gedetecteerde object is uitgevoerd
- Objecttype type van het gedetecteerde object
- **Proces** het proces dat werd uitgevoerd en dat ertoe leidde dat het potentieel gevaarlijke object werd opgeroepen en gedetecteerd

8.9. Updatebeheer



8.9.1. Updatebeheer principes

Geen enkel beveiligingsprogramma kan werkelijk garant staan voor bescherming tegen allerlei bedreigingen als het niet regelmatig wordt bijgewerkt! De makers van virussen zoeken steeds naar nieuwe tekortkomingen in software en besturingssystemen om uit te buiten. Elke dag verschijnen er nieuwe virussen, nieuwe malware en nieuwe hacker-aanvallen. Om die reden laten de leveranciers van software steeds nieuwe updates en beveiligingspatches verschijnen, om de gaten te dichten die in de beveiliging zijn ontdekt.

Het is cruciaal dat u regelmatig updates uitvoert voor AVG.

Het **Updatebeheer** helpt u bij het beheer van regelmatige updates. Met dit onderdeel kunt u automatische downloads plannen van update bestanden, van internet of via het lokale netwerk. Essentiële updates van virusdefinities dienen als dat mogelijk is, dagelijks te worden uitgevoerd. Minder urgente updates kunnen ook wekelijks worden uitgevoerd.

Opmerking: neem het hoofdstuk <u>AVG Updates</u> door voor meer informatie over typen updates en updateniveaus!

🛃 AVG Enterprise						
Bestand Onderdelen Historie Extra	Help					
🕌 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.					
	Updatebeheer Onderdeel					
🗊 Overzicht	. Updatebeheer beheert automatische updates van AVG via internet of het lokale netwerk.					
Updatebeheer	Het wordt aangeraden om een updateplan aan te maken waarmee u met regelmatige					
	essentiële updateb eschikbaar zijn, zodat u aktiv dover de nieuwste versie van de updatebestanden beschikt. Het is van cruciaal belang om AVG geregeld bij te werken als u zich up estiel de bescheringe teene uit-werdene uit-werdene uit-werdene uit-					
📝 Nu bijwerken	Updatebeheer-component is actief.					
	Laatste update: Virusdatabaseversie: 269.21.4/1313 Volgende geplande update: zaterdag 8 maart 2008, 18:26 Selecteer Extra / Geavanceerde instellingen in het systeemmenu voor meer gedetailleerde instellingen.					
Statistieken Laatste scan: Nog niet gescand Update: N/A Virusdatabase: 269.21.4/1313 AVG versie: 8.0.85 Vervaldatum licentie: 1-6-2008	Updatebeheer instellingen					

8.9.2. Updatebeheer interface

De interface van **Updatebeheer** biedt informatie over de functionaliteit van het



onderdeel, de huidige status (*Updatebeheer is actief.*) en relevante statistische gegevens:

- *Laatste update* de datum en het tijdstip waarop de database voor het laatst is bijgewerkt
- **Virusdatabaseversie** het nummer van de laatste virusdatabaseversie; dit nummer wordt bij iedere nieuwe versie één hoger

Basisconfiguratie van het onderdeel

Het onderste deel van het dialoogvenster is de sectie **Instellingen Updatebeheer** waar u een aantal wijzigingen kunt aanbrengen in de regels die het starten van de updateprocedure bepalen. U kunt opgeven dat updatebestanden automatisch moeten worden gedownload (**Automatische updates starten**) of alleen op verzoek. Standaard is de optie **Automatische updates starten** ingeschakeld; het is raadzaam die instelling aan te houden! Downloaden van de nieuwste updates op regelmatige tijdstippen is cruciaal voor het goed functioneren van welke vorm van beveiligingssoftware dan ook !

Bovendien bepaalt u hier wanneer de opstartprocedure moet worden gestart:

- o **Periodiek** geef een tijdsinterval op
- o **Op een specifiek tijdstip** geef datum en tijdstip op

Standaard is de optie zo ingesteld dat om de vier uur de procedure wordt gestart. We bevelen u met nadruk aan deze instelling aan te houden, tenzij u een goede reden hebt om die te wijzigen!

Opmerking: De leverancier van heeft alle onderdelen van AVG zo ingesteld dat ze optimaal presteren. Wijzig de configuratie van AVG niet, tenzij er een goede reden is om dat wel te doen. Wijzigingen in de instellingen dienen alleen te worden uitgevoerd door ervaren gebruikers. Als de noodzaak voor wijziging van de configuratie van AVG zich voordoet, selecteert u in het systeemmenu de optie **Bestand/Geavanceerde instellingen** en wijzigt u de AVG-configuratie in het dialoogvenster <u>Geavanceerde</u> **instellingen** AVG dat dan wordt geopend.

Knoppen

De interface van **Updatebeheer** heeft de volgende knoppen:



- **Nu bijwerken** op verzoek wordt een <u>onmiddellijke update</u> uitgevoerd
 - **Wijzigingen opslaan** klik op deze knop om de wijzigingen die u in het dialoogvenster hebt uitgevoerd op te slaan en toe te passen
 - Annuleren klik op deze knop om het dialoogvenster te sluiten zonder wijzigingen op te slaan, en terug te keren naar de standaard <u>AVG-</u> <u>gebrukersinterface</u> (het overzicht van onderdelen)

8.10.AVG Werkbalk Beveiliging

De **AVG Werkbalk Beveiliging** is ontwikkeld voor samenwerking met **MS Internet Explorer** (versie 6.0 of hoger) en **Mozilla Firefox** (versie 1.5 of hoger).

Als u de **AVG Werkbalk Beveiliging** hebt geïnstalleerd, wordt die standaard meteen onder de adresbalk van de browser geplaatst:

📲 AVG 🔻 powered by 🏋 HOO! SEARCH 🔽 Search 🔶 🍙 Active Surf-Shield 🔒 Search-Shield 🧔 AVG Info 🕶

Op de **AVG Werkbalk Beveiliging** staat het volgende:

- Knop AVG-logo achter deze knop gaat een menu schuil met werkbalkitems. Klik op de knop om naar de AVG website (<u>www.avg.com</u>) te gaan. Klikt u op het pijltje naast het logo, dan wordt een menu geopend met de volgende items:
 - Werkbalkinfo een koppeling naar de introductiepagina van de AVG
 Werkbalk Beveiliging met aanvullende informatie over de bescherming die de werkbalk biedt
 - o AVG 8.0 starten de interface openen van AVG 8
 - Opties een dialoogvenster openen voor het comfigureren van de AVG Werkbalk Beveiliging, waarin u de instellingen naar wens kunt aanpassen; het dialoogvenster heeft twee tabbladen:
 - Algemeen dit tabblad is verdeeld in twee secties: Knoppen en Indicaties.

In de sectie **Knoppen** kunt u opgeven welke knoppen op de AVG Werkbalk Beveiliging **moeten worden weergegeven. Standaard worden alle knoppen weergegeven.**

In de sectie *Indicaties* bepaalt u welke indicaties moeten worden



weergegeven voor uw zoekresultaten. Standaard worden alle indicaties weergegeven, maar u kunt sommige verbergen (*als u zoekt met Yahoo! Search, worden alleen veilige resultaten weergegeven*).

Options		×
General	Advanced	
Buttons		
Custom	ize which buttons are	e shown on AVG Toolbar:
🔽 Surf	Safe	
🗹 Sea	rch Shield	
🗹 AVG	i Info	
🗌 🗌 Get	More!	
Ratings		
Custom search	ize which type of ratir results pages:	ings Search Shield will show on the
🗹 Safe	e (Green)	
🗹 Que	stionable (Yellow)	
🗹 Risk	y (Orange)	
🗹 Unk	nown (Gray)	Learn more
		OK Cancel

Geavanceerd - op dit tabblad kunt u de beschermingsfuncties van de AVG Werkbalk Beveiliging aanpassen. Standaard zijn zowel <u>AVG Search-Shield</u> als <u>AVG Active Surf-Shield</u> ingeschakeld.

Options				X
General	Advanced			
Advan	iced options -			
Select from th	the protection le listed below	ns you would like to use with :	hin the Toolbar	
	AVG Search-	Shield		
	AVG Active 9	urf-Shield		
<u>Learn r</u>	nore	OK Car	ncel	

Update - controleren of er nieuwe updates beschikbaar zijn voor de AVG Werkbalk Beveiliging



Help - opties voor het openen van het Help-bestand, het opnemen van contact met de <u>AVG Technische ondersteuning</u> en de weergave van details van de huidige versie van de werkbalk

- **Yahoo! zoekvak** handige en veilige manier om te zoeken op internet met Yahoo! Search. Typ een woord of een zin in het zoekvak en klik op **Zoeken** om rechtstreeks te zoeken op de Yahoo! server, ongeacht welke pagina op dat moment wordt weergegeven. Aan het zoekvak is bovendien een keuzelijst gekoppeld met eerdere zoekopdrachten. De resultaten van zoekopdrachten die u via dit zoekvak opgeeft, worden geanalyseerd met AVG Search-Shield_.
- Knop AVG Active Surf-Shield een aan/uit-knop waarmee u <u>AVG Active</u> <u>Surf-Shield</u> in- en uitschakelt
- Knop AVG Search-Shield een aan/uit-knop waarmee u <u>AVG Search-Shield</u> in- en uitschakelt
- Knop AVG Info een koppeling naar belangrijke beveiligingsinformatie op de website van AVG (_)



9. AVG Geavanceerde instellingen

Het dialoogvenster voor een geavanceerde configuratie van **AVG 8.0 Anti-Virus** is het dialoogvenster **Geavanceerde AVG instellingen**. Het venster is onderverdeeld in twee secties: het linker deelvenster met een boomstructuur voor navigatie naar de opties voor programmaconfiguratie. Selecteer het onderdeel (*of een deel daarvan*) waarvoor u de configuratie wilt wijzigen om het bijbehorende dialoogvenster in het rechter deelvenster te openen.

9.1. Weergave

De eerste optie in de navigatiestructuur, **Weergave**, verwijst naar de algemene instellingen voor de <u>AVG gebruikersinterface</u> en een paar basisinstellingen voor de manier waarop de toepassing werkt:

🛃 Geavanceerde instellingen AVG	
Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield UinkScanner Scans Schema's E-mailscanner Resident Shield Update Extern beheer	Taalselectie Mijzigingen in de taal worden doorgevoerd na een herstart van de toepassing. Taal gebruikersinterface selecteren: Nederlands Image: Systeemvakmaldingen over updates weergeven. Image: Systeemvakmeldingen over updates weergeven. Image: Systeemvakmeldingen over scannen weergeven. Image: Systeemvakmeldingen over scannen weergeven. Image: Systeemvakmeldingen over scannen weergeven. Image: Systeemvakmeldingen over statuswijziging van onderdelen weergeven. Image: Systeemvakmeldingen met betrekking tot Firewallweergeven. Image: Systeemvakmeldingen met betrekking tot E-mailscanner weergeven. Image: Systeemvakmeldingen met betrekking tot E-mailscanner weergeven. Image: Systeemvakmeldingen met betrekking tot E-mailscanner weergeven. Image: Systeemvakmeldingen met betrekking tot E-mailscanner weergeven.
Standaard	Ok Annuleren Toepassen



Taalselectie

In de sectie **Taalselectie** kunt u in de vervolgkeuzelijst een taal selecteren; die taal wordt dan overal in de <u>AVG Gebruikersinterface</u> toegepast. In het vervolgkeuzemenu staan alleen de talen die u tijdens de <u>installatieprocedure</u>hebt geselecteerd (zie hoofdstuk <u>Aangepaste installatie - Onderdelen selecteren</u>). Voor het voltooien van de procedure om over te stappen op een andere taal, zult u de gebruikersinterface opnieuw moeten starten; ga als volgt te werk:

- Selecteer de gewenste taal voor de toepassing en bevestig uw selectie door op de knop *Toepassen* te klikken (in de rechterbenedenhoek)
- Klik op de knop OK om het dialoogvenster Geavanceerde instellingen AVG te sluiten
- U kunt de <u>AVG Gebruikersinterface</u> afsluiten in het <u>systeemmenu</u> via de optie <u>Bestand/Afsluiten</u>
- Open de <u>AVG gebruikersinterface</u> op een van de volgende manieren: dubbelklik op het <u>systeemvakpictogram van AVG</u>, dubbelklik op het pictogram van AVG op het bureaublad, of kies *Start/Alle programma's/AVG 8.0/AVG gebruikersinterface* (zie hoofdstuk *Toegang tot gebruikersinterface*). In de gebruikersinterface zal daarna de nieuwe taal worden gebruikt.

Ballontekstwaarschuwingen

In dit gedeelte kunt u de weergave van ballontekstwaarschuwingen over de status van de toepassing in- en uitschakelen. Standaard worden de ballontekstwaarschuwingen weergegeven en het is raadzaam die instelling aan te houden! De ballontekstwaarschuwingen geven informatie wanneer er iets in de status van een onderdeel verandert en verdienen daarom aandacht!

Als u echter om de een of andere reden de weergave van ballontekstwaarschuwingen wilt onderdrukken, of als u alleen bepaalde ballontekstwaarschuwingen wilt weergeven (van bijvoorbeeld een bepaald AVG onderdeel), kunt u uw voorkeuren opgeven door de volgende opties in- of uit te schakelen:

• **Systeemvakmeldingen weergeven** - standaard staat een vinkje bij deze optie (*ingeschakeld*) en worden Systeemvakmeldingen weergegeven. Schakel dit selectievakje uit als u in het geheel geen gebruik wilt maken van Systeemvakmeldingen. Als u de optie inschakelt, kunt u nader bepalen welke meldingen u wilt weergeven:



- Systeemvakmeldingen over <u>updates</u> weergeven maak een keuze of u meldingen van het starten, de voortgang en het voltooien van de AVG update wilt weergeven;
- Systeemvakmeldingen over <u>scannen</u> weergeven maak een keuze of u meldingen van het automatisch starten van geplande scans, de voortgang en de resultaten wilt weergeven;
- Systeemvakmeldingen met betrekking tot <u>Resident Shield</u>
 weergeven maak een keuze of u meldingen bij procedures voor het opslaan, kopiëren en openen van bestanden wilt weergeven of niet;
- Systeemvakmeldingen over statuswijziging van onderdelen weergeven - maak een keuze of u informatie over de activiteit/ inactiviteit van een onderdeel of mogelijk daarmee samenhangende problemen wilt weergeven. Bij het rapporteren van de foutstatus van een onderdeel, heeft deze optie hetzelfde effect als de informatieve functie van het systeemvakpictogram (kleurwijzigingen) dat een probleem aangeeft met een AVG onderdeel.

0

 Systeemvakwaarschuwingen die betrekking hebben op de emailscanner weergeven - maak een keuze of informatie over het scannen van alle binnenkomende en uitgaande e-mailberichten moet worden weergegeven.

9.2. Onderhoud

Als u op de optie **Onderhoud** klikt, wordt het dialoogvenster geopend waarin u de parameters kunt instellen voor het onderhoud van de <u>Quarantaine</u>:



9.2.1. Quarantaine

불 Geavanceerde instellingen AVG	
 Weergave Onderhoud Quarantaine PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Consistent Shield Update Extern beheer 	Onderhoud quarantaine Image: Grootte quarantaine beperken Image:
Standaard	Ok Annuleren Toepassen

In het dialoogvenster **Onderhoud quarantaine** kunt u verschillende parameters instellen voor het beheer van objecten die zijn opgeslagen in <u>Quarantaine</u>:

- Grootte Quarantaine beperken geef met behulp van de schuifbalk een maximale grootte op voor <u>Quarantaine</u>. U geeft de grootte op in verhouding met de grootte van de lokale schijf.
- Bestand automatisch verwijderen deze sectie bepaalt hoe lang objecten maximaal worden opgeslagen in <u>Quarantaine</u> (Bestanden verwijderen ouder dan ... dagen) en het aantal bestanden dat maximaal wordt opgeslagen in <u>Quarantaine</u> (Maximumaantal bestanden voor opslaan)



9.3. PUP-uitzonderingen

AVG is in staat om uitvoerbare toepassingen en DLL-bibliotheken te analyseren en detecteren die binnen het systeem mogelijk ongewenst zijn. De gebruiker zal in sommige gevallen bepaalde gedetecteerde ongewenste programma's willen behouden (bijvoorbeeld omdat het programma's betreft die de gebruiker opzettelijk heeft geïnstalleerd). Sommige programma's bevatten adware. Dat is vooral het geval bij gratis programma's. Dergelijke adware wordt door AVG mogelijk gedetecteerd en gerapporteerd als een **Potentieel ongewenst programma (PUP)**. Als u een dergelijk programma niet van uw computer wilt verwijderen, kunt u het desbetreffende programma definiëren als een uitzondering:

🕌 Geavanceerde instellingen AVG					
Weergave Gnderhoud	Potentieel ongewenste programma's - uitzonderingen				
 PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Schema's E-mailscanner Resident Shield Update Extern beheer 	Bestand	n Verwijderen	Checksum		ondering toevoegen
Standaard			Ok	Annuleren	Toepassen

In het dialoogvenster **Uitzonderingen voor mogelijk ongewenste programma's** staat een lijst met eerder als zodanig gedefinieerde en geldige uitzonderingen op mogelijk ongewenste programma's. U kunt uitzonderingen bewerken, verwijderen en toevoegen.



Knoppen

- Bewerken er wordt een nieuw dialoogvenster geopend (*identiek met het dialoogvenster voor het toevoegen van een nieuwe uitzondering, zie hieronder*) voor het bewerken van een eerder gedefinieerde uitzondering, waarin u parameters kunt wijzigen
- **Verwijderen** het geselecteerde item wordt verwijderd uit de lijst met uitzonderingen
- **Uitzondering toevoegen** er wordt een dialoogvenster geopend voor het bewerken van de parameters van een nieuw toe te voegen uitzondering:

불 Uitzon derin	gs definitie
Bestand:	I
Checksum:	
Bestandsinfo:	Extra bestandsinformatie niet beschikbaar.
	Elke locatie - gebruik geen volledig pad
•	Toevoegen Annuleren

- *Bestand* Typ het volledige pad naar het bestand dat u wilt markeren als een uitzondering
- Checksum de unieke "handtekening" van het gekozen bestand. Deze handtekening bestaat uit een automatisch gegenereerde tekenreeks op basis waarvan AVG het gekozen bestand onmiskenbaar van andere bestanden kan onderscheiden. Deze handtekening wordt gegenereerd en weergegeven nadat het bestand is toegevoegd.
- **Bestands info** alle aanvullende informatie die voor het bestand beschikbaar is (*licentie-/versie-informatie, enz.*)
- Elke locatie gebruik geen volledige locatie als u dit bestand alleen op deze specifieke locatie als uitzondering wilt definiëren, schakelt u dit selectievakje niet in



9.4. Web Shield

😹 Geavanceerde instellingen AVG		- 🗆 🗙
Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield Webbescherming Expresberichten LinkScanner Scans E-mailscanner Resident Shield Update Extern beheer	₩ebbescherming Inschakelen Web Shield	
Standaard	Ok Annuleren Toe	passen

In het dialoogvenster **Webbescherming** kunt u maar één optie instellen: als u op de optie **Web Shield inschakelen** klikt, kunt u het hele onderdeel <u>Web Shield</u> in- en uitschakelen (*standaard ingeschakeld*). Voor verdere geavanceerde instellingen voor dit onderdeel verwijzen we u naar de desbetreffende dialoogvensters die in de navigatiestructuur zijn opgenomen.



📸 Geavanceerde instellingen AVG		🔼
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield Expresberichten LinkScanner Scans Schema's F-mailscanner Resident Shield Update Extern beheer 	Webbescherming Archiefbestanden controleren Scannen op bedreigingen door mogelijk ongewenste programma's en spyware Heuristische analyse gebruiken Te scannen poorten 80, 8080, 3128 Maximale grootte te scannen bestand Image: Status of the scannen bestand <t< td=""><td>200 kB</td></t<>	200 kB
Standaard	Ok Annuleren	Toepassen

9.4.1. Webbescherming

In het dialoogvenster **Webbescherming** kunt u de configuratie van het onderdeel aanpassen met betrekking tot het scannen van de inhoud van websites. U kunt de volgende basisopties aanpassen:

- **Webbescherming** met deze optie geeft u op of <u>Web Shield</u> de inhoud van webpagina's moet scannen. Ervan uitgaande dat deze optie is ingeschakeld (*standaard*), kunt u nog de volgende functies in- en uit-schakelen:
 - Archiefbestanden controleren de inhoud van archieven scannen die zijn ingesloten op de webpagina's die u wilt weergeven .
 - Scannen op bedreigingen door Potentieel ongewenste programma's en spyware - potentieel ongewenste programma's scannen (spyware of adware in de vorm van uitvoerbare bestanden) die zijn ingesloten op de webpagina die u wilt weergeven, en scannen op spyware-infecties.



- Heuristische methode gebruiken de inhoud scannen van een weer te geven pagina met behulp van de methode voor <u>heuristische analyse</u> (dynamische emulatie van de instructies van gescande object en in een virtuele computeromgeving).
- Te scannen poorten in dit vak staan de standaard poortnummers voor httpcommunicatie. Als u een afwijkende computerconfiguratie hebt, kunt u de poortnummers naar wens wijzigen.

- Maximale grootte te scannen bestand Als er bestanden zijn inbegrepen op een weer te geven pagina, kunt u de inhoud daarvan ook scannen voordat ze naar uw computer wrden gedownload. Het scannen van grote bestanden neemt echter soms veel tijd in beslag, wat het downloaden van de webpagina aanzienlijk kan vertragen. Met behulp van de schuifbalk kunt u de maximale grootte opgeven van bestanden die nog moeten worden gescand met <u>Web Shield</u>. Zelfs als het gedownloade bestand groter is dan u hebt opgegeven, en dus niet wordt gescand met Web Shield, wordt u nog steeds beschermd: in het geval dat het bestand is geïnfecteerd, zal dat onmiddellijk worden gedetecteerd door <u>Resident Shield</u>.
- *Host/IP/domein uitsluiten* u kunt in het tekstvak de exacte naam van een server typen (of het IP-adres) of een domein dat niet moet worden gescand door <u>Web Shield</u> (sluit dus alleen een host uit waarvan u absoluut zeker weet dat die nooit gevaarlijke webinhoud zou leveren).



📷 Geavanceerde instellingen AVG		
Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield Webbescherming Expresberichten Geavanceerd ICQ Geavanceerd MSN LinkScanner Scans Comparison E-mailscanner Resident Shield Update E-xtern beheer	Instant Messaging Shield ✓ Inschakelen Instant Messaging Shield ✓ ICQ-bescherming ✓ MSN-bescherming	
Standaard	Ok Annuleren To	oepassen

9.4.2. Instant Messaging

In het dialoogvenster **Instant Messaging Shield** kunt u de instellingen van het onderdeel <u>Web Shield</u> bewerken die betrekking hebben op het scannen van expresberichten. Op dit moment worden slechts twee programma's voor expresberichten ondersteund: **ICQ** en **MSN** - schakel het selectievakje in bij de programma's waarvoor Web Shield de online communicatie moet bewaken.

Voor het specificeren van toegestane/geblokkeerde gebruikers kunt u de bij de programma's horende dialoogvensters (*Geavanceerd ICQ, Geavanceerd MSN*) openen en de *Witte lijst* (*lijst met gebruikers die u toelaat voor communicatie*) en de *Zwarte lijst* ((*lijst met gebrukers die moeten worden geblokkeerd*) invullen.



9.5. LinkScanner

🕌 Geavanceerde instellingen AVG		
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield McScanner Scans C Schema's E -mailscanner Resident Shield Update E xtern beheer 	LinkScanner instellingen ✓ AVG Search-Shield inschakelen (herstart van de browser vereist) ✓ AVG Active Surf-Shield inschakelen ✓ Rapportage van websites met exploits naar AVG inschakelen	
Standaard	Ok Annuleren Toepass	en

In het dialoogvenster **Instellingen LinkScanner** kunt u de twee elementaire functies van **LinkScanner** in- en uitschakelen:

- **Safe Search inschakelen** (*standaard ingeschakeld*): pictogrammen met een indicatie bij de resultaten van zoekopdrachten met Google, Yahoo en MSN, die wordt verkregen door vooraf de inhoud van sites die door de zoekmachine worden geretourneerd, te controleren. De functie ondersteunt de browsers Internet Explorer en Firefox.
- **Safe Surf inschakelen** (standaard ingeschakeld): actieve (real-time) bescherming tegen websites met exploits op het moment dat ze worden geadresseerd. Als zodanig bekend staande kwaadaardige sites en de inhoud met exploits worden geblokkeerd op het moment dat de gebruiker ze adresseert in de browser (of met een andere toepassing die HTTP gebruikt).



 Rapportage van websites met exploits naar AVG inschakelen - schakel dit selectievakje in voor rapportage van exploits en kwaadaardige sites waarmee gebruikers via Safe Surf of Safe Search zijn geconfronteerd, naar de database waarin gegevens worden verzameld over kwaadaardige praktijken op internet.

9.6. Scans

De geavanceerde scaninstellingen zijn onderverdeeld in drie categorieën die verwijzen naar specifieke typen scans die door de leverancier van de software zijn gedefinieerd:

- <u>Volledige computer scannen</u> vooraf gedefinieerde standaardscan waarbij de hele computer wordt gescand
- <u>Bepaalde mappen of bestanden scannen</u> vooraf gedefinieerde standaardscan waarbij een geselecteerd gedeelte van de computer wordt gescand
- <u>Scannen in Windows Verkenner</u> scannen van een specifiek object dat direct in Windows Verkenner is geselecteerd

9.6.1. De hele computer scannen

Met de optie **De hele computer scannen** opent u een dialoogvenster waarin u de parameters kunt aanpassen van één van de vooraf door de leverancier gedefinieerde scans, namelijk **Volledige computer scannen**:



Covariant en la constituir de scarragoorten instellen Covariant en la constituir de scarragoorten instellen Covariant en la constituir de scarragoorten instellen
Standaard Ok Annuleren Toepassen

Scaninstellingen

In de sectie **Scaninstellingen** staat een lijst met scanparameters die u kunt in- en uit-schakelen:

- **Infecties automatisch herstellen/verwijderen** als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch hersteld kan worden, of als u besluit deze optie uit te schakelen, wordt u bij detectie van een virus gewaarschuwd en zult u op dat moment moeten besluiten wat u wilt doen met de gedetecteerde infectie. Het is raadzaam het geïnfecteerde bestand te verplaatsen naar de guarantaine.
- **Potentieel ongewenste programma's scannen** deze parameter bepaalt de werking van de functie <u>Anti-Virus</u> die <u>detectie van potentieel ongewenste</u>



programma's mogelijk maakt (*spyware of adware in de vorm van uitvoerbare bestanden*), zodat ze kunnen worden geblokkeerd of verwijderd;

- **Scannen naar cookies** deze parameter van het onderdeel <u>Anti-Spyware</u> bepaalt of cookies bij het scannen moeten worden gedetecteerd; (*HTTPcookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*)
- **Scannen in archieven** met deze parameter bepaalt u of alle bestanden moeten worden gescand, ook die bestanden die zijn gecomprimeerd in archiefbestanden, bijv. ZIP, RAR, enz.
- **Heuristische methode gebruiken** heuristische analyse (*dynamische emulatie van de instructies van gescande object en in een virtuele computeromgeving*) wordt gebruikt als één van de methoden voor virusdetectie als de parameter is ingeschakeld;
- **Systeemgebieden scannen** bij het scannen worden ook de systeemgebieden van de computer betrokken;
- Alleen infecteerbare bestanden scannen als deze optie is ingeschakeld, worden bestanden die niet geïnfecteerd kunnen raken, niet bij het scannen betrokken. Dat kunnen bijvoorbeeld bestanden zijn met onopgemaakte tekst, of andere niet-uitvoerbare bestanden.
- **Scannen naar rootkits** schakel dit selectievakje in als u rootkitdetectie wilt opnemen in uw scan van de hele computer. Rootkitdetectie is afzonderlijk beschikbaar in het onderdeel <u>Anti-Rootkit</u>.

Prioriteit scanproces

In het gedeelte **Prioriteit scanproces** kunt u nader specificeren hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op o.a. het werkgeheugen van uw computer (systeembronnen). Standaard is deze optie ingesteld op een gemiddeld niveau van gebruik van systeembronnen. Als u sneller wilt scannen, duurt het scannen minder lang, maar wordt een aanzienlijk groter beslag gelegd op o.a. het werkgeugen tijdens het scannen, zodat andere activiteiten op de computer trager zullen verlopen (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt echter het beroep op o.a. het werkgeheugen ook verkleinen door te kiezen voor een langere scanduur.


Aanvullende scanrapporten instellen...

Klik op de koppeling **Aanvullende scanrapporten instellen...** om een afzonderlijk dialoogvenster te openen dat **Scanrapporten** heet, waarin u selectievakjes kunt inschakelen voor resultaten die moeten worden weergegeven:

🕌 Scanrapp	orten 🛛 🔀	
Scanrap	porten	
Rapport i	net wachtwoord beschermde archiefbestanden	
Rapport met wachtwoord beschermde documenten		
Rapport 1	/ergrendelde bestanden	
📃 Rapport I	bestanden met een macro	
Rapport 1	/erborgen extensies	
•	0k Annuleren	

9.6.2. Shell-extensie scannen

Net als bij het vorige item **De hele computer scannen** kunt u ook bij dit item **Scan van Shell-extensie** verschillende opties instellen om de vooraf door de leverancier gedefinieerde scan aan te passen. Dit keer heeft de configuratie betrekking op het scannen van specifieke objecten direct vanuit Windows Verkenner (Shell-uitbreiding), zie hoofdstuk <u>Scannen in Windows Verkenner</u>:



Geavanceer de instellingen AV	G
Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans De hele computer scannen Scan van Shell-extensie Bepaalde mappen of bestar Schema's E-mailscanner Resident Shield Update Extern beheer	Scaninstellingen Infecties automatisch herstellen/verwijderen Scannen op bedreigingen door mogelijk ongewenste programma's en spyware Scannen naar cookies Scannen in archieven Heuristische methode gebruiken Scansysteemomgeving Alleen infecteerbare bestanden scannen Scannen naar rootkits Prioriteit scanproces Automatische scan Aanvullende scanrapporten instellen
Standaard	Ok Annuleren Toepassen

De lijst met beschikbare parameters is dezelfde als die van <u>De hele computer</u> <u>scannen</u>. De standaardinstellingen verschillen echter wel: bij **De hele computer** scannen zijn de meeste parameters geselecteerd, terwijl bij **Scan van Shell**extensie (<u>Scannen in Windows Verkenner</u>) alleen de relevante parameters zijn ingeschakeld.

9.6.3. Bepaalde mappen of bestanden scannen

Het dialoogvenster voor het bewerken van de instellingen voor **Bepaalde mappen of bestanden scannen** is identiek aan het dialoogvenster voor het bewerken van instellingen voor <u>Volledige computer scannen</u>. Alle configuratie-opties zijn hetzelfde, al zijn de standaardinstellingen voor <u>Volledige computer scannen</u> strikter:



Ceavanceer de instellingen AVG	
 Scans De hele computer scannen Scan van Shell-extensie Eepaalde mappen of bestanden scannen Scansysteemomgeving Alleen infecteerbare bestanden scannen Scannen naar rootkits Prioriteit scanproces Automatische scan Aanvullende scanrapporten instellen	•
Standaard Ok Annuleren Toepassen	

Alle parameters die u instelt in dit configuratiedialoogvenster hebben alleen betrekking op het scannen met de optie **Bepaalde mappen of bestanden scannen**! Als u de optie **Scannen naar rootkits** in dit dialoogvenster inschakelt, wordt alleen een snelle test op rootkits uitgevoerd, dat wil zeggen dat alleen in de geselecteerde gebieden op rootkits wordt gescand.

Opmerking: Zie het hoofdstuk <u>Geavanceerde instellingen AVG / Scans /</u> <u>Volledige computer scannen</u> voor een beschrijving van specifieke parameters.

9.7. Schema's

In het gedeelte *Schema's* kunt u de standaardinstellingen bewerken van:

- <u>Schema volledige computer scannen</u>
- Updateschema virusdatabase



- <u>Updateschema programma</u>
 - Updateschema Anti-Spam

9.7.1. Geplande scan

U kunt op drie tabbladen parameters instellen voor het schema van de geplande scan (of een nieuw schema opstellen):

😹 Geavanceerde instellingen AVG						
Geavanceer de instellingen AVG	Schema-instellingen Hoe er gesca Naam Schema wordt uitgevoerd Uitvoeren elke: Uitvoeren op specifiek tijdstip: Gebaseerd op handeling: Geavanceerde schemaopties Uitvoeren bij het opstarten var Uitvoeren zelfs als de computei Taakinstellingen Veze taak inschakelen	nd moet worden Geplande scan 1 🔅 U Elke dag Bij het opstarte n de computer als r in energiebespa	Wat er gescar ur (uren) n van de c taak is overge ringsmodus is	12:00 4 slagen	orden	ni[]
Standaard		lk	Annuleren		Тоера	assen

Op het tabblad **Schema-instellingen** geeft u de scan die u maakt, een naam. Typ de naam in het tekstvak bij **Naam**. Probeer korte, maar niettemin veelzeggende namen te gebruiken voor scans zodat u ze achteraf te midden van andere scans kunt herkennen.

Voorbeeld: het is niet handig om een scan als naam "nieuwe scan" of "mijn scan" te



geven, omdat die namen geen aanduiding geven van wat de scan doet. Een naam als "Scan systeemgebieden" is daarentegen een voorbeeld van een veelzeggende naam voor een scan. Bovendien is het niet nodig om in de naam van de scan aan te geven of de hele computer wordt gescand of alleen een selectie van mappen en bestanden uw eigen scans zijn altijd aangepaste versies van het type <u>Bepaalde mappen of</u> <u>bestanden scannen</u>.

In dit dialoogvenster kunt u daarnaast nog de volgende parameters instellen:

- Schema wordt uitgevoerd geef een tijdsinterval op waarmee de nieuwe geplande scan moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als steeds terugkerende scan die na verloop van een bepaalde tijd (Uitvoeren elke ...) moet worden uitgevoerd, als scan die op een bepaalde datum en een bepaald tijdstip (Uitvoeren op specifiek tijdstip ...) moet worden uitgevoerd, of door een gebeurtenis te definiëren waaraan het uitvoeren van de scan moet worden gekoppeld (Actie bij het opstarten van de computer).
- **Geavanceerde schema-opties** in deze sectie kunt u bepalen onder welke omstandigheden de scan wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.
- **Taakinstellingen** in deze sectie kunt u het selectievakje **Deze taak inschakelen** uitschakelen als u de geplande scan tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient.



🕌 Geavanceerde instellingen AVG		_ 🗆 🔀
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Schema's Geplande scan Updateschema virusdatabase Updateschema erorgramma E-mailscanner Resident Shield Update Extern beheer 	Schema-instellingen Hoe er gescand moet worden Wat er gescand moet worden Infecties automatisch herstellen/verwijderen Scannen op bedreigingen door mogelijk ongewenste programma's en spyware Scannen naar cookies Scannen naar cookies Scannen in archieven Heuristische methode gebruiken Scansysteemongeving Alleen infecteerbare bestanden scannen Scannen naar rootkits Scannen naar rootkits Prioriteit scanproces Automatische scan Aanvullende scanrapporten instellen Aanvullende scaninstellingen	
Standaard	Ok Annuleren	Toepassen

Op het tabblad**Hoe er gescand moet worden** staat een lijst met scanparameters die kunnen worden in- en uit-geschakeld. Standaard zijn de meeste parameters ingeschakeld en wordt de desbetreffende functie gebruikt bij het scannen. We raden u aan deze vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om deze instellingen te wijzigen:

- **Infecties automatisch herstellen/verwijderen** (standaard ingeschakeld): als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch hersteld kan worden, of als u besluit deze optie uit te schakelen, wordt u bij detectie van een virus gewaarschuwd en zult u op dat moment moeten besluiten wat u wilt doen met de gedetecteerde infectie. Het is raadzaam het geïnfecteerde bestand te verplaatsen naar de Quarantaine.
- **Potentieel ongewenste programma's scannen** (standaard ingeschakeld): deze parameter bepaalt de werking van de functie <u>Anti-Virus</u> die <u>detectie van</u> <u>potentieel ongewenste programma's</u> mogelijk maakt (*spyware of adware in de*



vorm van uitvoerbare bestanden), zodat ze kunnen worden geblokkeerd of verwijderd;

- **Scannen naar cookies** (standaard ingeschakeld): deze parameter van het onderdeel <u>Anti-Spyware</u> bepaalt of cookies bij het scannen moeten worden gedetecteerd (; (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes);*
- **Scannen binnen archieven** (*standaard ingeschakeld*): deze parameter bepaalt of bij het scannen alle bestanden moeten worden gecontroleerd, ook als die op de een of andere manier zijn gecomprimeerd, bijv. ZIP, RAR, ...
- *Heuristische methode gebruiken* (*standaard ingeschakeld*): heuristische analyse (*dynamische emulatie van de instructies van gescande object en in een virtuele computeromgeving*) wordt gebruikt als één van de methoden voor virusdetectie als de parameter is ingeschakeld;
- Systeemgebieden scannen (standaard ingeschakeld): als de parameter is ingeschakeld worden ook de systeemgebieden gescand;
- Alleen infecteerbare bestanden scannen (standaard uitgeschakeld): als u deze parameter inschakelt, worden bestanden die niet kunnen worden geïnfecteerd, niet gescand. Dat kunnen bijvoorbeeld bestanden zijn met onopgemaakte tekst, of andere niet-uitvoerbare bestanden.
- Scannen naar rootkits schakel dit selectievakje in als u rootkitdetectie wilt opnemen in uw scan van de hele computer. Rootkitdetectie is afzonderlijk beschikbaar in het onderdeel <u>Anti-Rootkit</u>.

In het gedeelte **Prioriteit scanproces** kunt u nader specificeren hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op o.a. het werkgeheugen van uw computer (systeembronnen). Standaard is deze optie ingesteld op een gemiddeld niveau van gebruik van systeembronnen. Als u sneller wilt scannen, duurt het scannen minder lang, maar wordt een aanzienlijk groter beslag gelegd op o.a. het werkgeheugen tijdens het scannen, zodat andere activiteiten op de computer trager zullen verlopen (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt echter het beroep op o.a. het werkgeheugen ook verkleinen door te kiezen voor een langere scanduur.

Klik op de koppeling **Aanvullende scanrapporten instellen...** om een afzonderlijk dialoogvenster te openen dat **Scanrapporten** heet, waarin u selectievakjes kunt inschakelen voor resultaten die moeten worden weergegeven:





Klik op **Aanvullende scaninstellingen...** om een nieuw dialoogvenster **Opties voor uitschakelen computer**te openen waarin u kunt opgeven of de computer automatisch moet worden afgesloten zodra het scannen is voltooid. Als u die optie bevestigt (**Computer afsluiten na voltooien van scanproces**), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (**Geforceerd afsluiten als de computer vergrendeld is**).







Op het tabblad **Wat er gescand moet worden** kunt u opgeven welke scan moet worden uitgevoerd: <u>een scan van de hele computer</u> of <u>een scan van specifieke</u> <u>bestanden of mappen</u>. Als u kiest voor het scannen van specifieke bestanden of mappen, wordt de in het onderste deel van het dialoogvenster weergegeven mapstructuur actief, zodat u mappen kunt opgeven die moeten worden gescand.



9.7.2. Updateschema virusdatabase

Elementaire planning van updates voor de virusdatabase wordt beheerd met het onderdeel <u>Updatebeheer</u>. In dat dialoogvenster kunt u gedetailleerd parameters instellen voor het updateschema:

Op het tabblad **Schema-instellingen** geeft u het updateschema, voor de virusdatabase, dat u maakt een naam. Typ de naam in het tekstvak bij **Naam**. Probeer korte, maar niettemin veelzeggende namen te gebruiken voor updateschema's zodat u ze achteraf te midden van andere schema's kunt herkennen.

Schema wordt uitgevoerd - geef een tijdsinterval op waarmee het nieuwe virusdatabase-updateschema moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als steeds terugkerende update die na verloop van een bepaalde tijd (*Uitvoeren elke ...*) moet worden uitgevoerd, als update die op een bepaalde datum en een bepaald tijdstip (*Uitvoeren op specifiek tijdstip ...*) moet worden uitgevoerd, of door een gebeurtenis te definiëren waaraan het uitvoeren van de update moet worden gekoppeld (



Actie bij het opstarten van de computer).

- Geavanceerde schema-opties in deze sectie kunt u bepalen onder welke omstandigheden de virusdatabase-update wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.
- **Taakinstellingen** in deze sectie kunt u het selectievakje **Deze taak inschakelen** uitschakelen als u de geplande update voor de virusdatabase tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient.
- **Overige update-instellingen** schakel dit selectievakje in om ervoor te zorgen dat, als de internetverbinding verbroken wordt, en de updateprocedure mislukt, die onmiddellijk weer opnieuw zal worden uitgevoerd na herstel van de internetverbinding.

🧧 Geavanceer de instellingen AVG				_ 🗆 🔀
Geavanceer de instellingen AVG Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Comparise Updateschema virusdatabase Updateschema programma Resident Shield Update E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner E-mailscanner Standaard	Schema-instellingen Naam Schema wordt uitgevoerd Uitvoeren elke: Uitvoeren op specifiek tijdstip: Gebaseerd op handeling: Geavanceerde schemaopties Uitvoeren bij het opstarten var Uitvoeren zelfs als de computer Taakinstellingen Deze taak inschakelen	Updateschema programma 12 💽 Uur (uren) Elke dag Bij het opstarten van de c n de computer als taak is over r in energiebesparingsmodus	Sign Sign Sign Sign Sign Sign Sign Sign	() 10:00 () minuten []
	✓ Deze taak inschakelen Overige update-instellingen ○ Voer de update opnieuw uit zoo	dra de internetverbinding bes	achikbaar is,	Toepassen

9.7.3. Updateschema programma



Op het tabblad **Schema-instellingen** geeft u het programma-updateschema dat u maakt, een naam. Typ de naam in het tekstvak bij **Naam**. Probeer korte, maar niettemin veelzeggende namen te gebruiken voor updateschema's zodat u ze achteraf te midden van andere schema's kunt herkennen.

- Schema wordt uitgevoerd geef een tijdsinterval op waarmee de nieuwe programma-update moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als steeds terugkerende update die na verloop van een bepaalde tijd (*Uitvoeren elke ...*) moet worden uitgevoerd, als update die op een bepaalde datum en een bepaald tijdstip (*Uitvoeren op specifiek tijdstip ...*) moet worden uitgevoerd, of door een gebeurtenis te definiëren waaraan het uitvoeren van de update moet worden gekoppeld (*Actie bij het opstarten van de computer*).
- Geavanceerde schema-opties in deze sectie kunt u bepalen onder welke omstandigheden de programma-update wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.
- **Taakinstellingen** in deze sectie kunt u het selectievakje **Deze taak inschakelen** uitschakelen als u de programma-update tijdelijk niet wilt uitvoeren en weer inschakelen als de noodzaak daarvoor zich aandient.
- **Overige update-instellingen** schakel dit selectievakje in om ervoor te zorgen dat, als de internetverbinding verbroken wordt, en de updateprocedure mislukt, die onmiddellijk weer opnieuw zal worden uitgevoerd na herstel van de internetverbinding.



🛃 Geavanceerde instellingen AVG 📃 🗖 🔀				
Geavanceer de instellingen AVG	Schema-instellingen Naam Schema wordt uitgevoerd Uitvoeren elke: Uitvoeren op specifiek tijdstip: Gebaseerd op handeling: Gebaseerd op handeling:	Antispam-updateschema 2 Uur (uren) Elke dag Bij het opstarten van de c	 ✓ 9:00 ✓ 3 	
Geplande scan Geplande scan Geplande scan Geplande scan Geplande scan Geplande schema virusdatabase Geplande schema programma Geplande schema Geplande schema virusdatabase Geplande schema programma Geplande schema Gep	Geavanceerde schemaopties Uitvoeren bij het opstarten var ✓ Uitvoeren zelfs als de computer Taakinstellingen ✓ Deze taak inschakelen Overige update-instellingen Voer de update opnieuw uit zoo	n de computer als taak is ove r in energiebesparingsmodus dra de internetverbinding be	ergeslagen : is schikbaar is.	
Standaard		Ok	Annuleren	Toepassen

9.7.4. Anti-Spam updateschema

Elementaire planning van **Anti-Spam-**updates wordt beheerd met het onderdeel <u>Updatebeheer</u>. In dat dialoogvenster kunt u gedetailleerd parameters instellen voor het updateschema:

Op het tabblad **Schema-instellingen** geeft u het **Anti-Spam**-updateschema dat u maakt, een naam. Typ de naam in het tekstvak bij **Naam**. Probeer korte, maar niettemin veelzeggende namen te gebruiken voor updateschema's zodat u ze achteraf te midden van andere schema's kunt herkennen.

 Schema wordt uitgevoerd - geef een tijdsinterval op waarmee het nieuwe Anti-Spam-updateschema moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als steeds terugkerende Anti-Spamupdate die na verloop van een bepaalde tijd (Uitvoeren elke ...) moet worden uitgevoerd, als update die op een bepaalde datum en een bepaald tijdstip (Uitvoeren op specifiek tijdstip ...) moet worden uitgevoerd, of door een gebeurtenis te definiëren waaraan het uitvoeren van de update moet



worden gekoppeld (**Actie bij het opstarten van de computer**).

- Geavanceerde schema-opties in deze sectie kunt u bepalen onder welke omstandigheden de Anti-Spam-update wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.
- Taakinstellingen in deze sectie kunt u het selectievakje Deze taak inschakelen uitschakelen als u de geplande Anti-Spam-update tijdelijk niet wilt uitvoeren, en weer inschakelen als de noodzaak daarvoor zich aandient.
- **Overige update-instellingen** schakel dit selectievakje in om ervoor te zorgen dat, als de internetverbinding onderbroken wordt en de **Anti-Spam**-updateprocedure mislukt, die onmiddellijk weer opnieuw zal worden uitgevoerd na herstel van de internetverbinding.



9.8. E-mailscanner

🕌 Geavanceerde instellingen AVG	
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Schema's Emailscanner Certificatie Mailfiltering Logboeken en resultaten Servers Resident Shield Update Extern beheer 	E-mail scannen Ø Binnenkomende e-mail controleren E-mail certificeren Alleen met bijlagen Alleen met bijlagen Onderwerp wijzigen van met virus besmette berichten ****VIRUS**** Eigenschappen scannen Ø Heuristische methode gebruiken Ø Scannen op bedreigingen door mogelijk ongewenste programma's en spyware Ø Scannen in archieven Rapportage emailbijlagen Rapport met wachtwoord beschermde archiefbestanden Rapport bestanden met een macro Rapport Verborgen extensies Verplaats gerapporteerde bijlagen naar Quarantaine (alleen binnenkomende e-mails)
Standaard	Ok Annuleren Toepassen

Het dialoogvenster *E-mailscanner* is onderverdeeld in drie secties:

- *E-mail scannen* in deze sectie maakt u een keuze of u alle binnenkomende/ uitgaande e-mail wilt scannen, en of u aan alle e-mail een certificaat wilt koppelen of alleen aan e-mail met een bijlage (e-*mail virusvrij wordt niet ondersteund in HTML/RTF-opmaak*). U kunt daarnaast aangeven of het onderwerp van berichten die mogelijke virussen bevatten, door AVG moet worden gewijzigd. Schakel het selectievakje *Onderwerp wijzigen van met virus besmette berichten* in en wijzig eventueel de tekst (*de standaardtekst is* ****VIRUS****).
- **Scaneigenschappen** geef op of u de methode voor <u>heuristische analyse</u> wilt gebruiken bij het scannen (**Heuristische analyse gebruiken**), of u wilt scannen op de aanwezigheid van <u>Potententieel ongewenste programma's</u> (



Potentieel ongewenste programma's scannen) en of archieven moeten worden gescand (**Scannen in archieven**).

 Rapportage e-mailbijlagen - geef op of u via e-mail op de hoogte wilt worden gesteld van de detectie van met een wachtwoord beveiligde archieven, met een wachtwoord beveiligde documenten, bestanden die macro's bevatten en/of bestanden met verborgen extensies die als bijlagen aan gescande e-mail zijn gekoppeld. Geef, als bij het scannen een dergelijk bericht wordt gedetecteerd, op of het geïnfecteerde object moet worden verplaatst naar de <u>Quarantaine</u>.

9.8.1. Certificatie

In het dialoogvenster **Certificatie** kunt u precies opgeven wat moet worden weergegeven in de certificatietekst, en in welke taal. U geeft dit afzonderlijk op voor **binnenkomende e-mail** en **uitgaande e-mail**.



9.8.2. Mailfiltering

불 Geavanceer de instellingen AVG		
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Schema's E-mailscanner Certificatie Malifitering Logboeken en resultaten Servers Resident Shield Update Extern beheer 	Bijlagefilter Bijlagen verwijderen Alle uitvoerbare bestanden verwijderen Alle documenten verwijderen Bestanden met de volgende extensies verwijderen:	
Standaard	Ok Annuleren To	epassen

In het dialoogvenster **Bijlagefilter** kunt u parameters instellen voor het scannen van bijlagen bij e-mailberichten. Standaard is de optie **Bijlagen verwijderen** uitgeschakeld. Als u besluit die functie in te schakelen, worden alle bijlagen bij emailberichten die worden herkend als geïnfecteerd of potentieel gevaarlijk, automatisch verwijderd. Als u wilt specificeren dat bepaalde typen bijlagen moeten worden verwijderd, schakelt u één van de volgende opties in:

- Alle uitvoerbare bestanden verwijderen alle bestanden met de extensie exe worden verwijderd
- *Alle documenten verwijderen* alle bestanden met de extensie doc worden verwijderd
- **Bestanden met de volgende extensies verwijderen** alle bestanden met de nader te specificeren extensies worden verwijderd



📑 Geavanceerde instellingen AVG		
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield UnkScanner Scans Schma's E-mailscanner Certificatie Malifitiering Goboeken en resultaten Servers Resident Shield Update Extern beheer 	Onderhoud logboeken Oaglogboeken Maandlogboeken Automatische logboeken Maximale grootte logbestanden: Omer Drempel logniveau: Gemiddeld Map voor het opslaan van logbestanden C:\Documents and Settings\All Users\Application Data\avg8\Emc\Log	MB
Standaard	Ok Annuleren T	oepassen

9.8.3. Logboeken en resultaten

In het dialoogvenster dat u opent met de optie *Logboeken en resultaten* kunt u parameters opgeven voor het onderhoud van scanresultaten van e-mail. Het dialoogvenster is onderverdeeld in een aantal secties:

- **Onderhoud logboeken** hier kunt u opgeven of u de gegevens van het scannen van e-mail dagelijks, wekelijks, maandelijks,... wilt opslaan, en bovendien hoe groot het logbestand maximaal mag zijn (*in MB*)
- **Drempel logniveau** standaard is het gemiddelde niveau ingesteld u kunt een lager niveau kiezen (*registreren van elementaire verbindingsinformatie*) of een hoger niveau (*registreren van al het verkeer*)
- *Map voor het opslaan van logbestanden* hier kunt u de locatie van het logbestand opgeven



9.8.4. Servers

In de sectie **Servers** kunt u parameters wijzigen voor de servers van het onderdeel *E-mailscanner*, of een nieuwe server installeren voor binnenkomende en uitgaande e-mail: klik met de rechtermuisknop op POP3 (*binnenkomende mail*) of SMTP (*uitgaande mail*) om een snelmenu te openen, waarin u de optie *Nieuwe server* kunt selecteren.

😹 Geavanceerde instellingen AVG			
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Certificatie Malifiltering Logboeken en resultaten Servers POP3 AutoPOP3:10110 SMTP Resident Shield Update Extern beheer 	POP3 Servernaam AutoPOP3 Type aanmelding Automatisch GEBRUIKER/COMPUTER Vaste host Aanvullende instellingen Lokale poort (gebruikt in e-mailclient): APOP gebruiken indien beschikbaar Verbinding: Instellingen voor POP3 server e-mail Oorspronkelijk Activering POP3 server e-mailclient Activeer deze server en gebruik hem	Normaal ilclient voor het ontvangen van e-mail.	10110
Standaard		Ok Annuleren	Toepassen

In dit dialoogvenster (geopend met **Servers / POP3**) kunt u een nieuwe **Emailscanner**-server instellen die gebruikmaakt van het POP3-protocol voor binnenkomende e-mail:

• **POP3-servernaam** - Typ de naam van de server of handhaaf de standaardnaam AutoPOP3



- *Type aanmelding* bepaalt de methode voor het vaststellen van de mailserver die wordt gebruikt voor binnenkomende e-mailberichten:
 - Automatisch Aanmelding wordt automatisch uitgevoerd, afhankelijk van uw e-mailclientinstellingen.
 - GEBRUIKER/COMPUTER de eenvoudigste en meest gebruikte wijze om de doelmailserver te bepalen is de proxymethode. U gebruikt deze methode door de naam of het adres (of ook de poort) op te geven als deel van de aanmeldingsnaam van de gebruiker voor de specifieke mailserver. U scheidt de gegevens met het teken /. Zo gebruikt u user1/ pop.acme.com:8200 voor de aanmeldingsnaam voor de account user1 op de server pop.acme.com en de poort 8200.
 - Vaste host In dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. De aanmeldingsnaam blijft hetzelfde. U kunt een domeinnaam gebruiken (bijvoorbeeld pop.acme.com), evenals een IP-adres (bijvoorbeeld 123.45.67.89). Als de mailserver een niet-standaard poort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingsteken (bijvoorbeeld pop.acme.com:8200). De standaardpoort voor POP3-communicatie is 110.
 - Aanvullende instellingen Meer gedetailleerde parameters opgeven:
 - Lokale poort de poort waarop de communicatie van de mailtoepassing mag worden verwacht. U moet deze poort dan in uw e-mailtoepassing opgeven als de poort voor POP3-communicatie.
 - APOP gebruiken indien beschikbaar deze optie biedt een veiligere emailserver aanmelding. Zo zorgt u ervoor dat de *E-mailscanner* een andere methode gebruikt om het accountwachtwoord van de gebruiker voor de aanmelding door te sturen. Het wachtwoord wordt dan niet in een open maar een gecodeerde indeling naar de server verstuurd met behulp van een variabelenketen die van de server ontvangen is. Deze functie is uiteraard alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.
 - Verbinding met behulp van dit vervolgkeuzemenu kunt u opgeven welk type verbinding moet worden gebruikt (Normaal/SSL/SSL-standaard). Als u een SSL-verbinding kiest, worden de gegevens gecodeerd verzonden zonder dat ze door een derde partij gevolgd of gecontroleerd kunnen worden. Deze functie is ook alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.



 Activering POP3 server e-mailclient - hier staat beknopte informatie over de configuratie-instellingen die vereist zijn om uw e-mailclient goed te configureren (zodat de *E-mailscanner* alle binnenkomende e-mailberichten controleert). Dit is een overzicht dat is gebaseerd op de overeenkomende parameters die in dit dialoogvenster en andere verwante dialoogvensters zijn opgegeven.

🕌 Geavanceerde instellingen AVO	
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans Schema's E-mailscanner Certificatie Mailfiltering Logboeken en resultaten Servers Servers AutoPOP3:10110 SMTP AutoSMTP:10025 Extern beheer 	SMTP Servernaam AutoSMTP Relayhost Automatisch Vaste host Aanvullende instellingen Lokale poott (gebruikt in e-mailclient): 10025 Wachtrij verwerken: Automatisch Handmatig Verbinding: Normaal Beheerserver Beheerserver Beheerberichten verzenden naar serverpoort: AutoPOP3:10110 Instellingen voor SMTP server e-mailclient Dorspronkelijk Activeering SMTP server e-mailclient Activeer deze server en gebruik hem voor het verzenden van e-mail
Standaard	Ok Annuleren Toepassen

In dit dialoogvenster (geopend met **Servers / SMTP**) kunt u een nieuwe **Emailscanner instellen** server die gebruikmaakt van het SMTP-protocol voor uitgaande e-mail:

- **SMTP-servernaam** Typ de naam van de server of handhaaf de standaardnaam AutoSMTP
- Hostrelay Hiermee wordt de methode gedefinieerd voor het bepalen welke



mailserver wordt gebruikt voor uitgaande e-mail:

- Automatisch aanmelding wordt automatisch uitgevoerd, afhankelijk van uw e-mailclient instellingen
- Vaste host in dit geval gebruikt het programma altijd de server die hier opgegeven is. Geef het adres of de naam van uw mailserver op. U kunt een domeinnaam gebruiken (bijvoorbeeld smtp.acme.com), evenals een IP-adres (bijvoorbeeld 123.45.67.89). Als de mailserver een nietstandaard poort gebruikt, kunt u deze poort na de servernaam opgeven. Gebruik een dubbele punt als scheidingsteken (bijvoorbeeld smtp.acme. com:8200). De standaardpoort voor SMTP-communicatie is 25.
- Aanvullende instellingen Meer gedetailleerde parameters opgeven:
- Lokale poort de poort waarop de communicatie van de mailtoepassing mag worden verwacht. U moet vervolgens in uw mailtoepassing deze poort specificeren als poort voor SMTP-communicatie.
 - Wachtrij verwerken bepalen wat de *E-mailscanner* moet doen als de eisen voor het verzenden van e-mail worden verwerkt:
 - Automatisch uitgaande e-mail wordt direct verzonden naar de doelmailserver
 - Handmatig het bericht wordt in de wachtrij voor uitgaande berichten geplaatst en later verzonden
 - Verbinding met behulp van dit vervolgkeuzemenu kunt u opgeven welk type verbinding moet worden gebruikt (Normaal/SSL/SSL-standaard). Als u een SSL-verbinding kiest, worden de gegevens gecodeerd verzonden zonder dat ze door een derde partij gevolgd of gecontroleerd kunnen worden. Deze functie is alleen beschikbaar wanneer de doelmailserver de functie ondersteunt.
 - **Beheerserver** weergave van het nummer van de poort van de server die gebruikt wordt voor de omgekeerde levering van beheerrapporten. Deze berichten worden bijvoorbeeld gegenereerd wanneer de doelmailserver het uitgaande bericht afwijst of wanneer deze mailserver niet beschikbaar is.
 - **Instellingen voor SMTP-server e-mailclient** korte instructies voor de configuratie van de clientmailtoepassing. De uitgaande e-mailberichten worden dan gecontroleerd met behulp van de server met de meest recente instellingen voor het controleren van uitgaande e-mailberichten. Dit is een



overzicht dat is gebaseerd op de overeenkomende parameters die in dit dialoogvenster en andere verwante dialoogvensters zijn opgegeven.

9.9. Resident Shield

Het onderdeel <u>**Resident Shield</u>** voert live bescherming uit voor bestanden en mappen tegen virussen, spyware en andere malware.</u>

불 Geavanceerde instellingen AVG	
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans E-mailscanner E-mailscanner Geavanceerde instellingen Uitzonderingen Uitzonderingen Update Extern beheer 	Resident Shield Instellingen Inschakelen Resident Shield Cookies scannen Scannen op bedreigingen door mogelijk ongewenste programma's en spyware Bestanden scannen bij sluiten Bootsector van verwisselbare media scannen Heuristische methode gebruiken Automatisch herstel
Standaard	Ok Annuleren Toepassen

In het dialoogvenster **Instellingen Resident Shield** kunt u de bescherming door **Resident Shield** volledig in- en uitschakelen met het selectievakje **Resident Shield inschakelen** (*de optie is standaard ingeschakeld*). Bovendien kunt u instellen welke functies van **Resident Shield** moeten worden geactiveerd:

• **Scannen naar cookies** - hiermee bepaalt u of cookies bij het scannen moeten worden gedetecteerd. (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers,*



bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes)

- **Potentieel ongewenste programma's scannen** (standaard ingeschakeld) scannen op <u>Potentieel ongewenste programma's</u> (uitvoerbare toepassingen die zich kunnen manifesteren als verschillende typen spyware of adware)
- **Scannen bij afsluiten van proces** Scannen bij afsluiten zorgt ervoor dat actieve objecten (bijv. toepassingen, documenten, enz.) worden gescand als ze worden geopend en gesloten; de functie levert een bijdrage aan de bescherming tegen bepaalde geavanceerde virustypen
- Bootsector van verwisselbare media scannen (standaard ingeschakeld)
- *Heuristische methode gebruiken* (standaard ingeschakeld) <u>heuristische analyse (</u>dynamische emulatie van de instructies van gescande object *en in een virtuele computeromgeving*) wordt gebruikt als één van de methoden voor virusdetectie
- **Automatisch herstel** gedetecteerde infecties worden automatisch hersteld als er een remedie beschikbaar is



9.9.1. Geavanceerde instellingen

In het dialoogvenster **Bestanden gescand door Resident Shield** kunt u opgeven welke bestanden gescand moeten worden (*aan de hand van de extensies*):



Maak een keuze of u alle bestanden wilt scannen of alleen infecteerbare bestanden in dat laatste geval kunt u een lijst opgeven met extensies van bestanden die moeten worden genegeerd bij het scannen, en een lijst met extensies van bestanden die onder alle omstandigheden moeten worden gescand.



불 Geavanceerde instellingen AV	3 📃 🗆 🚬 📃 🔰
Geavanceer de Instellingen Average Image: Second State Im	Resident Shield - Uitgesloten mappen Uitgesloten gebruiken voor Resident Shield Pad toevoegen Lijst toevoegen Uitgesloten gebruiken voor Resident Shield Pad bewerken Lijst bewerken Uitgesloten gebruiken voor Resident Shield Pad verwijderen
Standaard	Ok Annuleren Toepassen

9.9.2. Uitzonderingen

In het dialoogvenster **Uitsluitingen voor directory met Resident Shield** kunt u mappen opgeven die <u>Resident Shield</u> moet negeren. Het wordt met klem aangeraden om geen mappen over te slaan, tenzij dit absoluut noodzakelijk is! Als u een map wilt instellen die tijdens het scannen door <u>Resident Shield</u> moet worden overgeslagen, schakelt u het selectievakje **Uitsluitingen gebruiken in Resident Shield** in. De nieuwe instellingen worden pas van kracht na een herstart van de computer!

Dit dialoogvenster heeft de volgende knoppen:

- Pad toevoegen klik op deze knop om mappen op te geven die tijdens het scannen moeten worden overgeslagen. U kunt deze mappen vervolgens één voor één selecteren in de navigatiestructuur van de lokale schijf
- Lijst toevoegen klik op deze knop als u een hele lijst met mappen wilt



toevoegen die tijdens het scannen door <u>Resident Shield</u> moeten worden overgeslagen

- Pad bewerken klik op deze knop als u het opgegeven pad naar een geselecteerde map wilt bewerken
- Lijst bewerken klik op deze knop om de lijst met mappen te bewerken
- Pad verwijderen klik op deze knop om het pad naar een geselecteerde map uit de lijst te verwijderen

9.10.Update

🕌 Geavanceerde instellingen AVG 👘	
 Weergave Onderhoud PUP-uitzonderingen Anti-Spam Web Shield LinkScanner Scans E-mailscanner Resident Shield Proxy Inbellen URL Extern beheer 	 Wanneer bestanden moeten worden bijgewerkt Update bij eerstvolgende start van de computer. (Bijgewerkte bestanden worden voorbereid en de update wordt voltooid bij de eerstvolgende herstart van de computer.) Onmiddellijk bijwerken Als de computer opnieuw moet worden opgestart: Bevestiging vragen van de gebruiker Onmiddellijk opnieuw opstarten Voltooien na eerstvolgende herstart van de computer Aanvullende opties voor updates Bevestiging vragen voor het afsluiten van programma's die worden uitgevoerd. Het kan voor AVG nodig zijn dat sommige programma's die worden afgesloten (bijv. MS Outlook).
Standaard	Ok Annuleren Toepassen

Met de optie **Update** in de navigatiestructuur links opent u een nieuw dialoogvenster waarin u parameters kunt instellen voor <u>AVG Update</u>:



Wanneer bestanden moeten worden bijgewerkt

In deze sectie kunt u kiezen uit twee mogelijkheden: u kunt een <u>update</u> plannen voor de eerstvolgende start van de pc, of <u>update</u> meteen uitvoeren. Standaard is de optie voor onmiddellijk uitvoeren van een update ingesteld, omdat AVG op die manier een maximaal beveiligingsniveau kan bereiken. Plannen van een update voor de eerstvolgende keer dat de pc wordt opgestart is alleen raadzaam als u zeker weet dat de computer regelmatig opnieuw wordt opgestart, minstens één keer per dag.

Als u besluit de standaardconfiguratie aan te houden en de updateprocedure meteen uit te voeren, kunt u opgeven onder welke omstandigheden een eventueel vereiste herstart van de computer moet worden uitgevoerd:

- **Bevestiging vragen van de gebruiker** u wordt gevraagd een herstart te bevestigen die nodig is voor het voltooien van de <u>updateprocedure</u>.
- **Onmiddellijk opnieuw opstarten** de computer wordt automatisch opnieuw gestart nadat de <u>updateprocedure</u> is voltooid, u hoeft daarvoor geen toestemming meer te verlenen
- Voltooien na opstarten van de computer de <u>updateprocedure</u> wordt pas voltooid als de computer opnieuw wordt opgestart - houd ook hierbij in het oog dat deze optie alleen raadzaam is als u zeker weet dat de computer regelmatig opnieuw wordt opgestart, minstens één keer per dag.

Aanvullende opties voor updates

Als u het selectievakje **Bevestiging vragen om actieve toepassingen te sluiten** (*standaard ingeschakeld*) inschakelt, weet u zeker dat er geen toepassingen die worden uitgevoerd, zullen worden afgesloten zonder uw expliciete toestemming mocht dat afsluiten nodig zijn voor het voltooien van de updateprocedure.



9.10.1.Proxy

🕌 Geavanceerde instellingen AVG		
Weergave	Installingen bijwerken - Provu	
Onderhoud	mstellingen bijwerken - i toxy	
PUP-uitzonderingen	Proxy niet gebruiken	×
⊕ 4 Anti-Spam	C Handmatig	
Web Shield		
EinkScanner	Server:	Poort: 3128
H B Cans	PROXY-verificatie gebruiken	
H. In Schemas	Varificatietupe	Willekeurig (standaard)
E-mailscanner	venincaciecype;	Willekeung (scanddard)
Hadata	Gebruikersnaam:	
	Wachtwoord	
	machemoord.	
E Evtern bebeer	Auto	
	💿 Uit browser	Internet Explorer
	🔘 Uit script	
	Automatisch detecteren	
	·	
Standaard		Ok Annuleren Toepassen

De proxyserver is een zelfstandige server of een service die op een pc wordt uitgevoerd, die de verbinding met internet veiliger maakt. U hebt, afhankelijk van de instellingen voor het netwerk, rechtstreeks toegang tot internet of via een proxyserver. Het kan ook zijn dat beide mogelijkheden zijn toegestaan. Bij de eerste optie in het dialoogvenster **Instellingen bijwerken - Proxy** kiest u in de keuzelijst uit:

- Proxy gebruiken
- Proxyserver niet gebruiken
- **Proberen te verbinden via proxy en als dat niet lukt direct verbinden** standaardinstelling

Als u een optie selecteert waarbij een proxyserver betrokken is, zult u aanvullende



gegevens moeten verstrekken. U kunt de instellingen voor de server handmatig maar ook automatisch configureren.

Handmatige configuratie

Als u kiest voor handmatige configuratie (schakel *het selectievakje* **Handmatig** *in om het desbetreffende deel van het dialoogvenster te activeren*), specificeert u de volgende gegevens:

- Server geef het IP-adres van de server of de naam van de server op
- **Poort** geef de poort op die internettoegang mogelijk maakt (*standaard* poort 3128; u kunt echter een andere poort instellen neem contact op met uw netwerkbeheerder voor meer informatie als u niet zeker weet welke poort u moet instellen)

Het is mogelijk op de proxyserver voor de afzonderlijke gebruikers verschillende regels in te stellen. Als dat voor uw proxyserver het geval is, schakelt u het selectievakje **PROXY-verificatie gebruiken** in om te controleren of uw gebruikersnaam en wachtwoord geldig zijn voor een verbinding met internet via de proxyserver.

Automatische configuratie

Als u voor een automatische configuratie kiest (*schakel het selectievakje in bij* **Auto** *om het desbetreffende deel van het dialoogvenster te activeren*), geeft u op waar de configuratie van de proxy van overgenomen moet worden:

- **Uit browser** de configuratie wordt overgenomen van de instellingen van uw standaardbrowser voor internet (*ondersteunde browsers zijn Internet Explorer, Firefox, Mozilla en Opera*)
- **Uit script** de configuratie wordt overgenomen uit een gedownload script, waarbij de functie het proxy-adres retourneert
- **Automatisch detecteren** De configuratie wordt automatisch vastgesteld vanuit de proxyserver



9.10.2.Inbellen

🕌 Geavanceerde instellingen AVG		_ 🗆 🗙
Ceavanceer de instellingen AVG	Instellingen bijwerken - Inbelverbinding □ Inbelverbinding ngebruiken □ Deze verbinding automatisch openen ☑ Inbelverbinding sluiten bij voltooien ④ Vragen voor verbinden	
Standaard	Ok Annuleren Toe	passen

Alle parameters die optioneel zijn gedefinieerd in het dialoogvenster **Instellingen bijwerken - Inbelverbinding** hebben betrekking op een inbelverbinding met internet. De opties op het tabblad zijn uitgeschakeld, tenzij u het selectievakje **Inbelverbindingen gebruiken** inschakelt.

Stel in of u automatisch een verbinding met internet tot stand wilt brengen (**Deze verbinding automatisch openen**) of geef aan dat u de verbinding telkens handmatig tot stand wilt brengen (**Vragen om verbinding**). Bij een automatische verbinding moet u ook nog aangeven of de verbinding moet worden verbroken nadat de update is voltooid (**Inbelverbinding sluiten bij voltooien**).



9.10.3.URL

😹 Geavanceerde instellingen AVG			
Geavanceer de instellingen AVG	Instellingen bijwerken - URL Naam U ✓ update primary server ht ✓ update backup server ht	JRL tp://update.avg.com/softw/80/upda tp://backup.avg.cz/softw/80/update	Toevoegen te/ Bewerken Verwijderen Standaard Omhoog verplaatsen Omlaag verplaatsen
Standaard	< (Ok Annulei	en Toepassen

Op het tabblad **URL** wordt een lijst met internetadressen weergegeven die u kunt gebruiken om de updatebestanden te downloaden. De lijst en de vermeldingen kunnen worden gewijzigd met behulp van de volgende knoppen:

- Toevoegen als u op deze knop klikt, wordt er een dialoogvenster geopend waarin u een nieuwe URL kunt opgeven die aan de lijst moet worden toegevoegd
- **Bewerken** als u op deze knop klikt, wordt er een dialoogvenster geopend waarin u de parameters van de geselecteerde URL kunt bewerken
- Verwijderen als u op deze knop klikt, wordt de geselecteerde URL uit de lijst verwijderd
- Beginwaarden als u op deze knop klikt, wordt de standaardlijst met URL's



opnieuw ingesteld

- Omhoog verplaatsen als u op deze knop klikt, wordt de geselecteerde URL één positie hoger op de lijst geplaatst
- **Omlaag verplaatsen** als u op deze knop klikt, wordt de geselecteerde URL één positie lager in de lijst geplaatst

9.11.Extern beheer

불 Geavanceerde instellingen AVG		
Geavanceer de instellingen AVG	Server:	
Standaard	Ok Annuleren	Toepassen

De instellingen voor **Extern beheer** hebben betrekking op de verbinding tussen het AVG clientstation en het systeem voor extern beheer. Als u van plan bent een verbinding tot stand te brengen tussen het desbetreffende station en extern beheer, geeft u de volgende parameters op:

• Server - de naam van de server (of het IP-adres van de server) waarop AVG



Admin Server is geïnstalleerd

- **Poort** geef het poortnummer op dat de AVG client gebruikt voor communicatie met AVG Admin Server(*het standaard poortnummer is 4158 - als dat poortnummer wordt weergegeven, hoeft u het niet expliciet te specificeren*)
- **Aanmelden** Als de communicatie tussen de AVG client en AVG Admin Server wordt gedefinieerd als beveiligd, geeft u uw gebruikersnaam op
- Wachtwoord ... en uw wachtwoord
- Poort voor binnenkomende berichten het nummer van de poort waarlangs de AVG client binnenkomende berichten van AVG Admin Server accepteert

Opmerking:Raadpleeg de documentatie van AVG Network Edition voor een uitgebreide beschrijving van extern beheer.



10. AVG scannen

Scannen is een cruciaal onderdeel voor de werking van **AVG 8.0 Anti-Virus** . U kunt tests op verzoek uitvoeren of u kunt ze <u>plannen, zodat ze periodiek worden</u> <u>uitgevoerd</u> op tijdstippen waarop het u schikt

10.1.Scaninterface

불 AVG I	Enterprise									_ 🗆 🖂
<u>B</u> estand	<u>O</u> nderdelen	Historie	<u>E</u> xtra	Help						
	AV	G			U bent beschr Alle beveiligingsfu	e rmd . Incties zijn up-to-dat	e en functioneren	correct.		
	Overzicht			Scannen	i op zoek naa	ar bedreiginge	n			
٩	Computers	canner		S s)e hele computer icaninstellingen wijzig	scannen Jen	Scani	alde mappen of bea nstellingen wijzigen	standen scar	
	Nu bijwerk	en								
				Scans plann Naam Geplande s	can	Volgende ge 4-3-2008, 12	plande run ::00:00			
Statist Laatste Update: Virusdal AVG ve	t ieken scan: 3-3-04 : 3-3-01 tabase: 269.2 arsie: 8.0.8	8, 23:17 8, 23:02 21.1/1300		Toevoege	en Scanschema	Bewerken Scansche	ma		Verwijderens	icanschema
Vervald	latum licentie: I elding wee l	1-6-2008 rgeven						Scanhistorie	Quarantaine	weergeven

U kunt de AVG interface voor het scannen oproepen via de snelkoppeling **Computerscanner** [****]. Klik op die koppeling om het dialoogvenster **Scannen op zoek naar bedreigingen** te openen. In dat dialoogvenster treft u het volgende aan:

- overzicht van <u>vooraf gedefinieerde scans</u> twee typen tests (gedefinieerd door de leverancier van de software), die u meteen kunt gebruiken of plannen;
- <u>scans plannen</u> naar wens definiëren van nieuwe tests en plannen van tests.

Knoppen

De testinterface heeft de volgende knoppen:



- Scanhistorie weergave van het dialoogvenster <u>Overzicht scanresultaten</u> met de volledige scanhistorie
 - Quarantaine weergeven er wordt een nieuw venster geopend met de <u>Quarantaine</u> - een opslagruimte waar gedetecteerde infecties worden opgeslagen

10.2.Vooraf ingestelde scans

Een van de hoofdfuncties van AVG is het op verzoek uitvoeren van scantaken. De tests op verzoek zijn ontworpen voor het scannen van verschillende onderdelen van uw computer in gevallen waarin u vermoedt dat er mogelijk sprake is van een virusinfectie. Het wordt met klem aangeraden om dergelijke tests regelmatig uitvoeren. Dat geldt ook als u vermoedt dat er geen virussen op uw computer zullen worden gevonden.

In **AVG 8.0 Anti-Virus** staan twee typen scans die vooraf zijn gedefinieerd door de leverancier van de software:

10.2.1.De hele computer scannen

De hele computer scannen - de hele computer wordt gescand op mogelijke infecties en/of potentieel ongewenste programma'sP Alle vaste schijven van de computer worden gescand, alle virussen worden gedetecteerd en hersteld of verplaatst naar de **Quarantaine**. Een scan van de hele computer dient op een werkstation minstens eenmaal per week te worden uitgevoerd.

Scan starten

U kunt **De hele computer scannen** direct vanuit de <u>scaninterface</u> starten door op het pictogram van de scan te klikken. U hoeft verder geen instellingen op te geven voor dit type scan, het scannen wordt onmiddellijk gestart in het dialoogvenster **Scan wordt uitgevoerd** (*zie schermafbeelding*). U kunt het scanproces tijdelijk onderbreken (**Onderbreken**) en afbreken (**Annuleren**), als dat nodig is.


🕌 AVG Enterprise			_ 🗆 🗙
AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren cor	rect.	
Overzicht	Scan wordt uitgevoerd	tast/Tefactio	
Computerscanner	bescanu resul	laaqiniettie	
De hele computer scannen			
📝 Nu bijwerken			
Statistieken Laatste scan: 3-3-08, 23:15 Update: 3-3-08, 23:02 Virusdatabase: 269.21.1/1300 AVG versie: 8.0.81 Vervaldatum licentie: 1-6:2008	Gescande objecten: 0 Gevonden bedreigingen: 0 Verstreken tijd: minder dan één seconde Bezig met scannen: Bootsectors Huidig object: Aanvullende scaninstellingen		
XMelding weergeven		Pauzeren	Annuleren

Scanconfiguratie bewerken

U kunt de vooraf gedefinieerde standaardinstellingen van **De hele computer** scannenwijzigen. Klik op de koppeling **Scaninstellingen wijzigen** om het dialoogvenster **Scaninstellingen wijzigen voor De hele computer scannen** te openen. Het is raadzaam de standaardinstellingen aan te houden, tenzij u een goede reden hebt om ze te wijzigen!



🕌 AVG Enterprise	
Bestand Onderdelen Historie Extra	a Help
	U bent beschermd.
AVG	Alle beveiligingsfuncties zijn up-to-date en functioneren correct.
	Scaninstellingen wijzigen voor De hele computer scannen
🗊 Overzicht	V Infartiar automatisch herstellen/verwiideren
	✓ Infector additional interaction volting and inte
All No. 1 Second and	Scannen naar cookies
Nu bijwerken	Scannen in archieven
	Heurisasche methode gebruiken Scansysteemomgeving
	Alleen infecteerbare bestanden scannen
	Scannen naar rootkits
	Prioriteit scanproces
	Automatische scan
Statistieken	Aanvullende scanrapporten instellen
Laatste scan: Nog niet gescand	Aanvullende scaninstellingen
Update: 3-3-08, 23:02 Virusdatabase: 269.21.1/1300	Huidige instellingen opslaan
AVG versie: 8.0.81 Vervaldatum licentie: 1.6.2008	
	Standaard Start scan Annuleren
XMelding weergeven	

- **Scanparameters** in de lijst met scanparameters kunt u scanparameters naar wens in- en uitschakelen. Standaard zijn de meeste parameters ingeschakeld, zodat ze bij het scannen automatisch worden toegepast.
- **Prioriteit scanproces** met de schuifbalk kunt u de priortieit voor het scanproces wijzigen. Standaard is de prioriteit ingesteld op gemiddeld (*Automatische scan*), waarbij de snelheid van het scanproces en het gebruik van systeembronnen (o.a. het werkgeheugen van uw computer) optimaal op elkaar zijn afgesteld. U kunt ook langzamer scannen, wat betekent dat een minder groot beroep wordt gedaan op systeembronnen (*dat is handig als u met de computer aan het werk bent en het u niet uitmaakt hoe lang het scanproces duurt*), of sneller, waarbij een groter beroep wordt gedaan op systeembronnen (*bijvoorbeeld op een moment dat u de computer niet gebruikt*).
- **Aanvullende scanrapporten instellen** als u op deze koppeling klikt, wordt een nieuw dialoogvenster geopend, **Scanrapporten**, waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:

AVG	
Tough on threats. Easy on you	ı.

🕌 Scanrappo	orten 🔀	
Scanrapp	porten	
Rapport n	et wachtwoord beschermde archiefbestanden	
Rapport met wachtwoord beschermde documenten		
Rapport Vergrendelde bestanden		
Rapport bestanden met een macro		
Rapport Verborgen extensies		
0	0k Annuleren	

 Aanvullende scaninstellingen - als u op deze koppeling klikt, wordt een nieuw dialoogvenster geopend, Opties voor uitschakelen computer, waarin u kunt aangeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (Computer afsluiten na voltooien van scanproces), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (Geforceerd afsluiten als de computer vergrendeld is).

Opties voor uitschakelen computer		
Comput	er uitschakelen na voltooien van scan	
Gefo	ceerd afsluiten als de computer blijft hangen	

Waarschuwing: deze scaninstellingen zijn gelijk aan die van een nieuw gedefinieerde scan - zoals beschreven in het hoofdstuk <u>AVG scannen / Scans</u> plannen / Hoe er gescand moet worden.

Mocht u besluiten de standaardconfiguratie van **De hele computer scannen** te wijzigen, dan kunt u uw nieuwe instellingen opslaan als standaardconfiguratie die voor alle toekomstige scans van de computer moet worden gebruikt.

10.2.2.Bepaalde mappen of bestanden scannen

Bepaalde mappen of bestanden scannen - alleen die gebieden worden gescand die u hebt geselecteerd voor het scannen (geselecteerde mappen, vaste schijven, diskettes, cd's, enz.). De voortgang bij het scannen in het geval dat een virus wordt gedetecteerd, en de manier waarop het virus wordt behandeld, is hetzelfde als bij een scan van de hele computer: een gedetecteerd virus wordt hersteld of in *quarantaine* geplaatst. Met de functie voor het scannen van bepaalde mappen of bestanden kunt u eigen scans plannen die tegemoet komen aan uw eisen.



Scan starten

U kunt **Bepaalde mappen of bestanden scannen** direct vanuit de <u>scaninterface</u> starten door op het pictogram van de scan te klikken. Er wordt een nieuw dialoogvenster, **Selecteer bestanden of mappen om te scannen**, geopend. Selecteer in de bestandsstructuur van de computer die mappen die u wilt scannen. Het pad naar elke geselecteerde map wordt automatisch gegenereerd en weergegeven in het tekstvak in het bovenste deel van het dialoogvenster. U kunt ook een map scannen, maar tegelijkertijd alle submappen van die map uitsluiten van het scannen; daartoe typt u een minteken "-" voor het automatisch gegenereerde pad (*zie de schermafbeelding*). Om uiteindelijk het scanproces te starten klikt u op de knop **Scannen starten**; het scanproces zelf is in principe gelijk aan het scanproces van Volledige computer scannen.

讃 AVG Enterpris	se		- 0 🛛
Bestand Onderdele	en Hi <u>s</u> torie	ie Extra Help	
🕌 A\	/G	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.	
		Selecteer bestanden of mappen om te scannen	
0verzicł	nt	C:\Test\;	~
Compute	erscanner	Bureaublad	
🛛 Nu bijwe	erken	A: A: B: D: D: Speciale locaties Speciale locaties Divise vaste schijven Divise vaste schij vaste schije schije schije schije schije schij	
Statistieken Laatste scan: 3-3 Update: 3-3 Virusdatabase: 26 AVG versie: 8.0 Vervaldatum licent XMelding wo	3-08, 23:15 3-08, 23:02 9.21.1/1300 0.81 ie: 1-6-2008 sergeven	Automatische scan	eren

Scanconfiguratie bewerken

U kunt de vooraf gedefinieerde standaardinstellingen van **Bepaalde mappen of bestanden scannen**wijzigen. Klik op de koppeling **Scaninstellingen wijzigen** om het dialoogvenster **Scaninstellingen wijzigen voor Bepaalde mappen of bestanden scannen** te openen. **Het is raadzaam de standaardinstellingen aan**



te houden, tenzij u een goede reden hebt om ze te wijzigen!

🕌 AVG Enterprise			
Bestand Onderdelen Historie Extra	Help		
📕 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.		
	Scaninstellingen wijzigen voor Bepaalde mappen of bestanden scanne		
Overzicht	✓ Infecties automatisch herstellen/verwijderen		
Computerscanner	☑ Scannen op bedreigingen door mogelijk ongewenste programma's en spyware		
🕼 Nu bijwerken	Scannen naar cookies Scannen in archieven Heuristische methode gebruiken Scansysteemomgeving Alleen infecteerbare bestanden scannen Scansen paar rontikts		
Statistieken Laatste scan: Nog niet gescand Update: 3-3-08, 23.02 Virusdatabase: 269,21,1/1300 AVR vereie: 8.0.81	Prioriteit scanproces Automatische scan Aanvullende scanrapporten instellen Aanvullende scaninstellingen Huidige instellingen opslaan		
Vervaldatum licentie: 1-6-2008	Standaard Volgende Annuleren		

- **Scanparameters** in de lijst met scanparameters kunt u naar wens parameters inen uitschakelen (*zie voor een gedetailleerde beschrijving van deze instellingen het hoofdstuk* <u>AVG Geavanceerde instellingen / Scans / Bepaalde mappen of bestanden</u> <u>scannen</u>).
- **Prioriteit scanproces** met de schuifbalk kunt u de priortieit voor het scanproces wijzigen. Standaard is de prioriteit ingesteld op gemiddeld (*Automatische scan*), waarbij de snelheid van het scanproces en het gebruik van systeembronnen (o.a. het werkgeheugen van uw computer) optimaal op elkaar zijn afgesteld. U kunt ook langzamer scannen, wat betekent dat een minder groot beroep wordt gedaan op systeembronnen (*dat is handig als u met de computer aan het werk bent en het u niet uitmaakt hoe lang het scanproces duurt*), of sneller, waarbij een groter beroep wordt gedaan op systeembronnen (*bijvoorbeeld op een moment dat u de computer niet gebruikt*).
- Aanvullende scanrapporten instellen als u op deze koppeling klikt, wordt een nieuw dialoogvenster geopend, Scanrapporten, waarin u kunt aangeven wat voor soort resultaten moeten worden gerapporteerd:

	AVG
Tough on t	hreats. Easy on you.

🕌 Scanrappe	orten	X
Scanrap	porten	
Rapport n	net wachtwoord beschermde archiefbestanden	
Rapport met wachtwoord beschermde documenten		
Rapport Vergrendelde bestanden		
Rapport bestanden met een macro		
🗌 Rapport \	/erborgen extensies	
•	0k Annuleren	

Aanvullende scaninstellingen - als u op deze koppeling klikt, wordt een nieuw dialoogvenster geopend, Opties voor uitschakelen computer, waarin u kunt aangeven of de computer automatisch moet worden uitgeschakeld als het scanproces is voltooid. Als u die optie bevestigt (Computer afsluiten na voltooien van scanproces), wordt een tweede optie actief waarmee u de computer geforceerd kunt afsluiten, zelfs als die op dat moment is vergrendeld (Geforceerd afsluiten als de computer vergrendeld is).

Opties voor uitschakelen computer			
Compu	er uitschakelen na voltooien van scan		
Gefo	rceerd afsluiten als de computer blijft hangen		

Waarschuwing: deze scaninstellingen zijn gelijk aan die van een nieuwe gedefinieerde scan - zoals beschreven in het hoofdstuk <u>AVG scannen / Scans</u> plannen / Hoe er gescand moet worden.

Mocht u besluiten de standaardconfiguratie van **Bepaalde mappen of bestanden scannen** te wijzigen, dan kunt u uw nieuwe instellingen opslaan als standaardconfiguratie die voor alle toekomstige scans van de computer moet worden gebruikt. De configuratie wordt bovendien gebruikt als sjabloon voor alle nieuwe geplande scans (<u>alle aangepaste scans worden gebaseerd op de dan actuele</u> configuratie van Bepaalde mappen of bestanden scannen).

10.3.Scannen in Windows Verkenner

Naast de mogelijkheden om met vooraf gedefinieerde scans de hele computer te scannen of een bepaald gedeelte, kunt u met AVG ook snel een specifiek object scannen in Windows Verkenner. Als u een onbekend bestand wilt openen en niet zeker weet of de inhoud veilig is, kunt u het op verzoek scannen. Ga als volgt te



werk:

🚞 \$AVG8.VAULT\$			
Cocuments and Settings			
MSOCache			
Program Files			
Scr	Openen		
C Sys	 Verkennen		
🚞 Tes	Zoeken		
🛅 tot			
🚞 WII	[] Delen en beveiliging		
🗐 add 🛛 Scannen met <u>A</u> VG			
T AU	Kopiëren <u>n</u> aar 🕨		
bod -			
🔤 Boc	Knippen		
🔤 CO	<u>K</u> opiëren		
🔟 hib	Spelkoppeling maken		
🚾 IO.	Verwijderen		
🔟 MSI	Naam wiizigen		
🚞 NT(NTI IVaam <u>Wijzigen</u>		
🖻 ntic	ntle Eigenschappen		
🔤 pagefile.sys			

- Selecteer in Windows Verkenner het bestand (of de map) die u wilt controleren
- Klik met de rechter muisknop op het object om het snelmenu te openen
- Kies de optie *Met AVG scannen* om het bestand te scannen met AVG

10.4.Scannen vanaf opdrachtregel

U kunt in **AVG 8.0 Anti-Virus** een scan uitvoeren vanaf de opdrachtregel. Die optie kunt u bijvoorbeeld op servers gebruiken, of voor het maken van een batch-script dat onmiddellijk na het opstarten van de computer moet worden uitgevoerd. U kunt vanaf de opdrachtregel scans starten met vrijwel alle parameters die beschikbaar zijn in de grafische gebruikersinterface van AVG.

Geef, als u AVG Scan vanaf de opdrachtregel wilt starten, de volgende opdracht in de map waar in AVG is geïnstalleerd:

- avgscanx voor 32-bits besturingssystemen
- avgscana voor 64-bits besturingssystemen

Hieronder volgt een lijst met parameters die u bij het scannen vanaf de opdrachtregel kunt gebruiken:

• /SCAN Scan /pad,pad/



• /COMP	De hele computer scannen
• /HEUR	Heuristische analyse gebruiken
• /EXCLUDE	Pad of bestanden uitsluiten van scan
• /@	Opdrachtbestand /bestandsnaam/
• /EXT	Deze extensies scannen /bijvoorbeeld EXT=EXE,DLL/
• /NOEXT	Deze extensies niet scannen /bijvoorbeeld NOEXT=JPG/
• /ARC	Archieven scannen
• /CLEAN	Automatisch opschonen
• /TRASH quarantaine	Geïnfecteerde bestanden verplaatsen naar de
• /QT Snelle	e test
• /MACROW	Macro's in rapport opnemen
• /PWDW opnemen	Bestanden met wachtwoordbeveiliging in rapport
• /IGNLOCKED	Vergrendelde bestanden negeren
• /REPORT	Rapporteren naar bestand /bestandsnaam/
• /REPAPPEND	Toevoegen aan het rapportbestand
• /REPOK	Niet geïnfecteerde bestanden als OK in rapport opnemen
• /NOBREAK	CTRL-BREAK niet toestaan voor afbreken
• <i>/BOOT</i>	MBR/BOOT-controle inschakelen
• /PROC	Scannen actieve processen
• /PUP opnemen	"Potentieel ongewenste programma's" in rapport
• /REG	Register scannen



- /COO Cookies scannen
 - /? Help over dit onderwerp weergeven
 - **/HELP** Help over dit onderwerp weergeven
 - /PRIORITY Scanprioriteit instellen /Laag, Auto, Hoog/
 - /SHUTDOWN Computer uitschakelen na voltooien van scan
 - /FORCESHUTDOWN Computer geforceerd uitschakelen na voltooien van scan
 - **/ADS** Alternatieve gegevensstromen scannen (alleen NTFS)

De opdracht volgt de onderstaande syntaxis:

- avgscanx /parameter ... bijv. avgscanx /comp voor het scannen van de hele computer
- avgscanx /parameter /parameter .. bij gebruik van meerdere parameters moeten deze achter elkaar worden geplaatst en van elkaar gescheiden door een spatie en een slash
- Als een parameter bepaalde waarden vereist (bijv. de /scan-parameter, die informatie nodig heeft over welke gebieden van de computer u wilt scannen, terwijl u een exact pad moet opgeven voor het geselecteerde gedeelte), worden die waarden van elkaar gescheiden met komma's, bijvoorbeeld: avgscanx /scan=C:\,D:\

Druk op *Enter*om de scan uit te voeren. Tijdens het scannen kunt u het proces stoppen door op *CTRL+C* of *CTRL+Pause* te drukken.

10.5.Scans plannen

Met **AVG 8.0 Anti-Virus** kunt u scans op verzoek uitvoeren (bijvoorbeeld als u vermoedt dat uw computer geïnfecteerd is geraakt) of volgens schema. Het is met nadruk raadzaam om de scans op basis van een schema uit te voeren: op die manier weet u zeker dat uw computer wordt beschermd tegen alle mogelijke infecties, en hoeft u zich geen zorgen te maken over de vraag of en wanneer u een scan moet uitvoeren.



Minimaal voert u <u>De hele computer scannen</u> regelmatig uit, minstens één maal per week. Als het echter mogelijk is, is het verstandig om de hele computer dagelijks te scannen - zoals ook is ingesteld in de standaardconfiguratie voor scanschema's. Als de computer altijd "aan staat", kunt u de scans buiten kantooruren plannen. Als de computer zo nu en dan wordt uitgeschakeld, kunt u plannen dat scans <u>worden</u> <u>uitgevoerd bij het opstarten van de computer, als er een scan is overgeslagen</u>.

Open het dialoogvenster <u>AVG scaninterface</u> en geef instellingen op in het onderste deel van het dialoogvenster **Scans plannen** als u nieuwe scanschema's wilt maken:

🛃 AVG Enterprise		
Bestand Onderdelen Historie Ext	ra <u>H</u> elp	
📕 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.	
	Scannen op zoek naar bedreigingen	
Overzicht		
Computerscanner	De hele computer scannen Scaninstellingen wijzigen Scaninstellingen wijzigen	
📝 Nu bijwerken	<i></i>	
	Scans plannen Naam Volgende geplande run Geplande scan 4-3-2008, 12:00:00	
Statistieken Laatste scan: 3-3.08, 23.17 Update: -3-3.08, 23.02 Virusdatabase: 269.21.1/1300 AVG versie: 8.0.81 Vervaldatum licentie: 1-6-2008	Toevoegen Scanschema Bewerken Scanschema Verwijderen Sc Scanhistorie Quarantaine	canschema weergeven

Knoppen voor Scans plannen

In de sectie voor het plannen van scans staan de volgende knoppen

- Scanschema toevoegen als u op deze knop klikt, wordt het dialoogvenster Instellingen voor geplande scan geopend met het tabblad <u>Schema-instellingen</u>. In dat dialoogvenster kunt u de instellingen opgeven voor de nieuwe scan.
- **Scanschema bewerken** deze knop is alleen actief als u eerst een bestaande scan uit de lijst met geplande scans hebt geselecteerd. In dat geval



wordt de knop actief en kunt u erop klikken om het dialoogvenster **Instellingen voor geplande scan** te openen, met het tabblad <u>Schema-</u> <u>instellingen</u>. De parameters van de bestaande scan worden weergegeven, u kunt die wijzigen.

> • Scanschema verwijderen - deze knop is eveneens alleen actief als u eerst een bestaande scan uit de lijst met geplande scans hebt geselecteerd. U kunt dat schema dan verwijderen als u op deze knop klikt. U kunt echter alleen uw eigen schema's verwijderen; het vooraf gedefinieerde Schema volledige computer scannen van de standaardinstellingen kan nooit worden verwijderd.

10.5.1.Schema-instellingen

Open het dialoogvenster **Instellingen voor geplande scan** als u een nieuwe scan wilt plannen en die regelmatig wilt uitvoeren. Het dialoogvenster heeft drie tabbladen: **Schema-instellingen** - zie de onderstaande afbeelding (het standaardtabblad dat automatisch wordt weergegeven), <u>Hoe er gescand moet</u> <u>worden</u> en <u>Wat er gescand moet worden</u>.

불 AVG Enterprise			- 0 🛛
Bestand Onderdelen Historie Extr	a <u>H</u> elp		
🛃 AVG	U bent beschermd. Alle beveiligingsfuncties	zijn up-to-date en functioneren correct.	
	Instellingen voor geplande	escan	
0verzicht	Schema-instellingen Hoe er gescand mo	et worden Wat er gescand moet worden	
Q Computerscanner	Naam	Geplande scan	
🕅 Nu bijwerken	Schema wordt uitgevoerd		
	🔘 Uitvoeren elke:	1 Uur (uren)	
	 Uitvoeren op specifiek tijdstip: 	Elke dag 💉 12:00	
	O Gebaseerd op handeling:	Bij het opstarten van de computer	
	Geavanceerde schemaopties		
	🔲 Uitvoeren bij het opstarten van de	computer als taak is overgeslagen	
	Uitvoeren zelfs als de computer in	energiebesparingsmodus is	
Statistieken	Taakinstellingen		
Laatste scan: 3-3-08, 23:15 Update: 3-3-08, 23:02 Virusdatabase: 268, 21.1/1300 AVG versie: 8.0.61 Vervaldatum licentie: 1-6-2008	🗹 Deze taak inschakelen		
XMelding weergeven		Opslaan A	Annuleren

Op het tabblad **Schema-instellingen** geeft u de scan die u maakt, een naam. Typ de naam in het tekstvak bij **Naam**. Probeer korte, maar niettemin veelzeggende namen



te gebruiken voor scans zodat u ze achteraf te midden van andere scans kunt herkennen.

Voorbeeld: het is niet handig om een scan als naam "nieuwe scan" of "mijn scan" te geven, omdat die namen geen aanduiding geven van wat de scan doet. Een naam als "Scan systeemgebieden" is daarentegen een voorbeeld van een veelzeggende naam voor een scan. Bovendien is het niet nodig om in de naam van de scan aan te geven of de hele computer wordt gescand of alleen een selectie van mappen en bestanden - uw eigen scans zijn altijd aangepaste versies van het type <u>Bepaalde mappen of bestanden scannen</u>.

In dit dialoogvenster kunt u daarnaast nog de volgende parameters instellen:

- Schema wordt uitgevoerd geef een tijdsinterval op waarmee de nieuwe geplande scan moet worden uitgevoerd. U kunt deze interval op verschillende manieren definiëren: als steeds terugkerende scan die na verloop van een bepaalde tijd (Uitvoeren elke ...) moet worden uitgevoerd, als scan die op een bepaalde datum en een bepaald tijdstip (Uitvoeren op specifiek tijdstip ...) moet worden uitgevoerd, of door een gebeurtenis te definiëren waaraan het uitvoeren van de scan moet worden gekoppeld (Actie bij het opstarten van de computer).
- Geavanceerde schema-opties in deze sectie kunt u bepalen onder welke omstandigheden de scan wel of niet moet worden uitgevoerd als de computer in een energiebesparingsmodus is of helemaal is uitgeschakeld.
- **Taakinstellingen** in deze sectie kunt u het selectievakje **Deze taak inschakelen** uitschakelen als u de geplande scan tijdelijk niet wilt uitvoeren en weer inschakelen als de noodzaak daarvoor zich aandient.

Knoppen in het dialoogvenster Instellingen voor scanschema

Er zijn twee knoppen op alle drie de tabbladen van het dialoogvenster **Instellingen voor scanschema (Schema-instellingen**, <u>Hoe er gescand moet worden</u> en <u>Wat er gescand moet worden</u>) en die hebben op alle drie de tabbladen dezelfde functies:

 Opslaan - opslaan van alle wijzigingen die u hebt uitgevoerd op dit tabblad of een van de twee andere tabbladen van het dialoogvenster, het dialoogvenster sluiten en terugkeren naar het <u>standaarddialoogvenster van de AVG</u> <u>scaninterface</u>. Klik daarom, als u testparameters op alledrie de tabbladen wilt instellen, alleen op de knop om instellingen op te slaan, nadat u al uw wensen hebt gespecificeerd.



 Annuleren - alle wijzigingen die u hebt aangebracht in instellingen op dit tabblad of één van de twee andere tabbladen van het dialoogvenster, ongedaan maken, het dialoogvenster sluiten en terugkeren naar het standaarddialoogvenster van de AVG scaninterface.

10.5.2. Hoe er gescand moet worden

🕌 AVG Enterprise	
<u>B</u> estand <u>O</u> nderdelen Hi <u>s</u> torie <u>E</u> xtra	Help
🕌 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.
	Instellingen voor geplande scan
0verzicht	Schema-Instellingen Hoe er gescand moet worden Wat er gescand moet worden
Q Computerscanner	Infecties automatisch herstellen/verwijderen
🕅 Nu bijwerken	Scannen op bedreigingen door mogelijk ongewenste programma's en spyware Scannen naar cookies Scannen in archieven Heuristische methode gebruiken Scansysteemomgeving Alleen infecteerbare bestanden scannen Scannen naar rootkits Prioriteit scanproces
Statistieken Laatste scan: 3-3-08, 23-15 Update: 3-3-08, 23-02 Virusdatabase: 269,21,1/1300 AVG versie: 8.0.81 Vervaldatum licentie: 1-6-2008 XMelding weergeven	Automatische scan Aanvullende scaninstellingen Aanvullende scaninstellingen Dpslaan Annuleren

Op het tabblad**Hoe er gescand moet worden** staat een lijst met scanparameters die kunnen worden in- en uit-geschakeld. Standaard zijn de meeste parameters ingeschakeld en wordt de desbetreffende functionaliteit gebruikt bij het scannen. We raden u aan deze vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om deze instellingen te wijzigen:

• **Infecties automatisch herstellen/verwijderen** - (standaard ingeschakeld): als tijdens het scannen een virus wordt gedetecteerd, wordt automatisch een herstelprocedure gestart, als die beschikbaar is. Als het geïnfecteerde bestand niet automatisch hersteld kan worden, of als u besluit deze optie uit te schakelen, wordt u bij detectie van een virus gewaarschuwd en zult u op dat moment moeten besluiten wat u wilt doen met de gedetecteerde infectie. Het is raadzaam het geïnfecteerde bestand te verplaatsen naar de <u>Quarantaine</u>.



- Potentieel ongewenste programma's scannen- (standaard ingeschakeld): deze parameter bepaalt de werking van de functie <u>Anti-Virus</u> die <u>detectie van</u> potentieel ongewenste programma's mogelijk maakt (spyware of adware in de vorm van uitvoerbare bestanden), zodat ze kunnen worden geblokkeerd of verwijderd;
 - Scannen naar cookies (standaard ingeschakeld): deze parameter van het onderdeel <u>Anti-Spyware</u> bepaalt of cookies bij het scannen moeten worden gedetecteerd (*HTTP-cookies worden gebruikt voor verificatie, tracking en het bijhouden van bepaalde informatie over gebruikers, bijvoorbeeld voorkeuren voor websites of de inhoud van winkelkarretjes*);
 - **Scannen binnen archieven** (*standaard ingeschakeld*): deze parameter bepaalt of bij het scannen alle bestanden moeten worden gecontroleerd, ook als die op de een of andere manier zijn gecomprimeerd, bijv. ZIP, RAR, ...
 - *Heuristische methode gebruiken* (*standaard ingeschakeld*): heuristische analyse (*dynamische emulatie van de instructies van gescande object en in een virtuele computeromgeving*) wordt gebruikt als één van de methoden voor virusdetectie als de parameter is ingeschakeld;
 - **Systeemgebieden scannen** (*standaard ingeschakeld*): als de parameter is ingeschakeld worden ook de systeemgebieden gescand;
 - Alleen infecteerbare bestanden scannen (standaard uitgeschakeld): als u deze parameter inschakelt, worden bestanden die niet kunnen worden geïnfecteerd, niet gescand. Dat kunnen bijvoorbeeld bestanden zijn met onopgemaakte tekst, of andere niet-uitvoerbare bestanden.

In het gedeelte **Prioriteit scanproces** kunt u nader specificeren hoe snel moet worden gescand in samenhang met het beroep dat wordt gedaan op o.a. het werkgeheugen van uw computer (systeembronnen). Standaard is deze optie ingesteld op een gemiddeld niveau van automatisch gebruik. Als u sneller wilt scannen, duurt het scannen minder lang, maar wordt een aanzienlijk groter beslag gelegd op o.a. het werkgeheugen tijdens het scannen, zodat andere activiteiten op de computer trager zullen verlopen (*u kunt deze optie inschakelen als er verder niemand van de pc gebruikmaakt*). U kunt echter het beroep o.a. het werkgeheugen ook verkleinen door te kiezen voor een langere scanduur.

Opmerking: Standaard is de scanconfiguratie ingesteld op optimale prestaties. Het is raadzaam de vooraf ingestelde configuratie aan te houden, tenzij u een goede reden hebt om de scaninstellingen te wijzigen. Alleen ervaren gebruikers dienen wijzigingen aan te brengen in de configuratie. Zie het dialoogvenster **Geavanceerde** <u>instellingen</u> dat u kunt openen via **Bestand/Geavanceerde instellingen** in het systeemmenu voor meer opties voor de scanconfiguratie.



Knoppen in het dialoogvenster Instellingen voor scanschema

Er zijn twee knoppen op alle drie de tabbladen van het dialoogvenster **Instellingen voor scanschema** (<u>Schema-instellingen</u>, **Hoe er gescand moet worden** en <u>Wat</u> <u>er gescand moet worden</u>) en die hebben op alle drie de tabbladen dezelfde functies:

- Opslaan opslaan van alle wijzigingen die u hebt uitgevoerd op dit tabblad of een van de twee andere tabbladen van het dialoogvenster, het dialoogvenster sluiten en terugkeren naar het <u>standaarddialoogvenster van de AVG</u> <u>scaninterface</u>. Klik daarom, als u testparameters op alledrie de tabbladen wilt instellen, alleen op de knop om instellingen op te slaan, nadat u al uw wensen hebt gespecificeerd.
- **Annuleren** alle wijzigingen die u hebt aangebracht in instellingen op dit tabblad of één van de twee andere tabbladen van het dialoogvenster, ongedaan maken, het dialoogvenster sluiten en terugkeren naar het <u>standaarddialoogvenster van de AVG scaninterface</u>.

Bestand Qnderdelen Higtorie Extra Help Image: Computerscanner Image: Computerscanner <t< th=""><th>讃 AVG Enterprise</th><th></th><th></th><th></th><th></th></t<>	讃 AVG Enterprise				
Verzieht Computerscanner Orbigen konnet Omputerscanner On beide computer scannen Oberde computer scannen	Bestand Onderdelen	Historie	<u>E</u> xtra	Help	
Instellingen voor geplande scan Computerscanner Image: Statisticken Laatste scan: 33.08, 23.15 Updar: 33.08, 23.15<	🛃 AVO	G		U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.	
Schema-instellingen Hoe er gescand moet worden Wat er gescand moet worden Image: Schema-instellingen Hoe er gescand moet worden Image: Schema-instellingen Hoe er gescand moet worden Image: Schema-instellingen Image: Schema-instellin				Instellingen voor geplande scan	
Computerscanner Image: Statisticken Lastite scan: 3-308, 23.15 Updas: 2.32.2 Virusddabase: 28.21.1/1300 AVT Gedeelde documenten Image: Statisticken Image: Statisticken Lastite scan: 3-308, 23.15 Updase: 2.82.11.1/1300 AVT Image: Statisticken Lastite scan: 1.62-0008	0verzicht			Schema-instellingen Hoe er gescand moet worden Wat er gescand moet worden	
Statistieken Laakte scan: 33:08, 23:15 Update: 33:08, 23:15 Virusdatabase: 28:32:1.1/1300 AV(reverais: 80:81 Vervaldatum licentie: 1-6-2003		anner		De hele computer scannen	
Statistieken Laatste scan: 3-308, 23 15 Update: 33-08, 23 02 Vruuddabase: 269 21.1/1300 AVG versie: 80.81 Vervaldatum licentie: 1-6-2008	📝 Nu bijwerke	n		Bepaalde mappen of bestanden scannen	
XMelding weergeven	Statistieken Laatste scan: 3-3-08, Update: 3-3-08, Virusdatabase: 259,21 AVG versie: 8.0.81 Vervaldatum licentie: 1 Vervaldatum licentie: 1	23:15 23:02 1/1300 -6-2008		Bureaublad Deze computer Deze computer Deze computer Deze computer Deze computer Deze constants Deze constants	nnuleren

10.5.3.Wat er gescand moet worden



Op het tabblad **Wat er gescand moet worden** kunt u opgeven welke scan moet worden uitgevoerd: <u>een scan van de hele computer</u> of <u>een scan van specifieke</u> <u>bestanden of mappen</u>. Als u kiest voor het scannen van specifieke bestanden of mappen, wordt de in het onderste deel van het dialoogvenster weergegeven mapstructuur actief, zodat u mappen kunt opgeven die moeten worden gescand.

Knoppen in het dialoogvenster Instellingen voor scanschema

Er zijn twee knoppen op alle drie de tabbladen van het dialoogvenster **Instellingen voor scanschema** (<u>Schema-instellingen</u>, <u>Hoe er gescand moet worden</u> en Wat er gescand moet worden) en die hebben op alle drie de tabbladen dezelfde functies:

- Opslaan opslaan van alle wijzigingen die u hebt uitgevoerd op dit tabblad of een van de twee andere tabbladen van het dialoogvenster, het dialoogvenster sluiten en terugkeren naar het <u>standaarddialoogvenster van de AVG</u> <u>scaninterface</u>. Klik daarom, als u testparameters op alledrie de tabbladen wilt instellen, alleen op de knop om instellingen op te slaan, nadat u al uw wensen hebt gespecificeerd.
- **Annuleren** alle wijzigingen die u hebt aangebracht in instellingen op dit tabblad of één van de twee andere tabbladen van het dialoogvenster, ongedaan maken, het dialoogvenster sluiten en terugkeren naar het <u>standaarddialoogvenster van de AVG scaninterface</u>.



10.6.0verzicht scanresultaten

불 AVG Enterprise						_ 🗆 🗙
<u>B</u> estand <u>O</u> nderdelen Hi <u>s</u> torie <u>E</u> x	ra <u>H</u> elp					
U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.						
51	Overzicht scanresultaten					
Uverzicht	Naam	Begintijd	Eindtijd	Geteste objecten	Infecties	Spyware
	Bepaalde mappen of bestanden scannen	3-3-2008, 23:13	3-3-2008, 23:13	16	8/8	2/2
Computerscanner	🖹 Scan van Shell-extensie	3-3-2008, 23:15	3-3-2008, 23:15	88	0/0	0/0
Katistieken						
Laatste scan: 3-3-08, 23:15 Update: 3-3-08, 23:02 Virusdatabase: 269.21.1/1300 AVG versie: 8.0.81 Vervaldatum licentie: 1-6-2008 XMelding weergeven	Cetails weergeven	Itaat			Te	> rug

U kunt het dialoogvenster **Overzicht scanresultaten** openen als u in de <u>AVG</u> <u>scaninterface</u> op de knop **Scanhistorie**klikt. In het dialoogvenster staat een lijst met alle eerder uitgevoerde scans en informatie over de resultaten:

 Naam - de naam van de scan; dat kan de naam zijn van een vooraf gedefinieerde scan, maar ook de naam van een door u zelf gedefinieerde scan. Bij elke naam staat ook een pictogram waarmee het scanresultaat wordt aangeduid:

> I een groen pictogram duidt erop dat er tijdens de scan geen infectie is gedetecteerd

> I - een blauw pictogram duidt erop dat er een infectie is gedetecteerd, maar dat het geïnfecteerde object automatisch is verwijderd

- een rood pictogram duidt erop dat er een infectie is gedetecteerd die AVG niet heeft kunnen verwijderen!



De pictogrammen kunnen volledig of voor de helft worden weergegeven - volledig weergegeven pictogrammen duiden erop dat de scan op de juiste manier volledig is uitgevoerd; een half pictogram betekent dat de scan is afgebroken of onderbroken.

Let op: Raadpleeg het dialoogvenster <u>Scanresultaten</u> dat u opent door op de knop **Details weergeven** (onder in dit dialoogvenster) te klikken, als u meer informatie wenst over een uitgevoerde scan

- Begintijd datum en tijdstip waarop de scan is gestart
- Eindtijd datum en tijdstip waarop de scan is beëindigd
- Geteste objecten het aantal objecten dat tijdens de scan is getest
- Infecties het aantal virusinfecties dat is gedetecteerd/verwijderd
- Spyware de hoeveelheid spyware die is gedetecteerd/verwijderd
- **Informatie scanlogboek** informatie over het scanverloop en -resultaat (gewoonlijk bij het voltooien of afbreken)

Knoppen

Het dialoogvenster **Overzicht scanresultaten** heeft de volgende knoppen:

- Details weergeven deze knop is alleen actief als een bepaalde scan is geselecteerd in het bovenstaande overzicht; klik op de knop om het dialoogvenster <u>Scanresultaten</u> te openen met gedetailleerde gegevens over de geselecteerde scan
- **Resultaat verwijderen** deze knop is alleen actief als een bepaalde scan is geselecteerd in het bovenstaande overzicht; klik op de knop om het geselecteerde onderdeel te verwijderen uit het overzicht met scanresultaten
- Terug terug naar het standaard dialoogvenster van de AVG scaninterface



10.7. Details scanresultaten

Als in het dialoogvenster **Overzicht scanresultaten** een bepaalde scan is geselecteerd, kunt u op de knop **Details weergeven** klikken om het dialoogvenster **Scan resultaten** te openen met gedetailleerde informatie over het verloop en de resultaten van de geselecteerde scan.

Het dialoogvenster heeft bovendien een aantal tabbladen:

- <u>**Resultatenoverzicht**</u> dit tabblad wordt steeds weergegeven en bevat statistische gegevens over de voortgang van het scanproces
- <u>Infecties</u> dit tabblad wordt alleen weergegeven als een <u>virusinfectie</u> is gedetecteerd tijdens het scannen
- <u>Spyware</u> dit tabblad wordt alleen weergegeven als <u>spyware</u> is gedetecteerd tijdens het scannen
- <u>Waarschuwingen</u> dit tabblad wordt alleen weergegeven als er tijdens het scannen is geconstateerd dat er objecten zijn die niet kunnen worden gescand
- Informatie dit tabblad wordt alleen weergegeven als er potentiële gevaren zijn gedetecteerd die niet in de bovenstaande categorieën kunnen worden ondergebracht; in dat geval staat er op het tabbblad een waarschuwing met betrekking tot de vondst



10.7.1.Tabblad Overzicht resultaten

🙀 AVG Enterprise		
Bestand Onderdelen Historie Extra	Help	
🛃 AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-date en functioneren correct.	
	Scapresultaten	
Overzicht	Resultatenoverzicht Infecties Spyware	
Computerscanner	Scan "Bepaalde mappen of bestanden scannen" is voltooid.	
🔮 Bepaalde mappen of bes	🕷 Infecties aangetroffen: 8	
Nu biiwarkan	Geïnfecteerde objecten verwijderd of hersteld 8	
Nu bijwerken	🔕 Niet verwijderd of hersteld. 0	
	2 Gevonden spyware: 2	
	Verwijderde spyware: 2	
	Viniet verwijderd:	
	Scan is gestart: maandag 3 maart 2008, 23:13:55	
	Totaal gescande objecten: 16	
	Verbruikte tijd: 2 seconde (n)	
Statistickon	Geconstateerde fouten: 0	
	Overzicht exporteren naar bestand	
Update: 3-3-06, 23:02		
Virusdatabase: 269.21.1/1300		
AVG versie: 8.0.81		
Vervaldatum licentie: 1-6-2008		_
	De scan is voltooid. Sluiten resultaten	
XMelding weergeven		_

Op het tabblad **Scanresultaten** staat gedetailleerd cijfermateriaal met informatie over:

- gedetecteerde virusinfecties / spyware
- verwijderde virusinfecties / spyware
- de hoeveelheid <u>virusinfecties</u> / <u>spyware</u> die niet kan worden verwijderd of hersteld

Bovendien staat er informatie over de datum en het precieze tijdstip waarop de scan is uitgevoerd, het totale aantal gescande objecten, de duur van de scan en het aantal fouten dat tijdens het scannen is opgetreden.

Knoppen

Dit dialoogvenster heeft slechts één knop. Als u op de knop **Sluiten** klikt, keert u terug naar het dialoogvenster **Overzicht scanresultaten**.



10.7.2.Tabblad Infecties

🕌 AVG Enterprise			
Bestand Onderdelen Historie Extra	Help		
AVG	U bent beschermd. Alle beveiligingsfuncties zijn up-to-c	late en functioneren correct.	
Overzicht	Resultatenoverzicht Infecties Spyware		
	Bestand	Infectie	Resultaat
	🔄 C:\Test\eicarcom2.zip:\eicar_com.zip:\eicar.com	Virus herkend EICAR_Test	Verplaatst naar de quarantaine
🤍 🔇 Bepaalde mappen of bes	🗣 C:\Test\eicarcom2.zip:\eicar_com.zip	Virus herkend EICAR_Test	Verplaatst naar de quarantaine
	👰 C:\Test\eicarcom2.zip	Virus herkend EICAR_Test	Verplaatst naar de quarantaine
Nu bijwerken	🗟 C:\Test\eicar_com.zip:\eicar.com	Virus herkend EICAR_Test	Verplaatst naar de guarantaine
	🚇 C:\Test\eicar_com.zip	Virus herkend EICAR_Test	Verplaatst naar de guarantaine
	🔄 C:\Test\Nt_rootkit0.40.zip:_rootsys	Trojaans paard BackDoor.Ntrootkit.C	Verplaatst naar de quarantaine
	🗣 C:\Test\Nt_rootkit0.40.zip:\deploy.exe	Trojaans paard BackDoor.Ntrootkit.A	Verplaatst naar de quarantaine
	🗟 C:\Test\Nt_rootkit0.40.zip	Trojaans paard BackDoor.Ntrootkit.C	Verplaatst naar de quarantaine
Statistieken			
Laatste scan: 3-3-08, 23:13 Update: 3-3-08, 23:02 Virusdatabase: 259,21.171300 AVG versie: 8.0.81 Vervaldatum licentie: 15:2008	Details weergeven	Geselecteerde infecties verwijderen	Alle niet-herstelde infecties verwijderen
XMelding weergeven	👔 De scan is voltooid.		Sluiten resultaten

Het Tabblad **Infecties** wordt alleen weergegeven in het dialoogvenster **Scanresultaten** als tijdens het scannen een <u>virusinfectie</u> is gedetecteerd. Het tabblad is onderverdeeld in drie secties met de volgende informatie:

- Bestand het volledige pad naar de oorspronkelijke locatie van het geïnfecteerde object
- **Infecties** de naam van het gedetecteerde <u>virus</u> (*Raadpleeg de online* <u>Virusencyclopedie</u> voor meer informatie over specifieke virussen)
- **Resultaat** De huidige status van het geïnfecteerde object dat tijdens het scannen is gedetecteerd:
 - *Geïnfecteerd* het geïnfecteerde object is gedetecteerd, maar niet van de oorspronkelijke locatie verwijderd (*bijvoorbeeld omdat u <u>de functie</u> <u>voor automatisch herstel hebt uitgeschakeld</u>bij bepaalde scaninstellingen)*
 - Hersteld het geïnfecteerde object is automatisch hersteld en niet van de oorspronkelijke locatie verwijderd



- Verplaatst naar de quarantaine het geïnfecteerde object is verplaatst naar de <u>quarantaine</u>
- o Verwijderd het geïnfecteerde object is verwijderd
- Toegevoegd aan de PUP-uitzonderingen er is vastgesteld dat het gevonden object tot de uitzonderingen behoort en het object is toegevoegd aan de lijst met PUP-uitzonderingen (geconfigureerd bij PUP-uitzonderingen in het dialoogvenster Geavanceerde instellingen)
- Vergrendeld bestand niet getest het object is vergrendeld en daarom kan AVG het niet scannen
- Mogelijk gevaarlijk object het object is gedetecteerd als mogelijk gevaarlijk, maar niet geïnfecteerd (*het kan bijvoorbeeld macro's bevatten*); de informatie moet worden opgevat als waarschuwing
- Herstart vereist voor het voltooien van bewerking het geïnfecteerde object kan niet worden verwijderd, voor volledig verwijderen is een herstart van de computer noodzakelijk

Knoppen

Het dialoogvenster heeft drie knoppen:

• **Details weergeven** - als u op de knop klikt, wordt een nieuw dialoogvenster **Details scanresultaten** geopend:

	maarao olgonbenap	
Objectnaam	C:\Test\eicarcom2.zip:\eicar_com.zip	
Detectienaam	Virus herkend EICAR_Test	
Objecttype	bestand	
SDK-type	Kern	
Resultaat	Verplaatst naar de guarantaine	
actiehistorie		



In dat dialoogvenster staat informatie over de locatie van het gedetecteerde geïnfecteerde object (**Naam eigenschap**). Met de knoppen **Vorige** / **Volgende** kunt u door de informatie over gedetecteerde objecten bladeren. Met de knop **Sluiten**sluit u het dialoogvenster weer.

- Geselecteerde infecties verwijderen klik op deze knop om het geselecteerde object te verplaatsen naar de <u>Quarantaine</u>
- Alle niet-herstelde infecties verwijderen als u op deze knop klikt, worden alle objecten verwijderd die niet kunnen worden hersteld of verplaatst naar de <u>Quarantaine</u>
- Sluiten het dialoogvenster wordt gesloten en u keert terug naar het dialoogvensterOverzicht scanresultaten

10.7.3.Tabblad Spyware

🕌 AVG Enterprise					
<u>B</u> estand <u>O</u> nderdelen Hi <u>s</u> torie <u>E</u> xtra	Help				
🕌 AVG	U bent bescherr Alle beveiligingsfunct	nd. ties zijn up-to-date e	n functioneren correct.		
	Scanresultaten				
0verzicht	Resultatenoverzicht Infecties Spy	ware			
Computerscanner	Bestand	Infectie	Resultaat		
	C:\Test\Adware\01210827.ex1	Adware Generic.IP	Verplaatst naar de quarantaine		
Bepaalde mappen of bes	🕎 C:\Test\Adware\01210828.ex1	Adware Generic.IZ	Verplaatst naar de quarantaine		
📝 Nu bijwerken					
Statistieken					
Laatste scan: 3-3-08, 23:13					
Update: 3-3-08, 23:02 Virusdatabase: 269.21.1/1300	Details weergeven	Gesel	ecteerde infecties verwijderen	Alle niet-herstelde i	nfecties verwijderen
AVta versie: 8.0.81 Vervaldatum licentie: 1-6-2008					
	🚺 De scan is voltooid.				Sluiten resultaten
VMelding weergeven					

Het Tabblad **Spyware** wordt alleen weergegeven in het dialoogvenster **Scanresultaten** als tijdens het scannen een <u>spyware</u> is gedetecteerd. Het tabblad is onderverdeeld in drie secties met de volgende informatie:

• Bestand - het volledige pad naar de oorspronkelijke locatie van het



geïnfecteerde object

- **Infecties** de naam van de gedetecteerde <u>spyware</u> (*Raadpleeg de online* <u>Virusencyclopedie</u> voor meer informatie over specifieke virussen)
- Resultaat De huidige status van het object dat tijdens het scannen is gedetecteerd:
 - Geïnfecteerd het geïnfecteerde object is gedetecteerd, maar niet van de oorspronkelijke locatie verwijderd (bijvoorbeeld omdat u <u>de functie</u> <u>voor automatisch herstel hebt uitgeschakeld</u>bij bepaalde scaninstellingen)
 - *Hersteld* het geïnfecteerde object is automatisch hersteld en niet van de oorspronkelijke locatie verwijderd
 - Verplaatst naar de quarantaine het geïnfecteerde object is verplaatst naar de <u>quarantaine</u>
 - o Verwijderd het geïnfecteerde object is verwijderd
 - Toegevoegd aan de PUP-uitzonderingen er is vastgesteld dat het gevonden object tot de uitzonderingen behoort en het object is toegevoegd aan de lijst met PUP-uitzonderingen (geconfigureerd bij <u>PUP-uitzonderingen</u> in het dialoogvenster Geavanceerde instellingen)
 - Vergrendeld bestand niet getest het object is vergrendeld en daarom kan AVG het niet scannen
 - Potentieel gevaarlijk object het object is gedetecteerd als potentieel gevaarlijk, maar niet geïnfecteerd (het kan bijvoorbeeld macro's bevatten); de informatie moet worden opgevat als waarschuwing
 - Herstart vereist voor het voltooien van bewerking het geïnfecteerde object kan niet worden verwijderd, voor volledig verwijderen is een herstart van de computer noodzakelijk

Knoppen

Het dialoogvenster heeft drie knoppen:

• **Details weergeven** - als u op de knop klikt, wordt een nieuw dialoogvenster **Details scanresultaten** geopend:



Naam eigenschap	Waarde eigenschap
Objectnaam	C:\Test\eicarcom2.zip:\eicar_com.zip
Detectienaam	Virus herkend EICAR_Test
Objecttype	bestand
5DK-type	Kern
Resultaat	Verplaatst naar de guarantaine
actiehistorie	

In dat dialoogvenster staat informatie over de locatie van het gedetecteerde geïnfecteerde object (*Naam eigenschap*). Met de knoppen *Vorige / Volgende* kunt u door de informatie over gedetecteerde objecten bladeren. Met de knop *Sluiten*sluit u het dialoogvenster weer.

- Geselecteerde infecties verwijderen klik op deze knop om het geselecteerde object te verplaatsen naar de <u>Quarantaine</u>
- Alle niet-herstelde infecties verwijderen als u op deze knop klikt, worden alle objecten verwijderd die niet kunnen worden hersteld of verplaatst naar de <u>Quarantaine</u>
- Sluiten het dialoogvenster wordt gesloten en u keert terug naar het dialoogvenster<u>Overzicht scanresultaten</u>

10.7.4.Tabblad Waarschuwingen

Op het tabblad **Waarschuwingen** staat informatie over "verdachte" objecten (*meestal bestanden*) die tijdens het scannen zijn gedetecteerd. Als ze worden gedetecteerd door <u>Resident Shield</u> worden deze bestanden geblokkeerd zodat ze niet meer toegankelijk zijn. Voorbeelden van dit soort objecten zijn: verborgen bestanden, cookies, verdachte registersleutels, met een wachtwoord beschermde documenten of archiefbestanden, enz.

10.7.5.Tabblad Informatie

Op het tabblad **Informatie** staan gegevens over objecten die niet kunnen worden ondergebracht bij infecties, spyware, e.d. Er kan niet worden vastgesteld dat ze gevaarlijk zijn, maar het is wel belangrijk er aandacht aan te besteden. Alle gegevens



op dit tabblad zijn louter informatief van aard.

10.8.Quarantaine

🛃 Historie				
Eventhistorie				
	Infectietype	Virusnaam	Pad naar het bestand	Datum van opslaan
	🗱 PUP	Adware Generic.IP	C:\Test\Adware\01210827.ex1	3-3-2008, 23:13:56
	🗱 PUP	Adware Generic.IZ	C:\Test\Adware\01210828.ex1	3-3-2008, 23:13:56
	🗱 Infectie	Virus herkend EICAR_Test	C:\Test\eicarcom2.zip	3-3-2008, 23:13:58
	🗱 Infectie	Virus herkend EICAR_Test	C:\Test\eicar_com.zip	3-3-2008, 23:13:58
	雛 Infectie	Trojaans paard BackDoor.Ntrootkit.C	C:\Test\Nt_rootkit0.40.zip	3-3-2008, 23:13:58
	Herstellen	Verwijderen Opnieuw scannen	Verzenden voor analyse Quar	antaine leegmaken
			Ok Annuleren	Toepassen

Quarantaine voorziet in een veilige omgeving voor het beheren van verdachte of geïnfecteerde objecten die tijdens AVG-tests zijn gedetecteerd. Als er tijdens het scannen een geïnfecteerd object wordt gedetecteerd, wordt u gevraagd wat er met het verdachte object moet gebeuren als het desbetreffende object niet automatisch kan worden hersteld. Het wordt aanbevolen om het object in een dergelijk geval naar de **Quarantaine** te verplaatsen, zodat het daar kan worden afgehandeld.

De interface van **Quarantaine** wordt in een eigen venster geopend, en biedt een overzicht met informatie over in quarantaine geplaatste, geïnfecteerde objecten:

- **Infectietype** er wordt onderscheid gemaakt in typen op basis van het infectieniveau (*alle opgesomde objecten kunnen daadwerkelijk of mogelijk geïnfecteerd zijn*)
- **Virusnaam** de naam van het gedetecteerde virus, zoals dat is geregistreerd in de <u>Virusencyclopedie</u> (online)
- Pad naar het bestand het volledige pad naar de oorspronkelijke locatie van het gedetecteerde geïnfecteerde bestand



Datum van opslaan - datum en tijdstip van detectie van het verdachte bestand en verplaatsing naar de Quarantaine

Knoppen

De interface van de **Quarantaine** heeft de volgende knoppen:

- *Herstellen* Het geïnfecteerde bestand wordt teruggeplaatst op de oorspronkelijke locatie
- Verwijderen Het geïnfecteerde bestand wordt volledig uit de Quarantaine verwijderd
- **Opnieuw scannen** het verdachte bestand wordt opnieuw gecontroleerd om zeker te weten of het geïnfecteerd is
- **Verzenden voor analyse** het verdachte bestand wordt naar de AVGlaboratoria voor virussen gestuurd voor diepgaande analyse



11. AVG Updates

11.1.Updateniveaus

AVG kent drie updateniveaus die u kunt selecteren:

- **Update van definities** bevat wijzigingen die noodzakelijk zijn voor een betrouwbare beveiliging tegen virussen, spam en malware. In een dergelijke update zijn normaal gesproken geen wijzigingen in de code opgenomen. Alleen de virusdatabase wordt bijgewerkt. Deze update moet worden toegepast zodra deze beschikbaar is.
- **Update van programma** bevat diverse programmawijzigingen, reparaties en verbeteringen.

Bij het <u>plannen van een update</u>, kunt u selecteren op welk prioriteitsniveau u wilt downloaden en updates wilt uitvoeren.

11.2.Soorten updates

Er zijn twee soorten updates te onderscheiden:

- **Een update op verzoek** is een onmiddellijke AVG-update die kan worden uitgevoerd zodra de noodzaak zich daartoe voordoet.
- **Geplande update** U kunt in AVG ook een <u>updateplan instellen</u>. De geplande update wordt vervolgens op basis van de ingestelde configuratie periodiek uitgevoerd. Wanneer er op de ingestelde locatie nieuwe updatebestanden beschikbaar zijn, worden deze rechtstreeks van internet of vanuit de netwerkmap gedownload. Als er geen nieuwe updates beschikbaar zijn, gebeurt er niets.

11.3.Updateprocedure

De updateprocedure kan als dat nodig is, onmiddellijk worden uitgevoerd als u op de snelkoppeling **Nu bijwerken** <u>klikt</u>. De koppeling is altijd actief in alle dialoogvensters van de<u>AVG gebruikersinterface</u>. Het blijft echter raadzaam om regelmatig updates uit te voeren met behulp van het updateschema dat u kunt bewerken in het onderdeel<u>Updatebeheer</u>.

Als u de updateprocedure start, wordt eerst gecontroleerd of er nieuwe updates beschikbaar zijn. Zo ja, dan worden die gedownload en wordt het proces voor het bijwerken op gang gebracht. Tijdens het uitvoeren van de updateprocedure wordt het



dialoogvenster **Update** geopend dat op grafische wijze de voortgang in beeld brengt en bovendien een overzicht geeft van de relevante statistische parameters (*grootte* updatebestand, ontvangen gegevens, downloadsnelheid, verstreken tijd, ...).



Ouaraptaine	Datum en tijd event	Gebruiker	Bron	Eventomschrijving
- Quarancanic	3-3-2008 22:07:46	NT AUTHORITY'SYSTEM	General	AVG wordt gestart
	3-3-2008, 22:08:06	NT AUTHORITY'SYSTEM	General	AVG wordt uitgevoerd.
	3-3-2008, 22:22:39	NT AUTHORITY SYSTEM	Undate	Undate is gestart.
	3-3-2008, 22:22:39	NT AUTHORITY\SYSTEM	Update	Update is niet afgerond.
	Lege lijst			Lijst vernieuwen

12. Gebeurtenishistorie

U kunt het dialoogvenster **Gebeurtenishistorie** openen met de <u>systeemmenu</u>-optie **Historie/Gebeurtenishistorie Logboek**. In het dialoogvenster wordt een overzicht weergegeven van belangrijke gebeurtenissen die tijdens het uitvoeren van **AVG 8.0 Anti-Virus** zijn opgetreden. **Gebeurtenishistorie** legt de volgende gebeurtenistypen vast:

- Informatie over updates van de AVG-toepassing
- Het begin en einde van een test, en of de test stopgezet is (inclusief automatisch uitgevoerde tests)
- Gebeurtenissen die verband houden met virusdetectie (door <u>Resident Shield</u> of tijdens <u>scannen</u>), waaronder de detectielocatie
- Andere belangrijke gebeurtenissen

Knoppen

• Lijst legen - alle items uit de lijst gebeurtenissen verwijderen



• *Lijst vernieuwen* - alle items in de lijst gebeurtenissen bijwerken



13. Veelgestelde vragen en technische ondersteuning

Mocht u problemen ondervinden met AVG, op zakelijk of technisch gebied, raadpleeg dan de sectie met **veelgestelde vragen (FAQ)** op de website van AVG: <u>www.avg.</u> <u>com</u>.

Vindt u op die manier geen oplossing, neem dan via e-mail contact op met de technische ondersteuningsdienst. Gebruik daarvoor het contactformulier dat u kunt oproepen in het systeemmenu via de optie *Help / Online Help*.