AVG 8.5 Anti-virus plus firewall udgave

Brugervejledning

Dokumentrevision 85.1 (26.1.2009)

Indhold

1. Introduktion

Denne brugervejledning indeholder omfattende dokumentation for **AVG 8.5 Anti-virus plus firewall**

Tillykke med købet af AVG 8.5 Anti-virus plus firewall!

AVG 8.5 Anti-virus plus firewall er et i en række af prisvindende AVG-produkter, der er designet til at give dig fred i sindet og komplet sikkerhed for din pc. Som for alle AVG-produkter er **AVG 8.5 Anti-virus plus firewall** blevet fuldstændig redesignet fra bunden for at levere AVG's berømte og velkendte sikkerhedsbeskyttelse på en ny, mere brugervenlig og effektiv måde.

Dit nye **AVG 8.5 Anti-virus plus firewall**-produkt har en strømlinet grænseflade kombineret med en mere aggressiv og hurtigere scanning. Flere sikkerhedsfunktioner er blevet automatiseret for nemheds skyld, og der er inkluderet nye 'intelligente' brugerindstillinger, så du kan tilpasse vores sikkerhedsfunktioner til din livsstil. Ingen kompromitterende brugervenlighed på bekostning af sikkerhed!

AVG er designet og udviklet for at beskytte dine computer- og netværksaktiviteter. Oplev fuld beskyttelse fra AVG.

2. AVG Installationskrav

2.1. Understøttede operativsystemer

AVG 8.5 Anti-virus plus firewall er udviklet til at beskytte arbejdsstationer med følgende operativsystemer:

- Windows 2000 Professional SP4 + Update Rollup 1
- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 og x64, alle udgaver)

(og muligvis senere servicepakker for specifikke operativsystemer)

2.2. Minimums-hardwarekrav

Minimums-hardwarekravene til **AVG 8.5 Anti-virus plus firewall** er følgende:

- Intel Pentium CPU 1,2 GHz
- 70 MB ledig harddiskplads (af installationsgrunde)
- 256 MB RAM

3. AVG Installationsmuligheder

AVG kan enten installeres fra den installationsfil, der findes på installations-cd'en, eller du kan downloade den sidste nye installationsfil fra AVG's websted (www.avg.com).

Inden du starter installation af AVG anbefales det kraftigt, at du besøger AVG's websted for at se, om der ligger nye installationsfiler. Derved kan du være sikker på, at du installerer den sidste nye version af AVG 8.5 Anti-virus plus firewall.

Vi anbefaler, at du prøver vores nye AVG Download Manager-værktøj, som hjælper dig med at vælge den rigtige installationsfil!

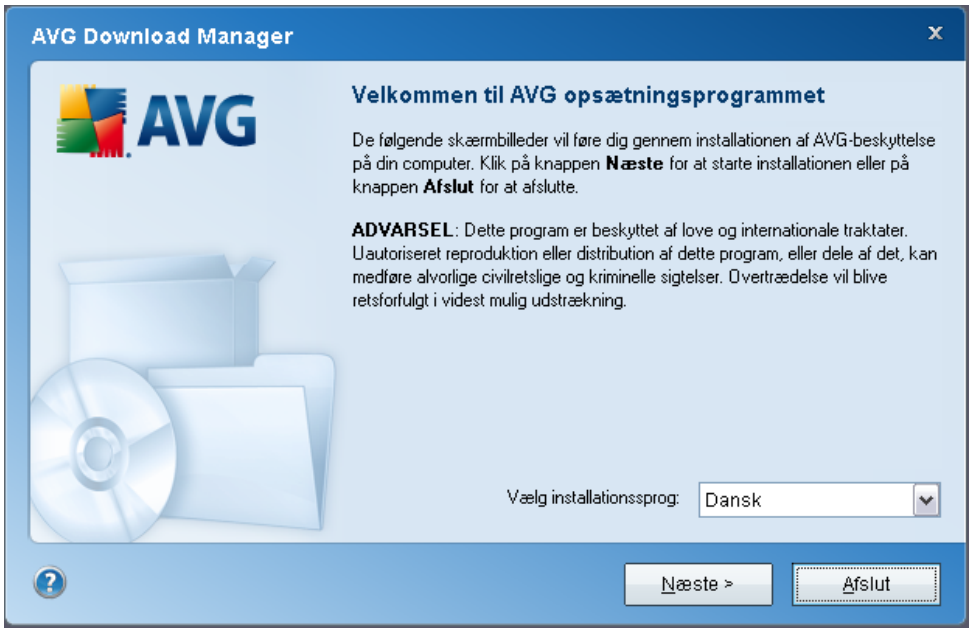
Under installationsprocessen bliver du bedt om dit licens-/salgsnummer. Sørg for, at det er til rådighed, inden du starter installationen. Salgsnummeret findes på cd'ens indpakning. Hvis du har købt din kopi af AVG online, er dit licensnummer blevet sendt via e-mail.

4. AVG Download Manager

AVG Download Manager er et simpelt værktøj, som hjælper dig med at vælge den rigtige installationsfil til dit AVG-produkt. Baseret på dine angivne data vælger administrationsprogrammet det specifikke produkt, licenstypen, ønskede komponenter og sprog. Til sidst fortsætter **AVG Download Manager** med at downloade og køre den korrekte installationsproces.

Herunder findes en kort beskrivelse af de enkelte trin, du skal foretage i **AVG Download Manager**:

4.1. Sprogvalg



I dette første trin af **AVG Download Manager** skal du vælge installationssproget i rullemenuen. Bemærk, at dit sprogvalg kun gælder for installationen. Efter installationen kan du vælge sprog direkte fra programindstillingerne. Tryk derefter på knappen ***Næste*** for at fortsætte.

4.2. Forbindelseskontrol

I det næste trin forsøger **AVG Download Manager** at oprette en internetforbindelse for at finde opdateringer. Du får ikke mulighed for at gå videre til download-processen, før **AVG Download Manager** har gennemført forbindelsestesten.

- Hvis testen ikke viser nogen forbindelse, skal du kontrollere, at du virkelig har forbindelse til internettet. Klik derefter på knappen ***Prøv igen***

- Hvis du bruger en proxy-forbindelse til internettet, skal du klikke på knappen ***Proxy-indstillinger*** for at angive dine proxy-oplysninger:

- Hvis kontrollen lykkedes, skal du trykke på knappen ***Næste*** for at fortsætte.

4.3. Proxy-indstillinger

Hvis **AVG Download Manager** ikke kunne identificere dine proxy-indstillinger, skal du angive dem manuelt. Udfyld følgende data:

- ***Server*** - indtast et gyldigt proxyservernavn eller IP-adresse
- ***Port*** - angiv det pågældende portnummer
- ***Bruger proxy-validering*** - marker dette afkrydsningsfelt, hvis din proxyserver kræver validering.
- ***Vælg validering*** - vælg valideringstypen fra rullemenuen. Vi anbefaler på det kraftigste, at du beholder standardværdien (*proxyserveren overfører så automatisk sine krav til dig*). Hvis du er en erfaren bruger, kan du også vælge valgmuligheden Basis (*kræves af visse servere*) eller NTLM (*kræves af alle ISA-servere*). Indtast derefter et gyldigt ***Brugernavn*** og en ***Adgangskode*** (eventuelt).

Bekræft dine indstillinger ved at trykke på knappen ***Anvend*** for at fortsætte til næste trin af **AVG Download Manager**.

4.4. Vælg licenstype

I dette trin bliver du bedt om at vælge licenstype for det produkt, du gerne vil downloade. Beskrivelsen gør det muligt for dig at vælge den, der passer dig bedst:

- ***Fuld version*** - dvs. ***AVG Anti-virus***, ***AVG Anti-virus plus Firewall*** eller ***AVG Internet-sikkerhed***
- ***Prøveversion*** - giver dig mulighed for at anvende alle funktionerne i et fuldt AVG-produkt i en begrænset periode på 30 dage
- ***Gratis version*** - giver gratis beskyttelse til hjemmebrugere, men applikationens funktioner er begrænsede! Den gratis version indeholder også kun nogle af funktionerne, der findes i betalingsproduktet.

4.5. Download filer til installation

Nu har du angivet alle de oplysninger, som er nødvendige for at **AVG Download Manager** kan starte download af installationspakken og køre installationen. Fortsæt til AVG installationsprocessen.

5. AVG Installationsproces

For at installere AVG på din computer skal du bruge den nyeste installationsfil. Du kan bruge installationsfilen på cd'en, der ligger i æsken, men denne fil kan være forældet.

Derfor anbefaler vi at hente den nyeste fil online. Du kan downloade filen fraAVG's websted (på www.avg.com) / sektionen ***Downloads.*** Eller du kan bruge vores nye **AVG Download Manager** -værktøj, som hjælper dig med at oprette og downloade den nødvendige installationspakke og køre installationsprocessen.

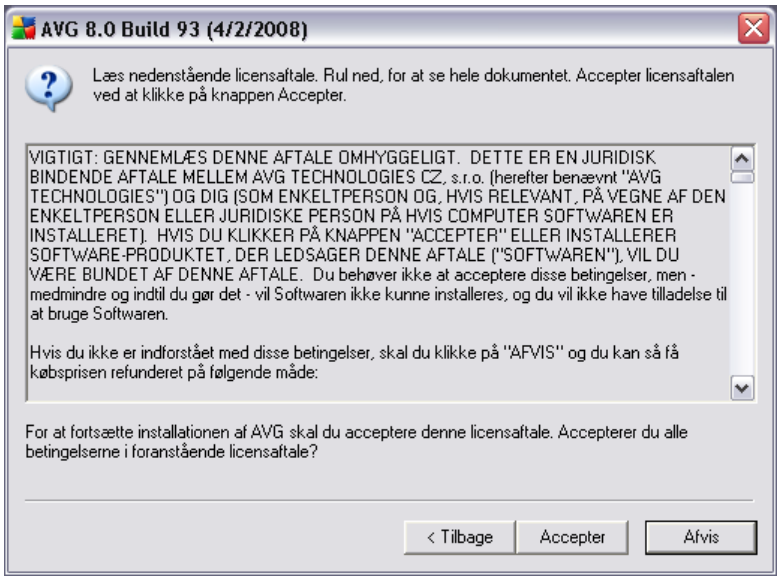
Installationen er en række af dialogvinduer med en kort beskrivelse af, hvad du skal gøre på hvert trin. Herunder giver vi en forklaring til hvert dialogvindue:

5.1. Installationskørsel

Installationsprocessen starter med vinduet ***Velkommen til installationsprogrammet til AVG***. Her vælger du det sprog, der skal bruges til installationen. Find punktet ***Vælg dit installationssprog*** i den nederste del af dialogvinduet, og vælg det ønskede sprog i rullemenuen. Klik derefter på knappen ***Næste*** for at bekræfte og fortsætte til næste dialog.

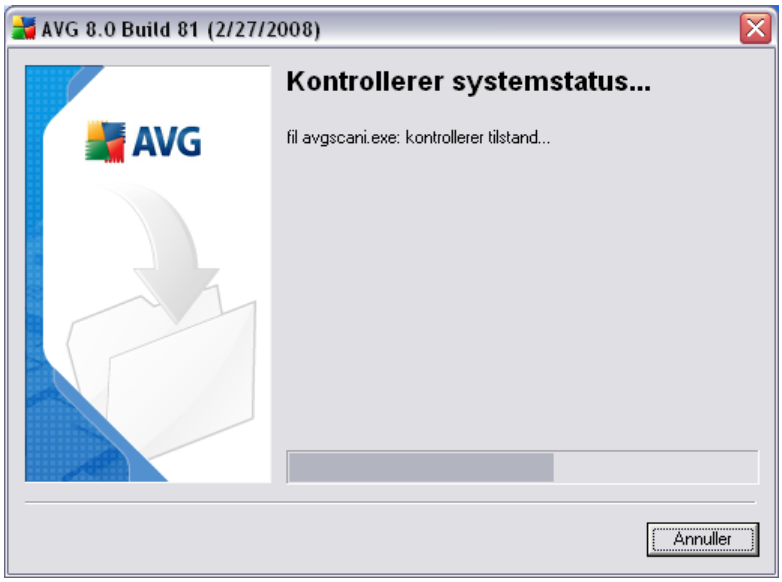
NB! *Her vælger du kun sprog til installationen. Du vælger ikke sprog for AVG-applikationen - det kan angives senere i installationsprocessen!*

5.2. Licensaftale



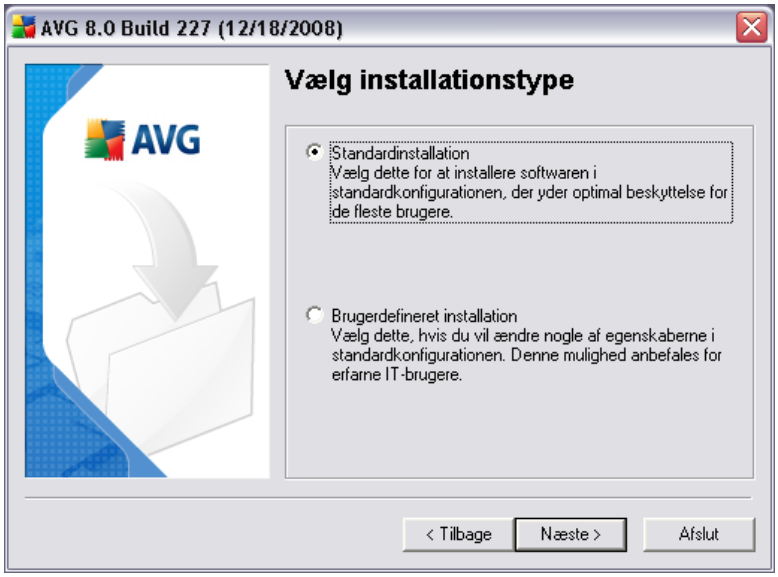
Dialogen ***Licensaftale*** indeholder den fulde ordlyd af AVG-licensaftalen. Læs den omhyggeligt og bekræft, at du har læst, forstået og accepterer aftalen ved at klikke på knappen ***Jeg accepterer***. Hvis du ikke er enig i licensaftalen skal du klikke på ***Jeg accepterer ikke***, og installationsprocessen bliver afsluttet med det samme.

5.3. Kontrollerer systemstatus



Når du har bekræftet licensaftalen, bliver du viderestillet til dialogen ***Kontrollerer systemstatus***. I denne dialog skal du ikke foretage dig noget. Dit system kontrolleres, før installationen af AVG kan starte. Vent, indtil processen er afsluttet, og fortsæt derefter automatisk til følgende dialog.

5.4. Vælg installationstype



I dialogboksen ***Vælg installationstype*** kan du vælge mellem to installationsmuligheder: ***standard*** og ***brugertilpasset*** installation.

For de fleste brugere anbefales det at holde sig til ***standardinstallationen***, der installerer AVG i fuldautomatisk tilstand med indstillinger, der er foruddefinerede af softwareleverandøren. Denne konfiguration giver maksimal sikkerhed kombineret med optimal anvendelse af ressourcer. Hvis der i fremtiden opstår behov for at ændre konfigurationen, har du altid mulighed for at gøre det direkte i AVG-applikationen.

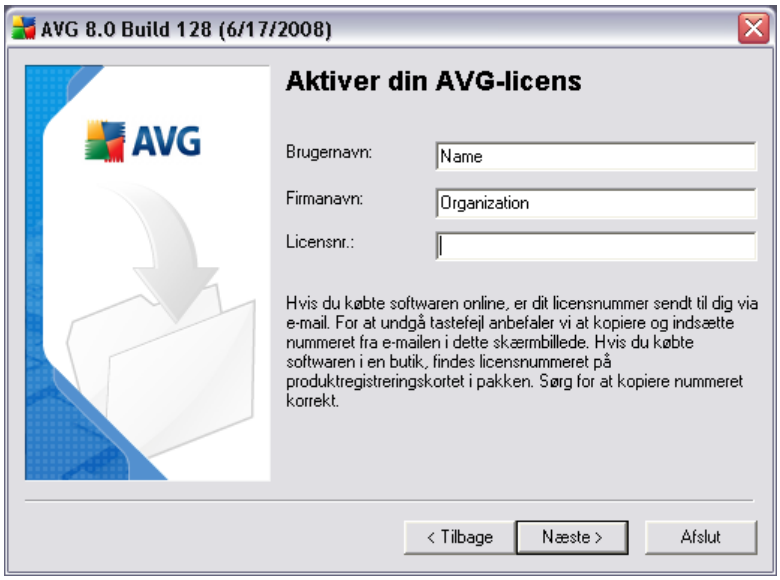
Brugertilpasset installation bør kun anvendes af erfarne brugeren, der har en god grund til at installere AVG uden standardindstillingerne. F.eks for at opfylde specifikke systemkrav.

5.5. Aktiver din AVG-licens

I dialogboksen ***Aktiver din AVG-licens*** skal du udfylde dine registreringsdata. Indtast dit navn (feltet ***Brugernavn***) og navnet på din organisation (feltet ***Firmanavn***).

Indtast derefter dit licens-/salsnummer i tekstfeltet ***Licens-/salgsnummer***. Salgsnummeret findes på cd-etuiet i AVG-æsken. Licensnummeret findes i den bekræftelses-e-mail, du modtog efter du købte AVG online. Du skal indtaste nummeret nøjagtig som det er vist. Hvis licensnummeret er tilgængeligt i digitalt

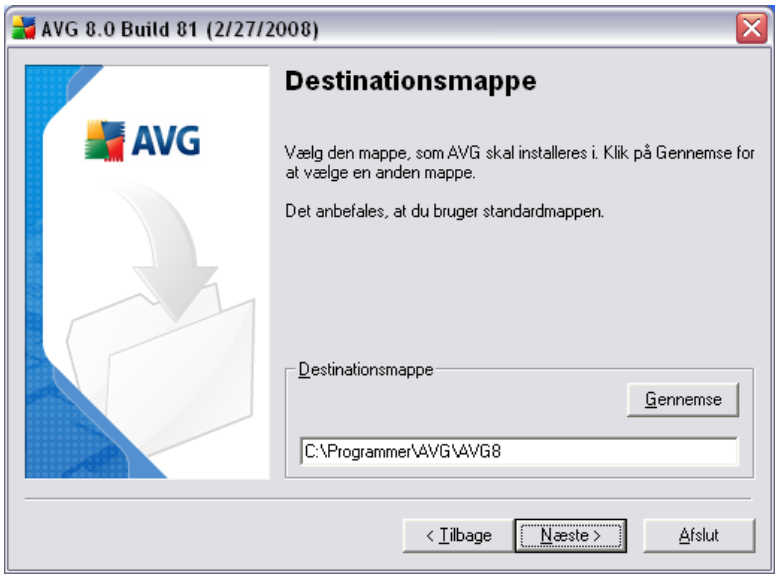
format (i e-mailen), anbefales det at indsætte det med kopier/sæt ind-metoden.



Klik på knappen ***Næste*** for at fortsætte installationsprocessen.

Hvis du har valgt standardinstallation i det forrige trin, bliver du viderestillet direkte til dialogboksen ***Installationsoversigt*** . Hvis du valgte brugertilpasset installation, fortsætter du med dialogboksen ***Destinationsmappe***.

5.6. Brugertilpasset installation - Destinationsmappe



I dialogen ***Destinationsmappe*** kan du angive, hvor AVG skal installeres. Som standard installeres AVG i programmappen på drev C:. Hvis du vil ændre denne placering, skal du bruge knappen ***Gennemse*** til at vise drevstrukturen og vælge den pågældende mappe. Klik på knappen ***Næste*** for at bekræfte.

5.7. Brugertilpasset installation - Valg af komponenter

Dialogen ***Valg af komponenter*** viser en oversigt over alle AVG-komponenter, der kan installeres. Hvis standardindstillingerne ikke passer dig, kan du fjerne/tilføje specifikke komponenter.

Du kan imidlertid kun vælge mellem de komponenter, der medfølger i den AVG-udgave, du har købt. Du bliver kun tilbudt at installere disse komponenter i dialogen Valg af komponenter!

I listen over komponenter, der skal installeres, kan du definere hvilke(*t*) sprog, AVG skal installeres på. Marker punktet ***Yderligere installerede sprog*** og vælg derefter de ønskede sprog i den pågældende menu.

Klik på elementet ***E-mail Scanner*** for at åbne det og beslutte, hvilket plug-in, der skal installeres for at garantere, din elektroniske mailsikkerhed. Som standard bliver ***Plugin til Microsoft Outlook*** installeret. En anden specifik valgmulighed er ***Plugin til The Bat!*** Hvis du bruger en anden e-mail-klient (*MS Exchange, Qualcomm Eudora, ...*), skal du bruge valgmuligheden ***Personlig e-mail-scanner*** for at sikre din e-mail-kommunikation automatisk, uanset hvilket e-mail-program du bruger.

Fortsæt ved at klikke på knappen ***Næste***.

5.8. AVG Sikkerhedsværktøjslinje

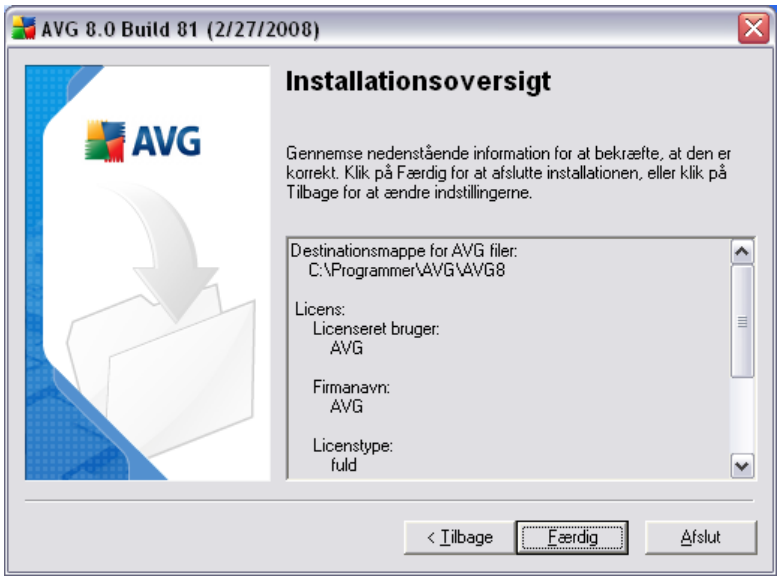
I dialogen ***AVG Sikkerhedsværktøjslinje*** skal du bestemme, om du vil installere ***AVG Sikkerhedsværktøjslinje*** - hvis du ikke ændrer standardindstillingerne, bliver denne komponent installeret automatisk i din internetbrowser for i samarbejde med AVG 8.0 og AVG XPL-teknologi, for at give dig en omfattende online beskyttelse, mens du surfer på internettet.

5.9. Windows Firewall

Licensnummeret, du har angivet i et af de tidligere opsætningstrin, svarer til **AVG 8.5 Anti-virus plus firewall** -udgaven, der indeholder AVG ***Firewall***. AVG ***Firewall*** kan ikke køre samtidig med en anden installeret firewall. I denne dialog skal du bekræfte, at du vil installere AVG ***Firewall***, og at du samtidig ønsker at deaktivere Windows Firewall.

Klik på knappen ***Næste*** for at fortsætte.

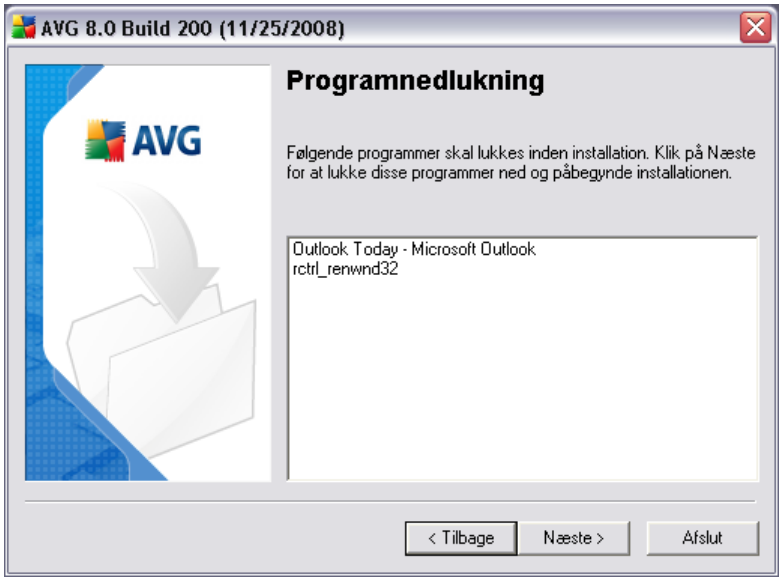
5.10.Installationsoversigt



Dialogen ***Opsætningsoversigt*** indeholder en oversigt over alle parametre i installationsprocessen. Sørg for, at alle oplysningerne er korrekte. Tryk derefter på knappen ***Afslut*** for at fortsætte. Ellers kan du bruge knappen ***Tilbage*** til at vende tilbage til den pågældende dialog og rette oplysningerne.

5.11.Programnedlukning

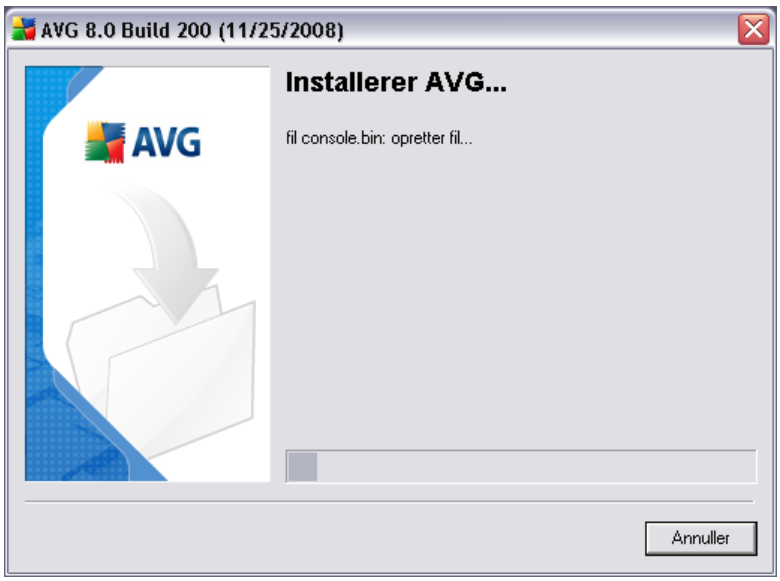
Før installationsprocessen starter, bliver du muligvis bedt om at afslutte nogle af de kørende programmer, der kan kollidere med installationen af AVG. I så fald vises dialogen ***Programnedlukning***. Denne dialog er kun til information, og den kræver ingen handling - hvis du accepterer at de anførte programmer lukkes automatisk, skal du klikke på ***Næste*** for at fortsætte:



Bemærk! *Kontrollér, at du har gemt alle dine data, før du bekræfter, at du vil have lukket det kørende program.*

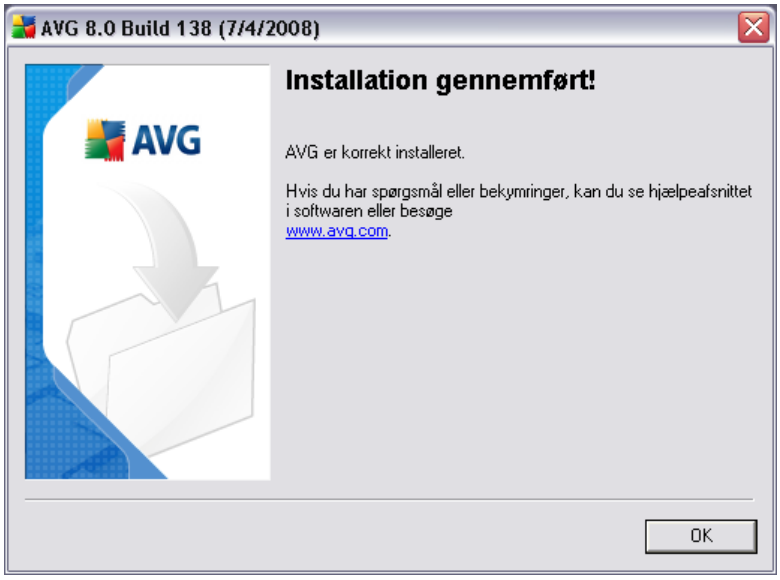
5.12.Installerer

Dialogen ***Installerer AVG***viser status for installationsprocessen, og du skal ikke foretage dig noget:



Vent til installationen er færdig. Derefter bliver du viderestillet til dialogen ***Installation gennemført***.

5.13.Installation gennemført



Installationen er færdig! dialog er det sidste trin i installationen af AVG. AVG er nu installeret på computeren og fuldt funktionsdygtig. Programmet kører i baggrunden i fuldautomatisk tilstand.

Efter installationen startes ***AVG grundlæggende konfigurationsguide*** automatisk og fører dig i nogle få trin gennem den elementære **AVG 8.5 Anti-virus plus firewall**-konfiguration. På trods af, at der er adgang til AVG-konfigurationen til enhver tid, mens AVG kører, anbefaler vi at bruge denne mulighed for at indstille den grundlæggende konfiguration ved hjælp af guiden.

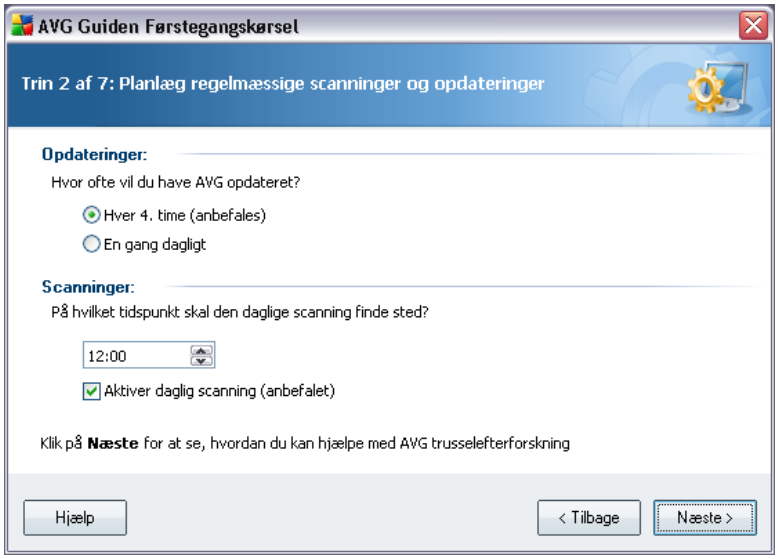
6. AVG Førstegangskørselsguide

Første gang du installerer AVG på din computer, vises ***AVG grundlæggende konfigurationsguide*** for at hjælpe dig med de indledende **AVG 8.5 Anti-virus plus firewall**-indstillinger. Selvom du kan indstille alle de anbefalede parametre senere, anbefales det at gennemgå guiden for med det samme at sikre computerens antivirusbeskyttelse på en enkel måde. Følg de trin, der beskrives i de enkelte vinduer i guiden :

6.1. Introduktion af AVG Førstegangskørselsguide

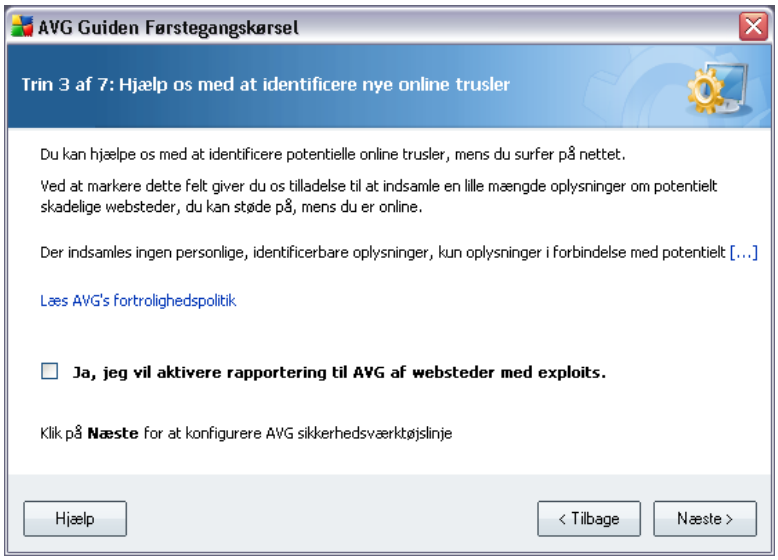
Velkomstvinduet ***Introduktion af AVG Førstegangskørselsguide*** opsummerer kortfattet status for AVG på din computer, og foreslår de trin, der skal gennemføres for at fuldstændiggøre beskyttelsen. Klik på ***Næste*** for at fortsætte.

6.2. Planlæg regelmæssige scanninger og opdateringer



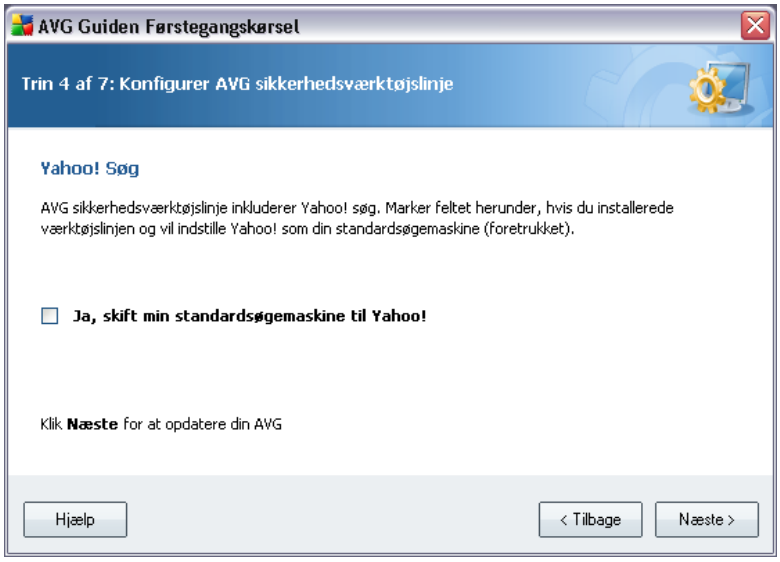
I dialogen ***Planlæg regelmæssige scanninger og opdateringer*** kan du indstille intervallet for søgning efter nye tilgængelige opdateringsfiler, og definere tidspunktet den planlagte scanning skal startes. Det anbefales at beholde standardværdierne. Klik på knappen ***Næste*** for at fortsætte.

6.3. Hjælp os med at identificere nye onlinetrusler



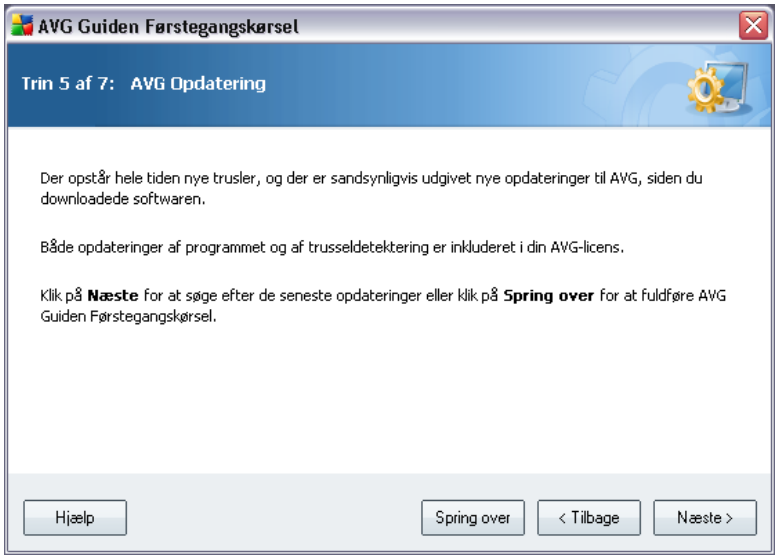
I dialogen ***Hjælp os med at identificere nye trusler*** skal du beslutte, om du vil aktivere indstillingen rapportering af exploits og ondsindede websteder, der findes af brugere, enten via ***AVG Surfskjold/ AVG Søgeskjold***-funktionerne i ***LinkScanner***-komponenten for at udbygge databasen, der indsamler oplysninger om ondsindet aktivitet på nettet. Det anbefales at bevare standardværdien og have rapporteringen aktiveret. Klik på knappen ***Næste*** for at fortsætte.

6.4. Konfigurer AVG Sikkerhedsværktøjslinjen



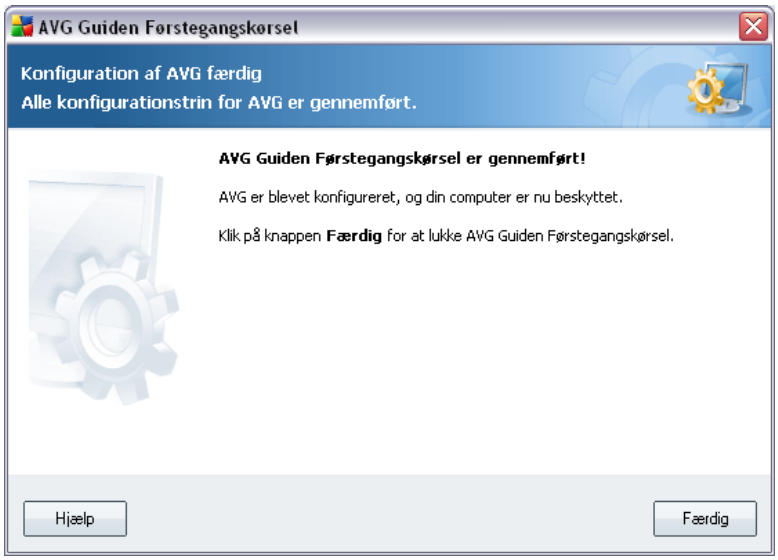
I dialogen ***Konfigurer AVG Sikkerhedsværktøjslinje*** kan du markere afkrydsningsfeltet for at definere, at du vil have Yahoo! som din standardsøgemaskine.

6.5. Opdater AVG-beskyttelse



Dialogen ***Opdater AVG-beskyttelse*** kontrollerer og downloader automatisk de seneste AVG-opdateringer. Klik på ***Næste*** for at downloade de seneste opdateringsfiler og udføre opdateringen.

6.6. AVG-konfiguration fuldført



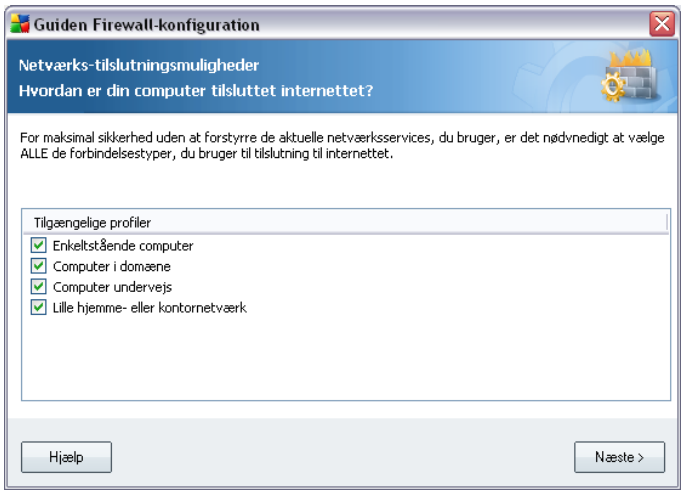
Nu er **AVG 8.5 Anti-virus plus firewall** konfigureret. Tryk på knappen ***Afslut*** for at starte med at bruge AVG.

7. Guiden Firewall-konfiguration

Guiden Firewall-konfiguration startes automatisk umiddelbart efter **AVG 8.5 Anti-virus plus firewall**-installationen. Selv om du kan konfigurere komponentens parametre senere, anbefales det, at du gennemgår guiden for at sikre, at ***Firewall*** fungere korrekt.

Guiden Firewall-konfiguration kan også kaldes direkte fra Firewal-grænsefladen ved at trykke på knappen ***Konfigurationsguide***.

7.1. Netværks-tilslutningsmuligheder



I denne dialog spørger ***Guiden Firewall-konfiguration***, hvordan din computer er sluttet til internettet. Eksempelvis kræver din notebook, der tilslutter sig Internettet fra mange forskellige steder (*lufthavne, hotelværelser mv.*) sikkerhedsregler, der er kraftigere end reglerne for en computer i et domæne (*virksomhedsnetværk, mv.*). Baseret på den valgte forbindelsestype vil ***Firewall***'s standardregler blive defineret med et passende sikkerhedsniveau.

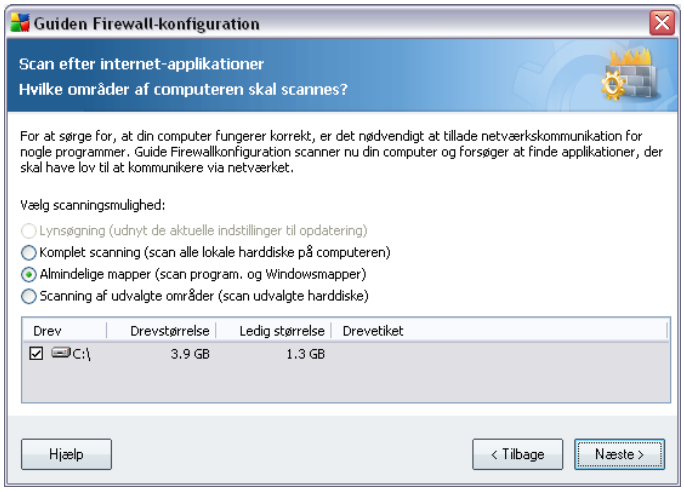
Du kan vælge mellem tre muligheder:

- ***Enkeltstående computer***
- ***Computer i domæne*** (virksomhedsnetværk)
- ***Computer undervejs*** (typisk en notebook)

- ***Lille hjemme- eller kontornetværk***

I denne dialogboks skal du vælge den/de forbindelsestype(r) der bedst passer din normale computerbrug. Du kan afkrydse flere valg, der modsvarer din aktuelle brug. Bekræft valget ved at trykke på knappen ***Næste*** og fortsætte til den næste dialog.

7.2. Scan efter Internet-applikationer



For at oprette den indledende ***Firewall***-konfiguration er det nødvendigt at scanne computeren og definere alle de applikationer og systemservices, der har brug for at kommunikere over netværket. Indledende .***Firewall***-regler bør oprettes for alle disse applikationer og services.

Bemærk: *Guiden detekterer alle generelt kendte applikationer, der kommunikerer over netværket, og definerer regler for disse applikationer. Den detekterer imidlertid muligvis ikke alle sådanne applikationer!*

I dialogen ***Scan efter internet-applikationer*** skal du beslutte, om du vil køre:

- ***Lynsøgning*** - denne mulighed er kun aktiv, hvis du har konfigureret ***Firewall*** tidligere, og der søges kun efter applikationer, der i aktuelt er gemt i den eksisterende ***Firewall***-konfiguration. Ny standardkonfiguration (dvs. anbefalet af producenten) bliver derefter anvendt på disse. Bemærk, at der ikke detekteres nye applikationer! Vi anbefaler denne mulighed, hvis du allerede har defineret ***Firewall***-regler og vil undgå at gentage hele scanningsprocessen.

- ***Komplet scanning*** - scan alle lokale harddiske på computeren

- ***Almindelige mapper*** - (*som standard*) scan kun program- og Windowsmapper, scanningstiden er væsentligt kortere

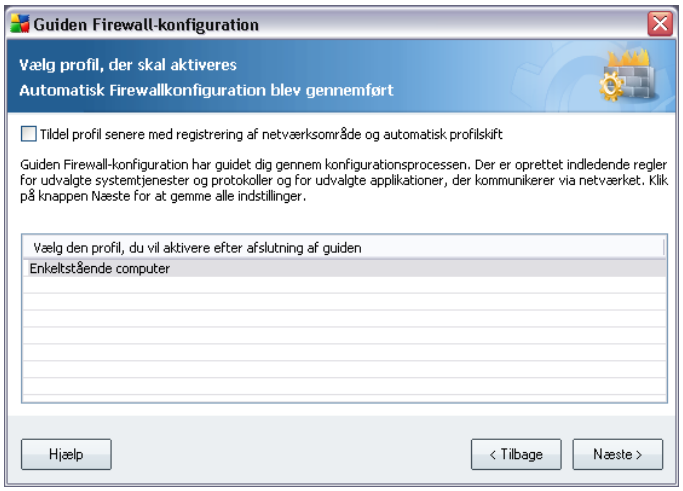
- ***Scanning af udvalgte områder*** - angiv udvalgte harddiske, der skal scannes

7.3. Vælg profil, der skal aktiveres

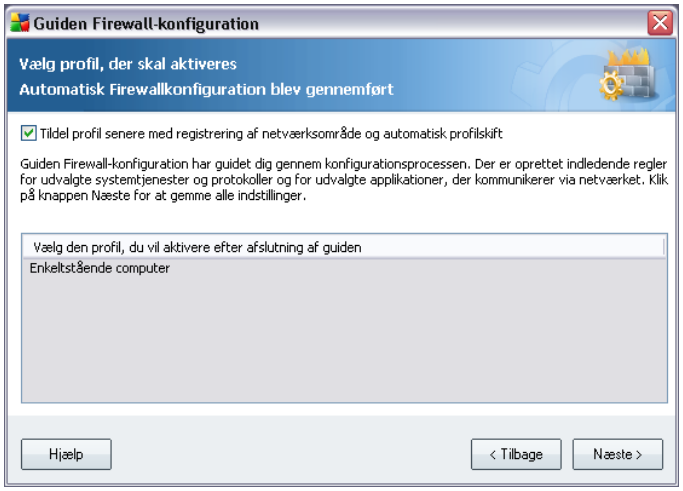
Dialogen ***Vælg profil, der skal aktiveres*** informerer om ***Firewall***-konfigurationen, der er indstillet i de forrige dialoger.

Før ***guiden Firewall-konfiguration*** lukkes, er det nødvendigt, at du vælger en profil, du vil bruge på din computer. Du kan vælge mellem op til tre indstillinger (enkeltstående computer, computer i domæne, og computer undervejs), baseret på de forbindelsesparametre, du har angivet i den første dialog (***Netværks-tilslutningsmuligheder***) i denne guide. Du kan senere skifte mellem de foruddefinerede ***Firewall***-profiler i henhold til din computers aktuelle krav.

Lige nu skal du helt enkelt vælge den ønskede profil på listen, og aktivere den ved at trykke på knappen ***Næste***:



Hvis du ikke ønsker at konfigurere profilerne manuelt, kan du aktivere funktionen til automatisk detektering af profil. Så vælger ***Firewallen*** automatically den bedst egnede profil, baseret på hvor og hvordan din computer i øjeblikket opretter forbindelse til netvøærket. Det automatiske profilvalg garanterer maksimal sikkerhed! For at vælge denne indstilling, skal du markere elementet ***Tildel profil senere med registrering af netværksområde og automatisk profilskift*** i den øverste del af dialogen:



På den måde bliver profillisten deaktiveret, og du skal bare trykke på knappen ***Næste*** for at fortsætte til den næste dialog i guiden.

7.4. Gennemse konfiguration

Dialogen ***Gennemse konfiguration*** afslutter ***guiden Firewall-konfiguration***. Tryk på knappen ***Afslut*** for at fuldføre de indledende indstillinger af ***Firewall***. Hvis du vil gennemse de indstillede parametre eller fortsætte med detaljeret konfiguration af ***Firewall***-komponenten, skal du trykke på knappen ***Åbn gennemsyn*** for at skifte til redigeringsgrænsefladen ***Firewallindstillinger***.

8. Efter installationen

8.1. Produktregistrering

Når installationen af **AVG 8.5 Anti-virus plus firewall** er afsluttet, bedes du registrere dit produkt online på AVG's websted, siden ***Registrering*** (*følg instruktionerne på siden*). Efter registreringen kan du få fuld adgang til din AVG-brugerkonto, nyhedsbrevet AVG Update og andre tjenester, der leveres eksklusivt til registrerede brugere.

8.2. Adgang til brugergrænseflade

Der er adgang til ***AVG Brugergrænsefladen*** på flere måder:

- dobbeltklik på AVG-ikonet i systembakken
- dobbeltklik på AVG-ikonet på skrivebordet
- fra menuen ***Start/Alle programmer/AVG 8.0/AVG Brugergrænseflade***

8.3. Scanning af hele computeren

Der er en potentiel risiko for, at en computervirus er blevet overført til din computer inden installationen af **AVG 8.5 Anti-virus plus firewall**. Derfor bør du køre en ***Scanning af hele computeren*** for at sikre, at der ikke er infektioner på din pc.

Se kapitlet ***AVG Scanning*** for vejledning i at køre en ***Scanning af hele computeren*** .

8.4. Eicar-test

For at bekræfte, at **AVG 8.5 Anti-virus plus firewall** er installeret korrekt, kan du udføre EICAR-testen.

EICAR-testen er en almindelig og absolut sikker måde, der anvendes til test af antivirussystemets funktion. Den er sikker at videregive, da det ikke er en rigtig virus, og den indeholder ikke fragmenter af viral kode. De fleste produkter reagerer, som om der var tale om en virus (*selv om de typisk rapporterer den med et åbenlyst navn som f.eks. "EICAR-AV-Test"*). Du kan downloade EICAR-virussen fra EICAR's websted på www.eicar.com, og her findes også al nødvendig EICAR-testinformation.

Prøv at downloade filen ***eicar.com***, og gem den på din lokale disk. Umiddelbart efter at du har bekræftet downloading af testfilen, vil ***Web Shield*** reagere med en advarsel. Denne ***Web Shield***-notits demonstrerer, at AVG er korrekt installeret på din computer.

Hvis AVG ikke kan identificere EICAR-testfilen som en virus, skal du kontrollere programkonfigurationen igen!

8.5. AVG Standardkonfiguration

Standardkonfigurationen (*dvs. hvordan applikationen er sat op umiddelbart efter installationen*) for **AVG 8.5 Anti-virus plus firewall** er konfigureret af softwareleverandøren, så alle komponenter og funktioner er indstillet til at opnå optimal ydelse.

Med mindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration! Ændringer i indstillingerne bør kun udføres af en erfaren bruger.

Nogle mindre redigeringer af indstillinger i AVG-komponenter er tilgængelige direkte fra den specifikke komponents brugergrænseflade. Hvis du synes, det er nødvendigt at ændre AVG's konfiguration, så den passer bedre til dine behov, skal du gå til ***AVG Avancerede indstillinger***: Vælg systemmenupunktet ***Værktøjer/Avancerede indstillinger*** og rediger AVG-konfigurationen i dialogen ***AVG Avancerede indstillinger***, der åbnes.

9. AVG-brugerflade

AVG 8.5 Anti-virus plus firewall åbn med hovedvinduet:

Hovedvinduet er opdelt i flere sektioner:

- ***Systemmenuen*** *(den øverste systemlinje i Windows)* er standardnavigationen, du bruger til at få adgang til alle AVG's komponenter, services og funktioner - detaljer >>
- ***Info om sikkerhedsstatus*** *(den øverste sektion i vinduet)* indeholder oplysninger om den aktuelle status for AVG-programmet - detaljer >>
- ***Lynlinks*** *(venstre sektion i vinduet)* gør det muligt hurtigt at få adgang til de hyppigst anvendte AVG-opgaver - detaljer >>
- ***Komponentoversigt*** *(midterste sektion i vinduet)* indeholder en oversigt

over alle de installerede AVG-komponenter - detaljer >>

- ***Statistik*** *(nederste venstre sektion i vinduet)* indeholder alle statistiske data vedrørende programmernes funktion - detaljer >>
- ***Systembakkeikon*** *(nederste højre hjørne af skærmen i systembakken)* indikerer AVG's aktuelle status - detaljer >>

9.1. Systemmenuen

Systemmenuen er standardnavigationen, der anvendes i alle Windows-applikationer. Den er placeret vandret i den øverste del af **AVG 8.5 Anti-virus plus firewall**'s hovedvindue. Brug systemmenuen til at få adgang til specifikke komponenter, funktioner og tjenester i AVG.

Systemmenuen er opdelt i fem hovedsektioner:

9.1.1. Fil

- ***Afslut*** - lukker **AVG 8.5 Anti-virus plus firewall**'s brugergrænseflade. AVG-applikationen fortsætter med at køre i baggrunden, og din computer er stadigvæk beskyttet!

9.1.2. Komponenter

Punktet ***Komponenter*** i systemmenuen indeholder link til alle installerede AV-komponenter og åbner deres standarddialogside i brugergrænsefladen:

- ***Systemoversigt*** - skift til brugergrænsefladens standarddialog med oversigten over alle installerede komponenter og deres status
- ***Anti-virus*** - åbner standardsiden for ***Anti-virus***-komponenten
- ***Anti-rootkit*** - åbner standardsiden for ***Anti-rootkit***-komponenten
- ***Anti-spyware*** - åbner standardsiden for ***Anti-spyware***-komponenten
- ***Firewall*** - åbner standardsiden for ***Firewall***-komponenten
-
-
- ***E-mail scanner*** - åbner standardsiden for ***E-mail scanner***-komponenten

- ***Licens*** - åbner standardsiden for ***Licens***-komponenten
- ***Linkscanner***- åbner standardsiden for ***Linkscanner***-komponenten
- ***Web Shield*** - åbner standardsiden for ***Web Shield***-komponenten
- ***Resident Shield*** - åbner standardsiden for ***Resident Shield***-komponenten
- ***Opdateringsadministrator*** - åbner standardsiden for ***Opdateringsadministrator***-komponenten

9.1.3. Historik

- ***Scanningsresultater*** - skifter til AVG's testgrænseflade, specifikt til dialogen ***Scanningsresultatoversigt***
- ***Resident Shield-detektering*** - åbn en dialog med en oversigt over trusler detekteret af ***Resident Shield***
- ***E-mail scanner-detektering*** - åbn en dialog med en oversigt over vedhæftede filer til e-mail-meddelelser, der er detekteret som farlige af ***E-mail scanner***-komponenten
- ***Web Shield-fund*** - åbn en dialog med en oversigt over trusler detekteret af ***Web Shield***
- ***Virus Vault*** - åbner grænsefladen til karantæneområdet (***Virus Vault***), hvortil AVG flytter alle detekterede infektioner, der af en eller anden årsag ikke kan helbredes automatisk. I dette karantæneområde isoleres de inficerede filer, og din computers sikkerhed er sikret. Samtidig opbevares de inficerede filer med mulighed for reparation i fremtiden.
- ***Hændelseshistoriklog*** - åbner historikloggrænsefladen med en oversigt over alle loggede **AVG 8.5 Anti-virus plus firewall** -handlinger
- ***Firewall*** - åbner Firewall-indstillingsinterfacet på fanen ***Logge*** med en detaljeret oversigt over alle Firewall-handlinger

9.1.4. Værktøj

- ***Scan computer*** - skifter til AVG scanningsgrænseflade og starter en scanning af hele computeren
- ***Scan udvalgte mapper*** - skifter til AVG scanningsgrænseflade og giver dig mulighed for at definere, hvilke filer og mapper der skal scannes, i

computerens træstruktur

- ***Scan fil*** - giver dig mulighed for at køre en on-demand-test af en enkelt fil, der vælges i diskens træstruktur

- ***Opdater*** - starter automatisk opdateringsprocessen for **AVG 8.5 Anti-virus plus firewall**

- ***Opdater fra mappe*** - kører opdateringsprocessen fra opdateringsfilerne placeret i en specificeret mappe på din lokale disk. Denne mulighed anbefales dog kun i nødstilfælde, f.eks. hvis der ikke er adgang til internettet (*for eksempel hvis din computer er inficeret og internetforbindelsen er afbrudt, eller din computer er tilsluttet en netværk uden adgang til internettet osv.*). I det nyåbnede vindue skal du vælge den mappe, hvor du tidligere placerede opdateringsfilen, og starte opdateringsprocessen.

- ***Avancerede indstillinger*** - åbner dialogen ***AVG avancerede indstillinger***, hvor du kan redigere **AVG 8.5 Anti-virus plus firewall-**konfigurationen. Generelt anbefales det at bevare standardindstillingerne for applikationen, der er definerede af softwareleverandøren.

- ***Firewall-indstillinger*** - åbn en enkeltstående dialog til avanceret konfiguration af ***Firewall***-komponenten

9.1.5. Hjælp

- ***Indhold*** - åbner AVG's hjælpefiler

- ***Find hjælp online*** - åbner AVG's websted på kundesupportcentrets side

- ***Dit AVG-site*** - åbner AVG's hjemmeside (på www.avg.com)

- ***Om vira og trusler*** - åbner det online ***Virus-opslagsværk*** , hvor du kan finde detaljerede oplysninger om den identificerede virus

- ***Genaktiver*** - åbner dialogen ***Aktiver AVG*** med de data, du har indtastet i dialogen ***Personliggør AVG*** under installationsprocessen. I denne dialog kan du indtaste dit licensnummer for enten at erstatte salgsnummeret (*nummeret du har installeret AVG med*), eller for at erstatte det gamle licensnummer (*f. eks. ved opgradering til et nyt AVG-produkt*).

- ***Registrer nu*** - opretter forbindelse til registreringswebstedet på www.avg.com. Udfyld dine registreringsdata. Kun kunder, der registrerer deres AVG-produkt kan modtage gratis teknisk support.

- ***Om AVG*** - åbner dialogen ***Information*** med fem faner, der indeholder data om programnavn, program- og virusdatabaseversion, systemoplysninger, licensaftale og kontaktoplysninger for ***AVG Technologies CZ***.

9.2. Info om sikkerhedsstatus

Sektionen ***Info om sikkerhedsstatus*** findes i den øverste del af AVG's hovedvindue. I denne sektion kan du altid finde oplysninger om den aktuelle sikkerhedsstatus for **AVG 8.5 Anti-virus plus firewall**. Herunder er en oversigt over ikoner, der kan være afbildet i denne sektion, og deres betydning:

 Det grønne ikon indikerer, at AVG er fuldt funktionsdygtig. Dit system er fuldstændig beskyttet, opdateret og alle installerede komponenter fungerer korrekt.

 Det orange ikon advarer om, at en eller flere komponenter er konfigureret forkert, og du bør være opmærksom på deres egenskaber/indstillinger. Der er ingen kritiske problemer i AVG, og du har sandsynligvis besluttet at deaktivere en komponent af en eller anden årsag. Du er stadig beskyttet af . Vær dog opmærksom på indstillingerne i den pågældende komponent! Dens navn er angivet i sektionen ***Info om sikkerhedsstatus*** .

Dette ikon vises også, hvis du af en årsag har besluttet at ignorere en komponents fejlstatus (indstillingen "***Ignorer komponenttilstand***" er tilgængelig i kontekstmenuen, der åbnes ved at højreklikke på den respektive komponents ikon i komponentoversigten i AVG's hovedvindue). Det kan være nødvendigt at bruge denne indstilling i en specifik situation, men det anbefales på det kraftigste at deaktivere indstillingen "***Ignorer komponenttilstand***" så hurtigt som muligt.

 Det røde ikon indikerer, at AVG's status er kritisk! En eller flere komponenter fungerer ikke korrekt, og AVG kan ikke beskytte din computer. Løs det rapporterede problem omgående. Kontakt AVG teknisk support, hvis du ikke kan afhjælpe fejlen på egen hånd.

Det anbefales på det kraftigste, at du lægger mærke til ***Info om sikkerhedsstatus*** og i tilfælde af, at rapporten indikerer et problem, prøver at løse det med det samme. Ellers er din computer i fare!

Bemærk: *AVG's statusinformation kan til enhver tid også findes vha. systembakkeikonet.*

9.3. Lynlink

Med Lynlink *(i venstre sektion af AVG Brugergrænsefladen)* kan du få øjeblikkelig adgang til de vigtigste og hyppigst anvendte funktioner i AVG:

- ***Oversigt*** - brug dette link til at skifte fra den aktuelt åbne AVG-grænseflade til standardgrænsefladen med en oversigt over alle installerede komponenter - se kapitlet ***Komponentoversigt >>***
- ***Computerscanner*** - brug dette link til at åbne AVG's scanningsgrænseflade, hvor du kan køre test direkte, planlægge scanninger eller redigere deres parametre - se kapitlet ***AVG Test >>***
- ***Opdater nu*** - dette link åbner opdateringsgrænsefladen og kører AVG's opdateringsproces med det samme - se kapitlet ***AVG Opdateringer >>***

Der er altid adgang til disse link fra brugergrænsefladen. Når du bruger et lynlink til at køre en specifik proces, skifter den grafiske brugergrænseflade til en ny dialogboks, men lynlinkene er stadig tilgængelige. Derudover bliver den kørende proces afbildet grafisk - *se billede 2*.

9.4. Komponentoversigt

Sektionen ***Komponentoversigt*** findes i den midterste del af AVG-brugergrænsefladen. Sektionen består af to dele:

- Oversigt over alle installerede komponenter, der består af et panel med komponentens ikon og oplysninger om, hvorvidt den pågældende komponent er aktiv eller inaktiv.
- Beskrivelse af en valgt komponent

I **AVG 8.5 Anti-virus plus firewall** indeholder sektionen ***Komponentoversigt*** oplysninger om følgende komponenter:

- ***Anti-virus*** sikrer at din computer er beskyttet mod virus, der forsøger at trænge ind i computeren - detaljer >>
- ***Anti-spyware*** scanner dine applikationer i baggrunden, mens du kører dem - detaljer >>
- ***Anti-rootkit*** detekterer programmer og teknologier, der forsøger at camouflere malware - detaljer >>
- ***Firewall*** kontrollerer, hvordan din computer udveklser data med andre computere på internettet eller lokale netværk - detaljer >>
- ***E-mail scanner*** kontrollerer al indkommende og udgående e-mail for virus - detaljer >>

- ***Licens*** indeholder den fulde ordlyd i AVG-licensaftalen - detaljer >>
- ***Linkscanner*** kontrollerer de søgeresultater, der vises i din internetbrowser - detaljer >>
- ***Web Shield*** scanner alle data, der downloades af en internetbrowser - detaljer >>
- ***Resident Shield*** kører i baggrunden og scanner filer, når de kopieres, åbnes eller gemmes - detaljer >>
- ***Opdateringsadministrator*** kontrollerer alle AVG-opdateringer - detaljer >>

Enkeltklik på en komponents ikon for at fremhæve den i komponent oversigten. Samtidig vises komponentens grundlæggende funktionsbeskrivelse i den nederste del af brugergrænsefladen. Dobbeltklik på ikonet for at åbne komponentens egen grænseflade med en liste over grundlæggende statistikdata.

Højreklik på musen over en komponents ikon for at udvide en kontekstmenu: Ud over at åbne komponentens grafiske brugerflade kan du vælge ***Ignorer komponenttilstand***. Vælg denne indstilling for at vise, at du er opmærksom på komponentens fejltilstand, men af en eller anden grund vil du bevare AVG på denne måde, og du vil ikke have en advarsel med den grå farve på systembakkeikonet.

9.5. Statistik

Sektionen ***Statistik*** findes i den nederste venstre del af AVG-brugergrænsefladen. Den indeholder en liste over oplysninger vedrørende anvendelsen af programmet:

- ***Seneste scanning*** - angiver den dato, hvor den seneste scanning blev udført
- ***Seneste opdatering***- angiver den dato, hvor den seneste opdatering blev udført
- ***Virus-DB*** - informerer om den aktuelle installerede version af virusdatabasen
- ***AVG-version*** - informerer om den installerede AVG-version *(nummeret har formatet 8.0.xx, hvor 8.0 er produktlinjeversionen, og xx står for buildnummeret)*
- ***Licens udløber*** - angiver udløbsdatoen for din AVG-licens

9.6. Systembakkeikon

Systembakkeikonet (*på Windows' proceslinje*) indikerer den aktuelle status for **AVG 8.5 Anti-virus plus firewall**. Det er altid synligt i din systembakke, uanset om AVG's hovedvindue er åbent eller lukket.

Hvis det er i klare farver , indikerer ***Systembakkeikonet***, at alle AVG-komponenter er aktive og fuldt funktionsdygtige. AVG-systembakkeikonet kan også vises i fuld farve, hvis AVG er i fejltilstand, men du er opmærksom på situationen og du med vilje har besluttet at ***Ignorere komponenttilstanden***.

En grå ikonfarve med et udråbstegn indikerer et problem (inaktiv komponent, fejlstatus osv.). Dobbeltklik på ***systembakkeikonet*** for at åbne hovedvinduet og redigere en komponent.

Systembakkeikonet informerer yderligere om aktuelle AVG-aktiviteter og mulige statusændringer i programmet (*f.eks. automatisk kørsel af en planlagt scanning eller opdatering, Firewall profilskift, en komponents statusændring, opståen af en fejltilstand osv.*) via et popup-vindue, der åbnes fra AVG-systembakkeikonet:

Systembakkeikonet kan også til enhver tid anvendes som lynlink til AVG's hovedvindue - dobbeltklik på ikonet. Ved at højreklikke på ***Systembakkeikonet*** åbner du en kortfattet kontekstmenu med følgende muligheder:

- ***Åbn AVG's brugergrænseflade*** - klik for at åbne AVG's brugergrænseflade
- ***Opdater*** - kører en omgående opdatering
- ***Afslut*** - klik for at lukke AVG *(Du lukker kun brugergrænsefladen, AVG fortsætter med at køre i baggrunden, og din computer er stadig fuldt beskyttet!)*

10. AVG Komponenter

10.1.Anti-virus

10.1.1.Anti-virus Principper

Antivirussoftwarens scanningsengine scanner alle filer og filaktiviteter (åbning/ lukning af filer osv.) for kendte vira. Alle detekterede vira bliver blokeret, så de ikke kan udføre handlinger, og bliver derefter renset eller sat i karantæne. De fleste antivirussoftware bruger også heuristisk scanning, hvor filer scannes for typiske viruskendetegn, såkaldte virale signaturer. Det betyder, at antivirusscanneren kan detektere en ny, ukendt virus, hvis den nye virus indeholder nogle typiske kendetegn fra eksisterende vira.

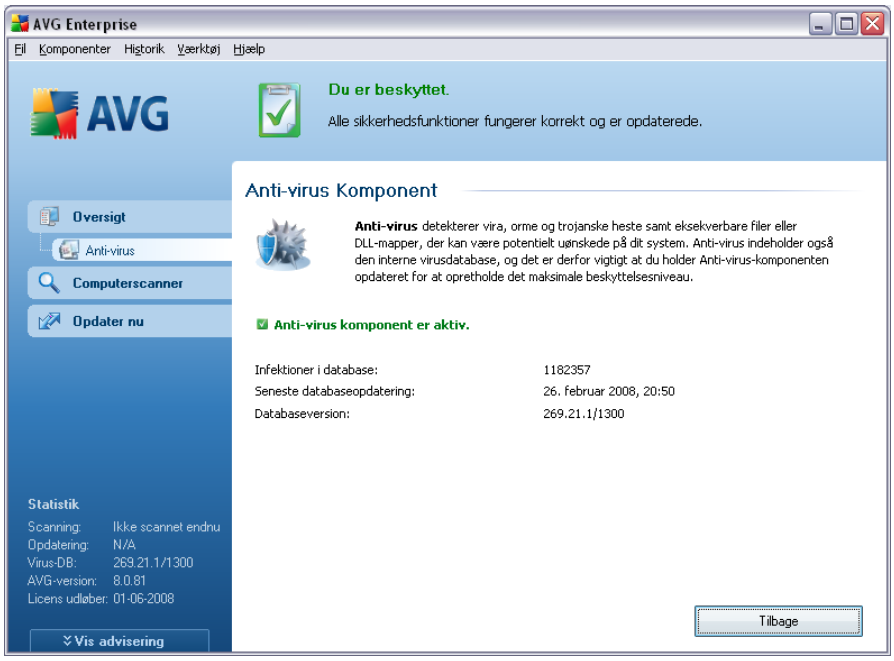
Den vigtige funktion ved antivirusbeskyttelse er, at ingen kendt virus kan køre på computeren.

Hvor det måske ville mislykkes for en enkelt teknologi at detektere eller identificere en virus, kombinerer ***Anti-virus*** flere teknologier for at sikre, at din computer er beskyttet mod virus:

- Scanning – søger efter tegnstrenge, der er karakteristiske for en given virus
- Heuristisk analyse – dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø
- Generisk detektering – detektering af instruktioner, der er karakteristiske for den givne virus/gruppe af vira

AVG kan også analysere og detektere eksekverbare applikationer og DLL-biblioteker, der er potentielt uønskede i systemet. Vi kalde den type trusler for potentielt uønskede programmer (forskellige typer af spyware, adware osv.). Yderligere scanner AVG din systemregistreringsdatabase for mistænkeligt indhold, midlertidige internet-filer og sporings-cookies, og gør det muligt for dig at behandle alle potentielt skadelige elementer på samme måde som enhver anden infektion.

10.1.2.Anti-virus-grænseflade



Anti-virus-komponentens grænseflade indeholder en kort oversigt over komponentens funktionalitet, oplysninger om komponentens aktuelle status (*Anti-virus-komponenten er aktiv.*) og en kort oversigt over ***Anti-virus***-statistikker:

- ***Infektionsdefinitioner*** - nummeret angiver antallet af vira, der er defineret i den opdaterede version af virusdatabasen
- ***Seneste databaseopdatering*** - angiver hvornår og på hvilket tidspunkt virusdatabasen blev opdateret
- ***Databaseversion*** - definerer nummeret på den seneste virusdatabaseversion. Dette nummer forøges for hver grundlæggende virusopdatering

Der er kun en betjeningsknap tilgængelig på denne komponents grænseflade (***Tilbage***) - tryk på knappen for at vende tilbage til den normale AVG-brugergrænseflade (komponentoversigt).

Bemærk: *Softwareleverandøren har indstillet alle AVG-komponenter til at yde optimal beskyttelse. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge*

*systemmenupunktet **Værktøjer / Avancerede indstillinger** og redigere AVG-konfigurationen i dialogen AVG Avancerede indstillinger , der åbnes.*

10.2.Anti-spyware

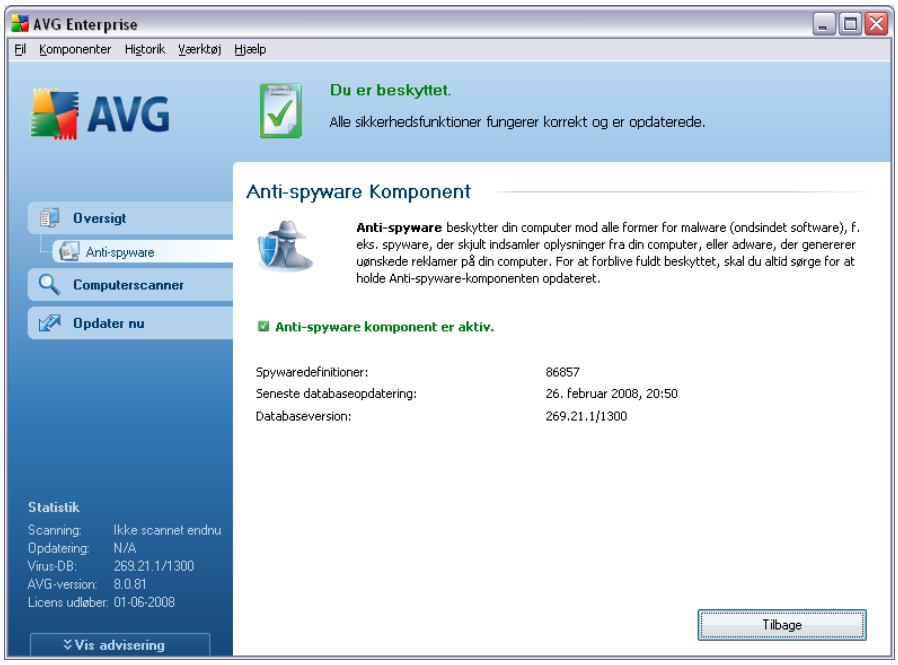
10.2.1.Anti-spyware Principper

Spyware defineres sædvanligvis som en type malware, dvs. software, der indsamler information fra en brugers computer uden brugerens viden eller samtykke. Visse spyware-applikationer kan også blive installeret med vilje, og de indeholder ofte annoncering, pop-up vinduer eller lignende typer irriterende software.

I øjeblikket er den mest almindelige kilde til infektioner websteder med potentielt farligt indhold. Andre transmissionsmetoder, f.eks. via e-mail eller transmission via orm og vira er også almindelige. Den vigtigste beskyttelse er at anvende en baggrundsscanner, der altid er aktiveret, ***Anti-spyware***, der fungerer som et indbygget skjold, der scanner dine applikationer i baggrunden under kørslen.

Der er også en potentiel risiko for, at malware er blevet transmitteret til din computer inden installation af AVG, eller at du har forsømt at holde **AVG 8.5 Anti-virus plus firewall** opdateret med de sidste nye database- og programopdateringer. Derfor er det med AVG muligt at scanne computeren for malware/spyware vha. scanningsfunktionen. Den detekterer også sovende og inaktiv malware, dvs. malware, der er downloadet men endnu ikke aktiveret.

10.2.2.Anti-spyware-grænseflade



Anti-Spyware-komponentens grænseflade indeholder en kort oversigt over komponentens funktionalitet, oplysninger om komponentens aktuelle status (*Anti-spyware-komponenten er aktiv.*), og nogle ***Anti-spyware***-statistikker:

- ***Spywaredefinitioner*** - tallet er det antal spywareeksempler, der er defineret i den seneste version af spywaredatabasen
- ***Seneste databaseopdatering*** - angiver hvornår og på hvilket tidspunkt spywaredatabasen blev opdateret
- ***Databaseversion*** - definerer nummeret på den seneste spywaredatabaseversion. Dette nummer forøges for hver grundlæggende virusopdatering

Der er kun en betjeningsknap tilgængelig på denne komponents grænseflade (***Tilbage***) - tryk på knappen for at vende tilbage til den normale AVG-brugergrænseflade (komponentoversigt).

Bemærk: *-softwareleverandøren har konfigureret alle AVG-komponenter til den optimale ydeevne. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge*

*systemmenupunktet **Værktøjer / Avancerede indstillinger** og redigere AVG-konfigurationen i dialogen AVG Avancerede indstillinger , der åbnes.*

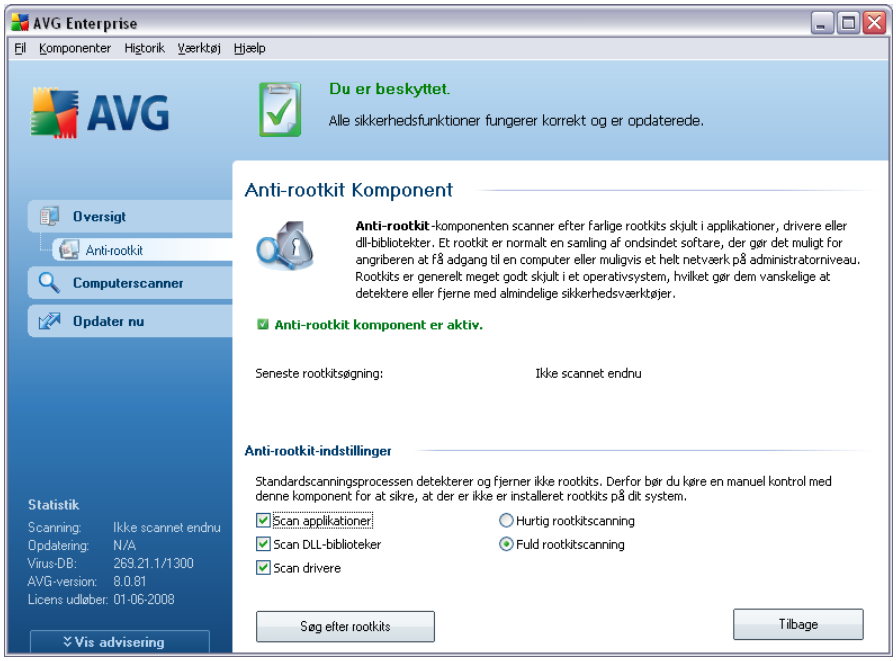
10.3.Anti-rootkit

10.3.1.Anti-rootkit-principper

Anti-rootkit er et specialiseret værktøj, der detekterer og effektivt fjerner farlige rootkits, dvs. programmer og teknologier, der kan camouflere tilstedeværelsen af skadelig software på computeren.

Et rootkit er et program, der er udviklet til at tage kontrollen over et computersystem, uden autorisation fra systemets ejere og legitime administratorer. Det er sjældent nødvendigt at opnå adgang til hardwaren, da et rootkit er beregnet til at overtage kontrollen over operativsystemet, der kører på hardwaren. Rootkits forsøger typisk at skjule deres tilstedeværelse på systemet ved at undertrykke eller undgå operativsystemets standardsikkerhedsmekanismer. Ofte er de også trojanske heste og narrer brugere til at tro, at de er sikre at køre på deres systemer. De teknikker der anvendes til at opnå dette, kan omfatte at skjule kørende processer for overvågningsprogrammer eller at skjule filer eller systemdata for operativsystemet.

10.3.2.Anti-rootkit-grænseflade



Anti-Rootkit-brugergrænsefladen indeholder en kort beskrivelse af komponentens funktionalitet, informerer om komponentens aktuelle status (*Anti-rootkit-komponent er aktiv.*) og indeholder oplysninger om sidste gang ***Anti-rootkit***-testen blev kørt.

I den nederste del af dialogen finder du sektionen ***Anti-Rootkit-indstillinger***, hvor du kan indstille nogle grundlæggende funktioner for scanning efter rootkits. Marker først de pågældende afkrydsningsfelter for at angive de objekter, der skal scannes:

- ***Scan applikationer***
- ***Scan DLL-biblioteker***
- ***Scan drivere***

Derudover kan du vælge rootkitscanningstilstanden:

- ***Hurtig rootkitscanning*** - scanner kun system-mappen (*normalt c:\Windows*)
- ***Fuld rootkitscanning*** - scanner alle tilgængelige drev, undtagen A: og B:

Betjeningsknapper tilgængelige:

- ***Søg efter rootkits*** - da rootkitscanningen ikke er en obligatorisk del af ***Scanning af hele computeren***, kan du køre rootkitscanningen direkte fra ***Anti-rootkit***-grænsefladen ved hjælp af denne knap
- ***Gem ændringer*** - tryk på denne knap for at gemme alle ændringer, der er foretaget på denne grænseflade, og vende tilbage til den almindelige ***AVG-brugerflade*** (komponentoversigt)
- ***Annuller*** - tryk på denne knap for at vende tilbage til den almindelige ***AVG brugerflade*** (komponentoversigt) uden at gemme eventuelle ændringer

10.4.Firewall

10.4.1.Firewall-principper

Firewall er et system, der gennemtvinger en adgangskontrol-politik mellem to eller flere netværk, ved at blokere/tillade trafik. En firewall indeholder et sæt regler, der beskytter det interne netværk imod udefra kommende angreb (typisk fra internettet) og som kontrollerer al kommunikation på de enkelte netværksporte.
Kommunikationen evalueres i henhold til de definerede regler, og er enten tilladt eller

forbudt. Hvis Firewall genkender et indtrængningsforsøg "blokerer" den forsøget, og tillader ikke indtrængeren at få adgang til computeren.

Firewall er konfigureret til at tillade eller afvise intern/ekstern kommunikation (begge veje, ind eller ud) gennem definerede porte og for definerede softwareprogrammer. For eksempel kan firewallen konfigureres til kun at tillade ind- og udgående passage af webdata ved hjælp af Microsoft Explorer. Ethvert forsøg på at overføre webdata med en anden browser bliver blokeret.

Firewall beskytter dine personlige, identificerbare oplysninger mod at blive sendt fra din computer uden din tilladelse. Den kontrollerer, hvordan din computer udveksler data med andre computere på internettet eller lokale netværk. I en organisation beskytter en firewall også den enkelte computer mod angreb, der iværksættes af interne brugere på andre computere i netværket.

Bemærk! *AVG Firewall er ikke beregnet til serverplatforme!*

Hvordan fungerer AVG Firewall

I AVG styrer ***Firewall***-komponenten al trafik på alle netværksporte i computeren. Baseret på de definerede regler evaluerer ***Firewall*** applikationer, der enten kører på computeren, eller som ønsker at etablere forbindelse til netværket (lokalt netværk eller internettet), eller applikationer, der udefra forsøger at etablere forbindelse til din pc. For hver af disse applikationer vil ***Firewall*** derefter enten tillade eller forbyde kommunikation via netværksportene. Som standard vil ***Firewall***, hvis applikationen er ukendt (dvs. ikke har definerede ***Firewall***-regler), spørge om du vil tillade eller blokere kommunikationsforsøget.

Hvad Firewall kan gøre:

- Tillade eller blokere kommunikationsforsøg fra kendte applikationer automatisk eller spørge dig om bekræftelse
- Bruge komplette profiler med foruddefinerede regler, der svarer til dine behov
- Bevare et arkiv over alle definerede profiler og indstillinger
- Skifte profil automatisk, når der oprettes forbindelse til forskellige netværk eller bruges forskellige netværksadaptere

10.4.2.Firewall-profiler

Firewall gør det muligt at definere specifikke sikkerhedsregler baseret på, om din computer er placeret i et domæne, om det er en standalone-computer eller om det er en notebook. Hver af disse muligheder kræver et anderledes beskyttelsesniveau, og niveauerne dækkes af de respektive profiler. Kort fortalt er en ***Firewall***-profil en specifik konfiguration af ***Firewall***-komponenten, og du kan bruge flere af disse foruddefinerede konfigurationer.

Tilgængelige profiler

- ***Tillad alle*** - en ***Firewall***-systemprofil, der er forudindstillet af producenten og altid forefindes. Når denne profil er aktiveret, er al netværkskommunikation tilladt, og der anvendes ingen sikkerhedspolitikker, som om ***Firewall***-beskyttelsen var slået fra *(dvs. alle applikationer er tilladt, men pakkerne bliver stadig kontrolleret - for at slå enhver filtrering helt fra, er du nødt til at deaktivere Firewall)*. Denne systemprofil kan ikke kopieres eller slettes, og dens indstillinger kan ikke ændres.

- ***Bloker alle*** - en ***Firewall***-systemprofil, der er forudindstillet af producenten og altid forefindes. Hvis denne profil aktiveres, blokeres al netværkstrafik, og computeren er ikke tilgængelig fra eksterne netværk, og kan heller ikke kommunikere eksternt. Denne systemprofil kan ikke kopieres eller slettes, og dens indstillinger kan ikke ændres.

- ***Brugerdefinerede profiler*** - profiler genereret med ***Guiden Firewall-konfiguration***. Der kan genereres maksimalt tre brugerdefinerede profiler med guiden:

    - *Standalone-computer* - velegnet til almindelige stationære computere i hjemmet, der er sluttet direkte til internettet.

    - *Computer i domæne* - velegnet til computere i et lokalt netværk, f.eks. et skole- eller virksomhedsnetværk. Det antages at netværket er beskyttet med yderligere foranstaltninger, så sikkerhedsniveauet kan være lavere end for en standalone-computer.

    - *Lille hjemme- eller kontornetværk* - velegnet for computere i et lille netværk, f.eks. i hjemmet eller i en lille virksomhed. Typisk kun nogle få computere, der er forbundet uden en "central" administrator.

    - *Computer på farten* - velegnet for bærbare computere. Det antages, at den som bærbar computer opretter forbindelse til internettet fra

forskellige ukendte og derfor fuldstændig usikre steder (netcafeer, hotelværelser osv.), og derfor indstilles det højeste sikkerhedsniveau.

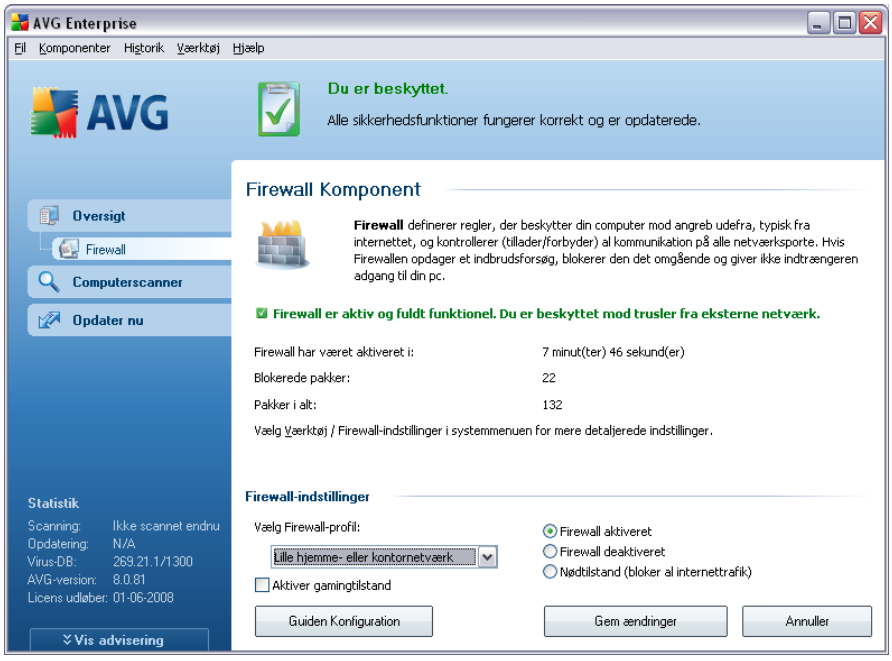
Profilskift

Funktionen Profilskift gør det muligt for ***Firewall*** automatisk at skifte til den definerede profil ved brug af en bestemt netværksadapter eller ved tilslutning til en bestemt netværkstype. Hvis der ikke er knyttet en profil til et netværksområde endnu, viser ***Firewall*** en dialog, der beder dig om at tilknytte en profil, næste gang der oprettes forbindelse til dette område.

Du kan knytte profiler til alle lokale netværksinterfaces eller -områder og angive yderligere indstillinger i dialogen ***Område- og adapterprofiler***, hvor du også kan deaktivere funktionen, hvis du ikke ønsker at bruge den (*i så fald bliver standardprofilen brugt til alle forbindelsestyper*).

Denne funktion er normalt praktisk for brugere af en bærbar computer, der bruger forskellige forbindelsestyper. Hvis du har en stationær computer, og du kun bruger en forbindelsestype (*f.eks. kabelforbindelse til internettet*), behøver du ikke at bekymre dig om profilskift, da du sandsynligvis aldrig kommer til at bruge det.

10.4.3.Firewall-grænseflade



Firewall-komponentens grænseflade indeholder nogle grundlæggende oplysninger om komponentens funktionalitet og en kortfattet oversigt over ***Firewall***-statistikker:

- ***Firewall har været aktiveret i*** - forløbet tid, siden Firewall sidst blev startet
- ***Blokerede pakker*** - antal blokerede pakker ud af det samlede antal kontrollerede pakker
- ***Pakker i alt*** - samlet antal pakker kontrolleret, mens Firewall har kørt

Firewall-indstillinger-sektion

- ***Vælg Firewall-profil*** - vælg en af de definerede profiler i rullemenuen - to profiler er altid tilgængelige (*standardprofilerne* ***Tillad alle*** *og* ***Bloker alle***), andre profiler er blevet tilføjet da du gennemgik ***guiden Firewall-konfiguration*** eller ved redigering af profiler i dialogen ***Profiler*** i ***Firewall-indstillinger***.
- Firewallstatus:
  - ***Firewall aktiveret*** - vælg denne indstilling for at tillade kommunikation til de applikationer, der har status som 'tilladt' i det definerede regelsæt i den valgte ***Firewall***-profil
  - ***Firewall deaktiveret*** - denne indstilling slår ***Firewall*** helt fra, al netværkstrafik tillades men kontrolleres ikke!
  - ***Nødtilstand (bloker al internettrafik)*** - vælg denne indstilling for at blokere al trafik på alle netværksporte. ***Firewall*** kører stadig, men al netværkstrafik stoppes
- ***Aktiver gamingtilstand*** - Marker denne indstilling for at sikre, at ***Firewall*** ikke viser dialoger, der spørger, om du vil tillade eller blokere kommunikation for ukendte applikationer, når du kører fuldskærmsapplikationer (spil, PowerPoint-præsentationer osv.). I tilfælde af at en ukendt applikation prøver at kommunikere via netværket imens, tillader eller blokere ***Firewall*** forsøget automatisk i overensstemmelse med indstillingerne i den aktuelle profil.

Bemærk: *Softwareleverandøren har indstillet alle AVG-komponenter til at yde optimal beskyttelse. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge systemmenupunktet* ***Filer / Firewall-indstillinger*** *og redigere Firewall-konfigurationen i dialogen* ***Firewall-indstillinger*** *, der åbnes.*

Betjeningsknapper tilgængelige er:

- ***Konfigurationsguide*** - tryk på knappen for at starte ***guiden Firewall-konfiguration*** , der trin for trin fører dig gennem konfigurationen af ***Firewall*** -komponenten
- ***Gem ændringer*** - klik på denne knap for at gemme og anvende de ændringer, der er foretaget i denne dialog
- ***Annuller*** - klik på denne knap for at vende tilbage til den normale AVG-brugergrænseflade(*komponentoversigt*)

10.5.E-mail Scanner

10.5.1.E-mail Scanner-principper

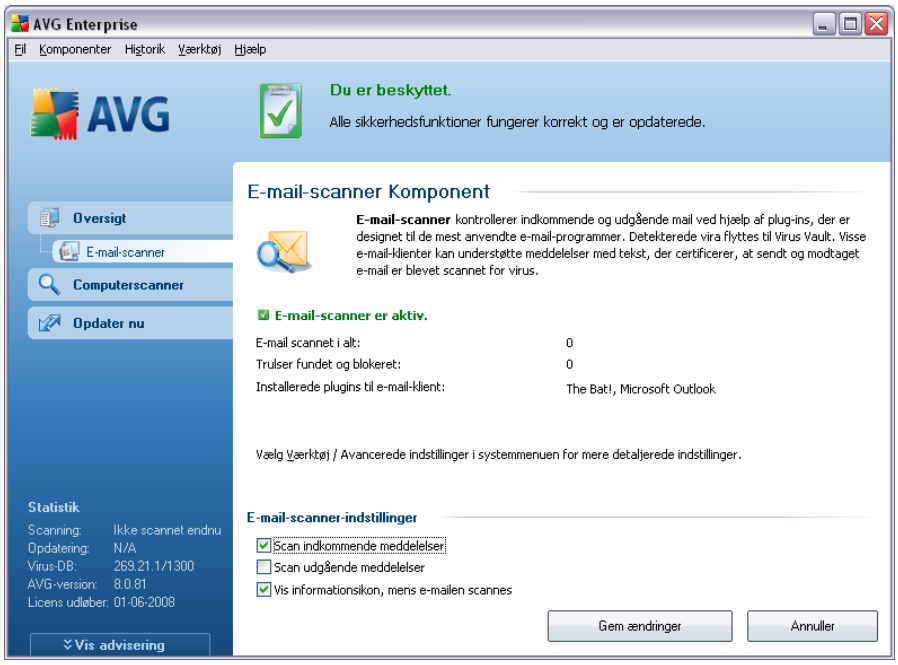
En af de mest udbredte kilder til vira og trojanske heste er via e-mail. Phishing og spam gør e-mail til en endnu større risikokilde. Gratis e-mail-konti er mere tilbøjelige til at modtage sådanne ondsindede e-mail (da de sjældent gør brug af anti-spam-teknologi), og hjemmebrugere benytter sig i høj grad af disse e-mail. Hjemmebrugere, der surfer på ukendte websteder og udfylder onlineformularer med personlige oplysninger (som f.eks. deres e-mail-adresse), øger også eksponeringen for angreb via e-mail. Virksomheder bruger normalt firma-e-mail-adresser og gør brug af anti-spam-filtre mv. for at reducere risikoen.

E-mail scanner-komponenten kontrollerer alle e-mail, der sendes eller modtages, og giver en yderst nødvendig beskyttelse mod e-mail-trusler. AVG understøtter alle førende e-mail-klienter inklusive MS Outlook, The bat!, Eudora og alle andre SMTP/POP3-baserede e-mail-klienter som f.eks. Outlook Express. Krypterede forbindelse vha. SSL understøttes også.

Bemærk! *AVG E-mail-scanner er ikke beregnet til serverplatforme!*

Når virus detekteres, bliver de omgående sat i karantæne i ***Virus Vault***. Visse e-mail-klienter kan understøtte meddelelser med tekst, der certificerer, at sendt og modtaget e-mail er blevet scannet for virus.

10.5.2.E-mail Scanner-grænseflade



I ***E-mail scanner***-komponentens dialog finder du en kort tekst, der beskriver komponentes funktionalitet, oplysninger om dens aktuelle status (*E-mail scanner er aktiv.*) og følgende statistikker:

- ***E-mail scannet i alt*** - hvor mange e-mail-meddelelser er blevet scannet siden ***E-mail scanner*** blev kørt sidst (*om nødvendigt kan denne værdi nulstilles, f.eks. til statistiske formål - Nulstil værdi*)
- ***Trusler fundet og blokeret*** - angiver antallet af detekterede infektioner i e-mail-meddelelser siden sidste kørsel af ***E-mail scanner***
- ***Installeret e-mail-beskyttelse*** - oplysninger om et specifikt e-mail-beskyttelses plugin, der refererer til din installerede standard-e-mail-klient

Grundlæggende komponentkonfiguration

I den nederste del af dialogen finder du sektionen med navnet ***E-mail scanner-indstillinger***, hvor du kan redigere nogle af komponentens grundlæggende funktioner:

- ***Scan indkommende meddelelser*** - marker punktet for at angive, at alle e-mail-meddelelser, der leveres til din konto, skal scannes for virus (*som standard er dette punkt slået til, og det anbefales ikke at ændre denne indstilling!*)

- ***Scan udgående meddelelser*** - marker elementet for at bekræfte, at alle e-mail-meddelelser, der sendes fra din konto skal scannes for vira (*som standard er dette element slået fra*)

- ***Vis informationsikon, mens e-mailen scannes*** - under scanningen viser ***E-mail scanner***-komponenten et informationsdialog, der informerer om den aktuelle opgave, komponenten behandler (*tilslutter til server, downloader en meddelelse, scanner meddelelsen, ...*)

Der er adgang til den avancerede konfiguration af ***E-mail scanner***-komponenten via punktet ***Filer/Avancerede indstillinger*** i systemmenuen. Avanceret konfiguration anbefales imidlertid kun for erfarne brugere!

Bemærk: *Softwareleverandøren har indstillet alle AVG-komponenter til at yde optimal beskyttelse. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge systemmenupunktet* ***Værktøjer / Avancerede indstillinger*** *og redigere AVG-konfigurationen i dialogen AVG Avancerede indstillinger , der åbnes.*

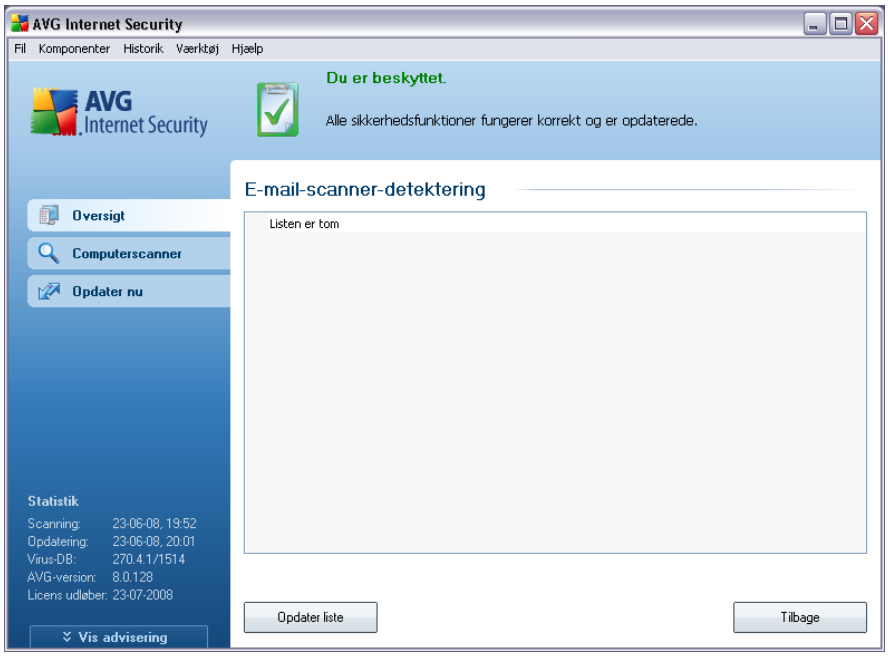
Betjeningsknapper

Betjeningsknapperne, der er tilgængelige i ***E-mail scanner***-grænsefladen, er som følger:

- ***Gem ændringer*** - klik på denne knap for at gemme og anvende de ændringer, der er foretaget i denne dialog

- ***Annuller*** - klik på denne knap for at vende tilbage til den normale AVG-brugergrænseflade (komponentoversigt)

10.5.3.E-mail scanner-detektering

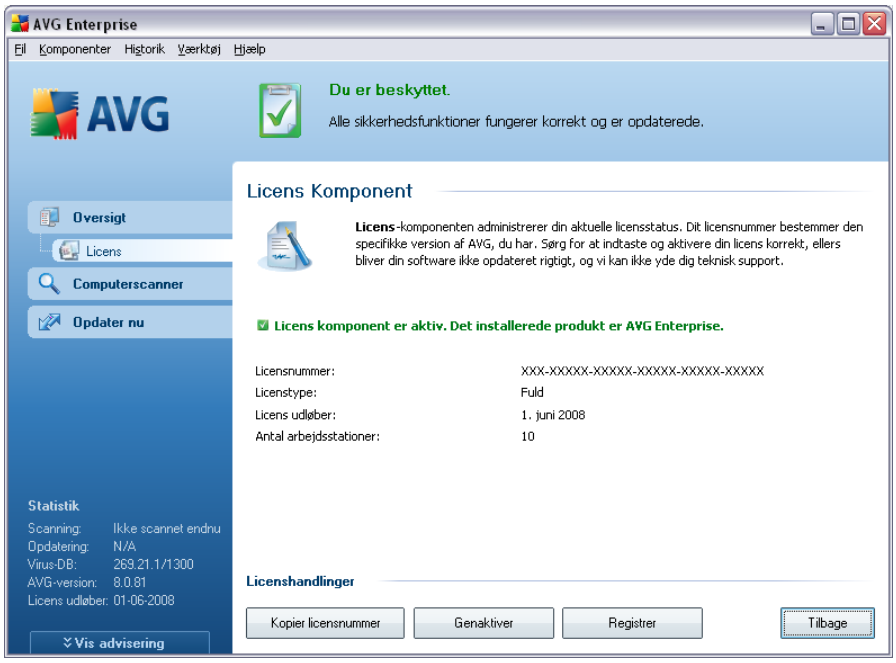


I dialogen ***E-mail scanner-detektering*** (*tilgængelig via systemmenupunktet Historik / E-mail Scanner-detektering*) kan du få vist en liste over alle fund detekteret af ***E-mail Scanner*** -komponenten. For hvert detekteret objekt findes følgende oplysninger:

- ***Infektion*** - beskrivelse af (muligvis også navn på) det detekterede objekt
- ***Objekt*** - objektets placering
- ***Resultat*** - handling udført med det detekterede objekt
- ***Objekttype*** - type for det detekterede objekt

I den nederste del af dialogen, under listen, finder du oplysninger om det totale antal detekterede objekter, der er anført ovenfor. Derudover kan du eksportere hele listen over detekterede objekter til en fil (***Eksporter liste til fil***) og slette alle poster om detekterede objekter (***Tøm liste***).

10.6.Licens



I ***Licens***-komponentens grænseflade finder du en kort tekst, der beskriver komponentens funktionalitet, oplysninger om dens aktuelle status (*Licens-komponenten er aktiv.*) og følgende oplysninger:

- ***Licensnummer*** - indeholder dit licensnummers nøjagtige form. Når du indtaster licensnummeret, skal du være fuldstændig præcis og indtaste det nøjagtig som vist. For nemheds skyld indeholder dialogen ***Licens*** knappen ***Kopier licensnummer***: tryk på knappen for at kopiere licensnummeret til udklipsholderen, og derefter kan du helt enkelt indsætte det, hvor du ønsker (***CTRL+V***).
- ***Licenstype*** - angiver produktudgaven, der er defineret af licensnummeret.
- ***Licens udløber*** - denne dato bestemmer licensens gyldighedsperiode. Hvis du vil fortsætte med at anvende AVG efter denne dato, skal licensen fornys. Fornyelse af licensen kan ske online på AVG's websted.
- ***Antal pladser*** - hvor mange arbejdsstationer du er berettiget til at installere AVG på.

Betjeningsknapper

- ***Kopier licensnummer*** - tryk på knappen for at indsætte det aktuelt anvendte licensnummer i udklipsholderen (*ligesom med CTRL+C*), så du kan indsætte, det hvor du skal bruge det
- ***Genaktiver*** - åbner dialogen ***Aktiver AVG*** med de data, du har indtastet i dialogen ***Personliggør AVG*** under installationsprocessen. I denne dialog kan du indtaste dit licensnummer for enten at erstatte salgsnummeret (*nummeret du har installeret AVG med*), eller for at erstatte det gamle licensnummer (*f. eks. ved opgradering til et nyt AVG-produkt*).
- ***Registrer*** - opretter forbindelse til registreringswebstedet på www.avg.com. Udfyld dine registreringsdata. Kun kunder, der registrerer deres AVG-produkt kan modtage gratis teknisk support.
- ***Tilbage*** - tryk på denne knap for at vende tilbage til den normale AVG-brugergrænseflade (komponentoversigt)

10.7.Linkscanner

10.7.1.Linkscanner-principper

LinkScanner samarbejder med Internet Explorer og Firefox (*1.5 og nyere*), og består af to funktioner: ***AVG Aktivt surfskjold*** og ***AVG Søgeskjold***.

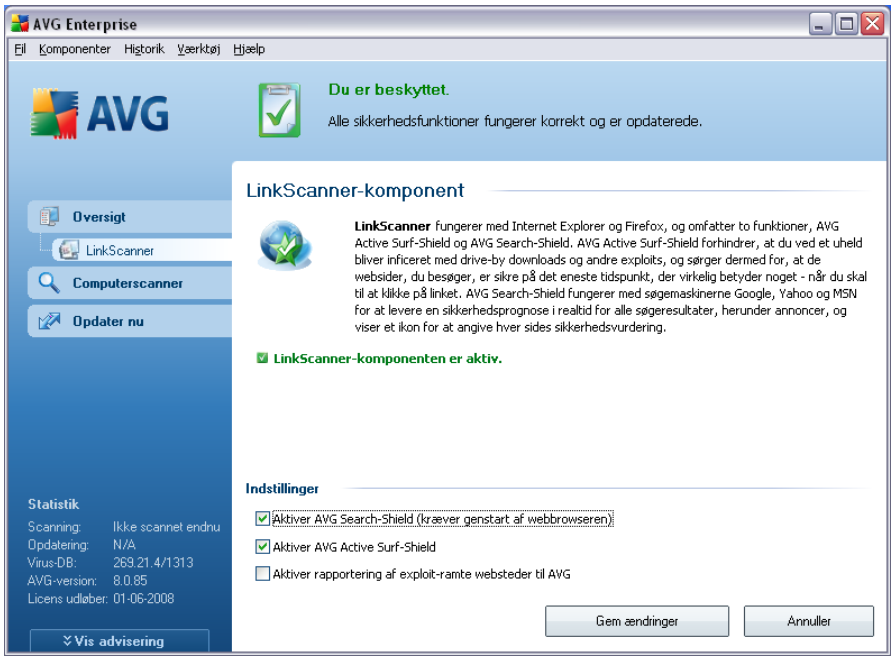
AVG Aktivt surfskjold forhindrer, at du ved et uheld bliver inficeret med drive-by downloads og andre exploits, og sørger dermed for, at de websider, du besøger, er sikre på det eneste tidspunkt, der virkelig betyder noget - når du skal til at klikke på linket.

AVG Søgeskjold fungerer med søgemaskinerne Google, Yahoo! og MSN og leverer en sikkerhedsprognose på alle søgeresultater i realtid, inklusive søgeannoncer, og viser et ikon for at vise sikkerhedsvurderingen for hvert websted.

Bemærk! *AVG Link Scanner er ikke beregnet til serverplatforme!*

10.7.2.Linkscanner-grænseflade

Linkscanner-komponenten består af to dele, du kan slå til/fra i ***Linkscanner-komponentens***-grænseflade:



- ***Aktiver AVG SearchShield*** - (*slået til som standard*): vejledende ikoner på søgninger udført i Google, Yahoo eller MSN efter forudgående kontrol af indholdet på de websteder, der returneres af søgemaskinen. De understøttede browsere er Internet Explorer og Firefox.

- ***Aktiver AVG Aktivt Surfskjold*** -(*slået til som standard*): aktiv (*realtids*-) beskyttelse mod sider med exploits, når de åbnes. Kendte forbindelser til ondsindede websteder og deres exploitindhold blokeres, når de åbnes af brugeren via en webbrowser (*eller enhver anden applikation, der bruger HTTP*).

- ***Tilbagerapportering af websider med exploits til AVG*** - marker dette punkt for at tillade rapportering af exploits og ondsindede websteder, der findes af brugere, enten via ***Sikker surf*** eller ***Sikker søgning*** for at udbygge databasen, der indsamler oplysninger om ondsindet aktivitet på nettet.

10.7.3.AVG Søgeskjold

Når du søger på internettet med ***AVG Søgeeskjold*** slået til, er alle søgeresultater, der returneres fra de mest populære søgemaskiner som Yahoo!, Google, MSN osv., evalueret for farlige eller mistænkelige link. Ved at kontrollere disse link og markere de dårlige link, advarer ***AVG Sikkerhedsværktøjslinje*** dig, før du klikker på farlige eller mistænkelige link, så du kan sørge for kun at besøge sikre websteder.

Mens et link evalueres på siden med søgeresultater, kan du se et grafisk tegn ved siden af linket, der informerer om at linkverificeringen er i gang. Når evalueringen er udført, vises det pågældende informationsikon:

Siden, der linkes til, er sikker (*med Yahoo!-søgemaskinen i AVG Sikkerhedsværktøjslinje vises dette ikon ikke!*).

Siden, der linkes til, indeholder ingen trusler men er mistænkelig (*tvivlsom oprindelse eller motiv og anbefales derfor ikke til e-handel osv.*).

Selve siden der linkes til kan være sikker men indeholde yderligere link til sider med farlig eller mistænkelig kode, men udgør i øjeblikket ikke en direkte trussel.

Siden der linkes til indeholder aktive trusler! For din egen sikkerhed får du ikke tilladelse til at besøge denne side.

Siden, der linkes til, er ikke tilgængelig og kunne derfor ikke scannes.

Hvis musen holdes over et individuelt ratingikon, vises detaljer om det pågældende link. Oplysningerne omfatter yderligere detaljer om truslen (hvis der er nogen), IP-adressen til linket, og hvornår siden blev scannet af AVG:

10.7.4.AVG Aktivt surf-skjold

Denne kraftfulde beskyttelse blokerer ondsindet indhold på enhver webside, du forsøger at åbne, og forhindrer at det downloades til din computer. Hvis du klikker på et link eller indtaster en URL til et farligt websted, hvis denne funktion er aktiveret, bliver åbning af websiden automatisk blokeret, hvorved du beskyttes mod at blive inficeret uden at vide det. Det er vigtigt at huske på, at websider med exploits kan inficere din computer blot ved at besøge den pågældende side. Derfor tillader ***AVG Sikkerhedsværktøjslinjen*** ikke din browser at vise farlige websider, der indeholder exploits eller andre alvorlige trusler.

Hvis du støder på et ondsindet websted vil ***AVG Sikkerhedsværktøjslinjen*** advare dog i din webbrowser med et skærmbillede lignende dette:

Hvis du stadig ønsker at besøge den inficerede side, er der et link tilgængeligt på skærmen, ***men det anbefales ikke at fortsætte til disse sider!***

10.8.Web Shield

10.8.1.Web Shield-principper

Web Shield er en form for indbygget realtidsbeskyttelse. Det scanner indholdet på besøgte websider (og evt. filer på dem), før de vises i din webbrowser eller downloades til din computer.

Web Shield detekterer om siden, du vil besøge, indeholder farligt javascript, og forhindrer at siden vises. Det genkender også malware på en side, og stopper øjeblikkeligt download af den, så det aldrig når frem til din computer.

Bemærk! *AVG Web Shield er ikke beregnet til serverplatforme!*

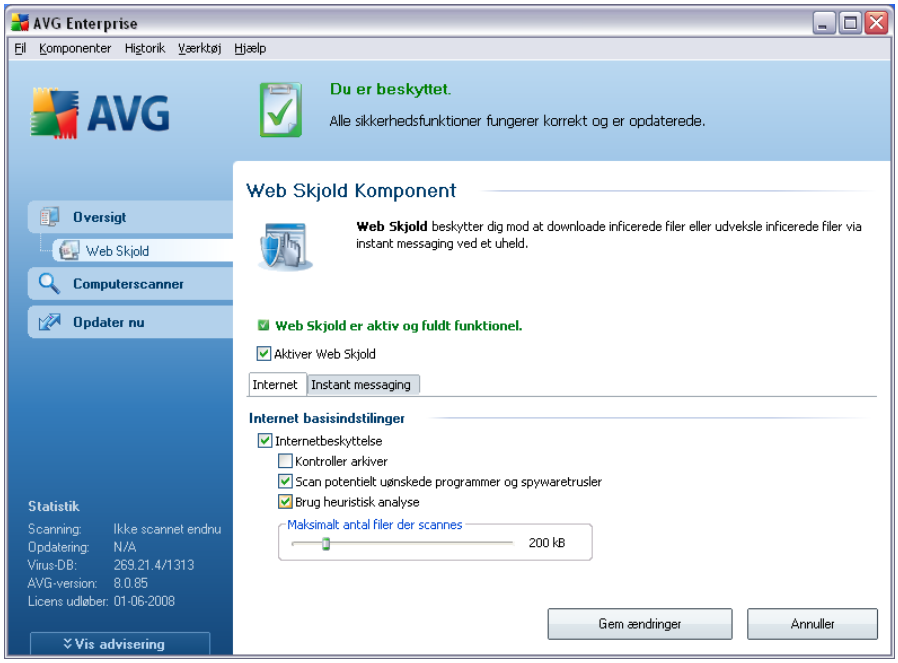
10.8.2.Web Shield-grænseflade

Web Shield-komponentens grænseflade beskriver opførslen for denne beskyttelsestype. Desuden kan du finde oplysninger om komponentens aktuelle status (*Web Shield er aktiv og fuldt funktionsdygtig.*). I den nederste del af dialogen kan du finde de elementære redigeringsmuligheder for denne komponents funktionalitet.

Grundlæggende komponentkonfiguration

Først og fremmest har du mulighed for omgående at slå ***Web Shield*** til/fra ved at markere elementet ***Aktiver Web Shield***. Denne indstilling er slået til som standard, og ***Web Shield***-komponenten er aktiv. Hvis du ikke har en god grund til at ændre denne indstilling, anbefaler vi at bevare komponenten aktiv. Hvis elementet er markeret, og ***Web Shield*** kører, er der adgang til flere konfigurationsindstillinger, der kan redigeres, på to faner:

- ***Internet*** - du kan redigere komponentens konfiguration vedrørende scanning af indhold på websteder. I redigeringsgrænsefladen kan du konfigurere følgende grundlæggende indstillinger:

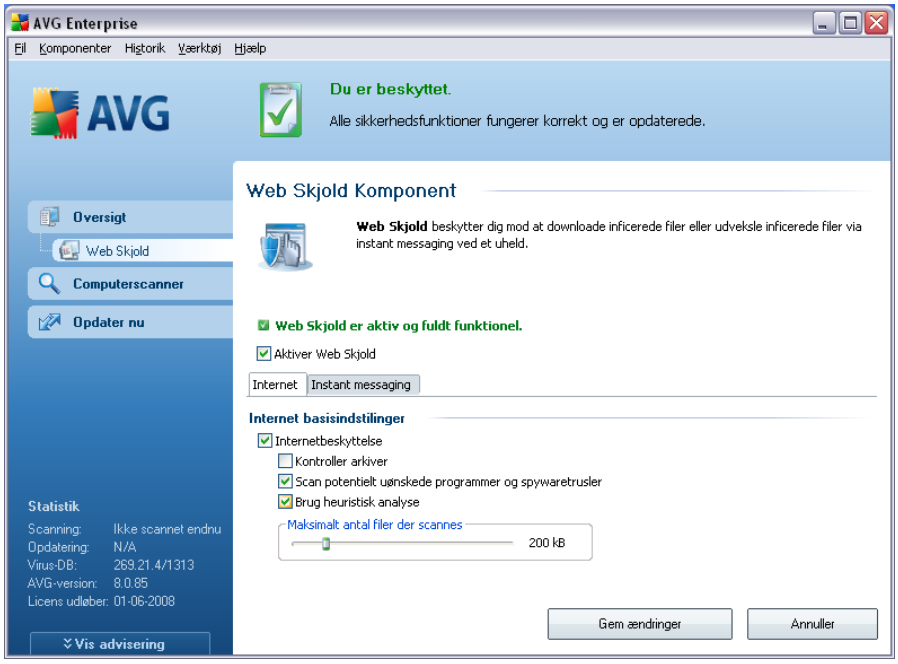


o ***Internetbeskyttelse*** - denne indstilling bekræfter, at ***Web Shield*** skal

udføre en scanning af indhold på www-sider. Hvis denne indstilling er slået til (*som standard*), kan du yderligere slå disse elementer til/fra:

- ***Kontroller arkiver*** - scan indholdet i arkiver, der muligvis er en del af www-siden, der skal vises
- ***Scan potentielt uønskede programmer*** - scan potentielt uønskede programmer (*eksekverbare programmer, der kan fungere som spyware eller adware*), der er en del af www-siden, der skal vises
- ***Brug heuristisk analyse*** - scan indholdet på siden, der skal vises, vha. heuristisk analyse *(dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø - se kapitlet Anti-virus-principper*)
- ***Maksimal scannet filstørrelse*** - hvis der er filer på den viste side, kan du også scanne deres indhold, før de downloades til din computer. Men scanning af store filer tager lang tid, og download af websiden kan blive markant langsommere. Du kan bruge skyderen til at angive den maksimale størrelse for en fil, der stadig skal scannes med ***Web Shield***. Selvom den downlaodede fil er større end angivet, og derfor ikke scannes med ***Web Shield***, er du stadig beskyttet. Hvis filen er inficeret, detekterer ***Resident Shield*** det øjeblikkeligt.

- ***Instant messaging*** - gør det muligt at redigere komponentens indstillinger vedrørende scanning af instant messaging (*f.eks. ICQ, MSN Messenger, Yahoo ...*).



-

  - Instant messaging-beskyttelse - marker dette element, hvis du vil have Web Shield til at verificere, at onlinekommunikationen er virusfri. Hvis denne indstilling er slået til, kan du yderligere angive, hvilken instant messaging-applikation, du vil kontrollere - aktuelt understøtter **AVG 8.5 Anti-virus plus firewall** applikationerne ICQ, MSN og Yahoo.

Bemærk: *-softwareleverandøren har konfigureret alle AVG-komponenter til den optimale ydeevne. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge systemmenupunktet* ***Værktøjer / Avancerede indstillinger*** *og redigere AVG-konfigurationen i dialogen AVG Avancerede indstillinger , der åbnes.*

Betjeningsknapper

Betjeningsknapperne, der er tilgængelige i ***Web Shield***-grænsefladen, er som følger:

- ***Gem ændringer*** - klik på denne knap for at gemme og anvende de ændringer, der er foretaget i denne dialog
- ***Annuller*** - klik på denne knap for at vende tilbage til den normale AVG-brugergrænseflade(*komponentoversigt*)

10.8.3.Webskjold detektering

Web Shield scanner indholdet på besøgte websider og eventuelle filer på dem, før de vises i din webbrowser eller downloades til din computer. Hvis en trussel detekteres, bliver du omgående advaret med følgende dialog:

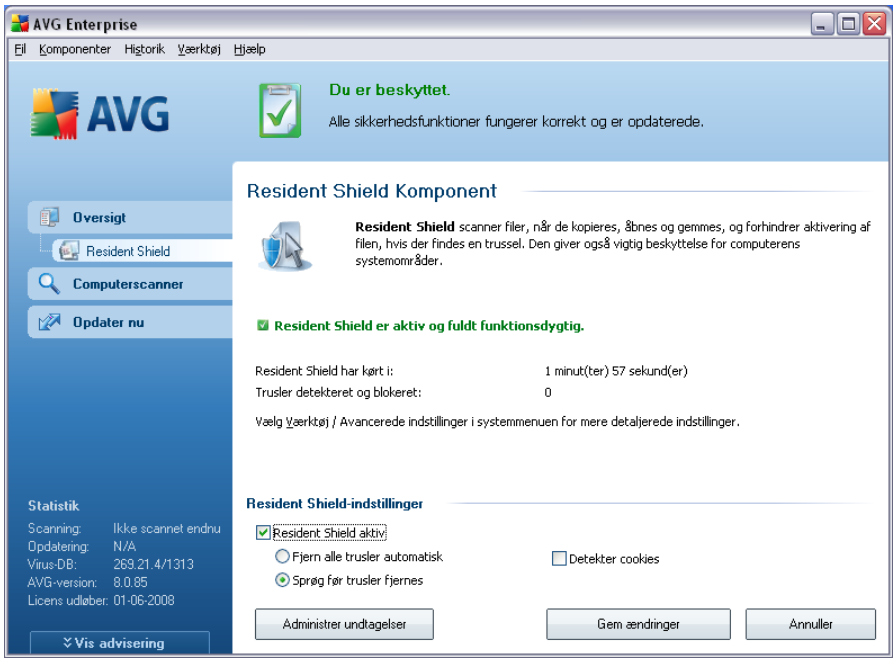
Den mistænkelige webside bliveri kke åbnet, og trusseldetekteringen bliver logget i listen over ***Web Shield-fund*** (*tilgængelig via systemmenuen Historik / Web Shield-fund*).

10.9.Resident Shield

10.9.1.Resident Shield Principper

Resident Shield scanner filer, når de kopieres, åbnes eller gemmes. Hvis ***Resident Shield*** opdager en virus i en fil, der aktiveres, stoppes den igangværende operation, og virussen får ikke lov til at aktivere sig selv. ***Resident Shield***, der indlæses i computerens hukommelse under opstart af systemet, yder også vital beskyttelse af computerens systemområder.

10.9.2.Resident Shield-grænseflade



Ud over en oversigt over de vigtigste statistiske data og oplysninger om komponentens aktuelle status (*Resident Shield er aktiv og fuldt funktionsdygtig*), indeholder ***Resident Shield***-grænsefladen også nogle elementære komponentindstillingsmuligheder. Statistikkerne er som følger:

- ***Resident Shield har været aktiv i*** - indeholder den forløbne tid, siden komponenten blev startet sidst
- ***Trusler detekteret og blokeret*** - antal detekterede infektioner, der blev forhindret i at køre/åbne (*om nødvendigt kan denne værdi nulstilles, f.eks. til statistiske formål - Nulstil værdi*)

Grundlæggende komponentkonfiguration

I den nederste del af dialogvinduet findes sektionen ***Resident Shield-indstillinger***, hvor du kan redigere nogle grundlæggende indstillinger for komponentens funktionalitet (*detaljeret konfiguration er som for alle andre komponenter tilgængelig via punktet Filer/Avancerede indstillinger i systemmenuen*).

Med indstillingen ***Resident Shield er aktiv*** kan du nemt slå komponentens

beskyttelse til/fra. Som standard er funktionen slået til. Med indbygget beskyttelse slået til kan du yderligere beslutte, hvordan eventuelt detekterede infektioner skal behandles (fjernes):

- enten automatisk (***Fjern alle trusler automatisk***)
- eller kun hvis brugeren godkender det (***Spørg før trusler fjernes***)

Dette valg har ingen betydning for sikkerhedsniveauet og det afspejler kun, hvad du foretrækker.

I begge tilfælde kan du stadig vælge, om du vil ***Fjerne cookies automatisk.*** I specifikke tilfælde kan du slå denne indstilling til for at opnå et maksimalt sikkerhedsniveau, men den er slået fra som standard. (*cookies = tekstpakker, der sendes fra en server til en webbrowser og derefter sendes tilbage uændret af browseren, hver gang den opretter forbindelse til denne server. HTTP-cookies bruges til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f. eks. foretrukne indstillinger på webstedet eller indholdet i deres elektroniske indkøbsvogne*).

Bemærk: *-softwareleverandøren har konfigureret alle AVG-komponenter til den optimale ydeevne. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge systemmenupunktet* ***Værktøjer / Avancerede indstillinger*** *og redigere AVG-konfigurationen i dialogen AVG Avancerede indstillinger , der åbnes.*

Betjeningsknapper

Betjeningsknapperne, der er tilgængelige i ***Resident Shield***-grænsefladen, er som følger:

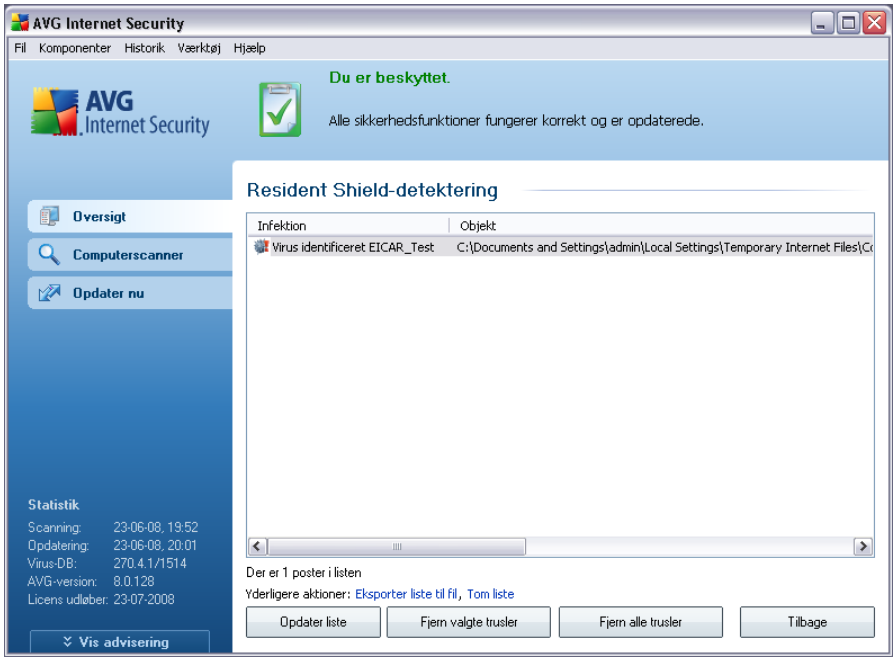
- ***Administrer undtagelser*** - åbner dialogen ***Resident Shield - Mappeundtagelser***, hvor du kan definere mapper, der ikke skal medtagees i ***Resident Shield***-scanningen
- ***Gem ændringer*** - klik på denne knap for at gemme og anvende de ændringer, der er foretaget i denne dialog
- ***Annuller*** - klik på denne knap for at vende tilbage til den normale ***AVG-brugergrænseflade*** (komponentoversigt)

10.9.3.Resident Shield-detektering

Resident Shield scanner filer, når de kopieres, åbnes eller gemmes. Når en virus eller enhver form for trussel detekteres, bliver du omgående advaret med følgende dialog:

Dialogen indeholder oplysninger om den detekterede trussel, og den beder dig om at afgøre, hvilken handling, der skal foretages nu:

- ***Helbred*** - hvis der findes en kur, helbreder AVG den inficerede fil automatisk. Denne valgmulighed er den anbefalede handling
- ***Flyt til Virus Vault*** - virussen flyttes til AVG ***Virus Vault***
- ***Ignorer*** - vi anbefaler på det kraftigste IKKE at anvende denne valgmulighed, medmindre du har en meget god grund til at gøre det!



Resident Shield-detektering tilbyder en oversigt over objekter, der blev detekteret af ***Resident Shield***, vurderet som farlige og enten helbredt eller flyttet til ***Virus Vault***. For hvert detekteret objekt findes følgende oplysninger:

- ***Infektion*** - beskrivelse af (muligvis også navn på) det detekterede objekt
- ***Objekt*** - objektets placering
- ***Resultat*** - handling udført med det detekterede objekt
- ***Objekttype*** - type for det detekterede objekt
- ***Proces*** - hvilken handling blev udført for at fremkalde det potentielt farlige objekt, så det kunne detekteres

I den nederste del af dialogen, under listen, finder du oplysninger om det totale antal detekterede objekter, der er anført ovenfor. Derudover kan du eksportere hele listen over detekterede objekter til en fil (***Eksporter liste til fil***) og slette alle poster om detekterede objekter (***Tøm liste***). Knappen ***Opdater liste*** opdaterer listen over fund detekteret af ***Resident Shield***. Knappen ***Tilbage*** skifter tilbage til den almindelige ***AVG brugerflade*** (komponentoversigt).

10.10. Opdateringsadministrator

10.10.1. Opdateringsadministrator-principper

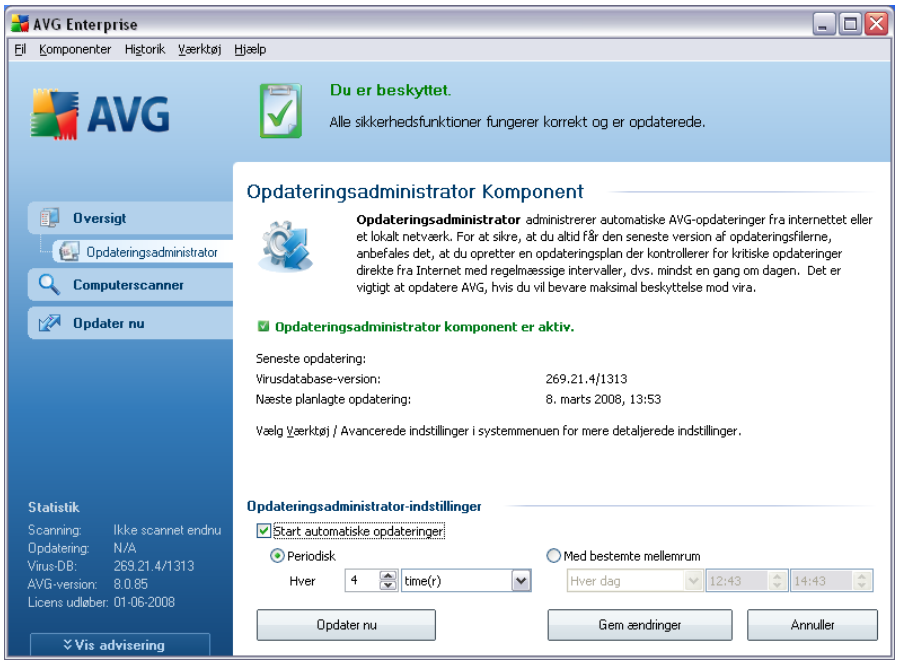
Ingen sikkerhedssoftware kan garantere reel beskyttelse mod forskellige typer af trusler, med mindre den opdateres regelmæssigt! Virusskribenter er altid på udkig efter nye sikkerhedshuller, de kan udnytte, i både software og operativsystemer. Nye vira, nye malware og nye hackingforsøg forekommer dagligt. Derfor udgiver softwareleverandører kontinuerligt opdateringer og sikkerhedspatches for at udbedre opdagede sikkerhedshuller.

Det er afgørende at AVG opdateres regelmæssigt!

Opdateringsadministrator hjælper dig med at kontrollere den regelmæssige opdatering. I denne komponent kan du planlægge automatiske downloads af opdateringsfiler fra internettet eller fra det lokale netværk. Vigtige opdateringer af virusdefinitioner bør om muligt foretages dagligt. Mindre vigtige programopdateringer kan foretages ugentligt.

Bemærk: *Se kapitlet AVG Opdateringer for yderligere oplysninger om opdateringstyper og -niveauer!*

10.10. Opdateringsadministrator-grænseflade



Grænsefladen til ***Opdateringsadministrator*** viser oplysninger om komponentens funktionalitet og dens aktuelle status (*opdateringsadministrator er aktiv.*), og indeholder de relevante statistiske data:

- ***Seneste opdatering*** - angiver, hvornår og på hvilket klokkeslæt databasen blev opdateret.
- ***Virusdatabaseversion*** - definerer nummeret på den seneste virusdatabaseversion. Dette nummer forøges for hver opdatering af virusdatabasen

Grundlæggende komponentkonfiguration

I den nederste del af dialogboksen finder du sektionen ***Indstillinger for opdateringsadministrator***, hvor du kan udføre nogle ændringer af reglerne for kørsel af opdateringsprocessen. Du kan definere, om du vil downloade opdateringsfilerne automatisk (***Start automatiske opdateringer***), eller kun når du ønsker det. Som standard er indstillingen ***Start automatiske opdateringer*** slået til, og vi anbefaler at bevare det på den måde! Regelmæssig downloading af de seneste opdateringsfiler er afgørende for enhver sikkerhedssoftwares funktionalitet!

Desuden kan du definere, hvornår opdateringen skal køres:

- ***Periodisk*** - definer tidsintervallet
- ***På et bestemt tidspunkt*** - definer nøjagtig dato og klokkeslæt

Som standard er opdateringen indstillet til hver 4. time. Det anbefales på det kraftigste at bevare denne indstilling, medmindre du har en god grund til at ændre den!

Bemærk: *-softwareleverandøren har konfigureret alle AVG-komponenter til den optimale ydeevne. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge systemmenupunktet* ***Værktøjer / Avancerede indstillinger*** *og redigere AVG-konfigurationen i dialogen AVG Avancerede indstillinger , der åbnes.*

Betjeningsknapper

Betjeningsknapperne, der er tilgængelige i ***Opdateringsadminstrator***-grænsefladen, er som følger:

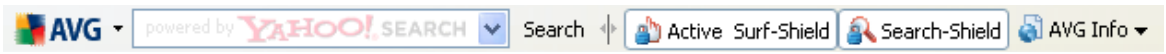
- ***Opdater nu*** - kører en øjeblikkelig opdatering, når du beder om det
- ***Gem ændringer*** - klik på denne knap for at gemme og anvende de ændringer, der er foretaget i denne dialog
- ***Annuller*** - klik på denne knap for at vende tilbage til den normale ***AVG-brugergrænseflade*** (komponentoversigt)

10.11. AVG Sikkerhedsværktøjslinje

AVG Sikkerhedsværktøjslinje er designet til at fungere med ***MS Internet Explorer*** (*version 6.0 eller nyere*) og ***Mozilla Firefox*** (*version 1.5 eller nyere*).

Bemærk! *AVG Sikkerhedsværktøjslinje er ikke beregnet til serverplatforme!*

Når den er installeret vil ***AVG Sikkerhedsværktøjslinje*** som standard være placeret lige under din browsers adresselinje:

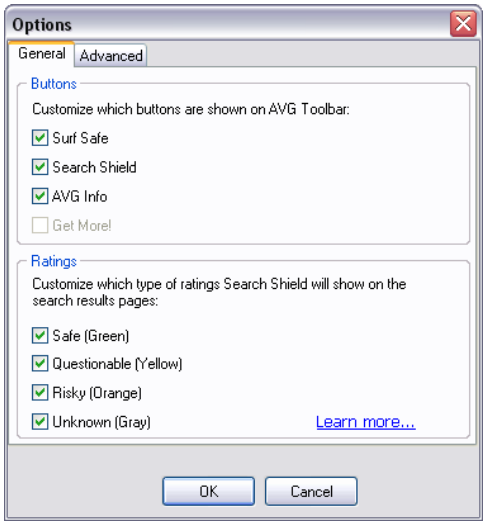


AVG Sikkerhedsværktøjslinje består af følgende:

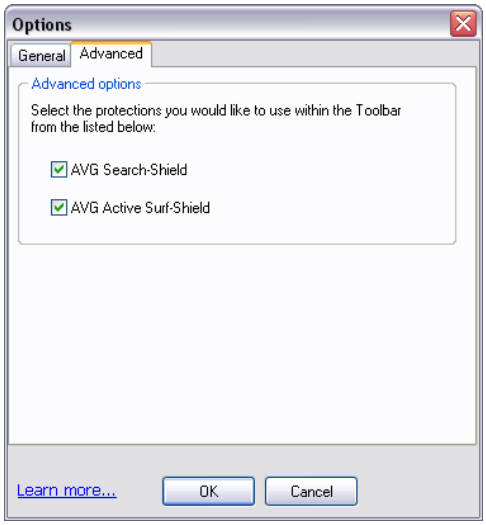
- ***AVG-logoknap*** - giver adgang til generelle elementer på værktøjslinjen. Klik på logoknappen for at komme videre til AVG's hjemmeside (www.avg.com). Hvis du klikker med markøren ved siden af AVG-ikonet åbnes det følgende:
  - ***Værktøjslinjeinfo*** - link til hjemmesiden for ***AVG Sikkerhedsværktøjslinje*** med detaljerede oplysninger om værktøjslinjens beskyttelse
  - ***Kør AVG 8.0*** - åbner AVG 8-brugergrænsefladen
  - ***Indstillinger*** - åbner en konfigurationsdialog, hvor du kan justere dine indstillinger for ***AVG Sikkerhedsværktøjslinje***, så de passer til dine behov. Dialogen er inddelt i to faner:
    - ***Generelt*** - på denne fane finder du de to sektioner ***Knapper*** og ***Rating***.

      I sektionen ***Knapper*** kan du konfigurere hvilke knapper, der er synlige eller skjulte på ***AVG Sikkerhedsværktøjslinje***. Som standard er alle knapper synlige.

      I sektionen ***Rating*** kan du bestemme hvilken type rating, du vil have vist for dine søgeresultater. Som standard er alle ratinger synlige, men du kan skjule nogle af dem (*når du søger fra Yahoo!-søgefeltet, vises kun sikre resultater*).



➢ ***Avanceret*** - på denne fane kan du redigere beskyttelsesfunktionerne på ***AVG Sikkerhedsværktøjslinje***. Som standard er både ***AVG Søgeskjold*** og ***AVG Aktivt surfskjold*** aktiveret.



o ***Opdater*** - søger efter nye opdateringer til din ***AVG Sikkerhedsværktøjslinje***

o ***Hjælp*** - indeholder muligheder for at åbne hjælpefilen, kontakte ***AVG teknisk support*** eller se detaljerne om den aktuelle version af værktøjslinjen

- ***Yahoo!-drevet søgefelt*** - nem og sikker måde at søge på nettet ved hjælp af Yahoo!-søgning. Indtast et ord eller en sætning i søgefeltet og tryk på ***Søg*** for at starte søgningen direkte på Yahoo!-serveren, uanset hvilken side der vises aktuelt. Søgefeltet viser også en liste over din søgehistorik. Søgninger foretaget med søgefeltet analyseres ved hjælp af ***AVG Søgeskjold***-beskyttelsen.

- ***AVG Aktivt surfskjold-knap*** - tænd/sluk-knappen kontrollerer status for ***AVG Aktivt søgeskjold***-beskyttelsen

- ***AVG Søgeskjold-knap*** - tænd/sluk-knappen kontrollerer status for ***AVG Søgeskjold***-beskyttelsen

- ***AVG Infoknap*** - indeholder link til vigtige sikkerhedsoplysninger på AVG's hjemmeside (www.avg.com)

11. Identitets beskyttelse

Identitets beskyttelse er en stand-alone komponent førhen kendt som Sana er fornylig blevet indarbejdet i**AVG 8.5 Anti-virus plus firewall**. Den installeres fra den samme installationsfil som med det passende licensnummer (*for detaljer om produkt valg og licensering venligst se AVG Download Manager*).

Identitets beskyttelse er for nærværende kun på Engelsk.

11.1.Identitets beskyttelses principper

Identificer tyveri beskyttelses software

Sana s teknologi kommer fra adfærds baseret sikkerhedssoftware Fordi det læser malware/ trussels karakteristisk adfærd, Sana s unikke og alsidige software forebygger PC angreb imod pludselige opståede og fremtidige trusler i real time (nul-dags beskyttelse). Som drengene på Sana siger: "øjeblikkelig og konstant beskyttelse".

11.2.Identitets beskyttelses brugerflade

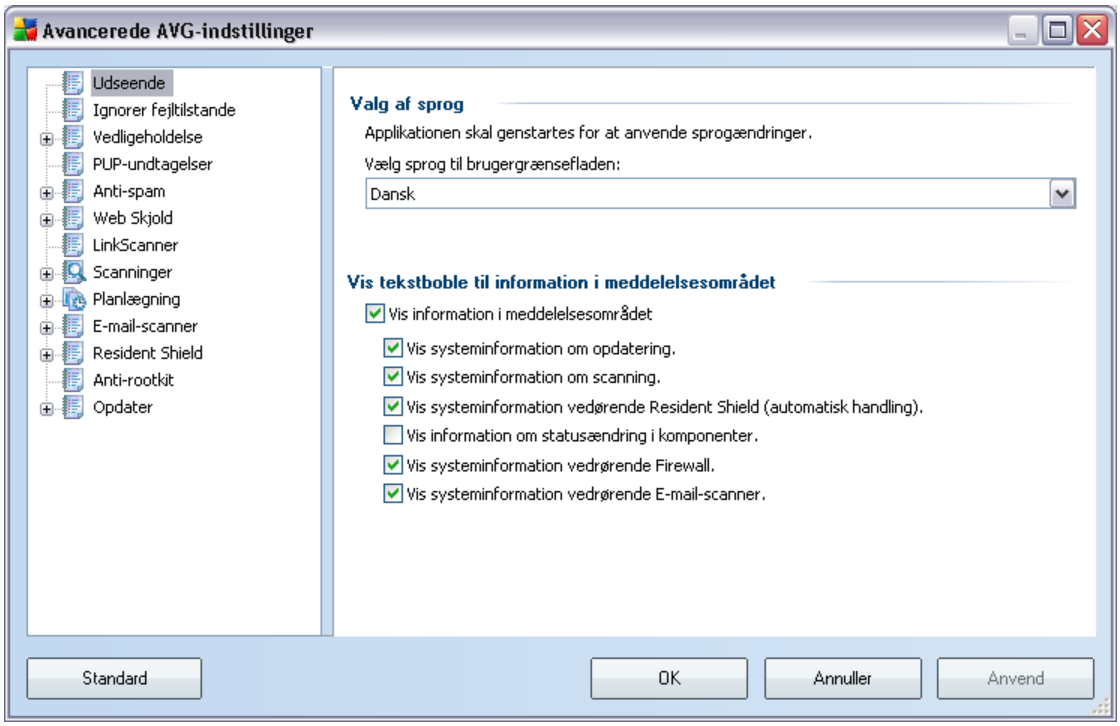
Indtast emnetekst her.

12. AVG Avancerede indstillinger

Den avancerede konfigurationsdialog i **AVG 8.5 Anti-virus plus firewall** åbnes i et nyt vindue med navnet ***Avancerede AVG-indstillinger***. Vinduet er inddelt i to sektioner: Venstre del indeholder et navigationstræ til programmets konfigurationsindstillinger. Vælg den komponent, du vil ændre konfigurationsen af (*eller den specifikke del*), for at åbne redigeringsdialogen i vinduets højre sektion.

12.1.Udseende

Det første element i navigationstræet, ***Udseende***, refererer til de generelle indstillinger for AVG-brugergrænsefladen og nogle få elementære indstillinger for applikationens opførsel:



Valg af sprog

I sektionen ***Valg af sprog*** kan du vælge dit ønskede sprog i rullemenuen. Derefter bruges sproget til hele AVG-brugergrænsefladen. Rullemenuen indeholder kun de sprog, du tidligere har valgt skulle installeres under installationsprocessen (se kapitlet Brugertilpasset installation - Valg af komponenter). For at fuldføre skiftet til

et andet applikationssprog, skal du dog genstarte brugergrænsefladen ved at følge disse trin:

- Vælg det ønskede applikationssprog og bekræft dit valg ved at trykke på knappen ***Anvend*** (nederste højre hjørne)
- Tryk på knappen ***OK*** for at lukke redigeringsdialogen ***Avancerede AVG-indstillinger***
- Luk AVG-brugergrænsefladen via systemmenuen, elementet ***Filer/Afslut***
- Åbn AVG-brugergrænsefladen igen på en af disse måder: dobbeltklik på AVG-systembakkeikonet, dobbeltklik på AVG-ikonet på skrivebordet, eller via menuen ***Start/Alle programmer/AVG 8.0/AVG Brugergrænseflade***(se kapitlet ***Adgang til brugergrænseflade***). Derefter vises brugergrænsefladen med det nyvalgte sprog.

Bakketekstbobler

I denne sektion kan du slå visning af tekstbobler i systembakken om applikationens status fra. Som standard er visning af bakketekstbobler tilladt, og det anbefales at beholde denne konfiguration! Bakketekstboblerne informerer typisk om statusændring i visse AVG-komponenter, og du bør holde øje med dem!

Men hvis du af en eller anden grund beslutter, at du ikke vil have vist disse tekstbobler, eller du kun vil have vist visse tekstbobler (vedrørende en bestemt AVG-komponent), kan du definere og angive dine ønsker ved at markere/afmarkere følgende indstillinger:

- ***Vis systembakketekstbobler*** - som standard er dette punkt markeret (*slået til*), og tekstbobler vises. Afmarker dette punkt for at deaktivere visning af alle bakketekstbobler fuldstændig. Når det er slået til, kan du yderligere vælge, hvilke specifikke tekstbobler, der skal vises:
  - ***Vis bakketekstbobler om opdatering*** - bestem, om oplysninger vedrørende kørsel, forløb og afslutning af AVG opdatering skal vises.
  - ***Vis bakketekstbobler om scanning*** - bestem, om oplysninger ved automatisk kørsel, forløb og resultater af planlagt scanning skal vises.
  - ***Vis bakketekstbobler vedrørende Resident Shield*** - bestem, om oplysninger vedrørende lagring, kopiering og åbning af filer skal vises eller tilsidesættes.

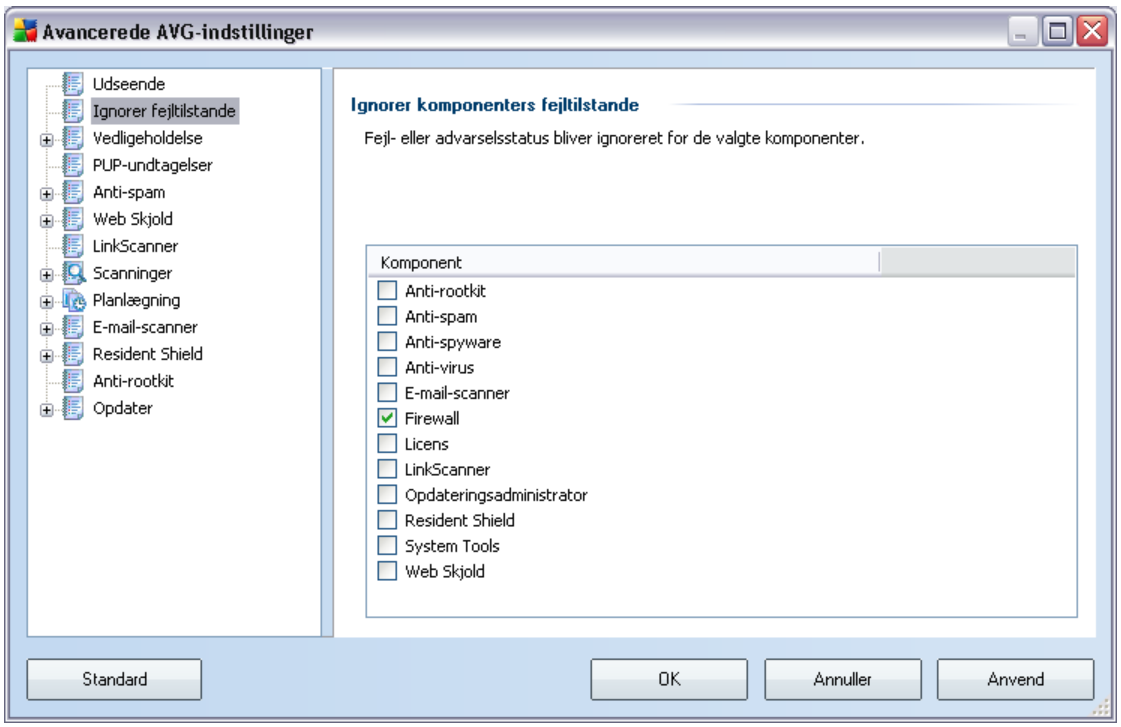
- ***Vis tekstbobler om komponenttilstandsændringer*** - bestem, om oplysninger vedrørende om komponenter er aktive/inaktive eller mulige problemer med dem skal vises. Ved rapportering af fejlstatus på en komponent svarer denne indstilling til informationsfunktionen i systembakkeikonet (farveændring), der rapporterer et problem i en vilkårlig AVG-komponent.

- ***Vis bakketekstbobler vedrørende Firewall*** - bestem, om oplysninger vedrørende Firewall-status og -processer, f.eks. advarsler om aktiver/deaktivering af komponenten, mulig blokering af trafik osv., skal vises.

- ***Vis bakketekstbobler vedrørende E-mail scanner*** - bestem, om oplysninger ved scanning af alle indkommende og udgåene e-mail-meddelelser skal vises.

12.2.Ignorer fejltilstande

I dialogen ***Ignorer komponenters fejltilstande*** kan du markere de komponenter, du ikke vil have informationer om:



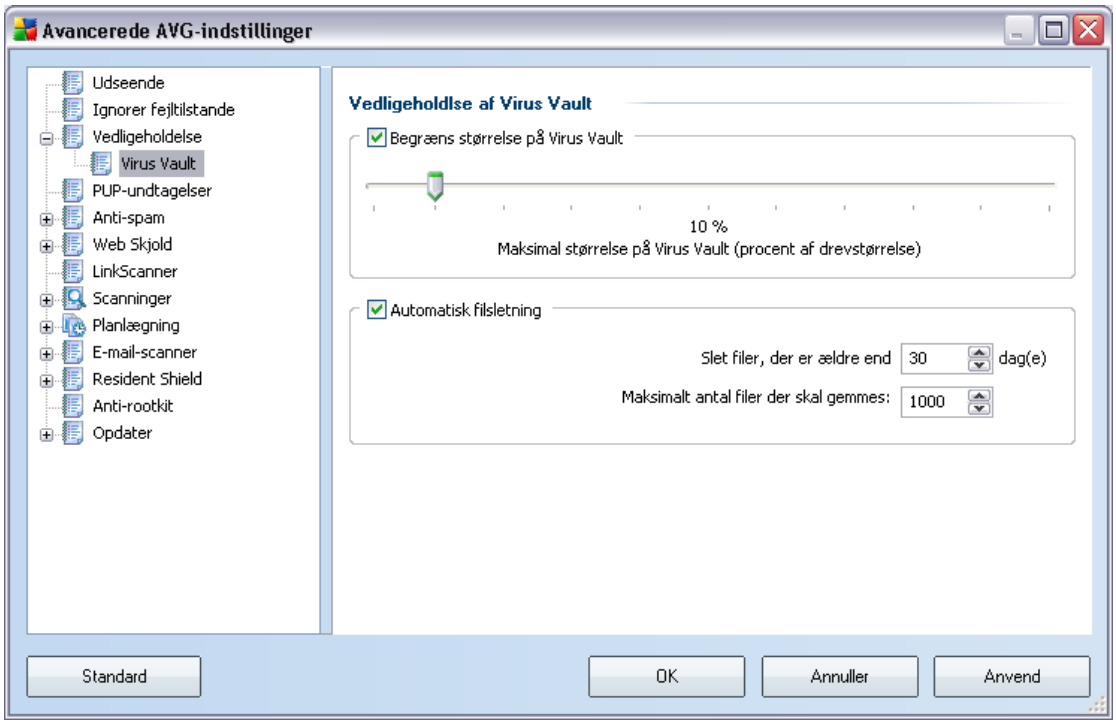
Som standard er ingen komponenter valgt på listen. Det betyder, at hvis en komponent får en fejlstatus, bliver du med det samme informeret om det via:

- ***systembakkeikonet*** - mens alle dele af AVG fungerer korrekt, vises ikonet i fire farver, men når der opstår en fejl, skifter ikonet til en grå farve med et rødt udråbstegn,
- tekstbeskrivelse af det eksisterende problem i sektionen ***Info om sikkerhedsstatus*** i AVG's hovedvindue

Der kan være en situation, hvor du af en årsag vil slå en komponent fra midlertidigt (*dette anbefales ikke, du bør forsøge at holde alle komponenter aktive permanent og i standardkonfigurationen, men det kan forekomme*). I dette tilfælde rapporterer systembakkeikonet automatisk komponentens fejltilstand. I dette tilfælde kan vi imidlertid ikke tale om en egentlig fejl, da du bevidst har skabt den, og du er opmærksom på den potentielle risiko. Samtidig kan ikonet ikke rapportere eventuelle yderligere fejl, der måtte opstå, da det allerede vises med gråt.

Derfor kan du i dialogen herover vælge komponenter, der kan være i en fejltilstand (*eller slået fra*), uden at du får information om det. Den samme mulighed for at ***Ignorere komponenttilstand*** er også tilgængelig for specifikke komponenter direkte fra komponentoversigten i AVG's hovedvindue.

12.3.Virus Vault



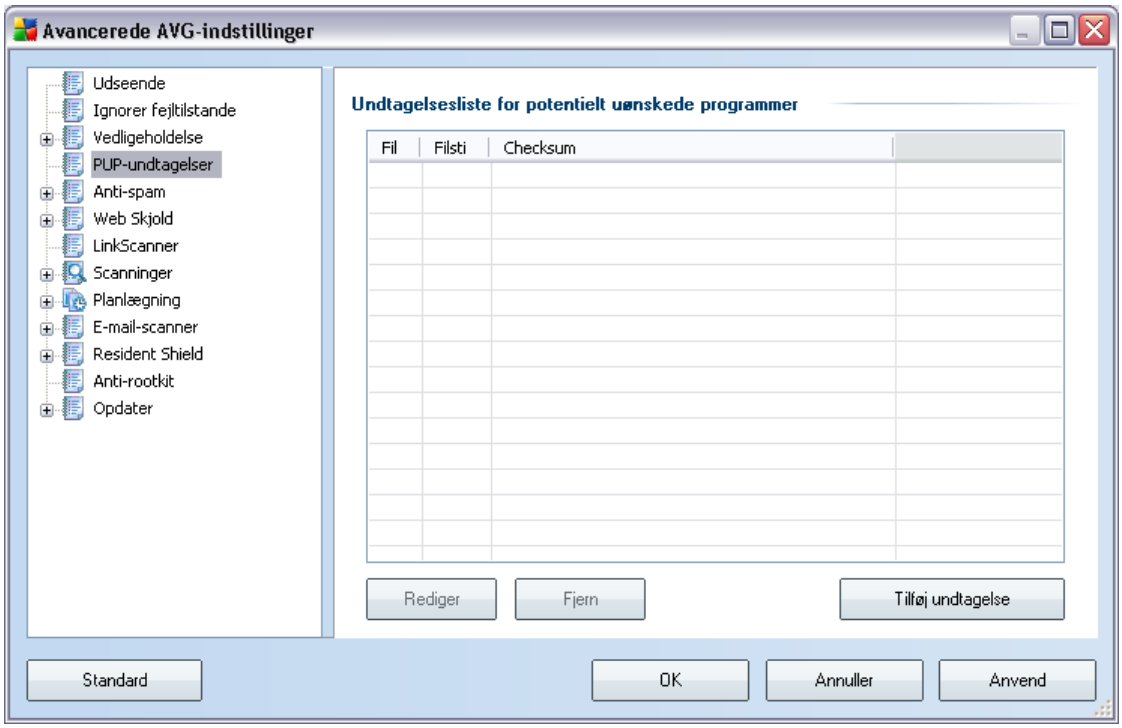
I dialogboksen ***Virus Vault-vedligeholdelse*** kan du definere adskillige parametre vedrørende administration af objekter, der opbevares i ***Virus Vault***:

- ***Begræns størrelse på Virus Vault*** - brug skyderen til at indstille den maksimale størrelse for ***Virus Vault***. Størrelsen angives proportionalt i forhold til størrelsen på den lokale disk.
- ***Automatisk filsletning*** - i denne sektion defineres det maksimale tidsrum, objekter kan lagres i ***Virus Vault*** (***Slet filer ældre end ... dage***), og det maksimale antal filer, der kan lagres i ***Virus Vault*** (***Maksimalt antal lagrede filer***)

12.4.PUP-undtagelser

AVG kan analysere og detektere eksekverbare applikationer og DLL-biblioteker, der er potentielt uønskede i systemet. I nogle tilfælde kan brugeren ønske at beholde visse uønskede programmer på computeren (programmer, der blev installeret med vilje). Nogle programmer, specielt gratis programmer, indeholder adware. Den slags adware kan detekteres og rapporteres af AVG som et ***potentielt uønsket program***. Hvis du

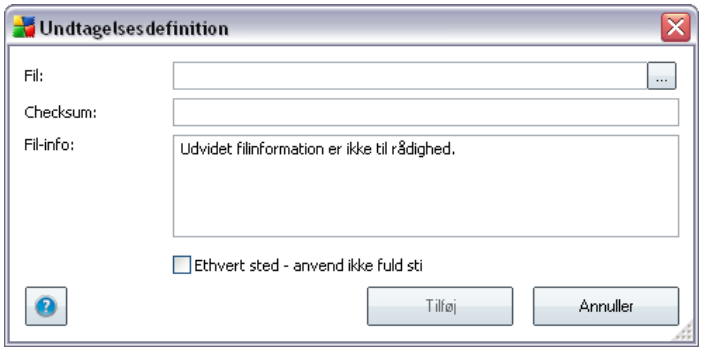
vil beholde et sådant program på computeren, kan du definere det som en potentielt uønsket program-undtagelse:



Dialogen ***Potentielt uønsket program-undtagelser*** viser en liste over allerede definerede og aktuelt gyldige undtagelser fra potentielt uønskede programmer. Du tilføjer, sletter eller tilføjer nye undtagelser.

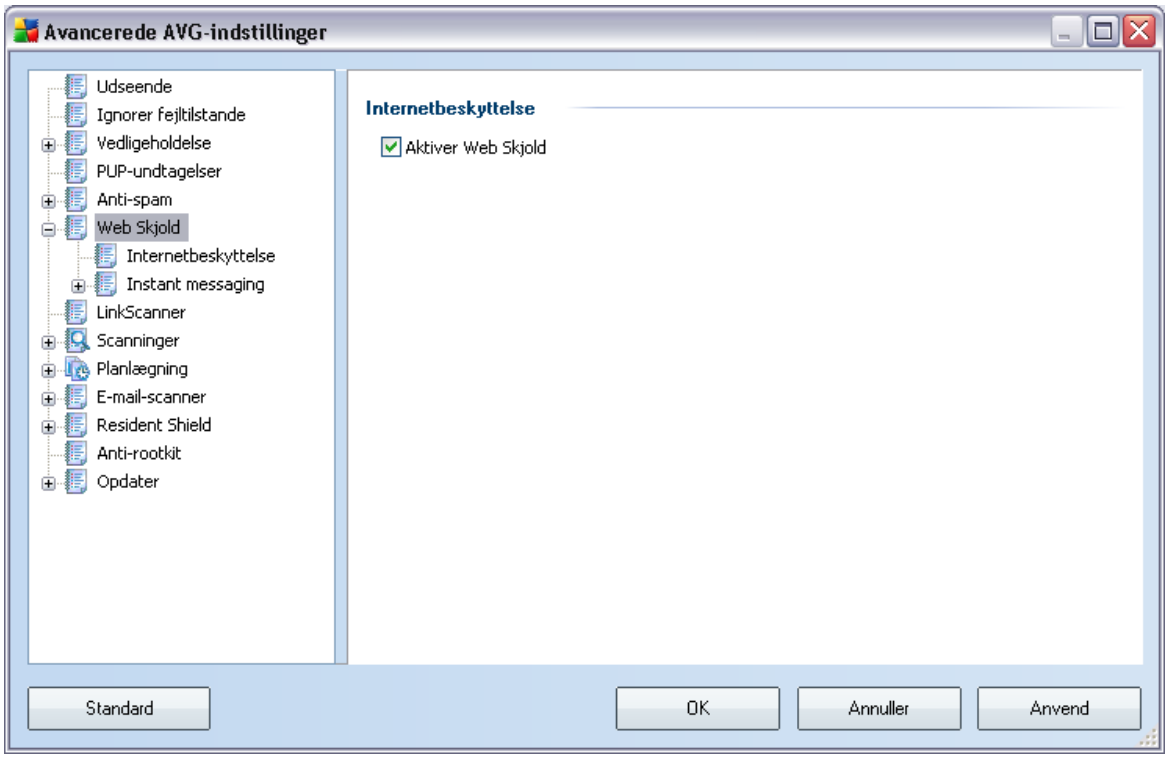
Betjeningsknapper

- ***Rediger*** - åbner en redigeringsdialog (*identisk med dialogen til definition af nye undtagelser, se nedenfor*) for en allerede defineret undtagelse, hvor du kan ændre undtagelsens parametre
- ***Fjern*** - sletter det valgte element fra listen over undtagelser
- ***Tilføj undtagelse*** - åbn en redigeringsdialog, hvor du kan definere parametre for den nye undtagelse, der skal oprettes:



- ***Fil*** - indtast den fulde sti til den fil, du vil mærke som en undtagelse
- ***Kontrolsum*** - viser den unikke 'signatur' for den valgte fil. Denne kontrolsum er en automatisk genereret tegnstreng, der gør det muligt for AVG endegyldigt at skelne den valgte fil fra andre filer. Kontrolsummen genereres og vises efter succesfuld tilføjelse af filen.
- ***Filinfo*** - viser yderligere tilgængelige oplysninger om filen (*oplysninger om licens/version mv.*)
- ***Ethvert sted - anvend ikke fuld sti*** - hvis du kun vil definere denne fil som en undtagelse for den specifikke placering, skal du lade dette afkrydsningsfelt stå tomt

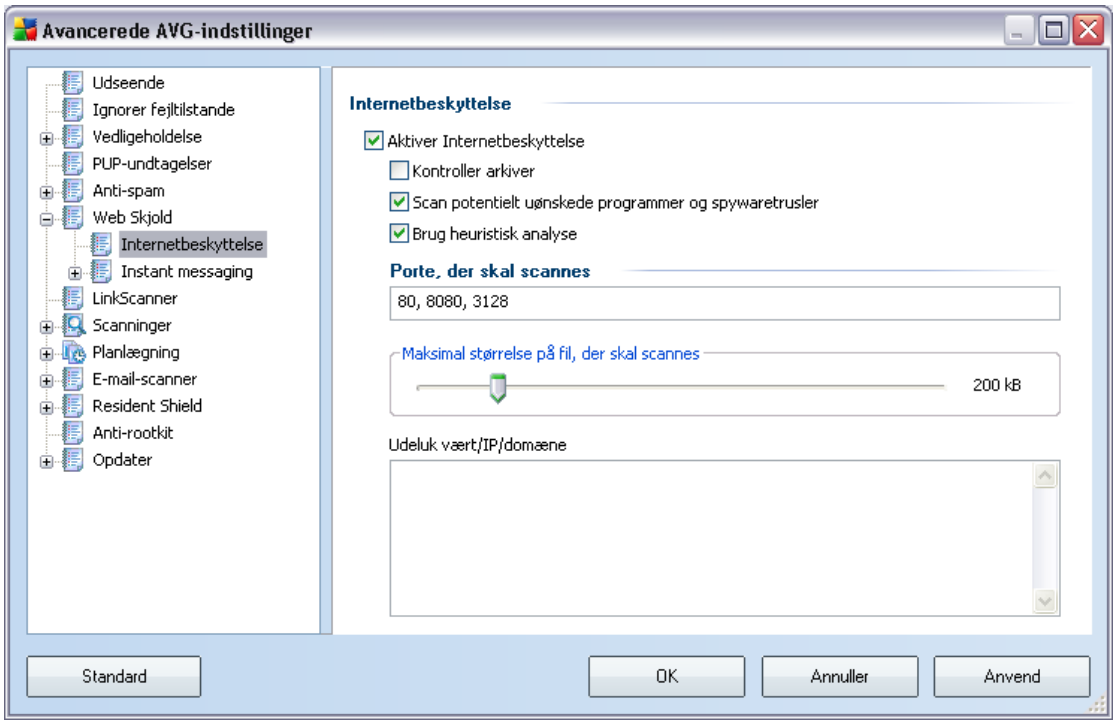
12.5.Web Shield



Med dialogen ***Internetbeskyttelse*** kan du aktivere/deaktivere hele ***Web Shield***-komponenten (*aktiveret som standard*). Fortsæt til de efterfølgende dialogbokse anført i navigationstræet for yderligere avancerede indstillinger af denne komponent.

I den nederste sektion i dialogen kan du vælge på hvilken måde, du vil informeres om mulige detekterede trusler: via standard popup-dialog, via bakketekstboble eller via bakkeikon.

12.5.1.Internetbeskyttelse



I dialogboksen ***Internetbeskyttelse*** kan du redigere komponentens konfiguration vedrørende scanning af indhold på websteder. I redigeringsgrænsefladen kan du konfigurere følgende grundlæggende indstillinger:

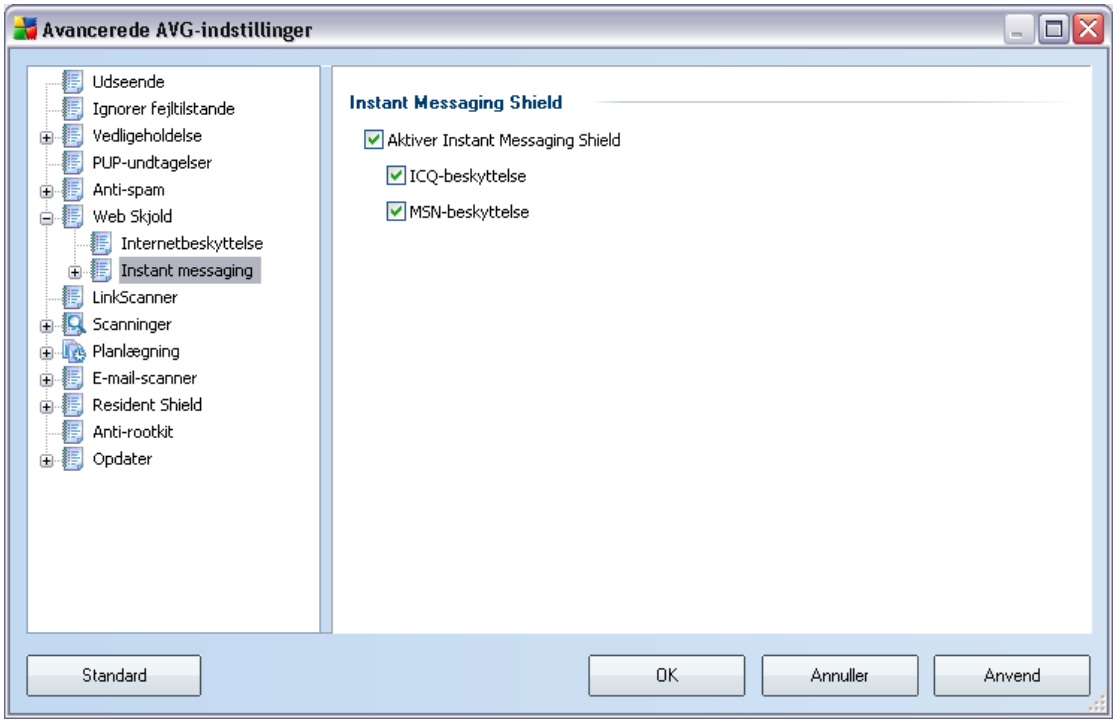
- ***Internetbeskyttelse*** - denne indstilling bekræfter, at ***Web Shield*** skal udføre en scanning af indhold på www-sider. Hvis denne indstilling er slået til (*som standard*), kan du yderligere slå disse elementer til/fra:
    - ***Kontroller arkiver*** - scan indholdet i arkiver, der muligvis er en del af www-siden, der skal vises .
    - ***Scan potentielt uønskede programmer og spywaretrusler*** - scan potentielt uønskede programmer (*eksekverbare programmer, der kan fungere som spyware eller adware*), der er en del af www-siden, der skal vises, og spyware-infektioner.
    - ***Brug heuristisk analyse*** - scan indholdet på siden, der skal vises, vha. heuristisk analyse (*dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø*).

- ***Porte, der skal scannes*** - dette felt anfører standardportnumrene for http-kommunikation. Hvis din computerkonfiguration afviger, kan du ændre portnumrene efter behov.

- ***Maksimal scannet filstørrelse*** - hvis der er filer på den viste side, kan du også scanne deres indhold, før de downloades til din computer. Men scanning af store filer tager lang tid, og download af websiden kan blive markant langsommere. Du kan bruge skyderen til at angive den maksimale størrelse for en fil, der stadig skal scannes med ***Web Shield***. Selvom den downlaodede fil er større end angivet, og derfor ikke scannes med Web Shield, er du stadig beskyttet. Hvis filen er inficeret, detekterer ***Resident Shield*** det øjeblikkeligt.

- ***Undtag vært/IP/domæne*** - i tekstfeltet kan du indtaste det nøjagtige navn på en server (*vært, IP-adresse, IP-adresse med maske eller URL*) eller et domæne, der ikke skal scannes af ***Web Shield***. Derfor bør du kun udelade væreter, som du kan være fuldstændig sikker på aldrig leverer provide farligt indhold.

12.5.2.Instant messaging

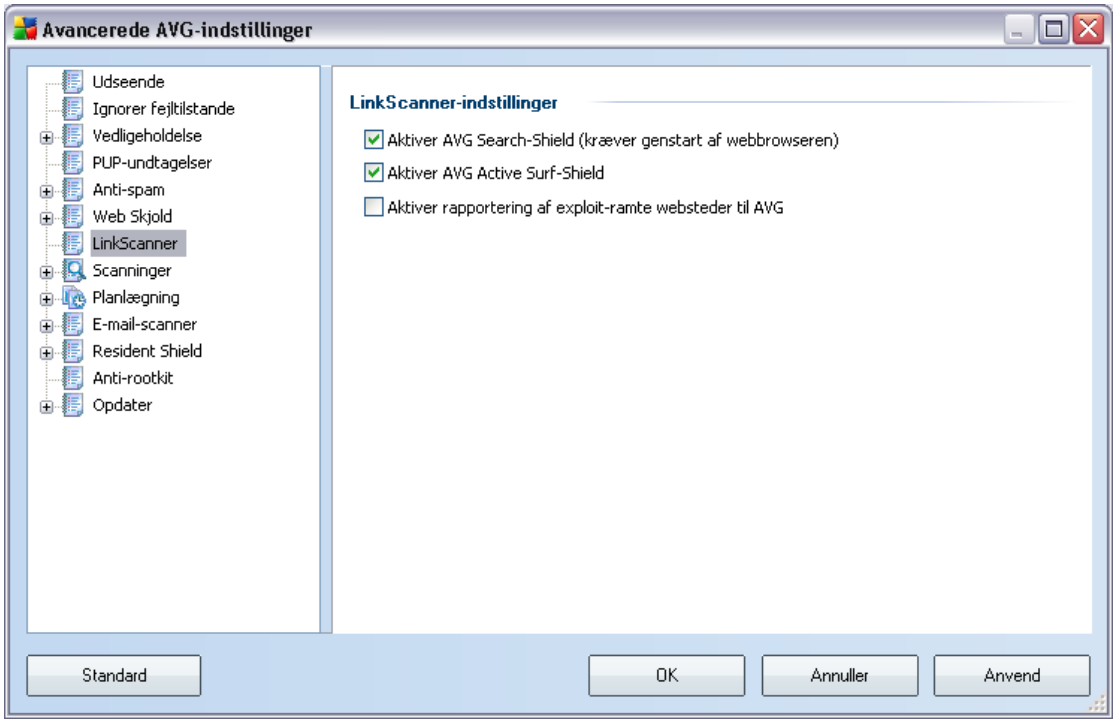


-

I dialogen ***Instant Messaging Shield*** kan du redigere ***Web Shield***-komponentens indstillinger vedrørende scanning af instant messaging. I øjeblikket understøttes kun tre instant messaging-programmer: ***ICQ*** , ***MSN*** og ***Yahoo*** - marker det pågældende punkt for hver af dem, hvis du vil have Web Shield til at verificere, om online-kommunikationen er virusfri.

For yderligere specifikation af tilladte/blokerede brugere kan du se og redigere den pågældende dialog (***Avanceret ICQ***eller ***Avanceret MSN***) og angive ***Hvidliste*** (*liste over brugere, der har tilladelse til at kommunikere med dig*) og ***Sortliste*** (*brugere der skal blokeres*).

12.6.Linkscanner



I dialogen ***Linkscannerindstillinger*** kan du slå de to elementære funktioner i ***Linkscanner*** til og fra:

- ***Aktiver sikker søgning*** - (*slået til som standard*): vejledende ikoner for søgninger udført i Google, Yahoo eller MSN efter forudgående kontrol af indholdet på websteder, der returneres af søgemaskinen. De understøttede browsere er Internet Explorer og Firefox.

- ***Aktiver Sikker surf*** - (*slået til som standard*): aktiv (*realtids*-) beskyttelse mod sider med exploits, når de åbnes. Kendte forbindelser til ondsindede websteder og deres exploitindhold blokeres, når de åbnes af brugeren via en webbrowser (*eller enhver anden applikation, der bruger HTTP*).

- ***Aktiver rapportering af websider med exploits til AVG*** - (*aktiveret som standard*): marker dette punkt for at tillade rapportering af exploits og ondsindede websteder, der findes af brugere, enten via ***Sikker surf*** eller ***Sikker søgning*** for at udbygge databasen, der indsamler oplysninger om ondsindet aktivitet på nettet.

12.7.Scanninger

De avancerede scanningsindstillinger er opdelt i tre kategorier, der refererer til specifikke scanningstyper, der er defineret af softwareleverandøren:

- ***Scan hele computeren*** - foruddefineret standardscanning af hele computeren

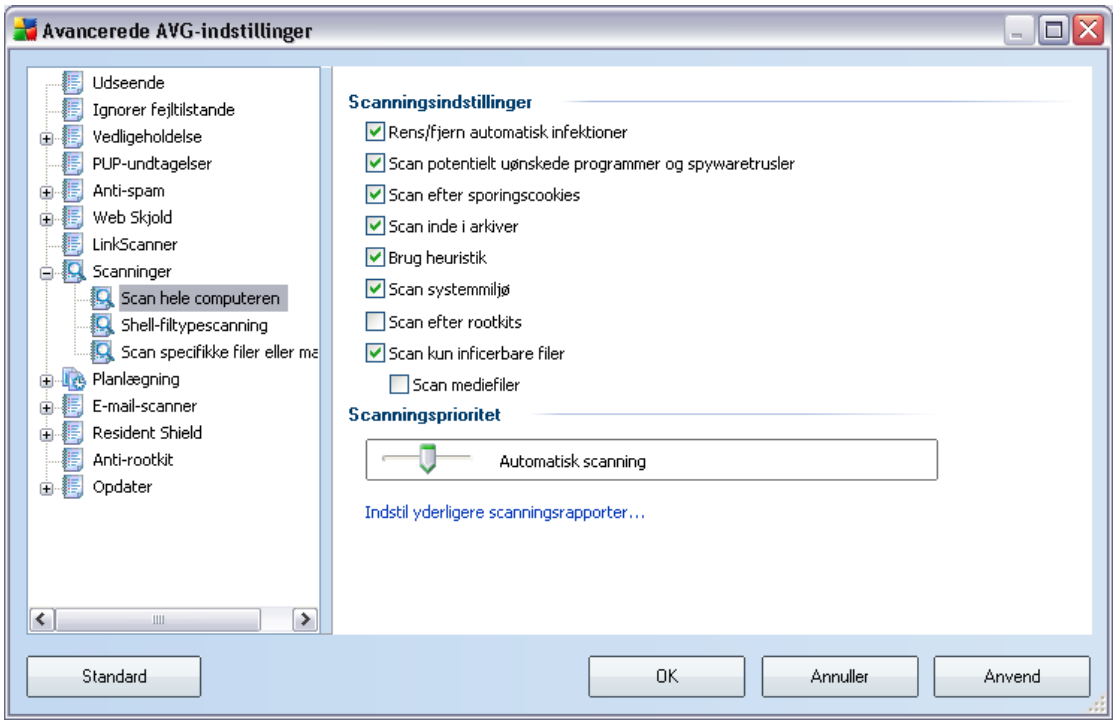
- ***Shell-udvidelsesscanning*** - specifik scanning af et udvalgt objekt direkte fra Windows stifinder

- ***Scan specifikke filer eller mapper*** - foruddefineret standardscanning af udvalgte områder af computeren

- ***Scanning af udtagelig enhed*** - specifik scanning af udtagelige enheder sluttet til computeren

12.7.1.Scan hele computeren

Indstillingen ***Scan hele computeren*** gør det muligt at redigere parametre for en af softwareleverandørens foruddefinerede scanninger, ***Scanning af hele computeren***:



Scanningsindstillinger

Sektionen ***Scanningsindstillinger*** indeholder en liste over scanningsparametre, der valgfrit kan slås til/fra.

- ***Helbred/fjern infektion automatisk*** - hvis der identificeres en virus under scanningen, kan den helbredes automatisk, hvis der er en kur tilgængelig . Hvis den inficerede fil ikke kan helbredes automatisk, eller hvis du beslutter at slå denne mulighed fra, modtager du information, når en virus detekteres, og du skal beslutte, hvad der skal gøres ved den detekterede infektion. Den anbefalede metode er at fjerne den inficerede fil til Virus Vault.

- ***Scan potentielt uønskede programmer*** - denne parameter kontrollerer Anti-virus-funktionaliteten, der tillader detektering af potentielt uønskede programmer (*eksekverbare filer, der kan køre som spyware eller adware*), og

disse kan derefter blokeres eller fjernes.

- ***Scan efter cookies*** - denne parameter i Anti-spyware-komponenten definerer, at cookies skal detekteres. (*HTTP-cookies anvendes til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på webstedet eller indhold i deres elektroniske indkøbsvogne*)

- ***Scan inde i arkiver*** - disse parametre definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i arkiver, f.eks. ZIP, RAR, ...

- ***Brug heuristik*** - heuristisk analyse (*dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø*) er en af metoderne, der anvendes til detektering af virus under scanningen.

- ***Scan systemmiljø*** - scanningen kontrollerer også computerens systemområder.

- ***Scan efter rootkits*** - marker dette punkt, hvis du vil inkludere rootkit-detektering i scanningen af hele computeren. Rootkit-detektering er også tilgængelig individuelt i ***Anti-rootkit***-komponenten;

- ***Scan kun inficerbare filer*** - med denne indstilling slået til, bliver filer, der ikke kan inficeres, ikke scannet. Det kan for eksempel være visse almindelige tekstfiler og andre ikkeeksekverbare filer.

    - ***Scan mediefiler*** – marker for at scanne mediefiler (video, audio osv.). Hvis du undlader at markere dette felt, reducerer det scanningstiden endnu mere, fordi filerne ofte er ret store og ikke har så stor sandsynlighed for at være inficeret med virus.

Scanningsprioritet

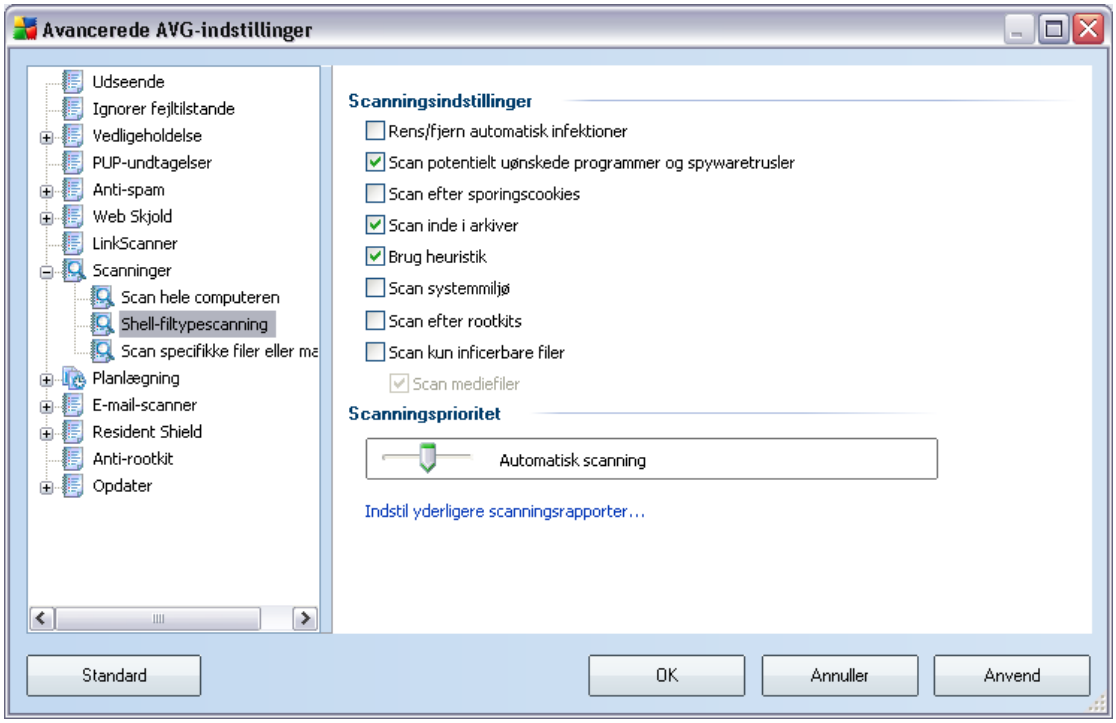
I sektionen ***Scanningsprioritet*** kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne indstillingsværdi sat til middelniveauet af automatisk ressourceforbrug. Hvis du vil have scanningen til at køre hurtigere, tager det kortere tid, men forbruget af systemressourcer øges markant under scanningen, og gør de andre aktiviteter på pc'en langsommere (*denne indstilling kan anvendes, når computeren er tændt, men der i øjeblikket ikke er nogen, der arbejder med den*). På den anden side kan du reducere forbruget af systemressourcer ved at forlænge scanningens varighed.

Indstil yderligere scanningsrapporter...

Klik på linket ***Indstil yderligere scanningsrapporter ...*** for at åbne det selvstændige dialogvindue ***Scanningsrapporter***, hvor du kan markere adskillige punkter for at definere, hvilke scanningsfund, der skal rapporteres:

12.7.2.Shell-udvidelsesscanning

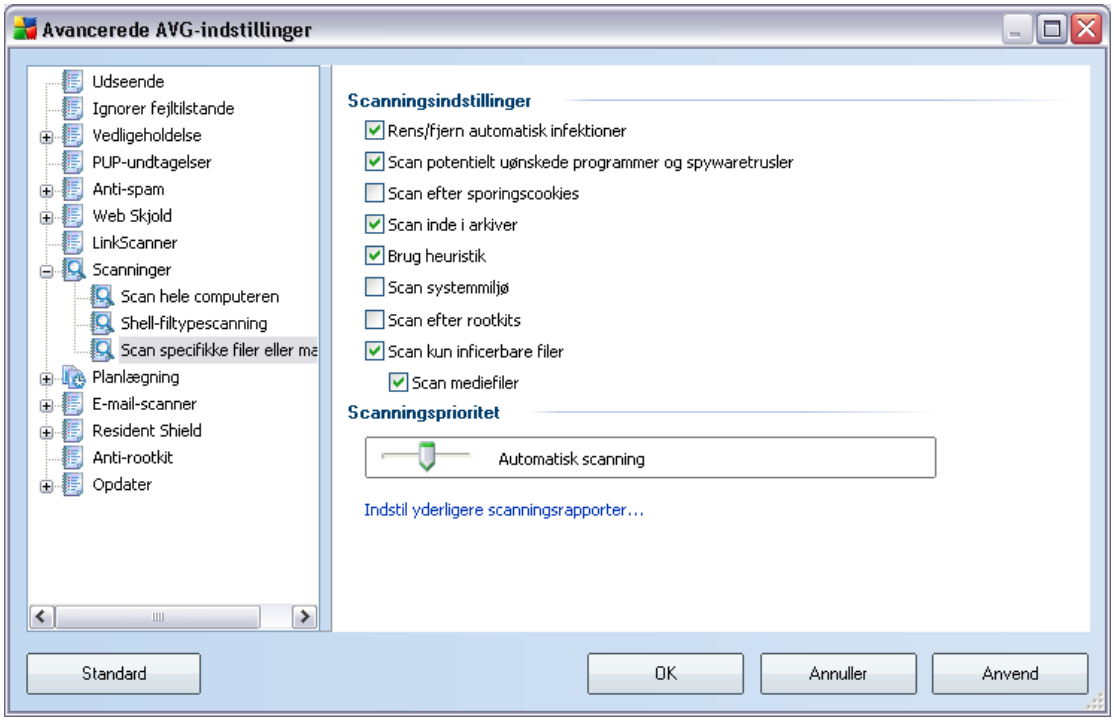
I lighed med det tidligere element ***Scan hele computeren*** tilbyder dette element med navnet ***Shelludvidelsesscanning*** også flere muligheder for at redigere den scanning, der er foruddefineret af softwareleverandøren. Denne gang vedrører konfigurationen scanning af specifikke objekter kørt direkte fra Windows stifinder (*shelludvidelse*), se kapitlet ***Scanning i Windows stifinder***:



Parameterlisten er magen til listerne for ***Scanning af hele computeren***. Standardindstillingerne er imidlertid forskellige: For ***Scanning af hele computeren*** er de fleste parametre valgt, hvorimod kun de relevante parametre er slået til for ***Shelludvidelsesscanning*** (***Scanning i Windows stifinder***).

12.7.3.Scan specifikke filer eller mapper

Redigeringsgrænsefladen for ***Scan specifikke filer eller mapper*** er magen til redigeringsdialogboksen for ***Scan hele computeren***. Alle konfigurationsindstillingerne er de samme, men standardindstillingerne er strengere for ***Scan hele computeren***:

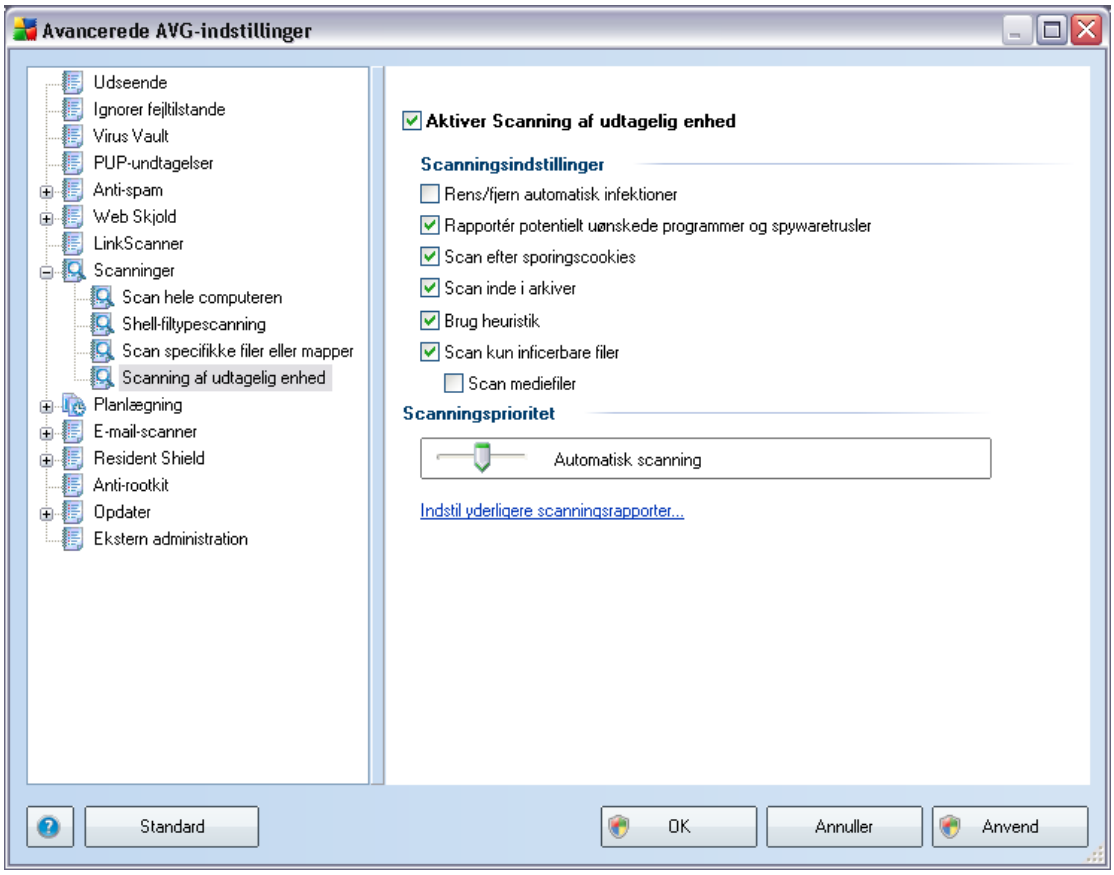


Alle parametre indstillet i denne konfigurationsdialog gælder kun for de områder, der er udvalgt til scanning med ***Scanning af specifikke filer eller mapper***! Hvis du markerer indstillingen ***Scan efter rootkits*** i denne konfigurationsdialog, udføres kun en hurtig rootkittest, dvs. kun rootkitscanning af udvalgte områder.

Bemærk: *Se kapitlet* ***AVG Avancerede indstillinger / Scanninger / Scan hele computeren*** *for en beskrivelse af specifikke parametre.*

12.7.4.Scanning af udtagelig enhed

Redigeringsgrænsefladen til ***Scanning af udtagelig enhed*** ligner også redigeringsdialogen til ***Scan hele computeren*** meget:



Scanning af udtagelig enhed køres automatisk, når du tilslutter en udtagelig enhed til din computer. Som standard er denne scanning slået fra. Det er imidlertid vigtigt at scanne udtagelige enheder for potentielle trusler, da de er en hyppig infektionskilde. For at have denne scanning gjort klar og kørt automatisk skal du markere valgmuligheden ***Aktiver Scanning af udtagelig enhed***

Bemærk: *Se kapitlet* ***AVG Avancerede indstillinger / Scanninger / Scan hele computeren*** *for en beskrivelse af specifikke parametre.*

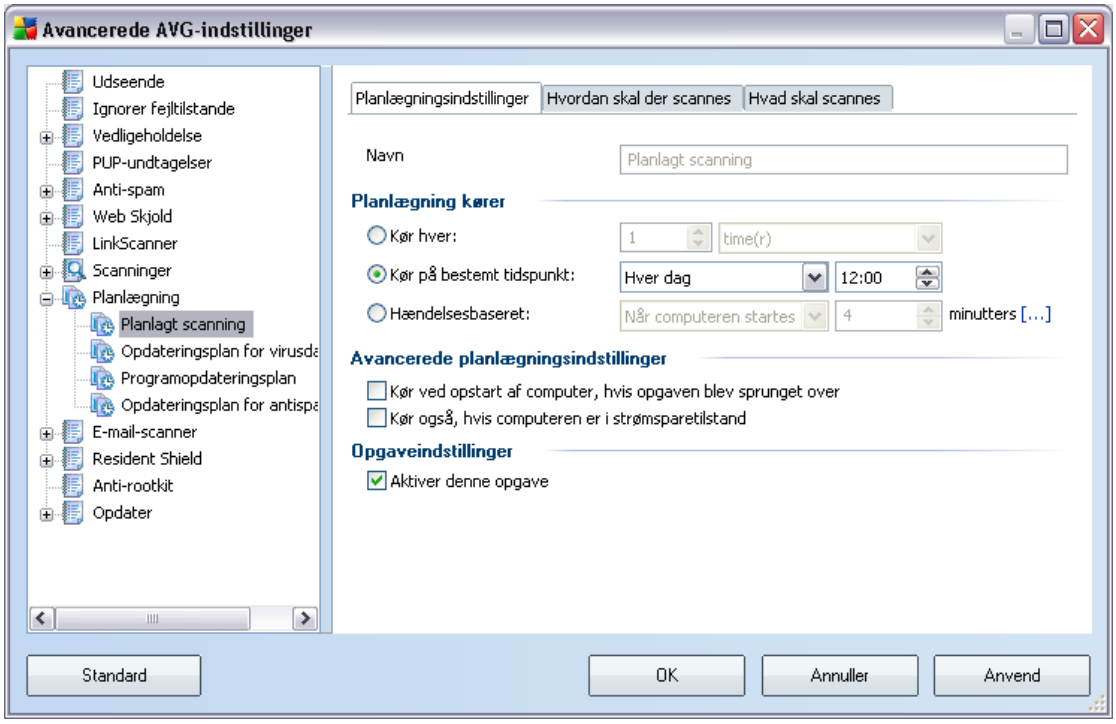
12.8.Planlægning

I sektionen ***Planlægning*** kan du redigere standardindstillingerne for:

- Scanningsplan for hele computeren
- Opdateringsplan for virusdatabase
- Programopdateringsplan
- Anti-spam-opdateringsplan

12.8.1.Planlagt scanning

Parametrene for den planlagte scanning kan redigeres (*eller en ny plan konfigureres*) på tre faner:



På fanen ***Planlægningsindstillinger*** kan du først markere/afmarkere elementet ***Aktiver denne opgave*** for helt enkelt at deaktivere den planlagte test midlertidigt, og slå den til igen, når behovet opstår.

Navngiv derefter den scanning, du skal til at oprette og planlægge. Indtast navnet i tekstfeltet ved elementet ***Navn***. Prøv at bruge korte, beskrivende og passende navne på scanninger for at gøre det nemmere at genkende scanningen senere.

Eksempel: *Det er ikke passende at kalde scanningen "Ny scanning" eller "Min scanning", da disse navne ikke angiver, hvad scanningen egentlig kontrollerer. Et eksempel på et godt, beskrivende navn kunne derimod være "Systemområdescanning" osv. Det er heller ikke nødvendigt at angive i scanningens navn, om det er en scanning af hele computeren eller blot en scanning af udvalgte filer eller mapper - dine egne scanninger vil altid være en specifik version af scanning af udvalgte filer eller mapper.*

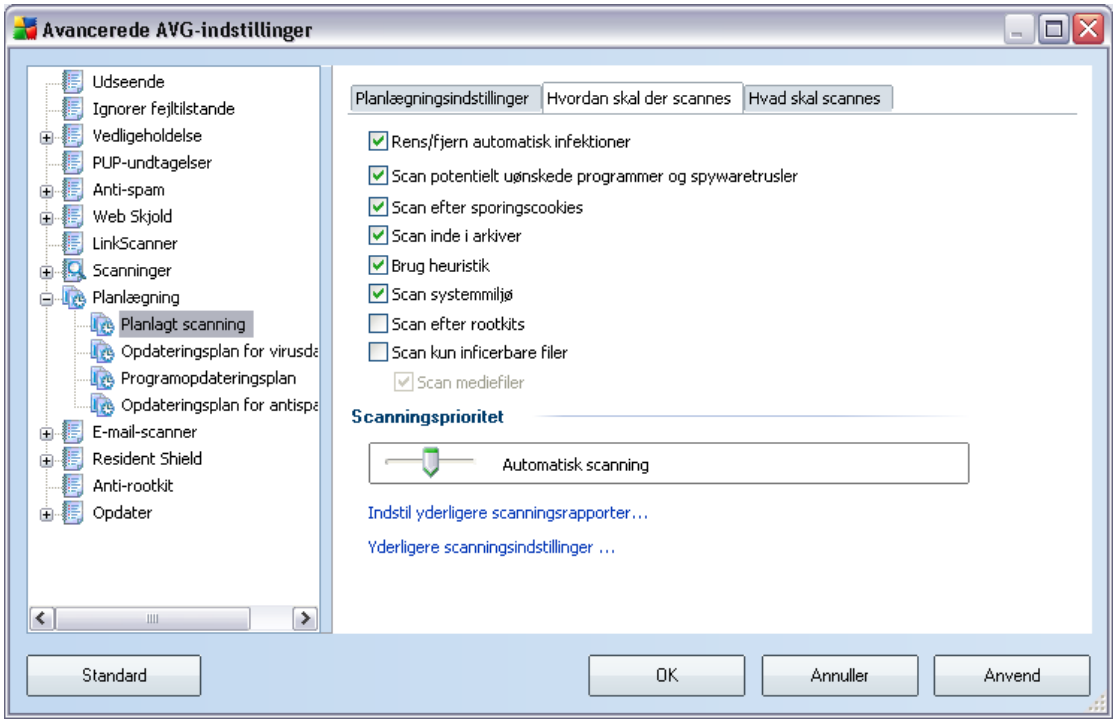
I denne dialog kan du yderligere definere følgende parametre for scanningen:

- ***Planlæg kørsel*** - angiv tidsintervallet for kørsel af den nye planlagte scanning. Timingen kan enten defineres med gentaget kørsel af scanningen efter et vist tidsrum (***Kør hver ...***) eller ved at definere en nøjagtig dato og klokkeslæt (***Kør på specifikt klokkeslæt ...***), eller muligvis ved at definere en hændelse, der knyttes til kørsel af scanningen (***Hændelsesbaseret ved opstart af computeren***).

- ***Avancerede planlægningsindstillinger*** - i denne sektion kan du definere, hvilke betingelser scanningen skal/ikke skal køres under, hvis computeren er i strømsparetilstand eller helt slukket.

Når den planlagte scanning køres på det tidspunkt, du har angivet, bliver du informeret om det via et popup-vindue, der åbnes over AVG systembakkeikonet:

Der vises nu et nyt AVG systembakkeikon (*i fuld farve med en hvid pil - se billede ovenfor*), der informerer om, at der køres en planlagt scanning. Højreklik på det AVG-ikonet for en kørende scanning for at åbne en kontekstmenu, hvor du kan vælge at afbryde den kørende scanning midlertidigt eller stoppe den helt:



På fanen ***Hvordan der skal scannes*** findes en liste over scanningsparametre, der valgfrit kan slås til/fra. Som standard er de fleste parametre slået til, og funktionaliteten anvendes under scanningen. Med mindre du har en god grund til at ændre disse indstillinger, anbefaler vi at bevare den forudindstillede konfiguration:

- ***Helbred/fjern infektion automatisk*** - (*slået til som standard*): hvis der identificeres en virus under scanningen, kan den helbredes automatisk, hvis der er en kur tilgængelig. Hvis den inficerede fil ikke kan helbredes automatisk, eller hvis du beslutter at slå denne mulighed fra, modtager du information, når en virus detekteres, og skal beslutte hvad der skal gøres ved den detekterede infektion. Den anbefalede handling er at fjerne den inficerede fil til Virus Vault.

- ***Scan potentielt uønskede programmer*** - (*slået til som standard*): denne parameter kontrollerer Anti-virus-funktionaliteten, der tillader detektering af potentielt uønskede programmer (*eksekverbare filer, der kan køre som spyware eller adware*), og disse kan derefter blokeres eller fjernes.

- ***Scan efter cookies*** - (*slået til som standard*): denne parameter i Anti-Spyware-komponenten definerer, at cookies skal detekteres under scanningen

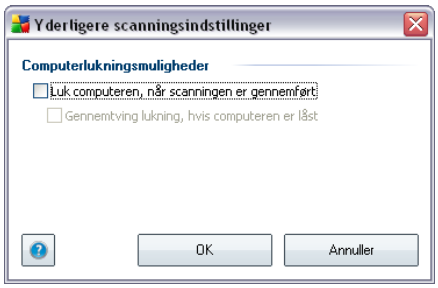
. (*HTTP-cookies anvendes til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på webstedet eller indhold i deres elektroniske indkøbsvogne*)

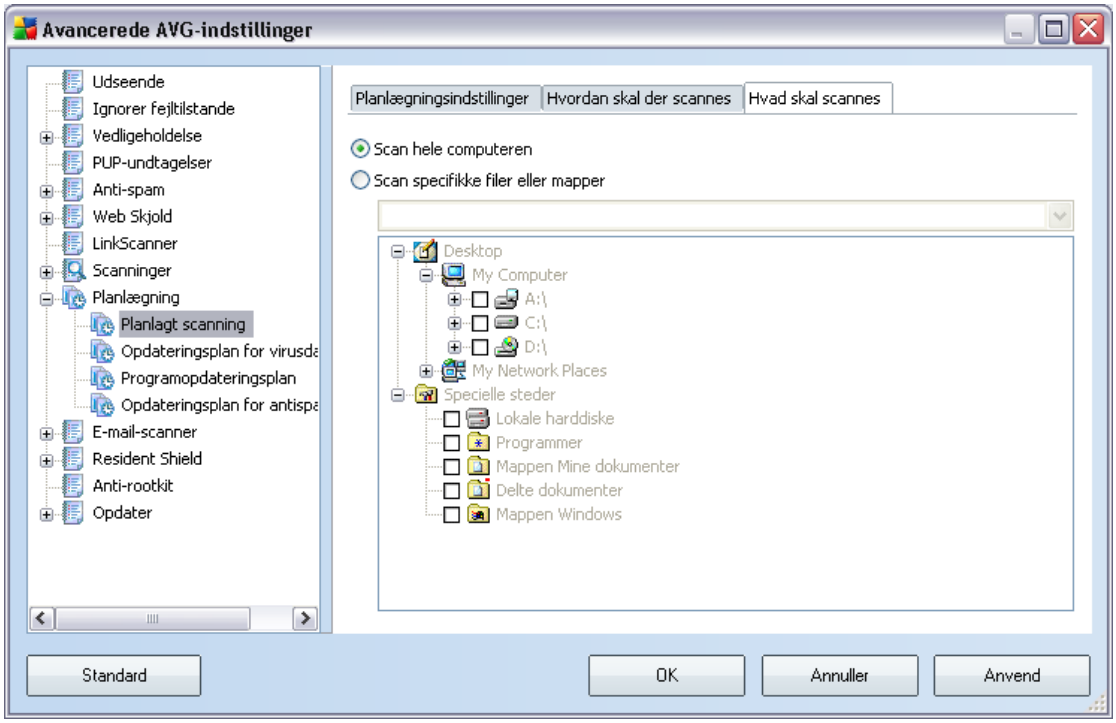
- ***Scan inde i arkiver*** - (*slået til som standard*): denne parameter definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i et arkiv, f.eks. ZIP, RAR, ...
- ***Brug heuristik*** - (*slået til som standard*): heuristisk analyse (*dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø*) er en af metoderne, der anvendes til detektering af virus under scanningen.
- ***Scan systemmiljø*** - (*slået til som standard*): scanningen kontrollerer også computerens systemområder.
- ***Scan efter rootkits*** - marker dette punkt, hvis du vil inkludere rootkit-detektering i scanningen af hele computeren. Rootkit-detektering er også tilgængelig individuelt i ***Anti-rootkit***-komponenten;
- ***Scan kun inficerbare filer*** - (*slået fra som standard*): med denne valgmulighed slået til bliver scanningen ikke udført på filer, der ikke kan inficeres. Det kan for eksempel være visse almindelige tekstfiler og andre ikkeeksekverbare filer.

I sektionen ***Scanningsprioritet*** kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne indstilling sat til middelniveauet af automatisk ressourceforbrug. Hvis du vil have scanningen til at køre hurtigere, tager det kortere tid, men forbruget af systemressourcer øges markant under scanningen, og gør de andre aktiviteter på pc'en langsommere (*denne indstilling kan anvendes, når computeren er tændt, men der i øjeblikket ikke er nogen, der arbejder med den*). På den anden side kan du reducere forbruget af systemressourcer ved at forlænge scanningens varighed.

Klik på linket ***Indstil yderligere scanningsrapporter ...*** for at åbne det selvstændige dialogvindue ***Scanningsrapporter***, hvor du kan markere adskillige punkter for at definere, hvilke scanningsfund, der skal rapporteres:

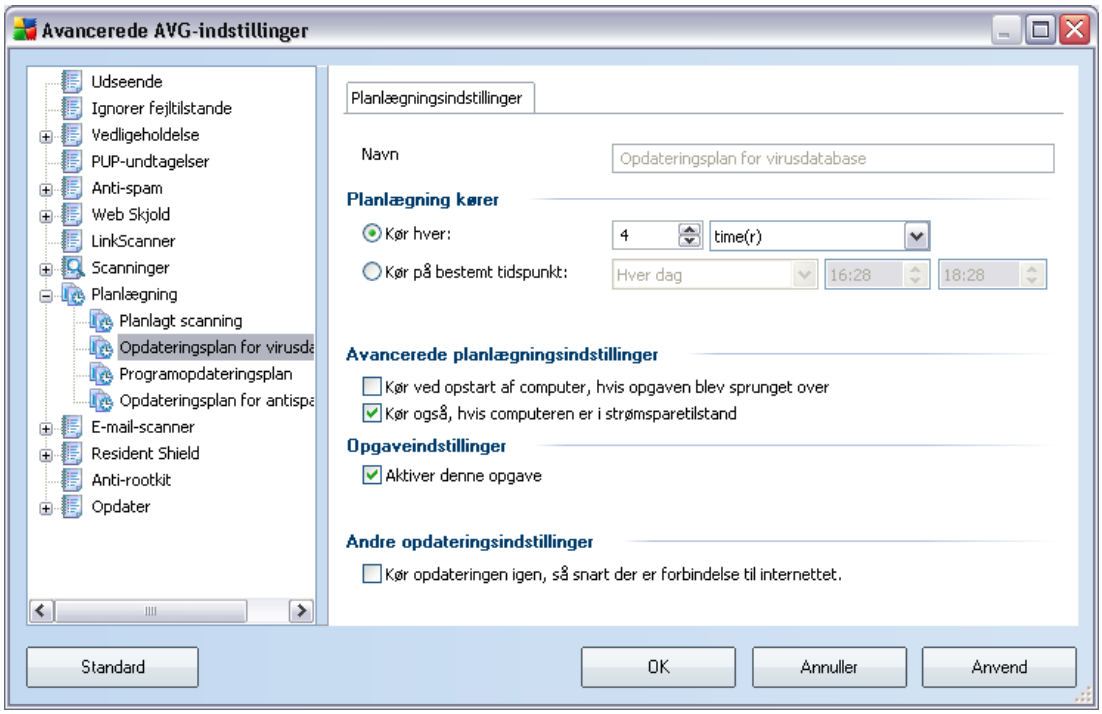
Klik på ***Yderligere scanningsindstillinger...*** for at åbne en ny ***Computerlukningsmuligheder***-dialog, hvor du kan beslutte, om computeren skal lukkes automatisk, når den igangværende scanning er færdig. Når denne indstilling er bekræftet (***Luk computeren, når scanningen er gennemført***), aktiveres en ny indstilling, som gør det muligt at lukke computeren, selvom den i øjeblikket er låst (***Gennemtving lukning, hvis computeren er låst***).





På fanen ***Hvad skal scannes*** kan du definere, om du vil planlægge scanning af hele computeren eller scanning af specifikke filer eller mapper. Hvis du vælger scanning af specifikke filer eller mapper, aktiveres træstrukturen nederst i denne dialogboks, og du kan angive mapper, der skal scannes.

12.8.2.Opdateringsplan for virusdatabase



På fanen ***Planlægningsindstillinger*** kan du først markere/afmarkere elementet ***Aktiver denne opgave*** for helt enkelt at deaktivere den planlagte virusdatabaseopdatering midlertidigt, og slå den til igen, når behovet opstår.

Den grundlæggende opdateringsplanlægning for virusdatabasen er beskrevet under ***Opdateringsadministrator***-komponenten. I denne dialog kan du konfigurere nogle detaljerede parametre for opdateringsplanlægningen for virusdatabasen:

Navngiv derefter den virusdatabaseopdateringsplan, du skal til at oprette. Indtast navnet i tekstfeltet ved elementet ***Navn***. Prøv at bruge korte, beskrivende og passende navne på opdateringsplaner for at gøre det nemmere at genkende planen senere.

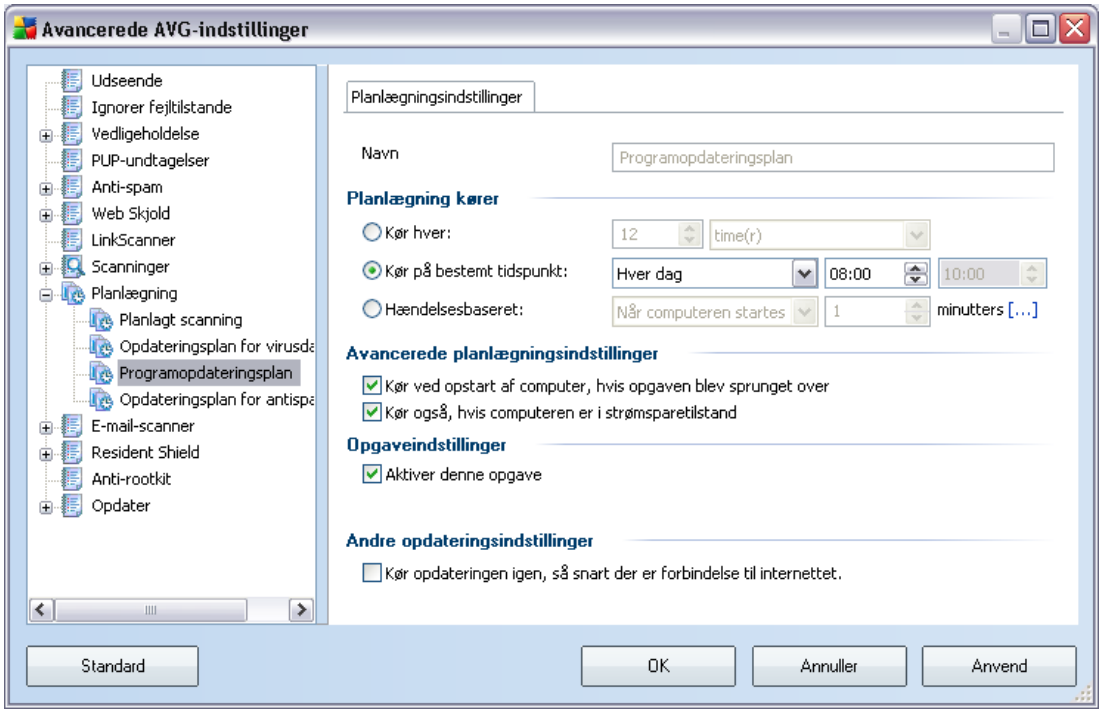
- ***Planlægningskørsel*** - angiv tidsintervaller for kørsel af den planlagte virusdatabase-opdatering. Timingen kan enten defineres med gentaget kørsel af opdateringen efter et vist tidsrum (***Kør hver ...***) eller ved at definere en nøjagtig dato og klokkeslæt (***Kør på specifikt klokkeslæt ...***), eller muligvis ved at definere en hændelse, der knyttes til kørsel af opdateringen (***Hændelsesbaseret ved opstart af computeren***).

- ***Avancerede planlægningsindstillinger*** - i denne sektion kan du definere, hvilke betingelser virusdatabase-opdateringen skal/ikke skal køres under, hvis computeren er i strømsparetilstand eller helt slukket.

- ***Andre opdateringsindstillinger*** - marker denne indstilling for at sørge for, at opdateringsprocessen, hvis internetforbindelsen bliver afbrudt og opdateringen mislykkes, bliver kørt igen, umiddelbart efter forbindelsen til internettet er genoprettet.

Når den planlagte scanning er kørt på det angivne tidspunkt, bliver du informeret om det med et popup-vindue, der åbnes over AVG-systembakkeikonet (*forudsat at du har bevaret standardkonfigurationen i dialogen **Avancerede indstillinger/Udseende***).

12.8.3.Programopdateringsplan



På fanen ***Planlægningsindstillinger*** kan du først markere/afmarkere elementet ***Aktiver denne opgave*** for helt enkelt at deaktivere den planlagte programopdatering midlertidigt, og slå den til igen, når behovet opstår.

Navngiv derefter den programopdateringsplan, du skal til at oprette. Indtast navnet i tekstfeltet ved elementet ***Navn***. Prøv at bruge korte, beskrivende og passende navne på opdateringsplaner for at gøre det nemmere at genkende planen senere.

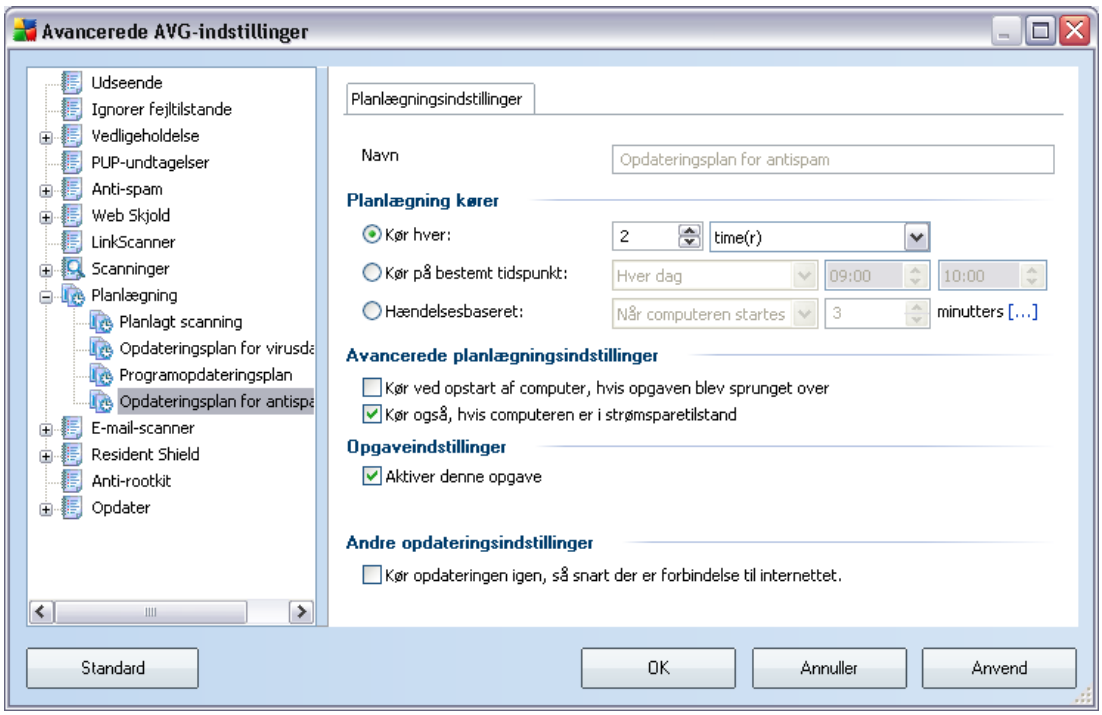
- ***Planlæg kørsel*** - angiv tidsintervallet for kørsel af den nye planlagte programopdatering. Timingen kan enten defineres med gentaget kørsel af opdateringen efter et vist tidsrum (***Kør hver ...***) eller ved at definere en nøjagtig dato og klokkeslæt (***Kør på specifikt klokkeslæt ...***), eller muligvis ved at definere en hændelse, der knyttes til kørsel af opdateringen (***Hændelsesbaseret ved opstart af computeren***).

- ***Avancerede planlægningsindstillinger*** - i denne sektion kan du definere, hvilke betingelser programopdateringen skal/ikke skal køres under, hvis computeren er i strømsparetilstand eller helt slukket.

- ***Andre opdateringsindstillinger*** - marker denne indstilling for at sørge for, at opdateringsprocessen, hvis internetforbindelsen bliver afbrudt og opdateringen mislykkes, bliver kørt igen, umiddelbart efter forbindelsen til internettet er genoprettet.

Når den planlagte scanning er kørt på det angivne tidspunkt, bliver du informeret om det med et popup-vindue, der åbnes over AVG-systembakkeikonet (*forudsat at du har bevaret standardkonfigurationen i dialogen **Avancerede indstillinger/Udseende***).

12.8.4.Anti-spam opdateringsplan



På fanen ***Planlægningsindstillinger*** kan du først markere/afmarkere elementet ***Aktiver denne opgave*** for helt enkelt at deaktivere den planlagte ***Anti-spam-*** opdatering midlertidigt, og slå den til igen, når behovet opstår.

Grundlæggende ***Anti-spam-***opdateringsplanlægning er beskrevet i ***Opdateringsstyring***-komponenten. I denne dialog kan du konfigurere nogle detaljerede parametre for opdateringsplanlægningen:

Navngiv derefter den ***Anti-spam***-opdateringsplan, du skal til at oprette. Indtast navnet i tekstfeltet ved elementet ***Navn***. Prøv at bruge korte, beskrivende og passende navne på opdateringsplaner for at gøre det nemmere at genkende planen senere.

- ***Planlægningskørsel*** - angiv tidsintervaller for kørsel af den planlagte ***Anti-spam-***opdatering. Timingen kan enten defineres med gentaget kørsel af ***Anti-spam-***opdatering efter et vist tidsrum (***Kør hver...***) eller ved at definere en nøjagtig dato og klokkeslæt (***Kør på specifikt klokkeslæt...***), eller muligvis ved at definere en hændelse, der knyttes til kørsel af opdateringen (***Hændelsesbaseret ved opstart af computeren***).

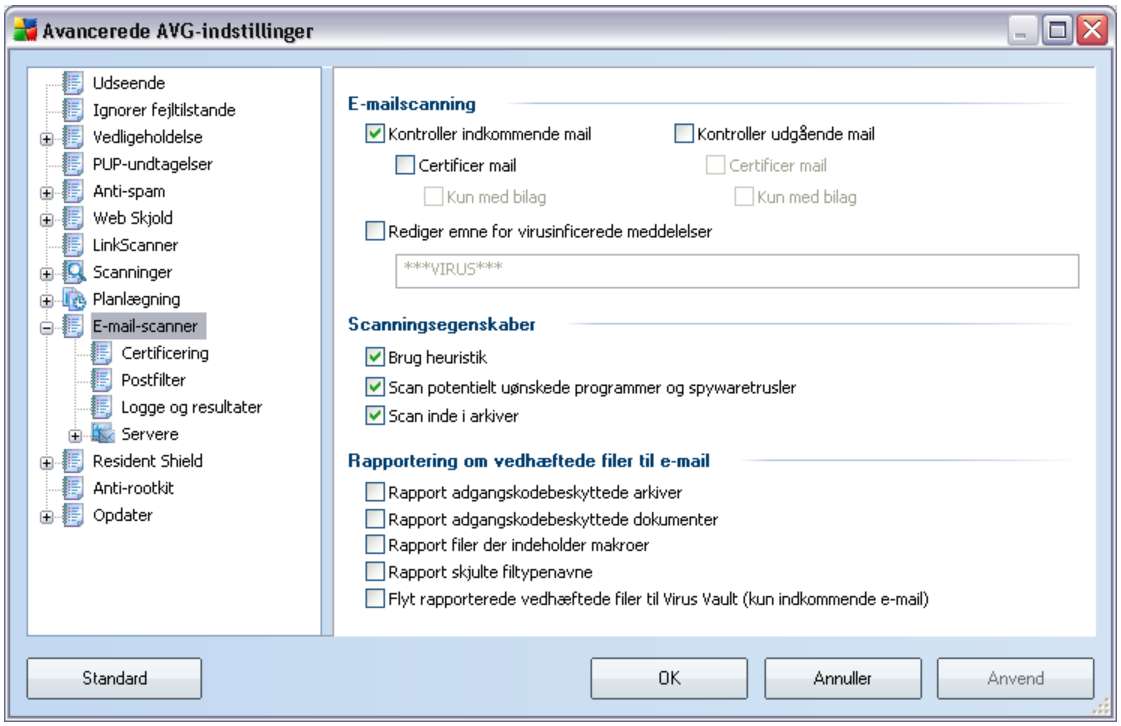
- ***Avancerede planlægningsindstillinger*** - i denne sektion kan du definere, hvilke betingelser ***Anti-spam-***opdateringen skal/ikke skal køres under, hvis computeren er i strømsparetilstand eller helt slukket.

- ***Opgaveindstillinger*** - i denne sektion kan du afmarkere punktet ***Aktiver denne opgave*** for helt enkelt at deaktivere den planlagte ***Anti-spam-*** opdatering midlertidigt og aktivere den igen, når der er behov for det.

- ***Andre opdateringsindstillinger*** - marker denne indstilling for at sørge for, at ***Anti-spam-***opdateringen, hvis internetforbindelsen bliver afbrudt og opdateringen mislykkes, bliver kørt igen, umiddelbart efter forbindelsen til internettet er genoprettet.

Når den planlagte scanning er kørt på det angivne tidspunkt, bliver du informeret om det med et popup-vindue, der åbnes over AVG-systembakkeikonet (*forudsat at du har bevaret standardkonfigurationen i dialogen* ***Avancerede indstillinger/Udseende***).

12.9.E-mail-scanner



Dialogen ***E-mail scanner*** består af tre sektioner:

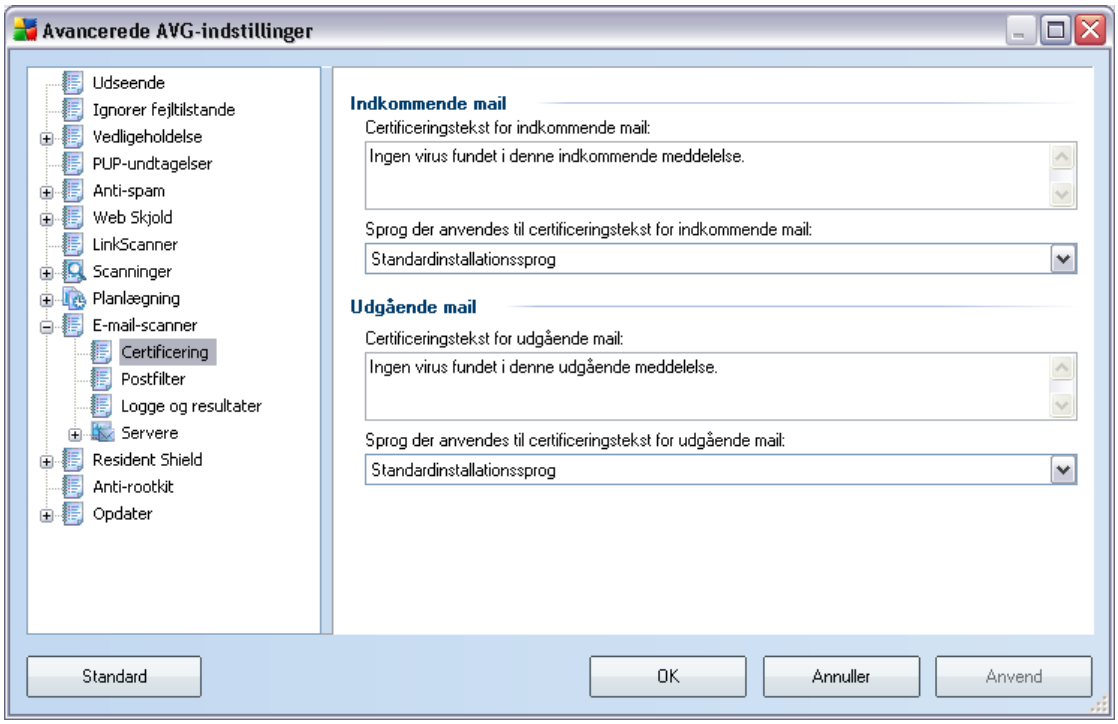
- ***E-mail-scanning*** - i denne sektion vælger du, om du vil scanne de indkommende/udgående e-mail-meddelelser, og om alle e-mail skal certificeres eller kun e-mail med vedhæftede filer (*e-mail virusfri-certificering understøttes ikke i HTML/RTF-format*). Her ud over kan du vælge, om AVG skal ændre emnelinjen i meddelelser, der indeholder potentielle vira. Marker afkrydsningsfeltet ***Rediger emnelinjen i virusinficerede meddelelser*** og rediger teksten tilsvarende (*standardværdien er ***VIRUS****).

- ***Scanningsegenskaber*** - angiv om metoden heuristisk analyse skal anvendes under scanningen (***Brug heuristik***), om du vil kontrollere for potentielt uønskede programmer (***Scan potentielt uønskede programmer***), og om arkiver også skal scannes (***Scan inde i arkiver***).

- ***Rapportering af vedhæftede filer***- angiv om du vil have information via e-mail om adgangskodebeskyttede arkiver, adgangskodebeskyttede dokumenter, filer der indeholder makroer og/eller filer med skjulte filtypenavne, der detekteres som vedhæftet fil til den scannede e-mail-

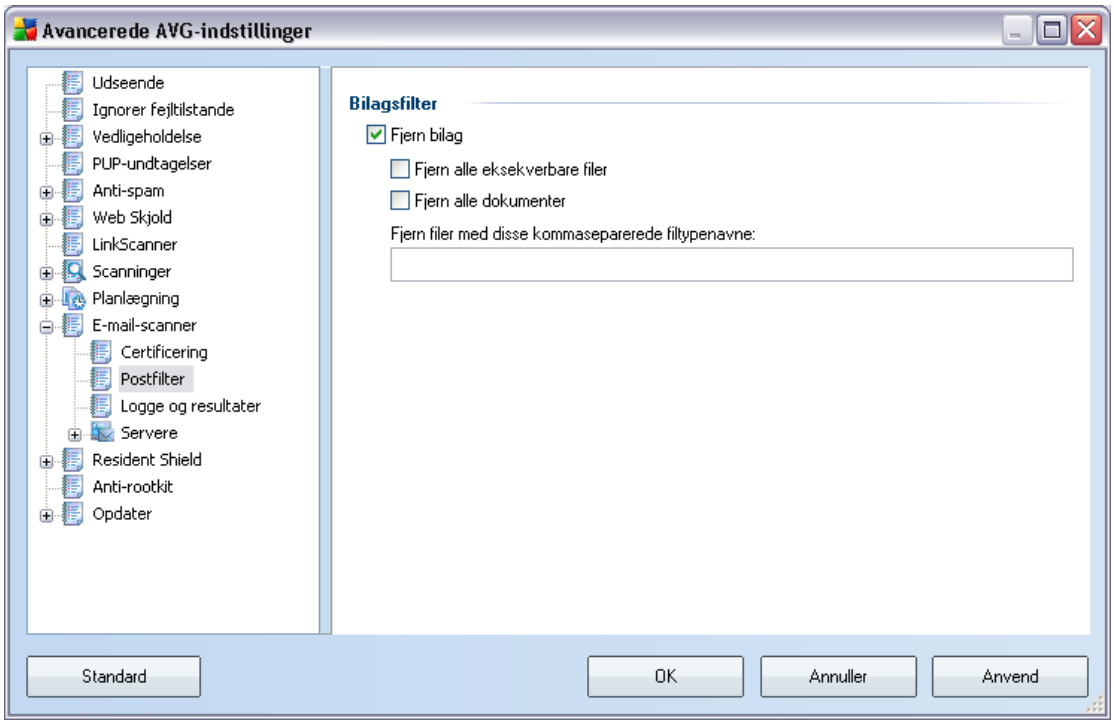
meddelelse. Hvis der identificeres en sådan meddelelse under scanningen, skal du definere, om det detekterede inficerbare objekt skal flyttes til ***Virus Vault***.

12.9.1.Certificering



I dialogen ***Certificering*** kan du angive nøjagtig hvilken tekst, som certificeringen skal indeholde, og på hvilket sprog. Dette bør angives separat for ***Indkommende e-mail*** og ***Udgående e-mail***.

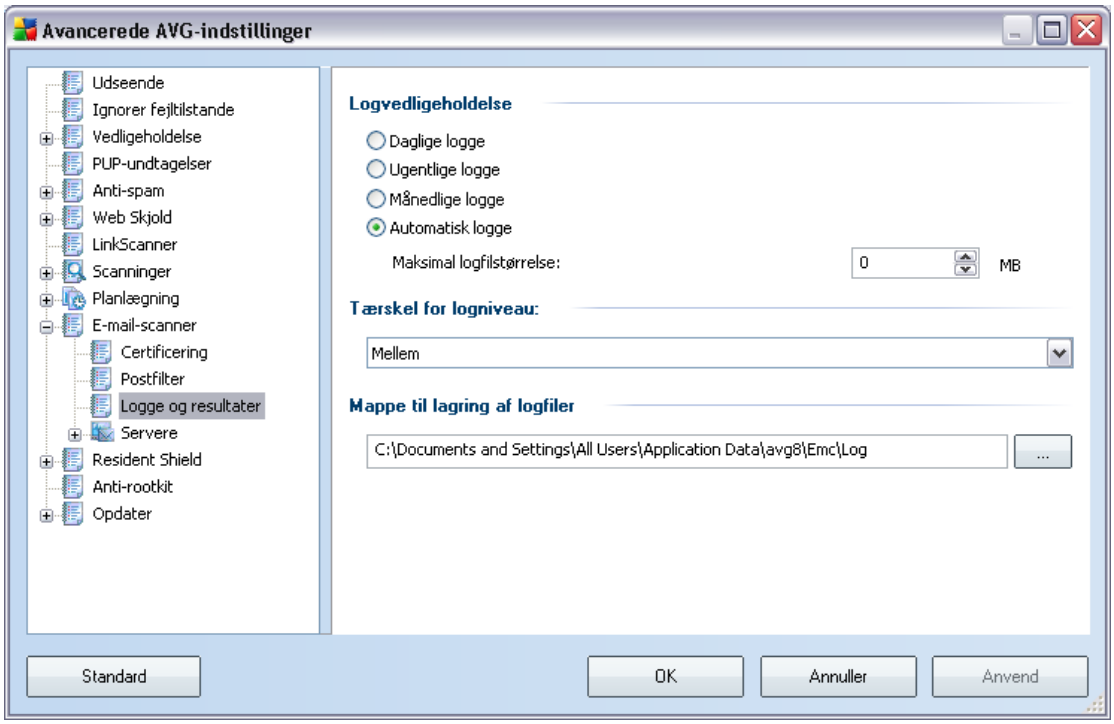
12.9.2.Postfilter



I dialogboksen ***Filter for vedhæftede filer*** kan du indstille parametre for scanning af vedhæftede filer i e-mail-meddelelser . Som standard er indstillingen ***Fjern vedhæftede filer*** slået fra. Hvis du beslutter at aktivere den, bliver alle vedhæftede filer i e-mail, der detekteres som inficerede eller potentielt farlige, fjernet automatisk. Hvis du vil definere specifikke typer at vedhæftede filer, der skal fjernes, skal du vælge den pågældende indstilling:

- ***Fjern alle eksekverbare filer*** - alle *.exe-filer bliver slettet
- ***Fjern alle dokumenter*** - alle *.doc-filer bliver slettet
- ***Fjern filer med disse filtypenavne*** - fjerne alle filer med de definerede filtypenavne

12.9.3.Logge og resultater

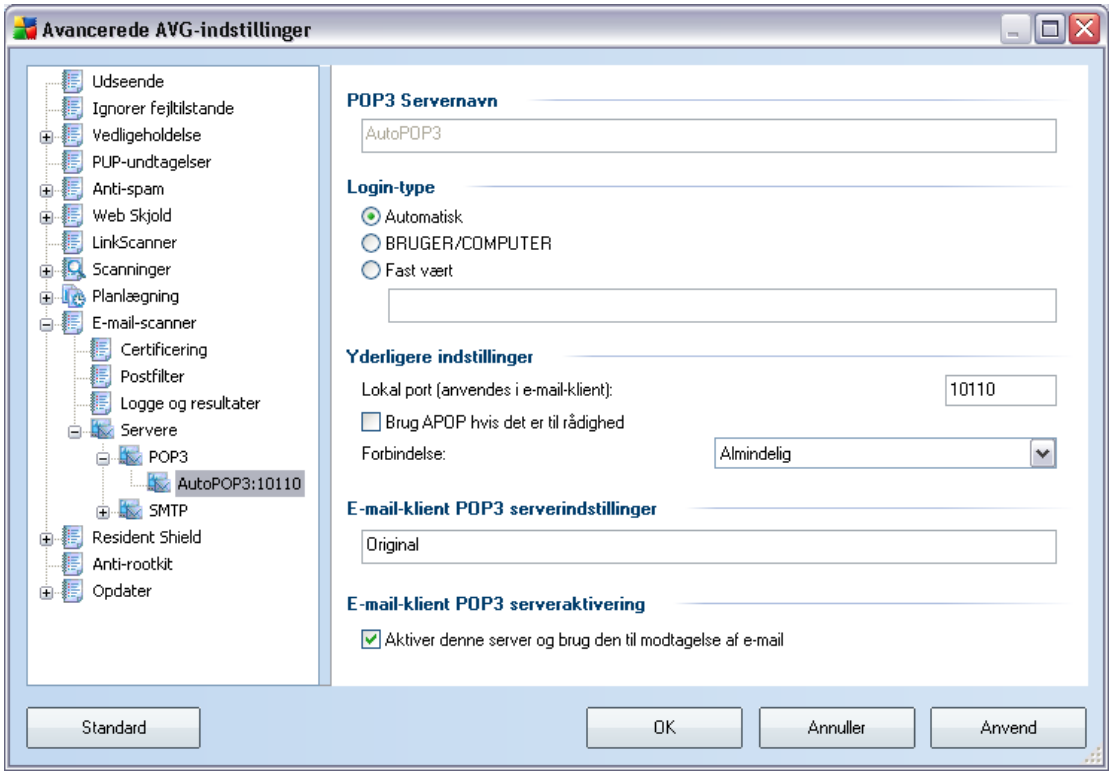


I dialogen, der åbnes via navigationselementet ***Logge og resultater***, kan du angive parametre for vedligeholdelse af e-mail-scanningsresultater. Dialogboksen er opdelt i flere sektioner:

- ***Logvedligeholdelse*** - definer, om du vil logge oplysninger om e-mail-scanning dagligt, ugentligt, månedligt, ... og angiv også logfilens maksimale størrelse (*i MB*)
- ***Logniveautærskel*** - middelniveauet er indstillet som standard - du kan vælge et lavere niveau (*logger elementrære forbindelsesoplysninger*) eller et højere niveau (*logger al trafik*)
- ***Mappe anvendt til at gemme logfiler*** - definer, hvor logfilen skal placeres

12.9.4.Servere

I sektionen ***Servere*** kan du redigere parametre for ***E-mail-scanner***-komponentservere, eller sætte en ny server op ved hjælp af knappen ***Tilføj ny server***.



I denne dialogboks (åbnes via ***Servere / POP3***) kan du konfigurere en ny ***E-mail scanner***-server vha. POP3-protokollen for indkommende e-mail:

- ***POP3-servernavn*** - indtast navnet på serveren eller behold AutoPOP3-standardnavnet
- ***Logintype*** - definerer metoden til at bestemme mailserveren, der anvendes til indkommende e-mail:
    - Automatisk - Login udføres automatisk i henhold til indstillingerne i e-mail-klienten.
    - BRUGER/COMPUTER - den simpleste og hyppigst anvendte metode til at bestemme destinationsmailserveren er proxymetoden. For at anvende denne metode skal du angive navn og adresse (eller også porten) som del af loinbrugernavnet for den pågældende mailserver, adskilt med tegnet /. For kontoen user1 på serveren pop.acme.com og port 8200, skal du for eksempel bruge user1/pop.acme.com:8200 som loginnavn.

- Fast vært - I dette tilfælde anvender programmet altid den server, der er angivet her. Angiv adressen eller navnet på din mailserver. Loginnavnet forbliver uændret. Som navn kan du anvende et domænenavn (for eksempel pop.acme.com) eller en IP-adresse (for eksempel 123.45.67.89). Hvis mailserveren ikke benytter en standardport, kan du angive denne port efter servernavnet med et kolon som separator (for eksempel pop.acme.com:8200). Standardporten for POP3-kommunikation er 110.

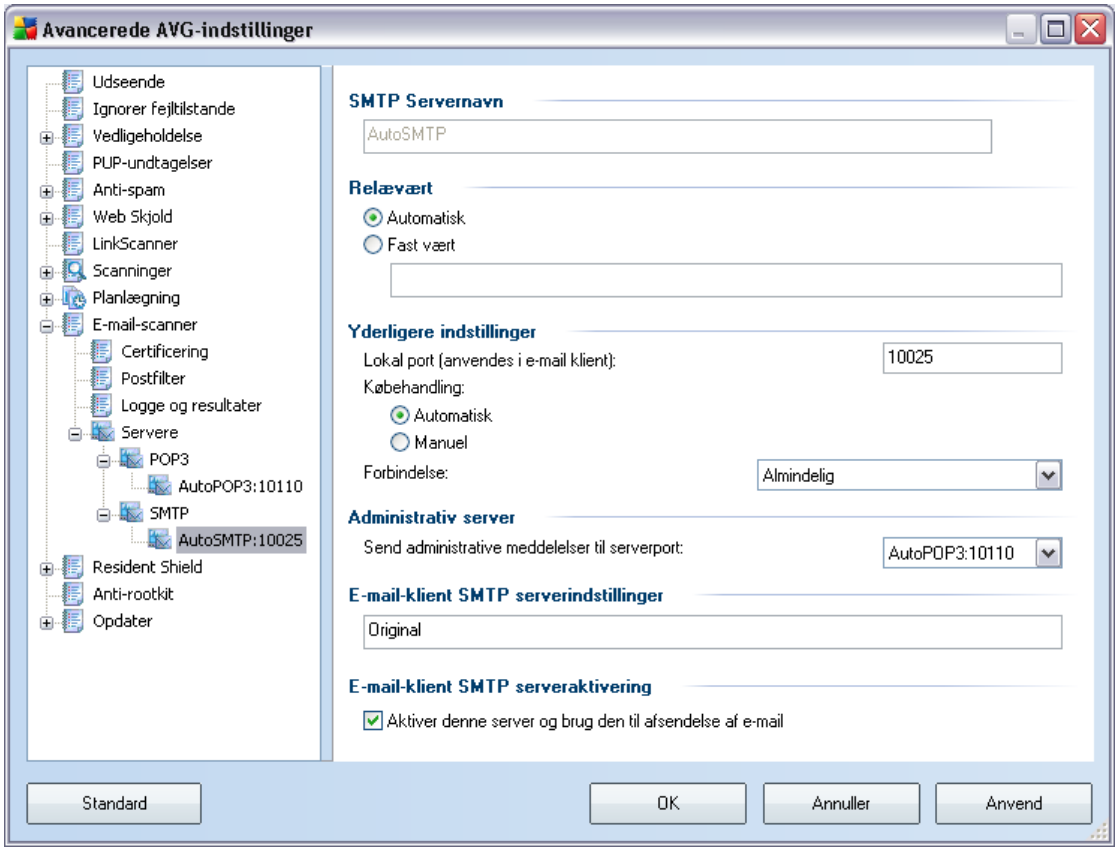
- ***Yderligere indstillinger*** - angiver mere detaljerede parametre:

  - Lokal port - angiver den port, hvor kommunikation fra din mailapplikation forventes. Du skal derefter angive denne port som port for POP3-kommunikation i dit e-mail-program.

  - Anvend APOP, hvis det er muligt - denne mulighed giver et sikrere login på mailserveren. Det sikrer, at ***E-mail scanner*** bruger en alternativ metode til at videresende brugerkontoens adgangskode til login ved ikke at sende adgangskoden til serveren i et åbent format men i et krypteret, ved brug af en variable kæde, der modtages fra serveren. Denne funktion er naturligvis kun tilgængelig, hvis destinationsmailserveren understøtter den.

  - Forbindelse - i rullemenuen kan du angive, hvilken forbindelsestype, der skal bruges (almindelig/SSL/SSL standard). Hvis du vælger SSL-forbindelse, bliver dataene sendt krypteret, uden risiko for at blive sporet eller overvåget af tredjepart. Denne funktion er også kun tilgængelig, hvis destinationsmailserveren understøtter den.

- ***Aktivering af e-mail-klientens POP3-server*** - indeholder kortfattede oplysninger om de konfigurationsindstillinger, der er nødvendige for at konfigurere din e-mail-klient korrekt (så ***E-mail scanner*** kontrollerer al indkommende e-mail). Dette er en sammenfatning, der er baseret på de tilsvarende parametre, der er specificeret i denne og andre tilhørende dialoger.



I denne dialogboks (åbnes via ***Servere / SMTP***) kan du konfigurere en ny ***E-mail scanner***-server vha. SMTP-protokollen for udgående e-mail:

- ***SMTP-servernavn*** - indtast navnet på serveren eller behold AutoSMTP-standardnavnet
- ***Relævært*** - definerer metoden til at bestemme mailserveren, der anvendes til udgående e-mail:
    - Automatisk - login udføres automatisk i henhold til indstillingerne i din e-mail-klient
    - Fast vært - i dette tilfælde anvender programmet altid den server, der er angivet her. Angiv adressen eller navnet på din mailserver. Du kan bruge et domænenavn (for eksempel smtp.acme.com) eller en IP-adresse (for eksempel 123.45.67.89) som navn. Hvis mailserveren ikke

benytter en standardport, kan du indtaste denne port efter servernavnet med et kolon som separator (for eksempel pop.acme.com:8200). Standardporten for SMTP-kommunikation er 25.

- ***Yderligere indstillinger*** - angiver mere detaljerede parametre:

o Lokal port - angiver den port, hvor kommunikation fra din mailapplikation forventes. Du skal derefter angive denne port som port for SMTP-kommunikation i dit e-mail-program.

o Køhåndtering - bestemmer ***E-mail scanners*** opførsel ved håndtering af kravene for at sende e-mail-meddelelser:

➢ Automatisk - den udgående e-mail afleveres (sendes) øjeblikkeligt til destinationsmailserveren

➢ Manuel - meddelelsen sættes ind i køen af udgående meddelelser og sendes senere

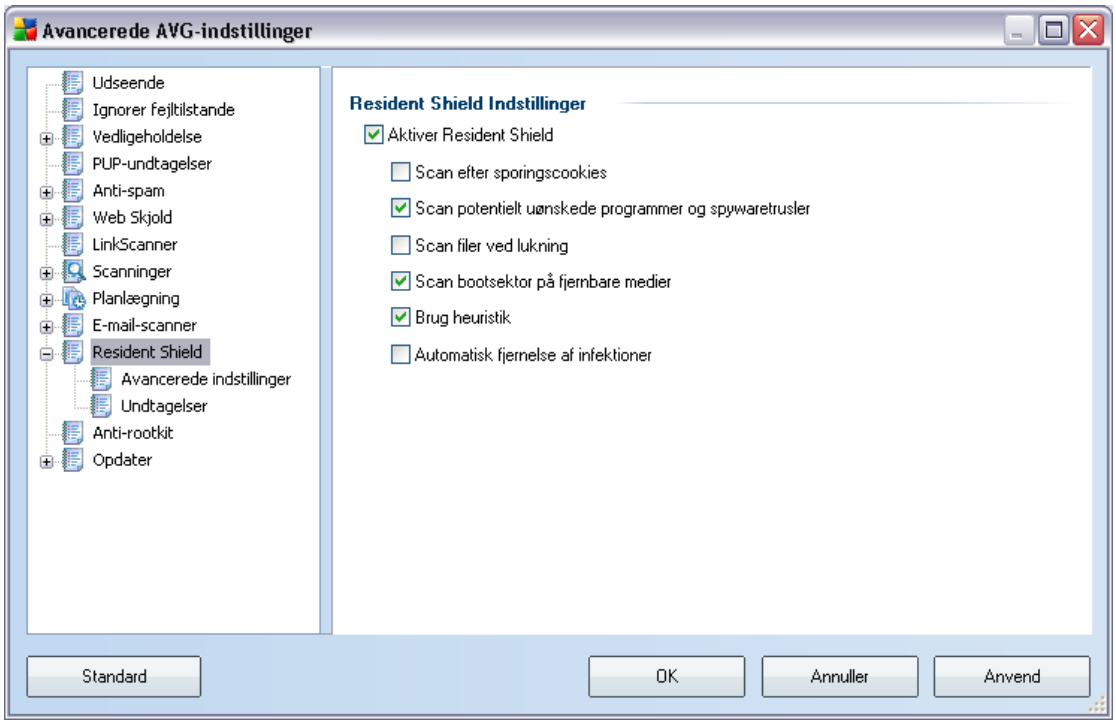
o Forbindelse - i denne rullemenu kan du angive, hvilken forbindelsestype, der skal bruges (almindelig/SSL/SSL standard). Hvis du vælger SSL-forbindelse, bliver dataene sendt krypteret, uden risiko for at blive sporet eller overvåget af tredjepart. Denne funktion er kun tilgængelig, hvis destinationsmailserveren understøtter den.

- ***Administrativ server*** - viser nummeret på den serverport, der anvendes til returlevering af administrative rapporter. Disse meddelelser genereres for eksempel, når destinationsmailserveren afviser den udgående meddelelse, eller hvis denne mailserver ikke er tilgængelig.

- ***Indstillinger til e-mail-klients SMTP-server*** - indeholder oplysninger om, hvordan e-mail-klienten konfigureres, så udgående e-mail-meddelelser kontrolleres ved hjælp af den aktuelle modificerede server til kontrol af udgående e-mail. Dette er en sammenfatning, der er baseret på de tilsvarende parametre, der er specificeret i denne og andre tilhørende dialoger.

12.1. Resident Shield

Resident Shield-komponenten udfører dynamisk beskyttelse af filer og mapper imod vira, spyware og anden malware.



I dialogboksen ***Resident Shield-indstillinger*** kan du aktivere eller deaktivere beskyttelsen fra ***Resident Shield*** fuldstændig ved at markere/afmarkere punktet ***Aktiver Resident Shield*** (*denne indstilling er slået til som standard*). Desuden kan du væge hvilke funktioner i ***Resident Shield***, der skal være aktiveret:

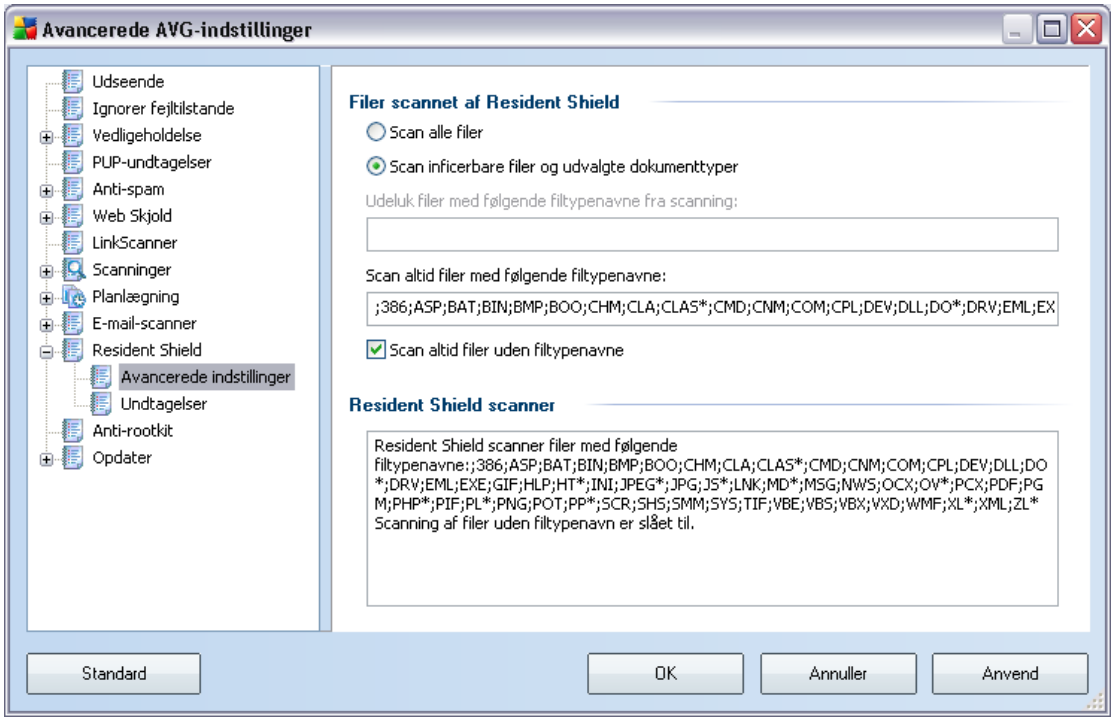
- ***Scan cookies*** - denne parameter definerer, at cookies skal detekteres under scanningen. (*HTTP-cookies bruges til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på webstedet eller indholdet i deres elektroniske indkøbsvogne*)
- ***Scan potentielt uønskede programmer*** - (*slået til som standard*) scanning efter potentielt uønskede programmer (*eksekverbare applikationer, der kan opføre sig som forskellige typer af spyware eller adware*)
- ***Scan ved lukning af proces*** - scanning ved lukning sikrer, at AVG scanner aktive objekter (f.eks. applikationer, dokumenter mv.), når de åbnes, og når

de lukkes. Denne funktion hjælper dig med at beskytte din computer mod visse typer af sofistikerede vira.

- ***Scan bottsektor på flytbare medier*** - (*slået til som standard*)
- ***Brug heuristik*** - (*slået til som standard*) heuristisk analyse anvendes til detektering (*dynamisk emulering af det scannede objekts instruktioner i et virutelt computermiljø*)
- ***Autohelbredelse*** - detekterede infektioner bliver helbredt automatisk, hvis der er en kur til rådighed

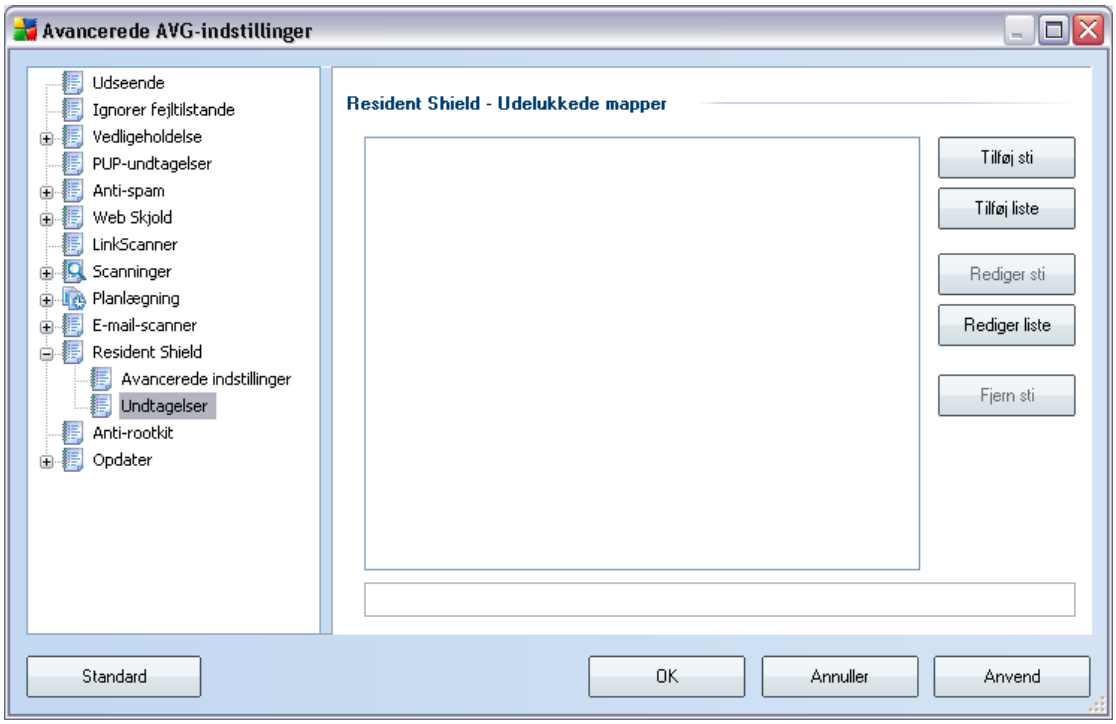
12.10.1. Avancerede indstillinger

I dialogen ***Filer scannet med Resident Shield*** er det muligt at konfigurere, hvilke filer, der bliver scannet (*med specifikke filtypenavne*):



Beslut, om du vil have scannet alle filer eller kun inficerbare filer - i så fald kan du yderligere angive en liste over filtypenavne for de filer, der ikke skal scannes, og en liste over filtypenavne for filer, der skal scannes under alle omstændigheder.

12.10. Undtagelser



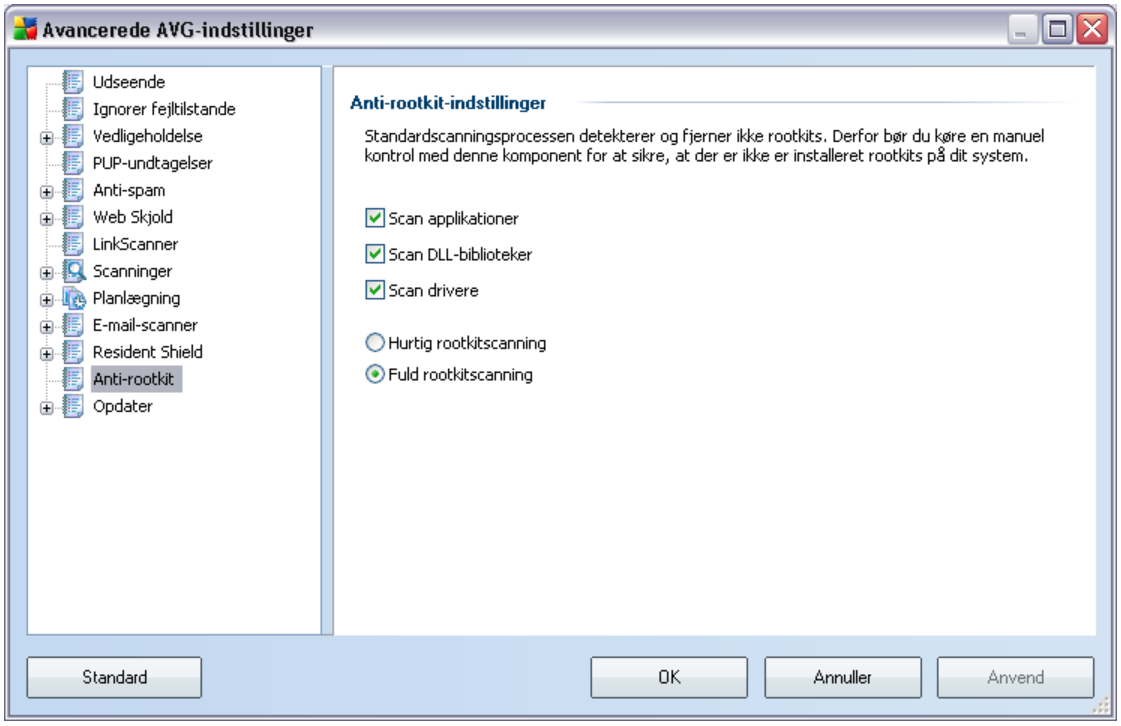
Dialogen ***Resident Shield - Biblioteksundtagelser*** giver mulighed for at definere mapper, der skal undtages fra ***Resident Shield***-scanningen. Hvis det ikke er nødvendigt, anbefales det ikke at udelukke nogen mapper! Hvis du belsutter at udelukke en mappe fra ***Resident Shield*** -scanning, bliver de nye indstillinger først taget i brug, efter computeren er genstartet!

Dialogboksen undeholder følgende betjeningsknapper:

- ***Tilføj sti*** - angiv mapper, der skal undtages fra scanningen ved at vælge dem én efter én i navigationstræet for den lokale disk
- ***Tilføj liste*** - giver mulighed for at indsætte en hel liste over mapper, der skal undtages fra ***Resident Shield***-scanningen
- ***Rediger sti*** - giver mulighed for at redigere den angivne sti til en valgt mappe
- ***Rediger liste*** - giver mulighed for at redigere mappelisten
- ***Fjern sti*** - giver mulighed for at fjerne stien til en valgt mappe på listen

12.11 Anti-rootkit

I denne dialog kan du redigere ***Anti-rootkit***-komponentens konfiguration:



Redigering af alle funktioner i ***Anti-rootkit***-komponenten, der findes i denne dialog, er også tilgængelige direkte fra ***Anti-rootkit-komponentens grænseflade***.

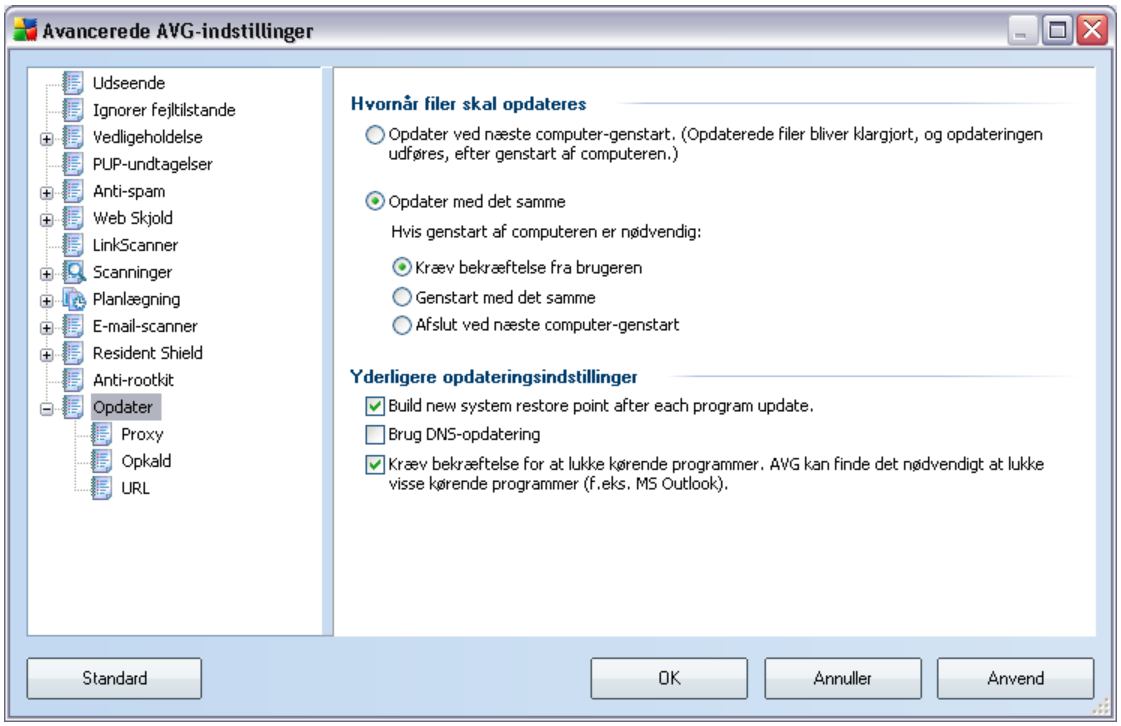
Marker de pågældende afkrydsningsfelter for at angive de objekter, der skal scannes:

- ***Scan applikationer***
- ***Scan DLL-biblioteker***
- ***Scan drivere***

Derudover kan du vælge rootkitscanningstilstanden:

- ***Hurtig rootkitscanning*** - scanner kun system-mappen (*normalt c:\Windows*)
- ***Fuld rootkitscanning*** - scanner alle tilgængelige drev, undtagen A: og B:

12.1. Opdatering



Navigationselementet ***Opdater*** åbner en ny dialogboks, hvor du kan angive generelle parametre vedrørende AVG-opdatering:

Hvornår filer skal opdateres

I denne sektion kan du vælge mellem to alternativer: opdatering kan planlægges til næste genstart af pc'en, eller du kan køre opdateringen med det samme. Som standard er opdatering med det samme valgt, for på den måde kan AVG sikre det maksimale sikkerhedsniveau. Det anbefales kun at planlægge en opdatering til næste genstart af pc'en, hvis du er sikker på, at computeren bliver genstartet regelmæssigt, mindst en gang dagligt.

Hvis du beslutter at beholde standardkonfigurationen og køre opdateringsprocessen med det samme, kan du angive, under hvilke omstændigheder en evt. påkrævet genstart skal udføres:

- ***Anmod om bekræftelse fra brugeren*** - du bliver bedt om at godkende en genstart af pc'en, der er nødvendig for at afslutte opdateringsprocessen

- ***Genstart med det samme*** - computeren genstartes automatisk, så snart opdateringsprocessen er færdig, og du behøver ikke at godkende det

- ***Fuldfør ved næste genstart af computeren*** - fuldførelse af opdateringsprocessen bliver udsat til computeren genstartes næste gang - husk igen på, at denne mulighed kun anbefales, hvis du kan være sikker på, at computeren bliver genstartet regelmæssigt, mindst en gang dagligt

Yderligere opdateringsindstillinger

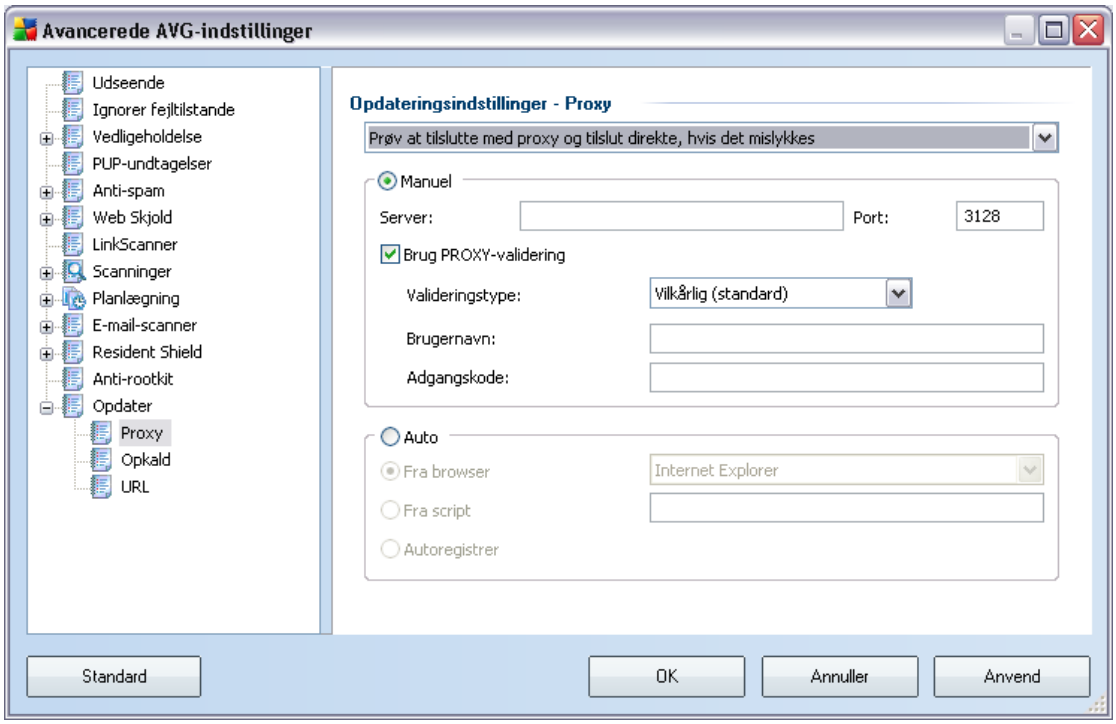
- ***Opret nyt systemgendannelsespunkt efter hver programopdatering*** - før hver AVG programopdatering oprettes et systemgendannelsespunkt. I tilfælde af at opdateringsprocessen mislykkes, og dit operativsystem går ned, kan du altid gendanne dit operativsystem i dets oprindelige konfiguration fra dette punkt. Denne mulighed er tilgængelig via Start / Alle programmer / Tilbehør / Systemværktøjer / Systemgendannelse, men ændringer anbefales kun for erfarne brugere! Hold dette afkrydsningsfelt markeret, hvis du ønsker at bruge denne funktion.

- ***Brug DNS-opdatering*** - marker dette afkrydsningsfelt, hvis du vil bruge detekteringsmetoden til opdateringsfiler, som eliminerer datamængden overført mellem opdateringsserveren og AVG-klienten;

- ***Anmod om bekræftelse for at lukke kørende applikationer*** (*slået til som standard*) hjælper dig med at sikre, at ingen kørende applikationer lukkes uden din tilladelse - hvis det er påkrævet for at fuldføre opdateringsprocessen;

- ***Kontrollér klokkeslæt på computeren*** - marker denne valgmulighed, hvis du vil adviseres i tilfælde af, at computeretiden afviger fra den korrekte tid med mere end et angivet antal timer.

12.12. Proxy



Proxy-serveren er en enkeltstående server eller en service, der kører på en pc, som sørger for en mere sikker forbindelse til internettet. I henhold til de specificerede netværksregler kan man enten have direkte adgang til internettet eller via en proxyserver. Begge muligheder kan også være tilladt samtidigt. Så skal du i det første element i dialogboksen ***Opdateringsindstillinger - Proxy*** vælge i kombinationsmenuen, hvilken metode, du vil bruge:

- ***Brug proxy***
- ***Brug ikke proxyserver***
- ***Prøv at tilslutte med proxy, og tilslut direkte, hvis det mislykkes*** - standardindstillinger

Hvis du vælger en indstilling, der gør brug af proxyserver, skal du angive yderligere data. Serverindstillingerne kan enten konfigureres manuelt eller automatisk.

Manuel konfiguration

Hvis du vælger manuel konfiguration (marker *indstillingen* ***Manuel****for at aktivere den pågældende sektion i dialogboksen*) skal du angive følgende punkter:

- ***Server*** - angiv serverens IP-adresse eller serverens navn
- ***Port*** - angiv nummeret på den port, der giver adgang til internettet (*som standard er dette nummer indstillet til 3128, men det kan indstilles til et andet- hvis du er i tvivl, kan du kontakte din netværksadministrator*)

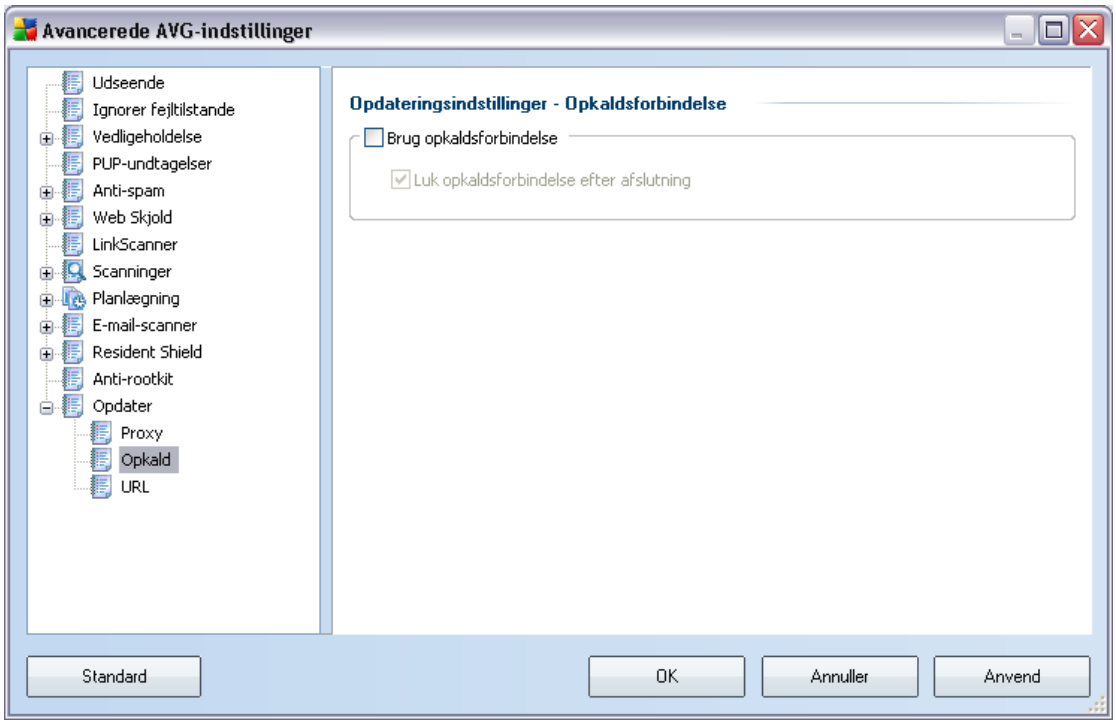
Proxyserveren kan også have specifikke regler defineret for hver bruger. Hvis din proxyserver er konfigureret på denne måde, skal du markere indstillingen ***Brug PROXY-validering*** for at verificere, at dit brugernavn og din adgangskode er gyldige til at oprette forbindelse til internettet via proxyserveren.

Automatisk konfiguration

Hvis du vælger automatisk konfiguration (*marker indstillingen* ***Auto*** *for at aktivere den pågældende sektion i dialogboksen*), skal du vælge hvor proxykonfigurationen skal hentes fra:

- ***Fra browser*** - konfigurationen læses fra din standard internetbrowser (*de understøttede browsere er Internet Explorer, Firefox, Mozilla og Opera*)
- ***Fra script*** - konfigurationen bliver læst fra et downloadet script, hvor funktionen returnerer proxyadressen
- ***Autodetektering*** - konfigurationen bliver detekteret automatisk, direkte fra proxyserveren

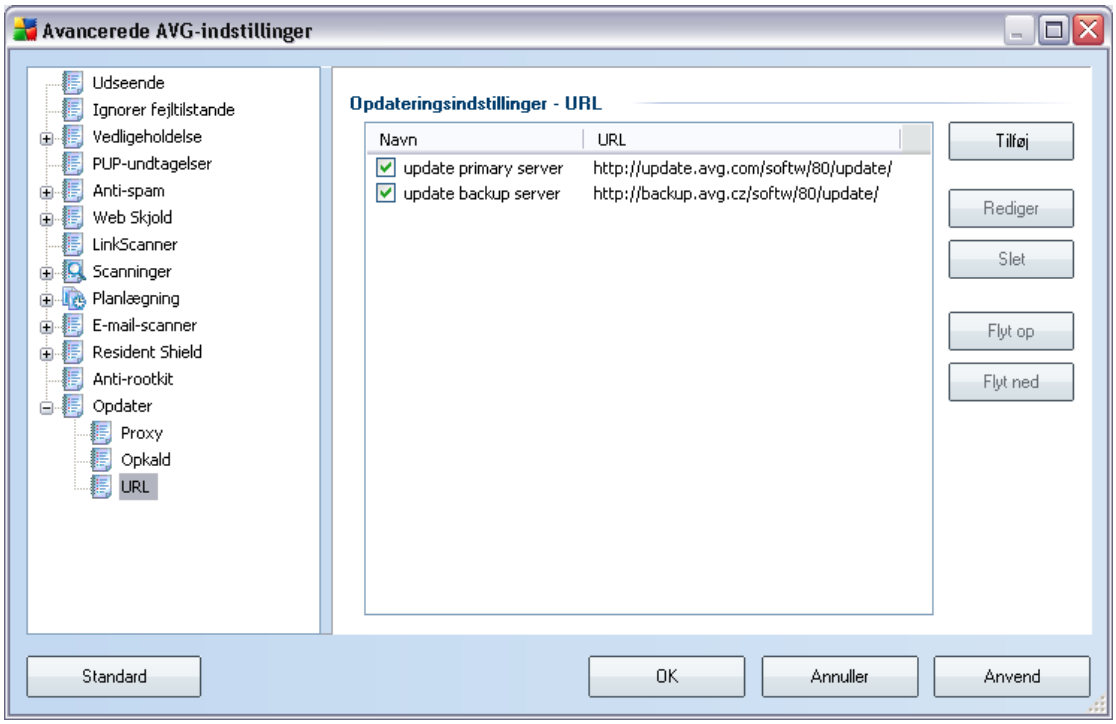
12.12. Opkald



Alle parametre, der valgfrit defineres i dialogen ***Opdateringsindstillinger - Opkaldsforbindelse*** vedrører opkaldsforbindelsen til internettet. Dialogens felter er inaktive, indtil du sætter kryds ved ***Brug opkaldsforbindelser***, som aktiverer disse felter.

Angiv om du automatisk vil oprette forbindelse til internettet (***Åbn automatisk denne forbindelse***) eller om du vil bekræfte forbindelsen manuelt hver gang (***Spørg inden forbindelse***). For at oprette forbindelse automatisk skal du yderligere vælge, om forbindelsen skal lukkes, når opdateringen er afsluttet (***Luk opkaldsforbindelse, når opdateringen er afsluttet***).

12.12. URL



Dialogboksen ***URL*** indeholder en liste over internet-adresser, hvorfra opdateringsfilerne kan downloades. Listen og dens elementer kan ændres vha. nedenstående betjeningsknapper:

- ***Tilføj*** - åbner en dialogboks, hvori du kan angive en ny URL, der skal føjes til listen
- ***Rediger*** - åbner en dialogboks, hvori du kan redigere de valgte URL-parametre
- ***Slet*** - sletter den valgte URL fra listen
- ***Standard*** - vender tilbage til standardlisten over URL'er
- ***Flyt op*** - flytter den valgte URL én position opad på listen
- ***Flyt ned*** - flytter den valgte URL én position nedad på listen

12.12. Administrer

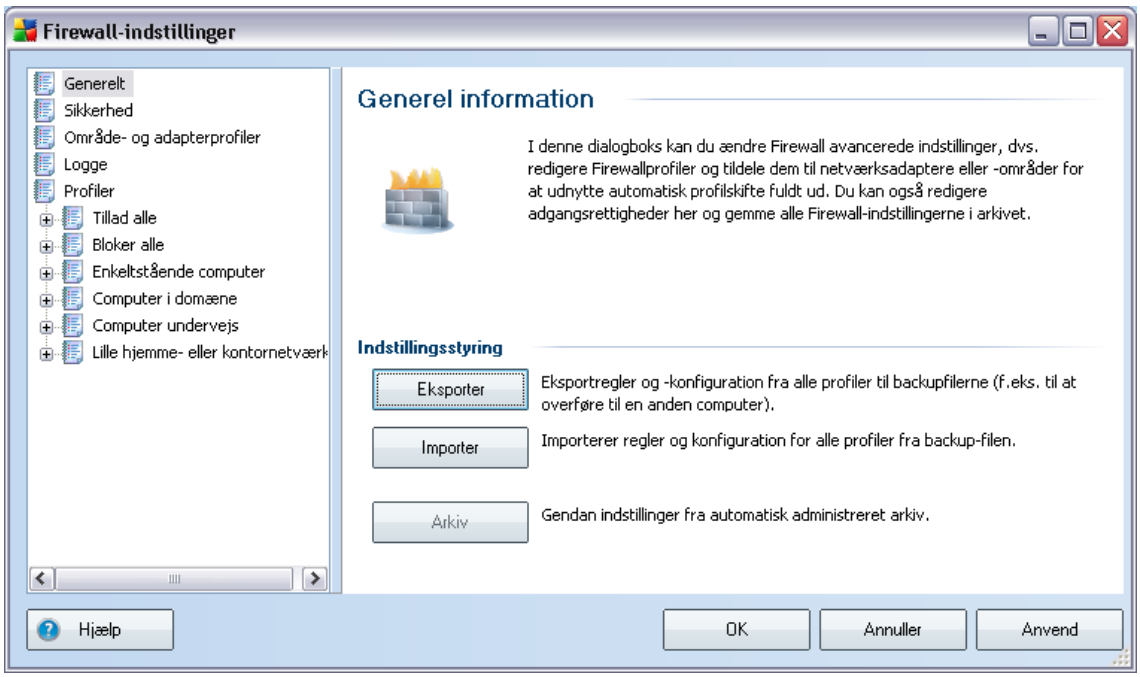
Dialogen ***Administrer*** indeholder to valgmuligheder, som er tilgængelige via to knapper:

- ***Slet midlertidige opdateringsfiler*** - tryk på denne knap for at slette alle unødvendige opdateringsfiler fra din harddisk (*som standard gemmes disse filer i 30 dage*)
- ***Gendan tidligere version af virusdatabasen*** – tryk på denne knap for at slette den seneste virusdatabaseversion fra din harddisk og vende tilbage til den tidligere gemte version (*en ny virusdatabaseversion bliver en del af den næste opdatering*)

13. Firewall-indstillinger

Firewall-konfigurationen åbnes i et nyt vindue, hvor der i adskillige dialoger kan indstilles meget avancerede parametre for komponenten. Den avancerede konfigurationsredigering er kun beregnet til eksperter og erfarne brugere. For alle andre brugere anbefaler vi på det kraftigste at bevare den konfiguration, der er indstillet via ***guiden Firewall-konfiguration***.

13.1.Generelt

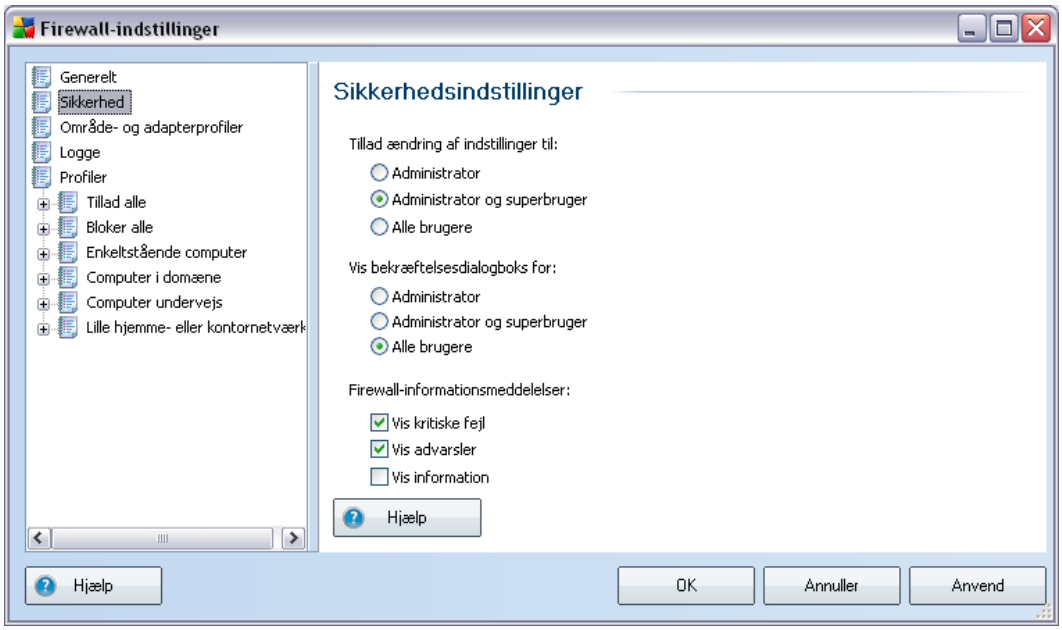


I ***Generelle oplysninger*** kan du eksportere/importer eller gemme ***Firewall***-konfigurationen:

- ***Eksporter / Importer*** - eksporter de definerede ***Firewall***-regler og -indstillinger til sikkerhedskopifiler, eller importer hele den sikkerhedskopierede fil.

- ***Arkiv*** - efter hver ***Firewall***-konfiguration gemmes hele den oprindelige konfiguration i et arkiv. Arkiverede konfigurationer kan derefter åbnes vha. knappen ***Indstillingsarkiv***. Hvis indstillingsarkivet er tomt, betyder det, at der ikke er foretaget ændringer, siden ***Firewall*** blev installeret. Det maksimale antal gemte registreringer er 10. Hvis du forsøger at gemme flere registreringer, vil de ældste registreringer blive overskrevet.

13.2.Sikkerhed



I dialogen ***Sikkerhedsindstillinger*** kan du definere generelle regler for ***Firewall***s opførsel uanset den valgte profil:

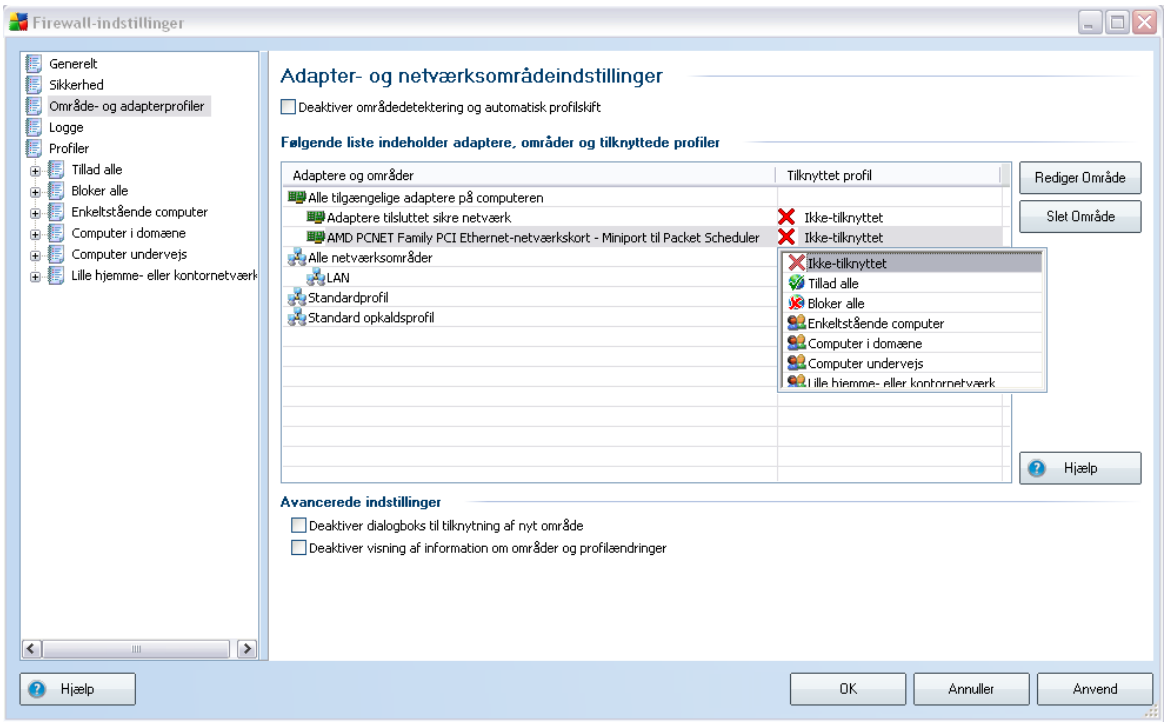
- ***Tillad ændringer i indstillingerne for*** - angiv hvem der har lov til at ændre ***Firewall***-konfigurationen
- ***Vis bekræftelsesdialog for*** - angiv hvem der skal have vist bekræftelsesdialoger (*dialoger der beder om en beslutning i situationer, der ikke er dækket af en defineret* ***Firewall****-regel*).

I begge tilfælde kan du tildele den specifikke rettighed til en af følgende brugergrupper:

- ***Administrator*** – har fuldstændig kontrol over pc'en, og har rettigheder til at knytte enhver bruger til grupper med specielt definerede autoriteter
- ***Administrator og power-bruger*** – administratoren kan knytte enhver bruger til en specificeret gruppe (*Power-bruger*) og definere autoriteter for gruppemedlemmerne
- ***Alle brugere*** – andre brugere, der ikke er knyttet til en specifik gruppe

- ***Firewall-informationsmeddelelse*** - beslut, hvilke ***Firewall***-informationsmeddelelser, der skal vises - det anbefales at få vist kritiske fejl og advarsler altid og bestemme frit for informationsmeddelelserne

13.3.Område- og adapterprofiler



I dialogerne for ***Adapter- og netværksområdeindstillinger*** kan du redigere indstillinger vedrørende tilknytning af definerede profiler til specifikke adaptere og refererende og pågældende netværk:

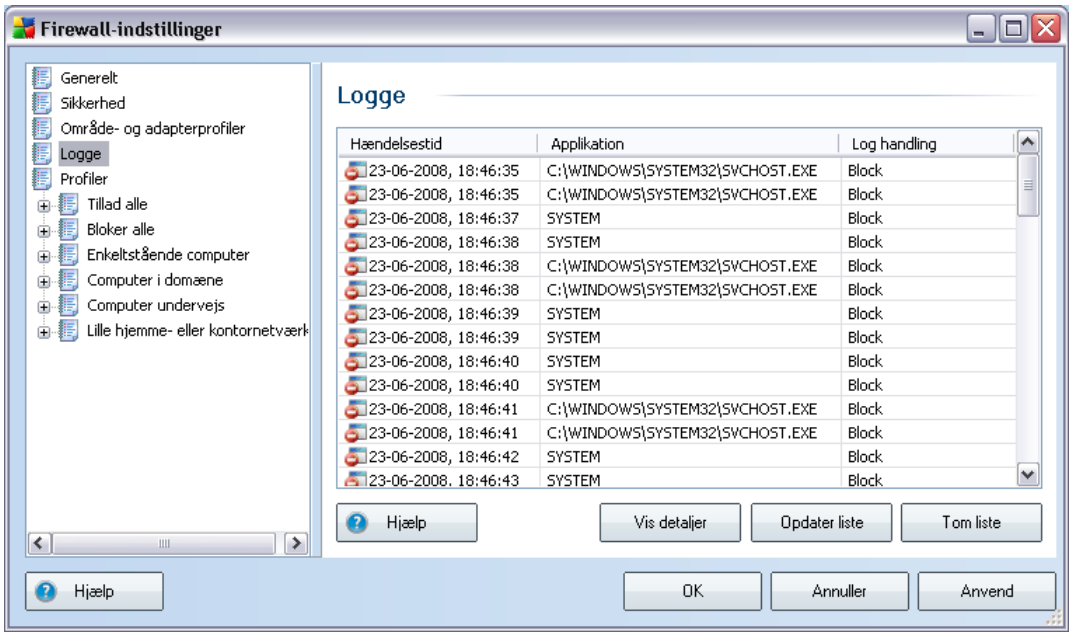
- ***Deaktiver områdedetektering og automatisk profilskift*** - en af de definerede profiler kan knyttes til hver type af netværksinterface, der anvendes for hvert område. Hvis du ikke vil definere specifikke profiler, anvendes en generel profil, der er defineret i ***Guiden Firewall-konfiguration*** . Men hvis du beslutter at skelne mellem profiler og knytte dem til specifikke adaptere og områder, og du på et senere tidspunkt midlertidigt vil skifte til denne opsætning, skal du markere indstillingen ***Deaktiver områdedetektering og automatisk profilskift***.

- ***Liste over adaptere, områder og tilknyttede profiler*** - i denne liste kan du finde en oversigt over detekterede adaptere og områder. Til hver af dem

kan du knytte en specifik profil fra menuen over definerede profiler (*alle profiler er primært defineret i **guiden Firewall-konfiguration**, eller du kan på et senere tidspunkt oprette nye profiler i dialogen **Profiler** i Firewall-indstillinger*). Klik på det pågældende element i listen over adaptere, og vælg profilen for at åbne denne menu.

- ***Avancerede indstillinger*** - ved at markere den pågældende indstilling deaktiveres funktionen til visning af en informationsmeddelelse

13.4.Logge



I dialogen ***Logge*** kan du gennemse listen over alle loggede ***Firewall***-handlinger og -hændelser med en detaljeret beskrivelse af de relevante parametre:

- ***Hændelsestid*** - nøjagtig dato og klokkeslæt hvor hændelsen forekom
- ***Applikation*** - navn på processen, den loggede hændelse vedrører
- ***Handling*** - den udførte handlingstype

Følgende betjeningsknapper er til rådighed:

- ***Hjælp*** - åbner de dialogrelaterede hjælpefiler.

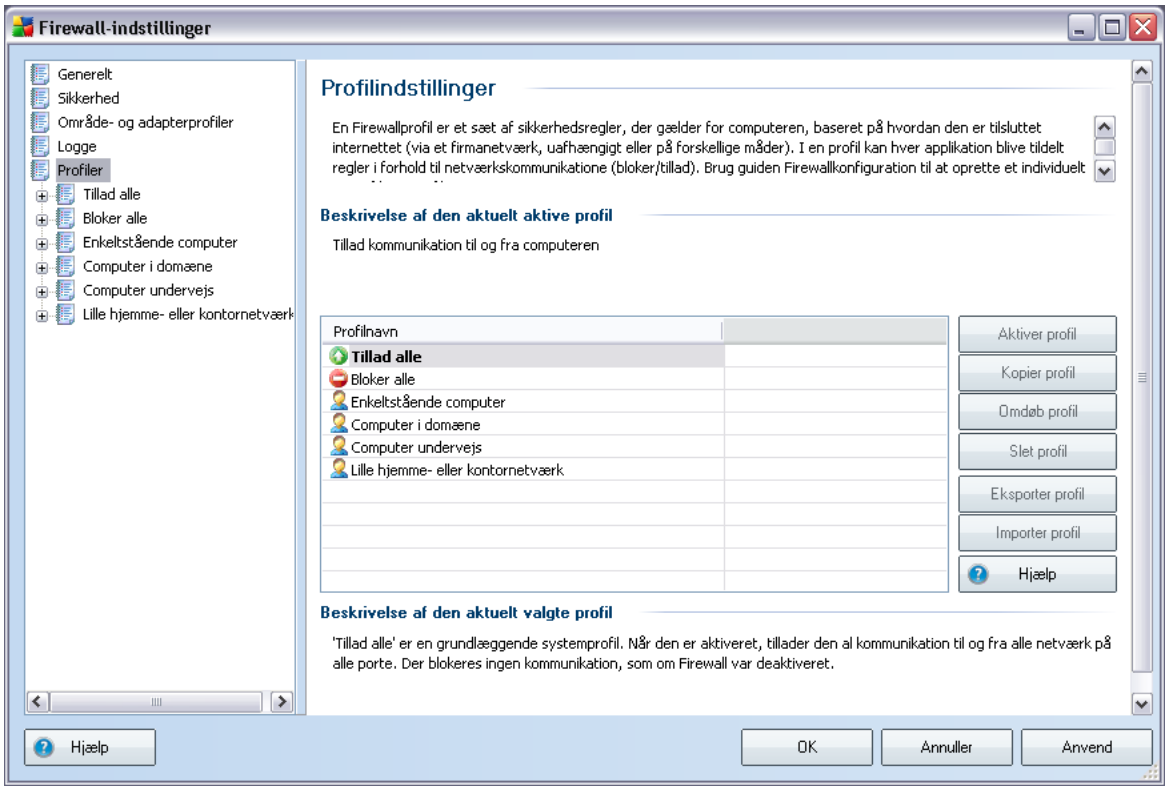
- ***Vis detaljer*** - hvis du synes de oplyste parametre er utilstrækkelige og vil se mere, kan du bruge denne knap til at skifte til den avancerede logfilsoversigt med yderligere oplysninger (om bruger, PID, retning, protokol, ekstern/lokal port, ekstern/lokal IP-adresse).

- ***Opdater liste*** - alle de loggede parametre kan sorteres efter den valgte attribut: kronologisk (*datoer*) eller alfabetisk (*andre kolonner*) - du skal bare klikke på den pågældende kolonneoverskrift. Brug knappen ***Opdater liste*** til at opdatere de aktuelt viste oplysninger.

- ***Tøm lis*** - slet alle poster i tabellen.

13.5.Profiler

I dialogen ***Profilindstillinger*** finder du en liste over alle tilgængelige profiler.



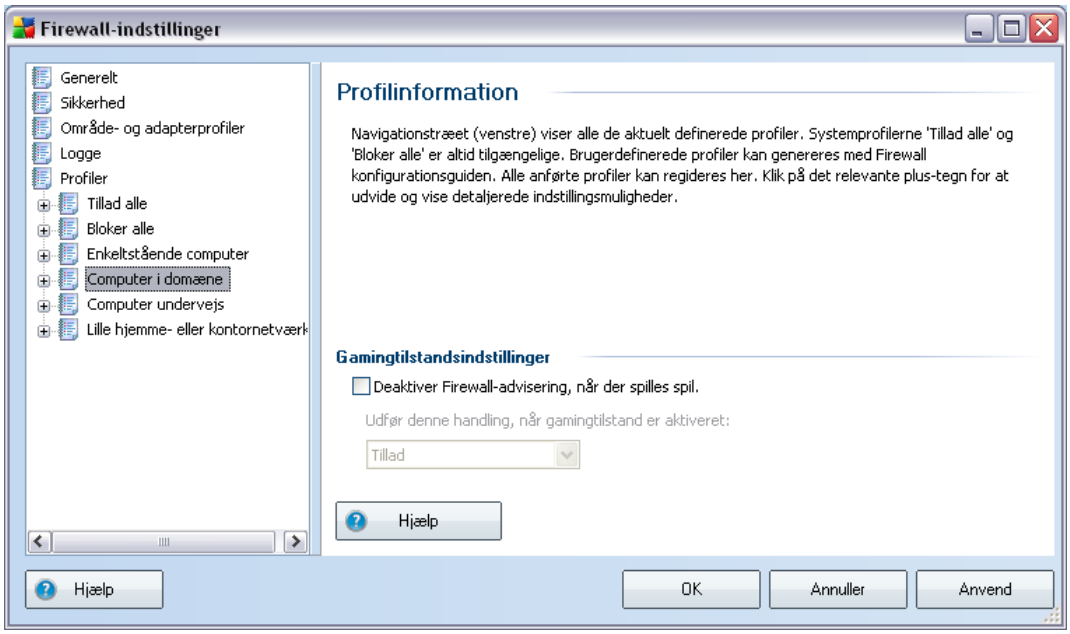
Alle andre end system-profiler kan derefter redigeres i denne dialog ved hjælp af følgende betjeningsknapper:

- ***Aktiver profil*** - denne knap indstiller den valgte profil som aktiv, hvilket indebærer, at den valgte profils konfiguration bruges af ***Firewall*** til at kontrollere netværkstrafikken
- ***Kopier profil***- opretter en identisk kopi af den valgte profil. Senere kan du redigere og omdøbe kopien for at oprette en ny profil baseret på den kopierede original
- ***Omdøb profil*** - gør det muligt at definere et nyt navn på en valgt profil
- ***Slet profil*** - sletter den valgte profil fra listen
- ***Eksporter profil*** - gemmer den valgte profils konfiguration i en fid, der gemmes til fremtidig brug
- ***Importer profil*** - konfigurerer den valgte profils indstilligner på baggrund af data eksporteret fra en sikkerhedskopieret konfigurationsfil
- ***Hjælp*** - åbner den dialogrelaterede hjælpefil

I dialogens nederste sektion findes beskrivelsen af den profil, der aktuelt er valgt i ovenstående liste.

Den venstre navigationsmenus struktur ændres på baggrund af antallet af definerede profiler, der er anført i listen i dialogen ***Profil***. Hver defineret profil opretter en specifik gren under elementet ***Profil***. Derefter kan specifikke profiler redigeres i de følgende dialoger (*der er identiske for alle profiler*):

13.5.1.Profilinformation



Dialogen ***Profiloplysninger*** er den første dialog i en sektion, hvor du kan redigere konfigurationen for hver profil i forskellige dialoger, der vedrører specifikke parametre for profilen.

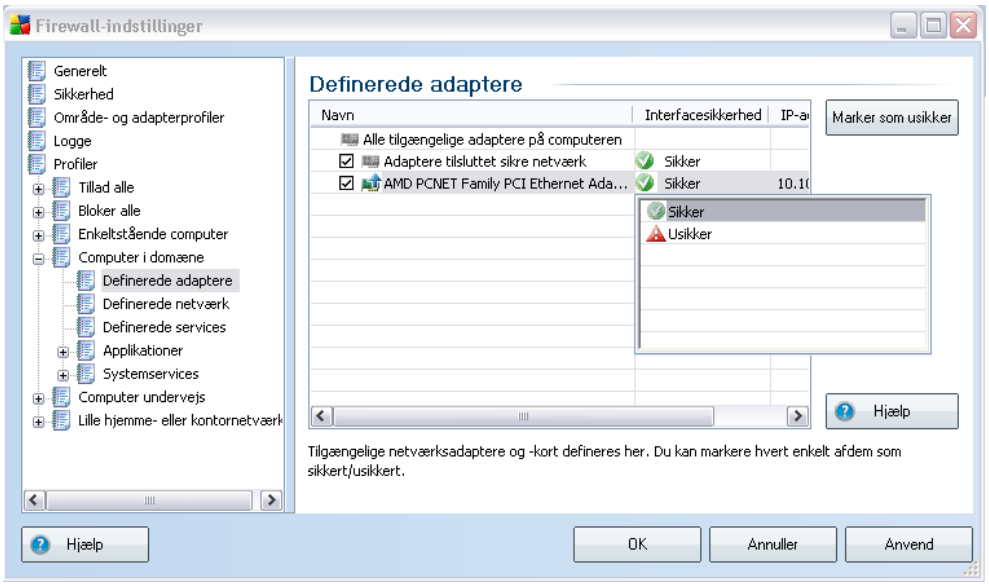
Aktiver Virtual Machines forbundet netværk - marker dette element for at tillade virtuelle maskiner i WMware for at oprette forbindelse direkte til netværket

Gamingtilstandsindstillinger

I sektionen ***Gamingtilstandsindstillinger*** kan du ved at krydse det pågældende element af bestemme og bekræfte, om du vil have ***Firewall*** til at vise informationsmeddelelser, selvom der kører en applikation i fuld skærm på din computer (*dette er typisk spil, men gælder også for andre fuldskærmsapplikationer, f. eks. PPT-præsentationer*). Da informationsmeddelelserne kan være forstyrrende, er funktionen slået fra som standard.

Hvis du markerer elementet ***Aktiver Firewall-advisering når der spilles spil*** i rullemenuen, skal du vælge hvilken handling, der skal foretages, hvis en ny applikation, der endnu ikke er angivet regler for, forsøger at kommunikere over netværket (*applikationer der normalt medfører en spørgsmålsdialog*). Alle disse applikationer kan enten tillades eller blokeres.

13.5.2.Definerede adaptere

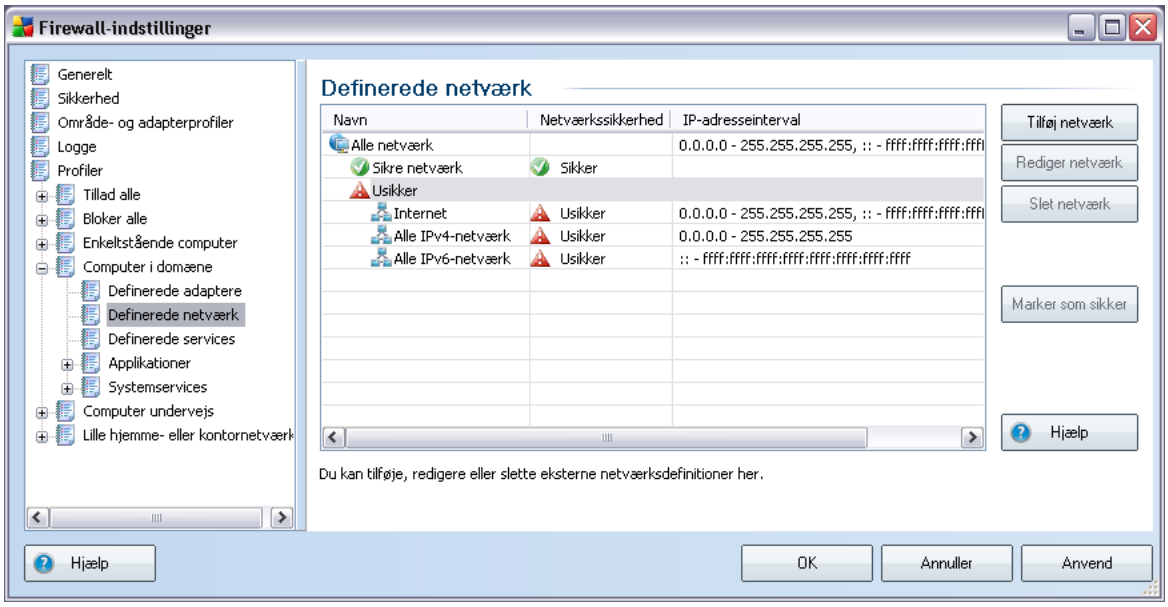


I dialogen ***Definerede adaptere*** findes en liste over alle adaptere, der blev detekteret på din computer. Et specifikt netværk refererer til hver adapter - se dialogen ***Definerede netværk*** for en liste over alle netværk.

Der findes følgende oplysninger for hver detekteret adapter:

- ***Adaptere*** - navneliste over alle detekterede adaptere, din computer anvender til at oprette forbindelse til specifikke netværk
- ***Interfacesikkerhed*** - som standard betragtes alle adaptere som usikre, og du kan kun tildele den sikker status, hvis du er sikker på, at den pågældende adapter (og det pågældende netværk) er sikker (*klik på listeelementet, der svarer til den pågældende adapter og vælg Sikker i kontekstmenuen, eller brug knappen* ***Marker som sikker***) - alle sikre adaptere og tilhørende netværk inkluderes derefter i gruppen, som applikationen kan kommunikere over, med applikationsreglen indstillet til ***Tillad for sikker***
- ***IP-adresseområde*** - hvert netværks (der refererer til en specifik adapter) område detekteres automatisk og specificeres i form af IP-adresseområder

13.5.3.Definerede netværk



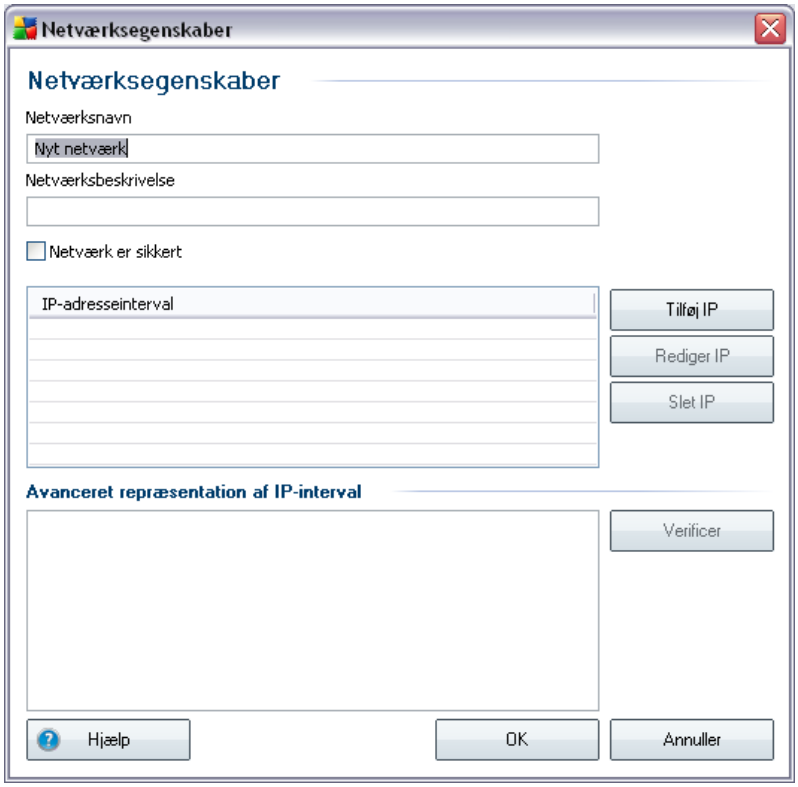
Dialogen ***Definerede netværk*** indeholder en liste over alle netværk, som din computer er tilsluttet. Hvert netværk refererer til en specifik adapter - se dialogen ***Definerede adaptere*** for en liste over alle adaptere.

Der findes følgende oplysninger for hvert detekteret netværk:

- ***Netværk*** - navneliste over alle netværk, som computeren er tilsluttet
- ***Netværkssikkerhed*** - som standard betragtes alle netværk som usikre, og du kan kun tildele det sikker status, hvis du er sikker på, at det pågældende netværk er sikkert (*klik på listeelementet, der svarer til det pågældende netværk og vælg Sikker i kontekstmenuen*) - alle sikre netværk inkluderes derefter i gruppen, som applikationen kan kommunikere over med applikationsreglen indstillet til ***Tillad for sikker***
- ***IP-adresseområde*** - hvert netværk detekteres automatisk og specificeres i form af IP-adresseområder

Betjeningsknapper

- ***Tilføj netværk*** - åbner dialogvinduet ***Netværksegenskaber***, hvor du kan redigere parametre for det nydefinerede netværk:



I denne dialog kan du angive ***Netværksnavn***, indtaste en ***Netværksbeskrivelse*** og muligvis tildele netværket sikke status. Det nye netværk kan enten defineres manuelt i en enkeltstående dialog, der åbnes med knappen ***Tilføj IP*** (alternativt ***Rediger IP*** / ***Slet IP***), i denne dialog kan du angive netværket ved at oplyse dets IP-område eller maske.

For et stort antal netværk, der skal defineres som en del af den nyoprettede netværk, kan du bruge indstillingen ***Avanceret repræsentation af IP-område***: indtast listen over alle netværkene i det pågældende tekstfelt (*alle standardformater understøttes*) og tryk på knappen ***Verificer*** for at sørge for, at formatet kan genkendes. Tryk derefter på ***OK*** for at bekræfte og gemme dataene.

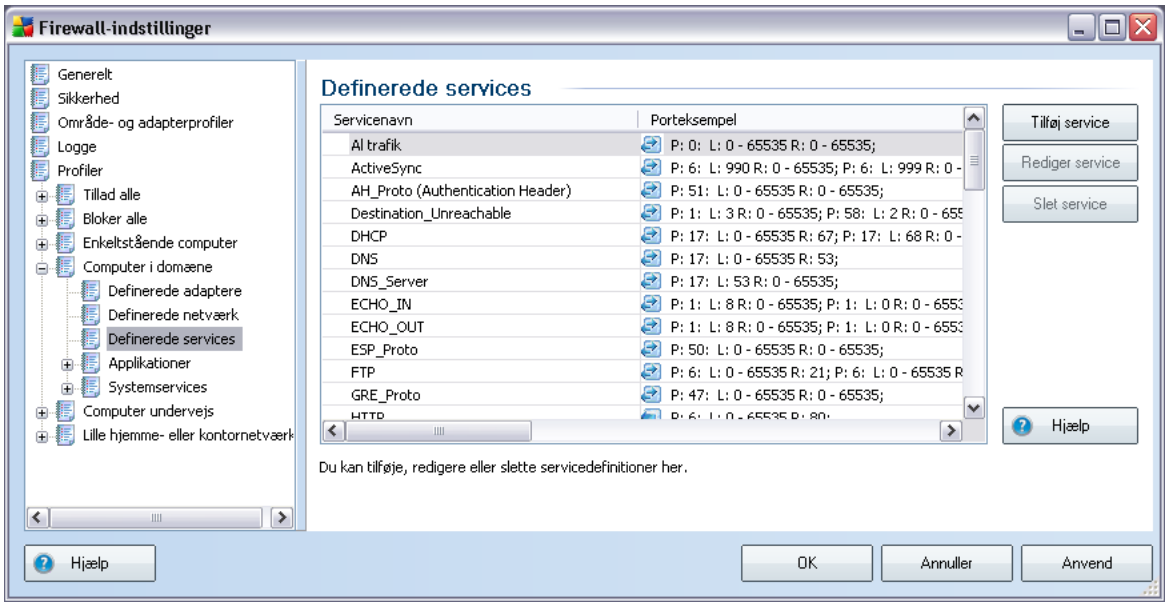
- ***Rediger netværk*** - åbner dialogen ***Netværksegenskaber*** (*se ovenfor*), hvor du kan redigere parametrene for et allerede defineret netværk (*dialogen er identisk med dialogen til at tilføje et ny netværk, se beskrivelsen i forrige afsnit*)

- ***Slet netværk*** - fjerner posten med et valgt netværk fra listen over netværk

- ***Marker som sikkert*** - som standard betragtes alle netværk som usikre, og kun hvis du ikke er på, at det pågældende netværk er sikkert, kan du bruge denne knap til at tildele det denne status.

- ***Hjælp*** - åbner den dialogrelaterede hjælpefil

13.5.4.Definerede services



Dialogen ***Definerede services*** åbner en liste over alle services, der er defineret for applikationen i standardkonfigurationen, og services der allerede er defineret af brugeren. Dialogboksen er opdelt i to kolonner:

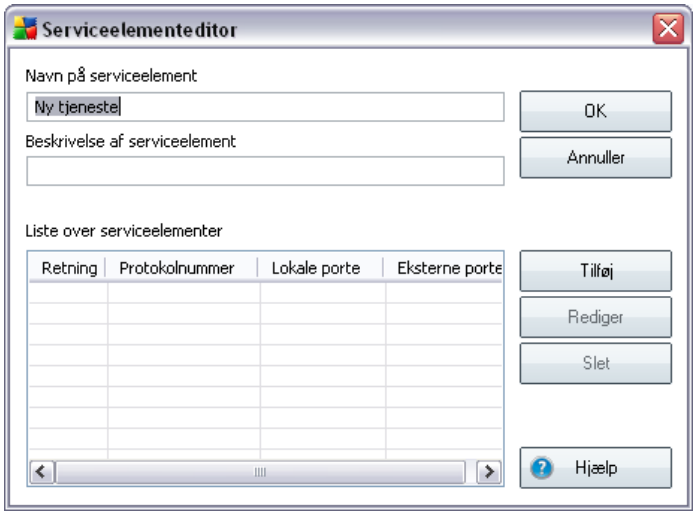
- ***Servicenavn*** - indeholder navnet på servicen

- ***Porteksempel*** - pile angiver indkommende/udgående kommunikation, derudover findes nummeret eller navnet på den anvendte protokol (P) og nummeret eller området for anvendte lokale (L) / eksterne (R) porte

Du kan tilføje, redigere og/eller slette specifikke services.

Betjeningsknapper

- ***Tilføj service*** - åbner et nyt ***Serviceelementeditor***-dialogvindue , hvor du kan definere parametrene for den service, der tilføjes:

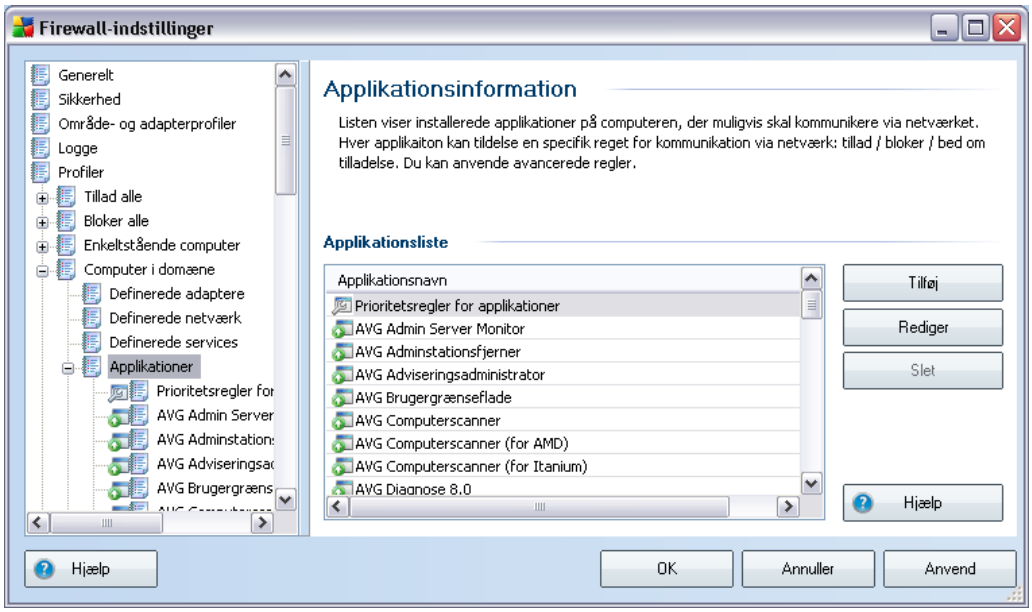


I dialogen kan du angive ***Serviceelementnavn*** og give en kort ***Serviceelementbeskrivelse***. I sektionen ***Serviceelementliste*** kan du derefter tilføje (*og redigere eller slette*) serviceelementer ved at angive følgende parametre:

- ***Retning*** - indkommende, udgående, begge veje
- ***Protokolnummer*** - protokoltype (*vælg fra menuen*)
- ***Lokale porte*** - områdeliste for lokale porte
- ***Eksterne porte*** - områdeliste for eksterne porte

- ***Rediger service*** - åbner dialogen ***Serviceelementeditor*** (*se ovenfor*), hvor du kan redigere parametrene for en allerede defineret service (*dialogen er identisk med dialogen til at tilføje en ny service, se beskrivelsen i forrige afsnit*)
- ***Slet service*** - fjerner posten med en valgt service fra listen
- ***Hjælp*** - åbner den dialogrelaterede hjælpefil

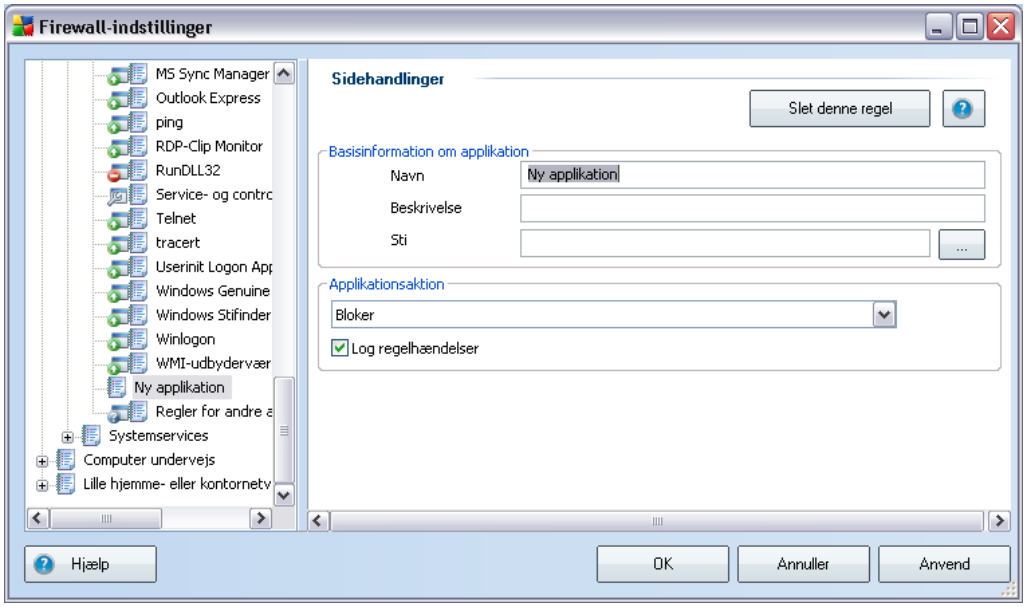
13.5.5.Applikationer



I dialogen ***Applikationsinformation*** finder du en oversigt over alle applikationer, der kommunikerer over netværket, der blev detekteret på din computer, enten under søgningen i ***Guiden Firewall-konfiguration*** i dialogen ***Scan efter internet-applikationer*** eller på et senere tildspunkt. Denne liste kan redigeres ved hjælp af følgende betjeningsknapper:

- ***Tilføj*** - åbner dialogen til at definere et nyt applikationsregelsæt
- ***Rediger*** - åbner dialogen til at redigere et eksisterende applikationsregelsæt
- ***Slet*** - fjerner den valgte applikation fra listen
- ***Hjælp*** - åbner den dialogrelaterede hjælpefil

Dialogen til definition af nye applikationsregelsæt åbnes med knappen ***Tilføj*** fra dialogen ***Applikationer*** i ***Firewall-indstillinger***:



I denne dialog kan du definere:

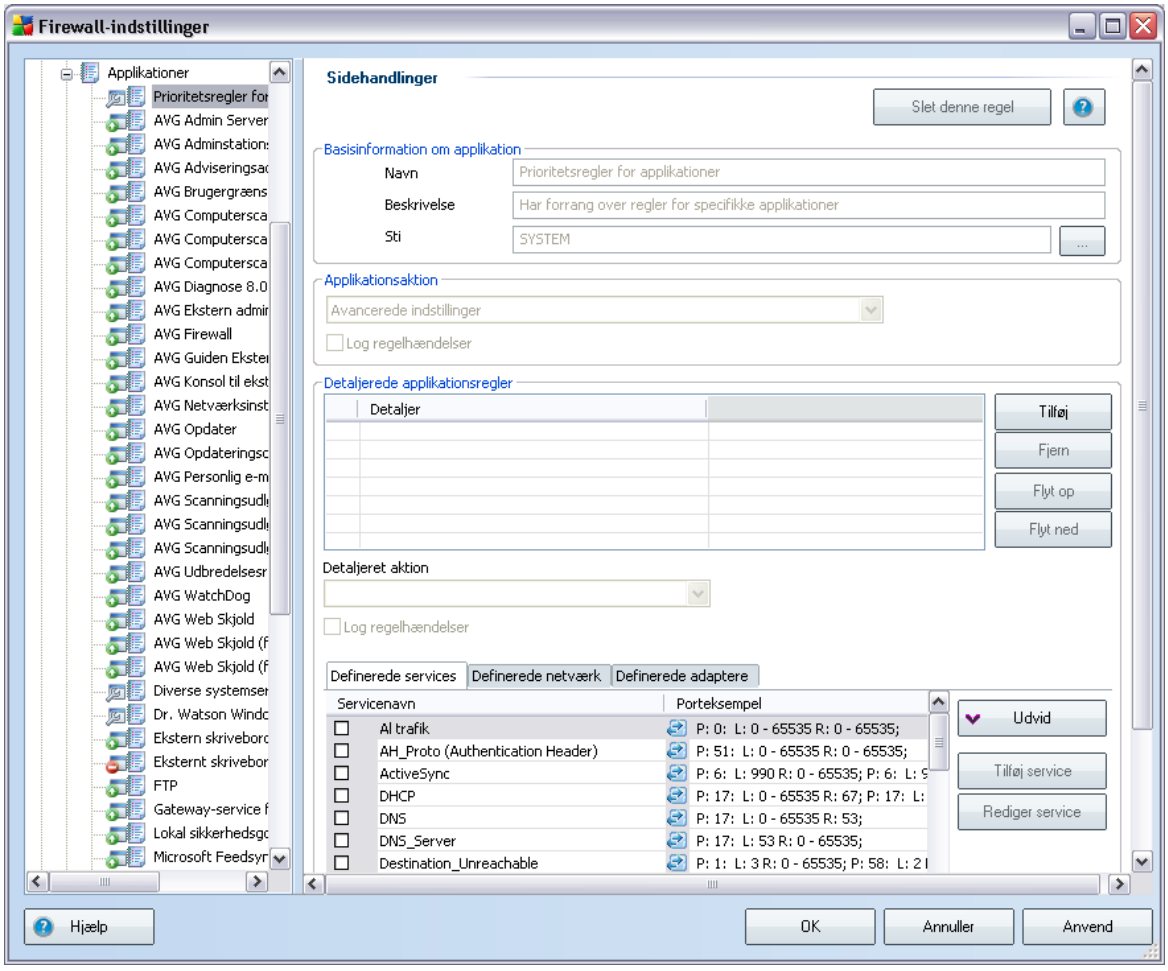
- ***Basisinformation om applikation*** - navn på applikation, kort beskrivelse af den og en sti til dens placering på disken
- ***Applikationshandling*** - vælg en regel i rullemenuen, der skal føjes til applikationens opførsel:
  - ***Avancerede indstillinger -*** giver dig mulighed for at redigere regelsættet i detaljer i den nederste del af dialogen. *Se kapitlet* ***Rediger applikation*** *for en beskrivelse af denne sektion*
  - ***Tillad for alle*** - alle kommunikationsforsøg for applikationen tillades
  - ***Tillad for sikre -*** applikationen får kun tilladelse til at kommunikere over sikre netværk (*for eksempel tillades kommunikation til det beskyttede firmanetværk, hvorimod kommunikation til internettet blokeres*). Se dialogen ***Netværk*** for en oversigt og beskrivelse af sikre netværk

- ***Spørg -*** hver gang applikationen forsøger at kommunikere over netværket, bliver du spurgt, om kommunikationen skal tillades eller blokeres

- ***Bloker -*** alle kommunikationsforsøg for applikationen blokeres

- ***Log regelhændelser*** - marker denne indstilling for at bekræfte, at du vil have logget alle ***Firewall***-hændelser vedrørende den applikation, du har konfigureret regelsættet for. De pågældende logposter kan derefter findes i dialogen ***Logge***.

Dialogen til redigering af eksisterende applikationsregelsæt åbnes med knappen ***Rediger*** fra dialogen ***Applikationer*** i ***Firewall-indstillinger***:



I denne dialog kan du redigere alle applikationens parametre:

- ***Basisinformation om applikation*** - navn på applikation, kort beskrivelse af den og en sti til dens placering på disken
- ***Applikationshandling*** - vælg en regel i rullemenuen, der skal føjes til applikationens opførsel:

- ***Avancerede indstillinger -*** med denne indstilling kan du redigere regelsættet i detaljer i den nederste del af denne dialog

- ***Tillad for alle*** - alle kommunikationsforsøg for applikationen tillades

- ***Tillad for sikre -*** applikationen får kun tilladelse til at kommunikere over sikre netværk (*for eksempel tillades kommunikation til det beskyttede firmanetværk, hvorimod kommunikation til internettet blokeres*). Se dialogen ***Netværk*** for en oversigt og beskrivelse af sikre netværk

- ***Spørg -*** hver gang applikationen forsøger at kommunikere over netværket, bliver du spurgt, om kommunikationen skal tillades eller blokeres

- ***Bloker -*** alle kommunikationsforsøg for applikationen blokeres

- ***Log regelhændelser*** - marker denne indstilling for at bekræfte, at du vil have logget alle ***Firewall***-hændelser vedrørende den applikation, du har konfigureret regelsættet for. De pågældende logposter kan derefter findes i dialogen ***Logge***.

- ***Detaljerede applikationsregler*** - denne sektion åbnes kun for redigering, hvis du først har valgt indstillingen for ***Avancerede indstillinger*** i rullemenuen ***Applikationshandling.*** Alle detaljerede indstillinger (anført i kolonnen ***Detaljer***) kan redigeres ved hjælp af disse betjeningsknapper:

  - ***Tilføj*** - brug knappen til at oprette en ny detaljeret regel for en specifik applikation. På fanen ***Detaljer*** vises et nyt element, og du skal angive dets parametre ved at væge de netværk, som applikationen kan kommunikere med (fanen ***Netværk***), adaptere som applikationen kan bruge (fanen ***Adaptere***), og services som applikationen kan gøre brug af (fanen ***Servicenavn***).

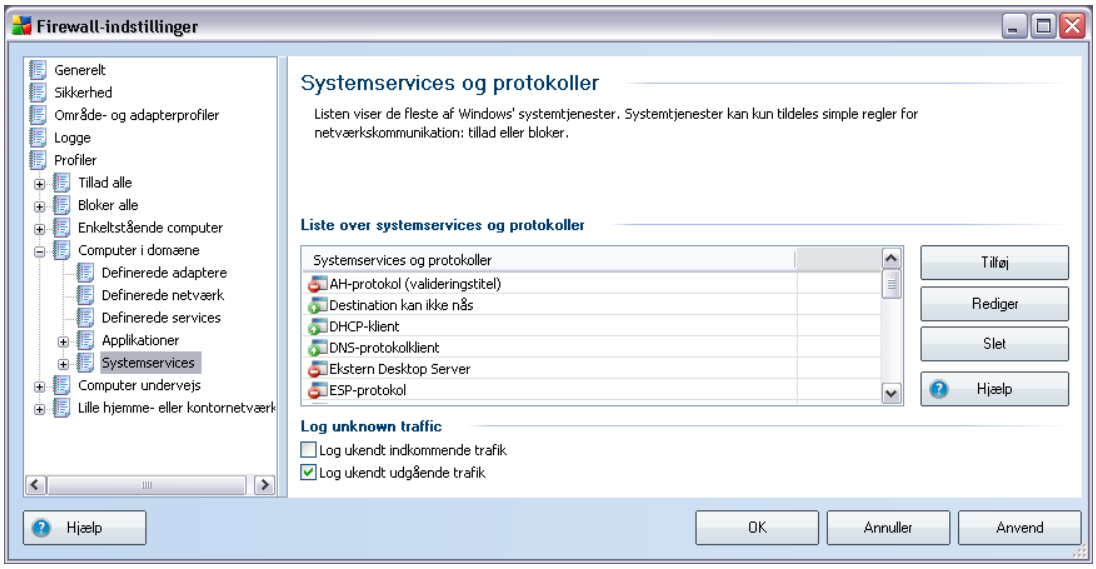
  - ***Fjern*** - fjerner den valgte post på en detaljeret regel fra listen

  - ***Flyt op / Flyt ned*** - detaljerede regler er sorteret efter deres prioritet. Hvis du vil ændre reglens prioritet, bruger du knapperne ***Flyt op*** og ***Flyt ned*** til at flytte de detaljerede indstillinger efter behov.

Hver detaljeret indstilling specificerer yderligere, hvilke ***Definerede services / Definerede netværk / Definerede adaptere***, der bruges.

13.5.6.Systemservices

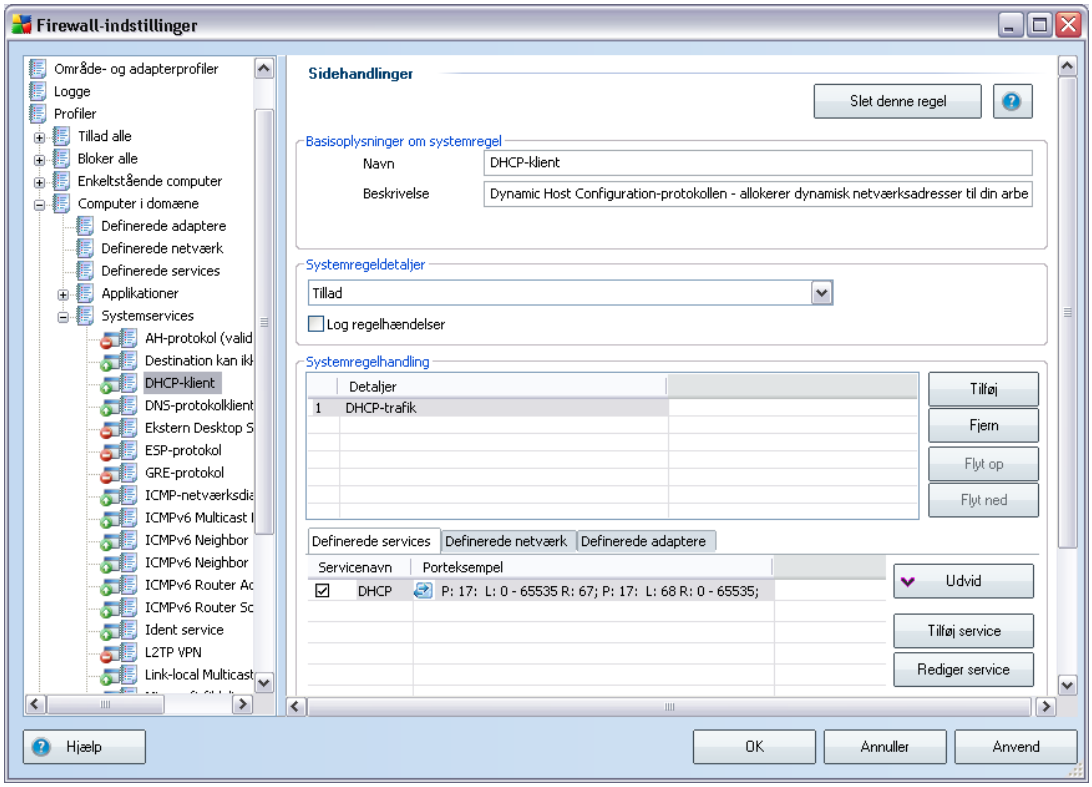
Redigering i dialogen Systemservices og protokoller anbefales kun for erfarne brugere!



Dialogen ***Systemservices og protokoller*** åbner en oversigt over systemservices og protokoller, der kommunikerer over netværket. Under listen findes to indstillinger: marker/afmarker dem for at bekræfte, at du vil have logget al ukendt trafik i begge retninger (*indkommende eller udgående*).

Betjeningsknapper

- ***Tilføj / Rediger*** - begge knapper åbner den samme dialog, hvori du kan redigere systemserviceparametre. Knappen ***Tilføj*** åbner en tom dialog i grundlæggende tilstand (*ingen sektion med avancerede indstillinger, men denne sektion kan åbnes ved at vælge avancerede indstillinger for applikationshandlingen*), knappen ***Rediger*** åbner den samme dialog udfyldt med data, der vedrører den valgte systemservice:



- **_Basisinformation om applikation_** - navn på applikationen og en kort beskrivelse

- **_Applikationshandling_** - vælg en regel i rullemenuen, der skal føjes til systemservicens opførsel (*sammenlignet med applikationer er der kun tre tilgængelige handlinger for systemservices*):

  - **_Bloker_** - alle kommunikationsforsøg for systemservicen blokeres

  - **_Tillad for sikre_** - systemservicen får kun tilladelse til at kommunikere over sikre netværk (*for eksempel tillades kommunikation til det beskyttede firmanetværk, hvorimod kommunikation til internettet blokeres*). Se dialogen **_Netværk_** for en oversigt og beskrivelse af sikre netværk.

  - **_Tillad for alle_** - alle kommunikationsforsøg for systemservicen tilllades

- **_Log regelhændelser_** - marker denne indstilling for at bekræfte, at du

vil have logget alle ***Firewall***-hændelser vedrørende den systemservice, du har konfigureret regelsættet for. De pågældende logposter kan derefter findes i dialogen ***Logge***.

- ***Detaljerede applikationsregler*** - for hver systemservice kan du yderligere angive detaljerede regler i sektionen ***Detaljerede applikationsregler***. Alle detaljerede indstillinger (anført på fanen ***Detaljer***) kan redigeres ved hjælp af disse betjeningsknapper:
  - ***Tilføj*** - brug knappen til at oprette en ny detaljeret regel for en systemservice. På fanen ***Detaljer*** vises et nyt element, og du skal angive dets parametre ved at væge de netværk, som systemservicen kan kommunikere med (fanen ***Netværk***), adaptere som systemservicen kan bruge (fanen ***Adaptere***), og services som applikationen kan gøre brug af (fanen ***Servicenavn***).
  - ***Fjern*** - fjerner den valgte post på en detaljeret regel fra listen
  - ***Flyt op / Flyt ned*** - detaljerede regler er sorteret efter deres prioritet. Hvis du vil ændre reglens prioritet, bruger du knapperne ***Flyt op*** og ***Flyt ned*** til at flytte de detaljerede indstillinger efter behov.

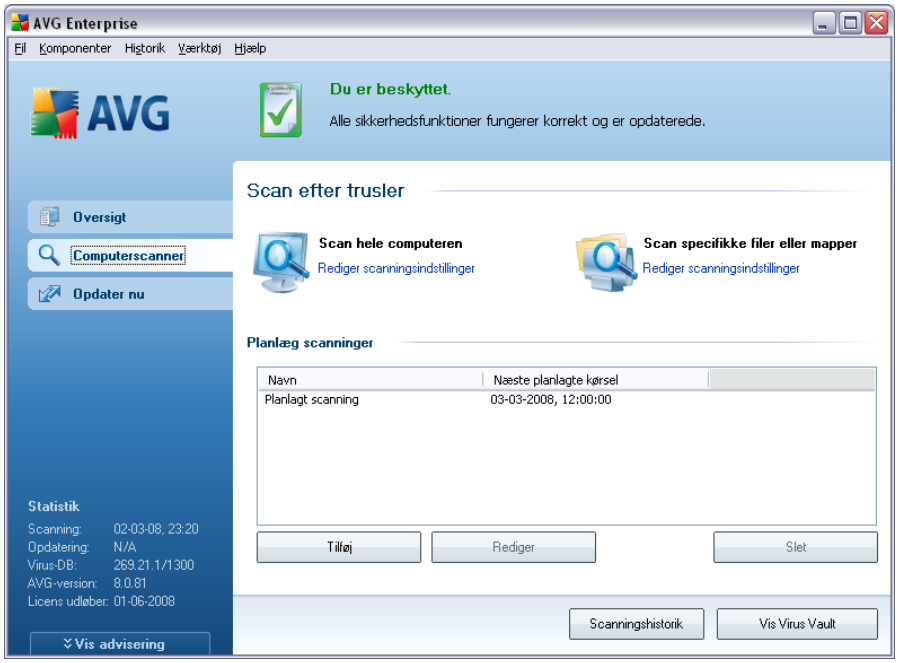
  Hver detaljeret indstilling specificerer yderligere, hvilke ***Definerede services / Definerede netværk / Definerede adaptere***, der bruges.

- ***Slet*** - fjerner den valgte post på en systemservice fra listen ovenfor
- ***Hjælp*** - åbner den dialogrelaterede hjælpefil

14. AVG Scanning

Scanning er en vigtig del af **AVG 8.5 Anti-virus plus firewall**'s funktionalitet. Du kan køre on-demand tests eller planlægge dem til periodisk kørsel, når det er bekvemt for dig.

14.1.Scanning-grænseflade



Der er adgang til AVG's scanningsgrænseflade via lynlinket ***Computerscanner***. Klik på dette link for at skifte til dialogboksen ***Scan efter trusler***. I denne dialogboks finder du følgende:

- oversigt over foruddefinerede scanninger - to testtyper (defineret af softwareleverandøren) er klar til omgående brug efter behov eller planlagt.
- scanningsplanlægning-sektionen - hvor du kan definere nye test og oprette nye planer efter behov.

Betjeningsknapper

Følgende betjeningsknapper er tilgængelige i testgrænsefladen:

- ***Scanningshistorik*** - viser dialogboksen Scanningsresultatoversigt med hele scanningshistorikken
- ***Vis Virus Vault*** - åbner et nyt vindue med Virus Vault - et sted, hvor detekterede infektioner sættes i karantæne

14.2.Foruddefinerede scanninger

En af hovedfunktionerne i AVG er on-demand scanning. On-demand-test er designede til at scanne forskellige dele af computeren, når der opstår mistanke om virusinfektion. Alligevel anbefales det kraftigt at udføre sådanne test regelmæssigt, også selv om du mener, at der ikke findes vira på din computer.

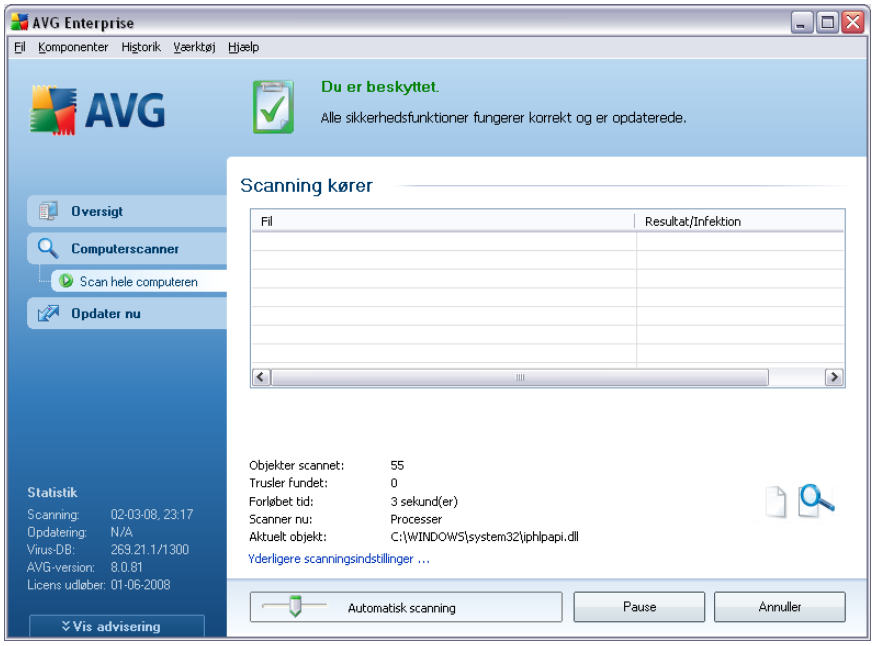
I **AVG 8.5 Anti-virus plus firewall** finder du to scanningstyper, der er foruddefinerede af softwareleverandøren:

14.2.1.Scan hele computeren

Scan hele computeren - scanner hele din computer for mulige infektioner og/eller potentielt uønskede programmer. Denne test scanner alle computerens harddiskdrev, detekterer og helbreder fundne vira eller fjerner den detekterede infektion til ***Virus Vault***. Scanning af hele din computer bør planlægges på en arbejdsstation mindst en gang ugentligt.

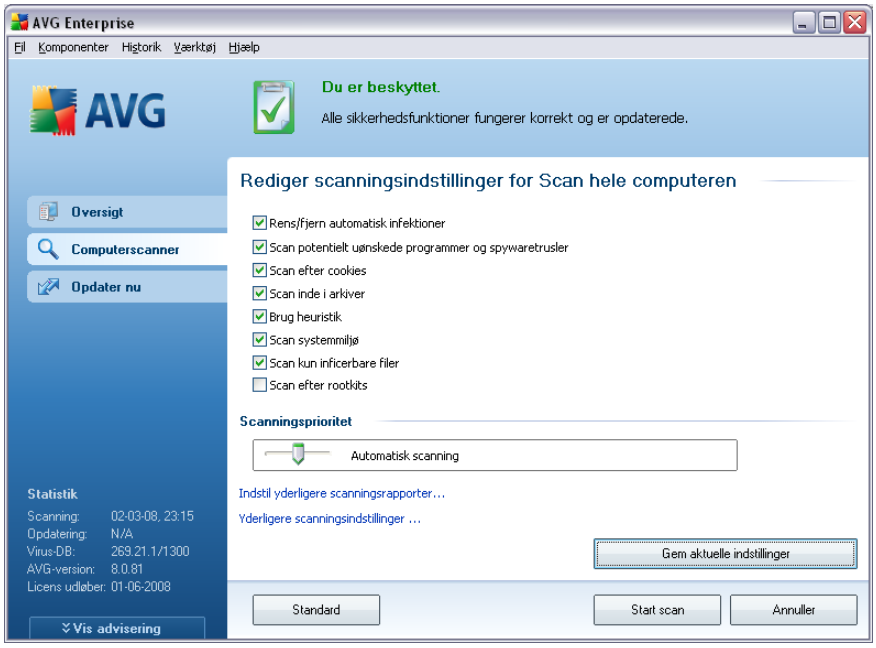
Scanningskørsel

Scanning af hele computeren kan køres direkte fra scanningsgrænsefladen ved at klikke på ikonet for scanningen. Der skal ikke konfigureres flere specifikke indstillinger for denne scanningstype, scanningen starter med det samme i dialogen ***Scanning kører*** (*se skærmbillede*). Scanningen kan afbrydes midlertidigt (***Pause***) eller annulleres (***Annuller***) om nødvendigt.



Redigering af scanningskonfiguration

Du har mulighed for at redigere de foruddefinerede standardindstillinger for ***Scanning af hele computeren***. Tryk på linket ***Rediger scanningsindstillinger*** for at komme til dialogen ***Rediger scanningsindstillinger for Scan hele computeren***. ***Det anbefales at bevare standardindstillingerne, medmindre du har en god grund til at ændre dem!***

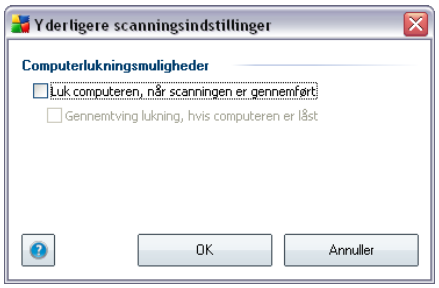


- ***Scanningsparametre*** - i listen over scanningsparametre kan du slå specifikke parametre til/fra efter behov. Som standard er de fleste af parametrene slået til, og de anvendes automatisk under scanningen.

- ***Scanningsprioritet*** - du kan bruge skyderen til at ændre scanningsprioriteten. Som standard er prioriteten indstillet til mellemniveau (*Automatisk scanning*), der optimerer scanningshastigheden og brugen af systemressourcer. Alternativelt kan du køre scanningen langsommere, hvilket betyder, at belastningen på systemressourcerne minimeres (*praktisk, hvis du skal arbejde på computeren, men er ligeglad med, hvor lang tid scanningen tager*), eller hurtigere med øgede krav til systemressourcer (*f.eks. når computeren midlertidgt ikke er i brug*).

- ***Indstil yderligere scanningsrapporter*** - linket åbner en ny ***Scanningsrapporter***-dialo, hvor du kan vælge, hvilke typer af mulige fund, der skal rapporteres:

- ***Yderligere scanningsindstillinger*** - linket åbner en ny ***Computerlukningsmuligheder***-dialog, hvor du kan beslutte, om computeren skal lukkes automatisk, når den igangværende scanning er færdig. Når denne indstilling er bekræftet (***Luk computeren, når scanningen er gennemført***), aktiveres en ny indstilling, som gør det muligt at lukke computeren, selvom den i øjeblikket er låst (***Gennemtving lukning, hvis computeren er låst***).



Advarsel: *Disse scanningsindstillinger er magen til parametrene for en ny defineret scanning - som beskrevet i kapitlet* ***AVG Scanning / Scanningsplanlægning / Hvordan der skal scannes****.*

Hvis du beslutter at ændre standardkonfigurationen for ***Scan hele computeren***, kan du gemme den nye indstilling som standardkonfiguration, der skal bruges til alle fremtidige scanninger af hele computeren.

14.2.2.Scan specifikke filer eller mapper

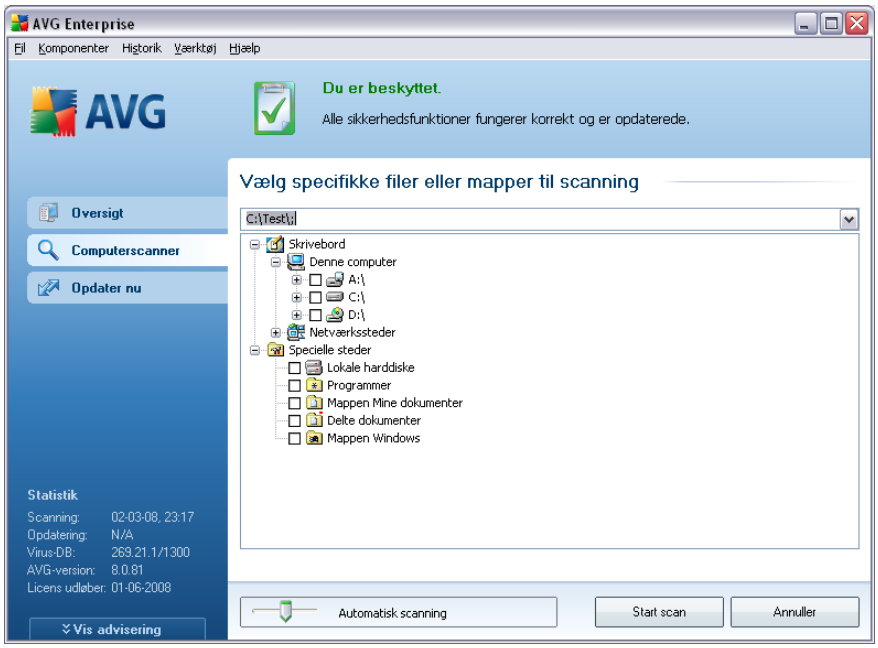
Scan specifikke filer eller mapper - scanner kun de områder af computeren, som du har valgt skal scannes (valgte mapper, harddiske, disketter, cd'er osv.). Scanningens forløb i tilfælde af detektering af virus og behandlingen af denne er den samme som ved scanning af hele computeren: fundne virus helbredes eller fjernes til ***Virus Vault***. Scanning af specifikke filer eller mapper kan anvendes til at oprette dine egne test og planlægning af dem på baggrund af dine behov.

Scanningskørsel

Scanning af specifikke filer eller mapper kan køres direkte fra scanningsgrænsefladen ved at klikke på ikonet for scanningen. En ny dialog med navnet ***Vælg specifikke filer eller mapper til scanning*** åbnes. Vælg de mapper, du vil have scannet, i computerens træstruktur. Stien til hver valgt mappe genereres automatisk og vises i tekstboksen øverst i denne dialog.

Det er også muligt at få scannet en specifik mappe, mens alle dens undermapper er undtaget fra denne scanning. Det gør du ved at skrive et minustegn "**-**" foran den automatisk genererede sti (*se skærmbillede*). Brug parameteren "!" for at undtage hele mappen fra scanning.

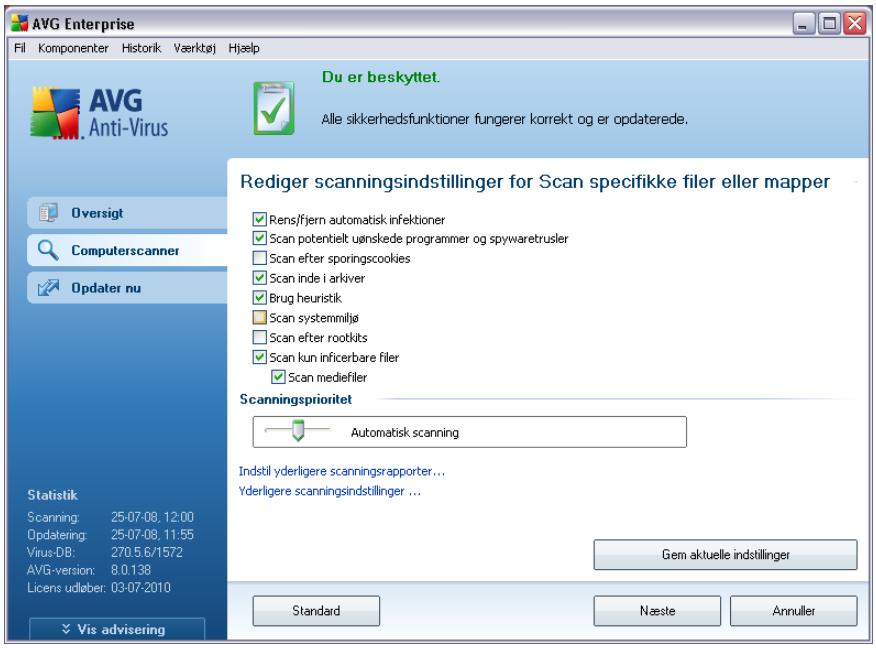
For til sidst at køre scanningen, skal du trykke på knappen ***Start scanning***. Selve scanningsprocessen er grundlæggende magen til scanning af hele computeren.



Redigering af scanningskonfiguration

Du har mulighed for at redigere de foruddefinerede standardindstillinger for ***Scanning af specifikke filer eller mapper***. Tryk på linket ***Rediger scanningsindstillinger*** for at komme til dialogen ***Rediger scanningsindstillinger***

for Scan specifikke filer eller mapper*. *Det anbefales at bevare standardindstillingerne, medmindre du har en god grund til at ændre dem!

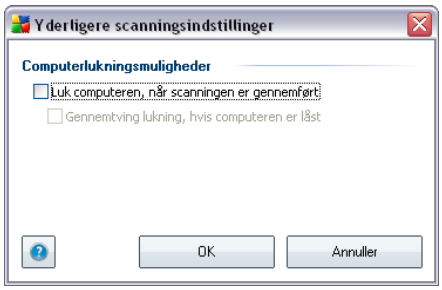


- ***Scanningsparametre*** - i listen over scanningsparametre kan du slå specifikke parametre til/fra efter behov (*se kapitlet AVG Avancerede indstillinger / Scanninger / Scan specifikke filer eller mapper* for yderligere oplysninger om disse indstillinger).

- ***Scanningsprioritet*** - du kan bruge skyderen til at ændre scanningsprioriteten. Som standard er prioriteten indstillet til mellemniveau (*Automatisk scanning*), der optimerer scanningshastigheden og brugen af systemressourcer. Alternativelt kan du køre scanningen langsommere, hvilket betyder, at belastningen på systemressourcerne minimeres (*praktisk, hvis du skal arbejde på computeren, men er ligeglad med, hvor lang tid scanningen tager*), eller hurtigere med øgede krav til systemressourcer (*f.eks. når computeren midlertidigt ikke er i brug*).

- ***Indstil yderligere scanningsrapporter*** - linket åbner en ny ***Scanningsrapporter***-dialo, hvor du kan vælge, hvilke typer af mulige fund, der skal rapporteres:

- ***Yderligere scanningsindstillinger*** - linket åbner en ny ***Computerlukningsmuligheder***-dialog, hvor du kan beslutte, om computeren skal lukkes automatisk, når den igangværende scanning er færdig. Når denne indstilling er bekræftet (***Luk computeren, når scanningen er gennemført***), aktiveres en ny indstilling, som gør det muligt at lukke computeren, selvom den i øjeblikket er låst (***Gennemtving lukning, hvis computeren er låst***).

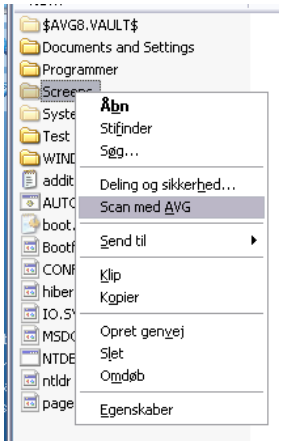


Advarsel: *Disse scanningsindstillinger er magen til parametrene for en ny defineret scanning - som beskrevet i kapitlet* ***AVG Scanning / Scanningsplanlægning / Hvordan der skal scannes****.*

Hvis du beslutter at ændre standardkonfigurationen for ***Scan specifikke filer eller mapper***, kan du gemme den nye indstilling som standardkonfiguration, der skal bruges til alle fremtidige scanninger af specifikke filer eller mapper. Denne konfiguration bliver også anvendt som skabelon for alle dine nye planlagte scanninger (*alle brugerdefinerede scanninger er baserede på den aktuelle konfiguration af Scan specifikke filer eller mapper*).

14.3.Scanning i Windows stifinder

Ud over de foruddefinerede scanninger af hele computeren eler udvalgte områder af den, giver AVG også mulighed for en lynscanning af et specifikt objekt, direkte fra Windows stifinder. Hvis du vil åbne en ukendt fil, og du ikke er sikker på dens indhold, vil du måske have den kontrolleret, når du ønsker det. Følg disse trin:



- Marker den fil (eller mappe), du vil kontrollere i Windows stifinder
- Højreklik med musen på objektet for at åbne kontekstmenuen
- Vælg ***Scan med AVG*** for at få AVG til at scanne filen

14.4.Kommandolinjescanning

I **AVG 8.5 Anti-virus plus firewall** er der mulighed for at køre scanningen fra kommandolinjen. Du kan for eksempel bruge denne mulighed på servere, eller når du opretter et batchscript, der skal køres automatisk efter opstart af computeren. Fra kommandolinjen kan du køre scanningen med de fleste parametre, ligesom i AVG's grafiske brugerflade.

For at køre AVG-scanning fra kommandolinjen skal du køre følgende kommando i den mappe, hvor AVG er installeret:

- ***avgscanx*** for 32 bit-operativsystemer
- ***avgscana*** for 64 bit-operativsystemer

Kommandoens syntaks

Kommandoens syntaks følger:

- ***avgscanx /parameter*** ... f.eks. ***avgscanx /comp*** for scanning af hele whole computeren

- ***avgscanx /parameter /parameter*** .. med flere parametre skal disse opstilles på linje og adskilles med et mellemrum og en skråstreg

- hvis en parameter kræver at en specifik værdi angives (f.eks. ***/scan***-parameteren, som kræver oplysninger om, hvilke udvalgte områder af computeren, der skal scannes, og du skal oplyse en nøjagtig sti til den valgte del), opdeles værdierne med kommaer, for eksempel: ***avgscanx /scan=C:\,D:***

Scanningsparametre

For at få vist en komplet oversigt over tilgængelige parametre skal du indtaste den pågældende kommando med parameteren /? eller /HELP (f.eks. ***avgscanx /?***). Den eneste obligatoriske parameter er /SCAN for at specificere, hvilke dele af computeren, der skal scannes. Se oversigt over kommandolinjeparametre for en mere detaljeret forklaring af mulighederne.

Tryk på ***Enter*** for at køre scanningen. Under scanningen kan du stoppe processen med ***Ctrl+C*** eller ***Ctrl+Pause***.

CMD-scanning kørt fra den grafiske brugerflade

Når du start computeren i Windows Fejlsikret tilstand, er der også mulighed for at køre kommandolinjescanningen fra den grafikse brugerflade. Selve scanningen køres fra kommandolinjen, dialogen ***Kommandolinjeforfatter*** gør det kun muligt at angive de fleste scanningsparametre i den komfortable grafiske brugerflade.

Siden dialogen kun er tilgængelig i Windows Fejlsikret tilstand, bedes du se i hjælpefilen, der åbnes direkte fra dialogen, for en detaljeret beskrivelse af den.

14.4.1.CMD-scanningsparametre

Herunder findes en liste over alle parametre, der kan anvendes til kommandolinjescanning:

- ***/SCAN*** Scan specifille filer eller mapper /SCAN=sti;sti (f.eks. /SCAN=C:\;D:\)
- ***/COMP*** Scan hele computeren
- ***/HEUR*** Brug heuristisk analyse

- ***/EXCLUDE*** Udeluk sti eller filer fra scanning
- ***/@*** Kommandofil /fil navn/
- ***/EXT*** Scan disse filtypenavne /for eksempel EXT=EXE,DLL/
- ***/NOEXT*** Scan ikke disse filtypenavne /for eksempel NOEXT=JPG/
- ***/ARC*** Scan arkiver
- ***/CLEAN*** Rens automatisk
- ***/TRASH*** Flyt inficerede filer til Virus Vault
- ***/QT*** Lyntest
- ***/MACROW*** Rapporter makroer
- ***/PWDW*** Rapporter adgangskodebeskyttede filer
- ***/IGNLOCKED*** Ignorer låste filer
- ***/REPORT*** Rapporter til fil /filnavn/
- ***/REPAPPEND*** Føj til rapportfilen
- ***/REPOK*** Rapporter ikke inficerede filer som OK
- ***/NOBREAK*** Tillad ikke afbrydelse med CTRL-BREAK
- ***/BOOT*** Aktiver MBR/BOOT-kontrol
- ***/PROC*** Scan aktive processer
- ***/PUP*** Rapporter "Potentielt uønskede programmer"
- ***/REG*** Scan registreringsdatabase
- ***/COO*** Scan cookies
- ***/?*** Vis hjælp om dette emne
- ***/HELP*** Vis hjælp om dette emne
- ***/PRIORITY*** Indstil scanningsprioritet /Lav, Auto, Høj/ (se Avancerede

indstillinger / Scanninger)

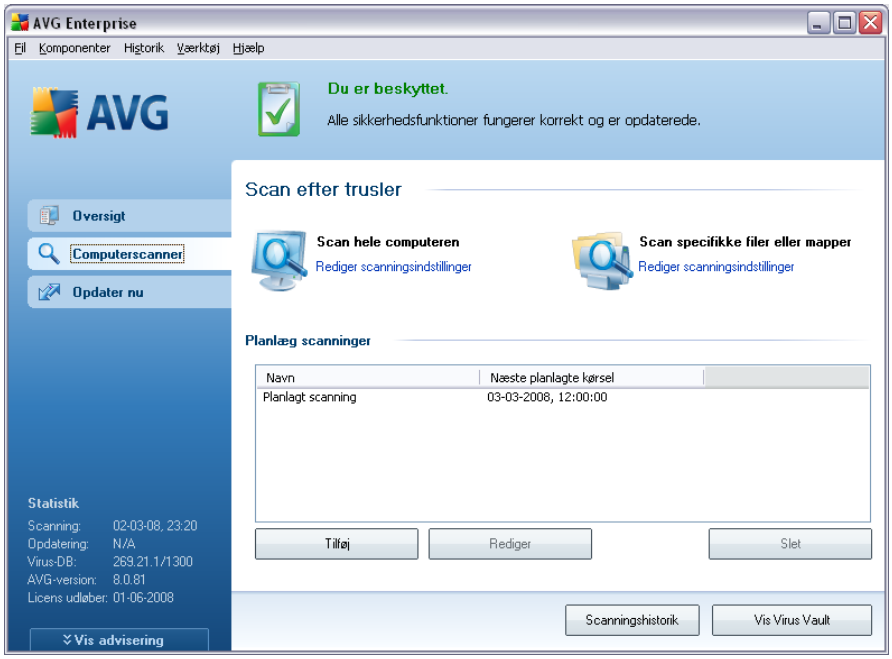
- ***/SHUTDOWN*** Luk computeren, når scanningen er fuldført
- ***/FORCESHUTDOWN*** Gennemtving computerlukning, når scanningen er fuldført
- ***/ADS*** Scan alternative datastrømme (kun NTFS)

14.5.Scanningsplanlægning

Med **AVG 8.5 Anti-virus plus firewall** kan du køre scanninger on demand (for eksempel hvis du har mistanke om, at en infektion er blevet overført til din computer) eller baseret på planlægning. Det anbefales på det kraftigste at køre planlagte scanninger. På denne måde kan du sikre, at din computer er beskyttet mod enhver mulighed for at blive inficeret, og du behøver ikke at tænke på om og hvornår, du skal køre scanningen.

Du bør køre ***Scan hele computeren*** regelmæssigt, mindst en gang ugentligt. Hvis det er muligt, bør du køre en scanning af hele computeren dagligt - som indstillet i standardkonfigurationen for scanningsplanlægning. Hvis computeren er "altid tændt", kan du planlægge scanninger uden for arbejdstiden. Hvis computeren er slukket af og til, kan du planlægge scanninger til at blive udført ved opstart af computeren, hvis opgaven ikke blev udført.

Se AVG's scanningsgrænseflade og finde sektionen med navnet ***Planlæg scanninger*** for at oprette nye scanningsplaner:



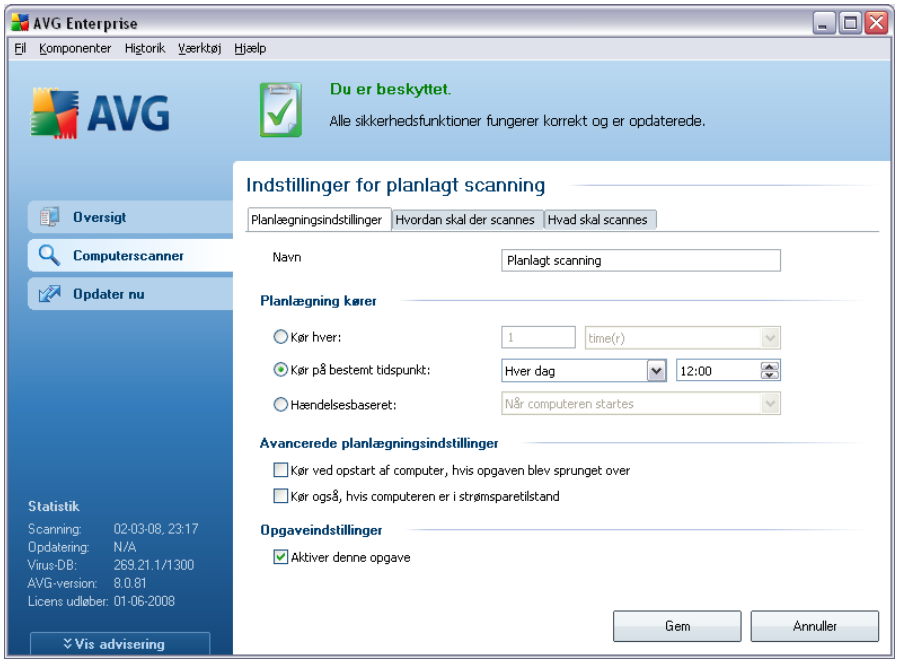
Betjeningsknapper for scanningsplanlægning

I redigeringssektionen findes følgende betjeningsknapper:

- ***Tilføj scanningsplan*** - knappen åbner dialogboksen ***Indstillinger for planlagt scanning*** fanen ***Planlægningsindstillinger***. I denne dialogboks kan du angive parametrene til den nye definerede test.
- ***Rediger scanningsplan*** - denne knap kan kun bruges, hvis du i forvejen har valgt en eksisterende test fra listen over planlagte test. I dette tilfælde vises knappen som aktiv, og du kan klikke på den for at skifte til dialogboksen ***Indstillinger for planlagt scanning*** fanen ***Planlægningsindstillinger***. Her er parametrene for den valgte test allerede angivet og kan redigeres.
- ***Slet scanningsplan*** - denne knap er også aktiv, hvis du i forvejen har valgt en eksisterende test fra listen over planlagte test. Denne test kan så slettes fra listen ved at klikke på betjeningsknappen. Du kan imidlertid kun fjerne dine egne test. ***Scanningsplan for hele computeren***, der er foruddefineret i standardindstillingerne, kan ikke slettes.

14.5.1.Planlægningsindstillinger

Hvis du vil planlægge en ny test og regelmæssig kørsel af den, skal du åbne dialogboksen ***Indstillinger for planlagt test***. Dialogboksen er opdelt i tre faner: ***Planlægningsindstillinger*** - *se nedenstående billede* (standardfanen, du automatisk viderestilles til), ***Hvordan der skal scannes*** og ***Hvad skal scannes***.



På fanen ***Planlægningsindstillinger*** kan du først markere/afmarkere elementet ***Aktiver denne opgave*** for helt enkelt at deaktivere den planlagte test midlertidigt, og slå den til igen, når behovet opstår.

Navngiv derefter den scanning, du skal til at oprette og planlægge. Indtast navnet i tekstfeltet ved elementet ***Navn***. Prøv at bruge korte, beskrivende og passende navne på scanninger for at gøre det nemmere at genkende scanningen senere.

Eksempel: *Det er ikke passende at kalde scanningen "Ny scanning" eller "Min scanning", da disse navne ikke angiver, hvad scanningen egentlig kontrollerer. Et eksempel på et godt, beskrivende navn kunne derimod være "Systemområdescanning" osv. Det er heller ikke nødvendigt at angive i scanningens navn, om det er en scanning af hele computeren eller blot en scanning af udvalgte filer eller mapper - dine egne scanninger vil altid være en specifik version af scanning af udvalgte filer eller mapper.*

I denne dialog kan du yderligere definere følgende parametre for scanningen:

- ***Planlæg kørsel*** - angiv tidsintervallet for kørsel af den nye planlagte scanning. Timingen kan enten defineres med gentaget kørsel af scanningen efter et vist tidsrum (***Kør hver ...***) eller ved at definere en nøjagtig dato og klokkeslæt (***Kør på specifikt klokkeslæt ...***), eller muligvis ved at definere en hændelse, der knyttes til kørsel af scanningen (***Hændelsesbaseret ved opstart af computeren***).

- ***Avancerede planlægningsindstillinger*** - i denne sektion kan du definere, hvilke betingelser scanningen skal/ikke skal køres under, hvis computeren er i strømsparetilstand eller helt slukket.

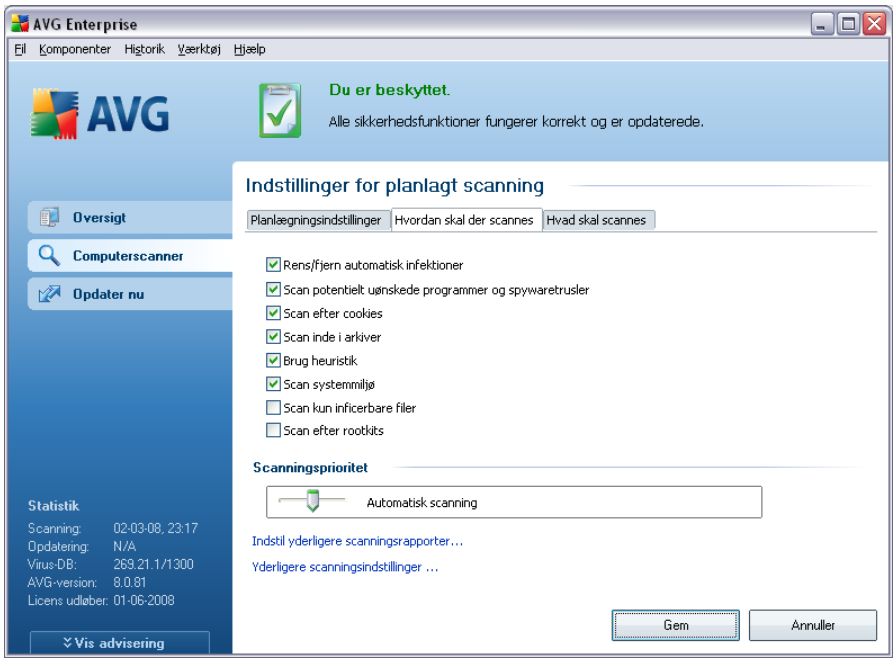
Betjeningsknapper i dialogen Indstillinger for planlagt scanning

Der er to betjeningsknapper på hver af de tre faner i dialogen ***Indstillinger for planlagt scanning*** (***Planlægningsindstillinger***, ***Hvordan der scannes*** og ***Hvad skal scannes***), og de har den samme funktionalitet, uanset hvilken fane du befinder dig på:

- ***Gem*** - gemmer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogen, og skifter tilbage til AVG-scanningsgrænsefladens standarddialog. Hvis du vil konfigurere testparametrene på alle faner, skal du derfor først trykke på knappen for at gemme dem, når du har angivet alle dine krav.

- ***Annuller*** - annullerer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogen, og skifter tilbage til AVG-scanningsgrænsefladens standarddialog.

14.5.2.Hvordan skal der scannes



På fanen ***Hvordan der skal scannes*** findes en liste over scanningsparametre, der valgfrit kan slås til/fra. Som standard er de fleste parametre slået til, og funktionaliteten anvendes under scanningen. Med mindre du har en god grund til at ændre disse indstillinger, anbefaler vi at bevare den forudindstillede konfiguration:

- ***Helbred/fjern infektion automatisk*** - (*slået til som standard*): hvis der identificeres en virus under scanningen, kan den helbredes automatisk, hvis der er en kur tilgængelig. I tilfælde af at den inficerede fil ikke kan helbredes automatisk, eller hvis du beslutter at slå denne mulighed fra, modtager du information, når en virus detekteres, og skal beslutte hvad der skal gøres ved den detekterede infektion. Den anbefalede handling er at fjerne den inficerede fil til Virus Vault.

- ***Scan potentielt uønskede programmer*** - (*slået til som standard*): denne parameter kontrollerer Anti-virus-funktionaliteten, der tillader detektering af potentielt uønskede programmer (*eksekverbare filer, der kan køre som spyware eller adware*), og disse kan derefter blokeres eller fjernes.

- ***Scan efter sporingscookies*** - (*slået til som standard*): Denne parameter i Anti-spyware-komponenten definerer, at cookies skal detekteres under scanningen (*HTTP-cookies anvendes til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på*

webstedet eller indhold i deres elektroniske indkøbsvogne).

- ***Scan inde i arkiver*** - (*slået til som standard*): denne parameter definerer, at scanningen skal kontrollere alle filer, også hvis de er pakket i en form for arkiv, f.eks. ZIP, RAR, ...

- ***Brug heuristik*** - (*slået til som standard*): heuristisk analyse (*dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø*) er en af metoderne, der anvendes til detektering af virus under scanningen.

- ***Scan systemmiljø*** - (*slået til som standard*): scanningen kontrollerer også computerens systemområder.

- ***Scan efter rootkits*** - marker dette punkt, hvis du vil inkludere rootkit-detektering i scanningen af hele computeren. Rootkit-detektering er også tilgængelig individuelt i ***Anti-rootkit***-komponenten;

    - ***Scan kun inficerbare filer*** - (*slået fra som standard*): med denne valgmulighed slået til bliver scanningen ikke udført på filer, der ikke kan inficeres. Det kan for eksempel være visse almindelige tekstfiler og andre ikkeeksekverbare filer.

I sektionen ***Scanningsprioritet*** kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne indstillingsværdi sat til middelniveauet af automatisk ressourceforbrug. Hvis du vil have scanningen til at køre hurtigere, tager det kortere tid, men forbruget af systemressourcer øges markant under kørslen, og gør de andre aktiviteter på pc'en langsommere (*denne indstilling kan anvendes, når computeren er tændt, men der i øjeblikket ikke er nogen, der arbejder med den*). På den anden side kan du reducere forbruget af systemressourcer ved at forlænge scanningens varighed.

Bemærk: *Som standard er scanningskonfigurationen indstillet til optimal ydelse. Med mindre du har en god grund til at ændre scanningsindstillingerne, anbefales det på det kraftigste at bevare den forudindstillede konfiguration. Ændringer i konfigurationen bør kun udføres af erfarne brugere: Se dialogen* ***Avancerede indstillinger****, der findes via systemmenupunktet* ***Filer / Avancerede indstillinger*** *for yderligere indstillinger af scanningskonfigurationen.*

Betjeningsknapper i dialogen Indstillinger for planlagt scanning

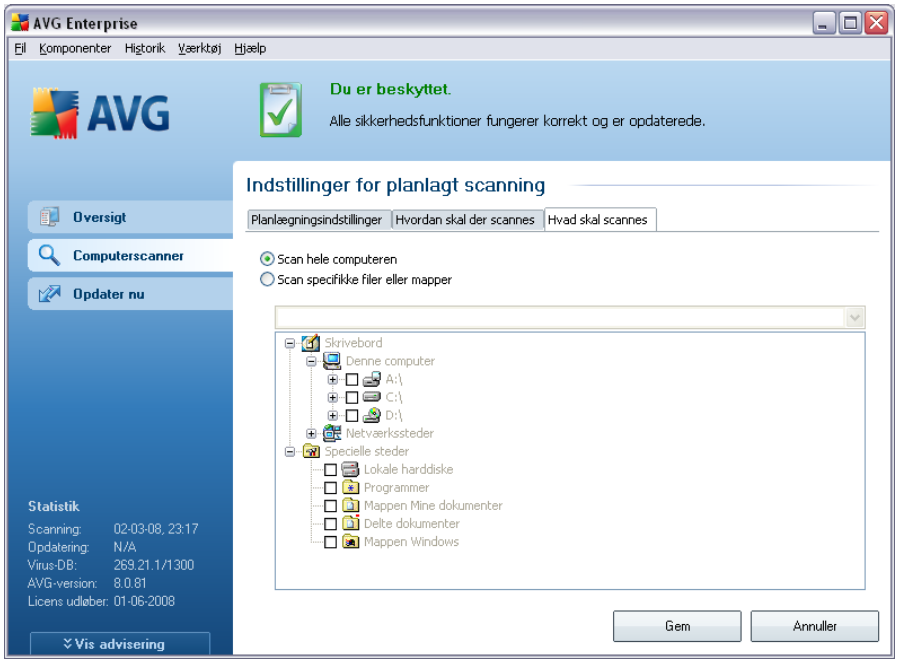
Der er to betjeningsknapper på hver af de tre faner i dialogen ***Indstillinger for planlagt scanning*** (***Planlægningsindstillinger***, ***Hvordan der scannes*** og ***Hvad skal scannes***), og de har den samme funktionalitet, uanset hvilken fane du befinder

dig på:

- ***Gem*** - gemmer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogen, og skifter tilbage til AVG-scanningsgrænsefladens standarddialog. Hvis du vil konfigurere testparametrene på alle faner, skal du derfor først trykke på knappen for at gemme dem, når du har angivet alle dine krav.

- ***Annuller*** - annullerer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogen, og skifter tilbage til AVG-scanningsgrænsefladens standarddialog.

14.5.3.Hvad skal scannes



På fanen ***Hvad skal scannes*** kan du definere, om du vil planlægge scanning af hele computeren eller scanning af specifikke filer eller mapper. Hvis du vælger scanning af specifikke filer eller mapper, aktiveres træstrukturen nederst i denne dialogboks, og du kan angive mapper, der skal scannes.

Betjeningsknapper i dialogen Indstillinger for planlagt scanning

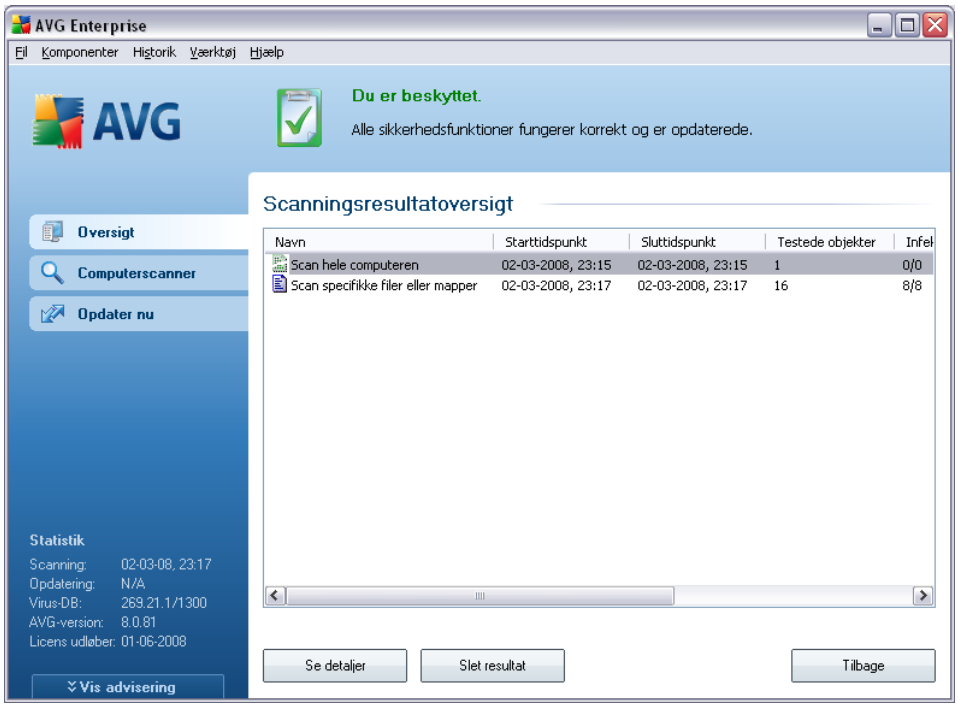
Der er to betjeningsknapper på hver af de tre faner i dialogen ***Indstillinger for***

planlagt scanning (***Planlægningsindstillinger***, ***Hvordan der scannes*** og ***Hvad skal scannes***), og de har den samme funktionalitet, uanset hvilken fane du befinder dig på:

- ***Gem*** - gemmer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogen, og skifter tilbage til AVG-scanningsgrænsefladens standarddialog. Hvis du vil konfigurere testparametrene på alle faner, skal du derfor først trykke på knappen for at gemme dem, når du har angivet alle dine krav.

- ***Annuller*** - annullerer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogen, og skifter tilbage til AVG-scanningsgrænsefladens standarddialog.

14.6.Scanningsresultatoversigt



Dialogboksen ***Scanningsresultatoversigt*** åbnes fra AVG-scanningsgrænsefladen via knappen ***Scanningshistorik***. Dialogboksen indeholder en liste over alle tidligere kørte scanninger og oplysninger om resultatet af dem:

- ***Navn*** - scanningsnavn. Det kan enten være navnet på en af de

foruddefinerede scanninger eller et navn, du har givet din egen planlagte scanning. Hvert navn inkluderer et ikon, der angiver scanningsresultatet:

 - grønt ikon betyder, at der ikke blev detekteret infektioner under scanningen

 - blåt ikon betyder, at der blev detekteret en infektion under scanningen, men det inficerede objekt blev fjernet automatisk

 - rødt ikon advarer om, at der blev detekteret en infektion under scanningen, og at den ikke kunne fjernes!

Ikonerne kan enten være hele eller skåret midt over - det hele ikon står for en scanning, der blev gennemført og afsluttet korrekt. Det overskårne ikon betyder, at scanningen blev annulleret eller afbrudt.

Bemærk: *Se dialogboksen **Scanningsresultater**, der åbnes med knappen **Vis detaljer** (nederst i denne dialogboks) for yderligere oplysninger om hver scanning.*

- ***Starttidspunkt*** - dato og klokkeslæt, hvor scanningen blev kørt
- ***Sluttidspunkt*** - dato og klokkeslæt, hvor scanningen blev afsluttet
- ***Testede objekter*** - antallet af objekter, der blev kontrolleret under scanningen
- ***Infektioner*** - antallet af virusinfektioner, der blev detekteret / fjernet
- ***Spyware*** - antallet af spyware, der blev detekteret / fjernet
- ***Scanningslogoplysninger*** - oplysninger vedrørende scanningens forløb og resultat (typisk når den aflsuttes eller afbrydes)

Betjeningsknapper

Betjeningsknapperne i dialogboksen ***Scanningsresultatoversigt*** er:

- ***Vis detaljer*** - denne knap er kun aktiv, hvis en specifik scanning er valgt i ovenstående oversigt. Klik på den for at skifte til dialogboksen ***Scanningsresultater*** for at se detaljerede data for den valgte scanning
- ***Slet resultat*** - denne knap er kun aktiv, hvis en specifik scanning er valgt i

ovenstående oversigt. Klik på den for at fjerne det valgte element fra scanningsresultatoversigten

- ***Tilbage*** - skifter tilbage til standarddialogboksen for AVG's scanningsgrænseflade

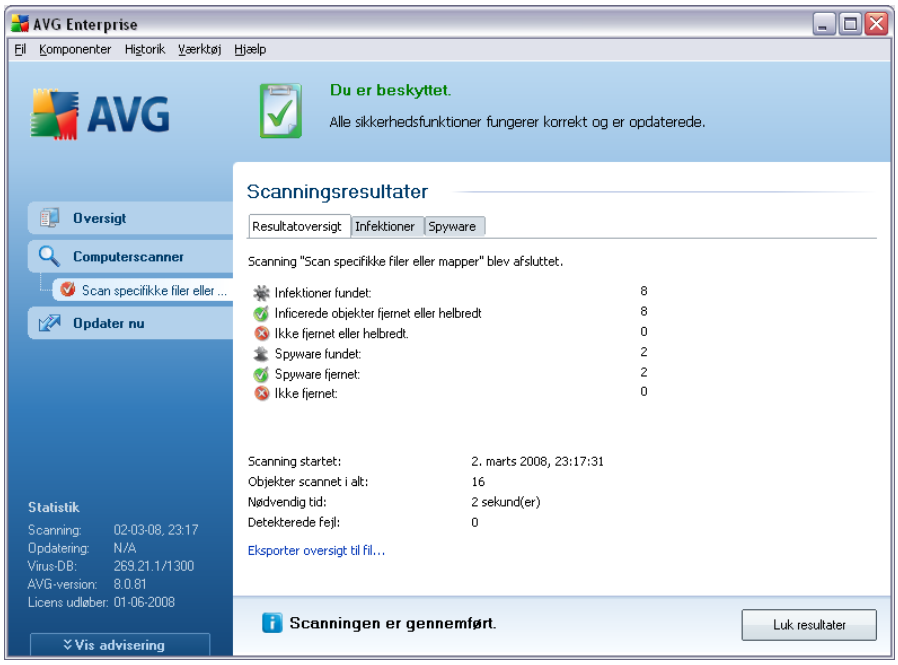
14.7.Scanningsresultatdetaljer

Hvis der er valgt en specifik scanning i dialogboksen ***Scanningsresultatoversigt***, kan du klikke på knappen ***Vis detaljer*** for at skifte til dialogboksen ***Scanningsresultater*** med detaljerede data om forløb og resultat for den valgte scanning.

Dialogboksen er yderligere opdelt i flere faner:

- ***Resultatoversigt*** - denne fane vises altid og indeholder statistiske data, der beskriver scanningsforløbet
- ***Infektioner*** - denne fane vises kun, hvis der blev detekteret en virusinfektion under scanningen
- ***Spyware*** - denne fane vises kun, hvis der blev detekteret spyware under scanningen
- ***Advarsler*** - denne fane vises kun, hvis der blev detekteret objekter, der ikke kunne scannes, under scanningen
- ***Rootkits*** - denne fane vises kun, hvis der blev detekteret rootkits under scanningen
- ***Information*** **-** denne fane vises kun, hvis der blev detekteret potentielle trusler, men disse ikke kunne klassificeres i nogen af de ovenstående kategorier. Fanen indeholder da en advarselsmeddelelse om fundet

14.7.1.Fanen Resultatoversigt



På fanen ***Scanningsresultater*** kan du finde detaljeret statistik med oplysninger om:

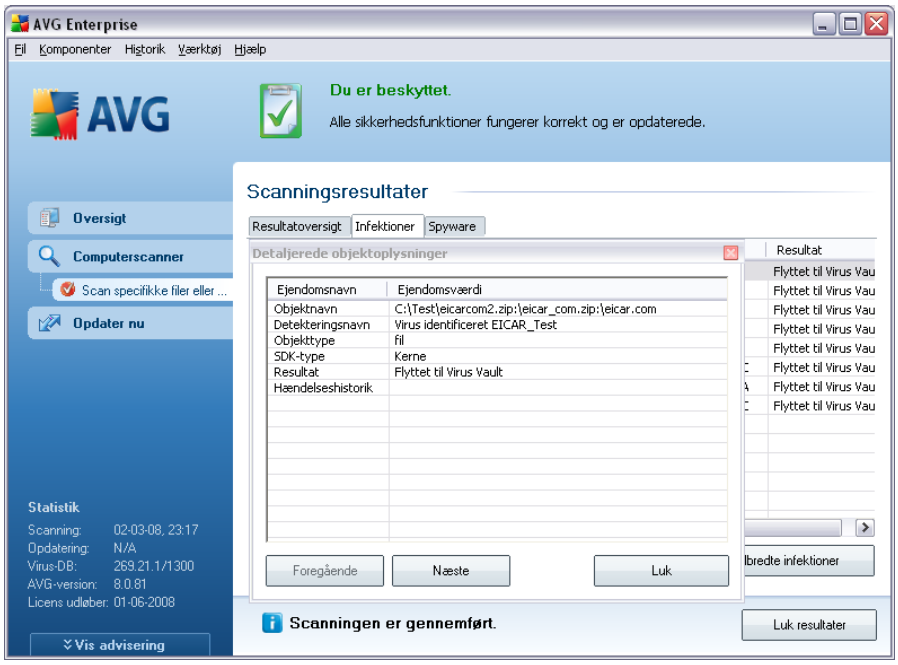
- detekterede virusinfektioner / spyware
- fjernede virusinfektioner / spyware
- antallet af virusinfektioner / spyware, der ikke kan fjernes eller helbredes

Desuden findes der oplysninger om dato og nøjagtigt klokkeslæt for kørsel af scanningen, det totale antal scannede objekter, canningens varighed og antallet af fejl, der opstod under scanningen.

Betjeningsknapper

Der er kun en betjenignsknap til rådighed i denne dialogboks. Knappen ***Luk resultater*** vender tilbage til dialogboksen ***Scanningsresultatoversigt***.

14.7.2.Fanen Infektioner



Fanen ***Infektioner*** vises kun i dialogen ***Scanningsresultater***, hvis der blev detekteret en virusinfektion under scanningen. Fanen består af tre sektioner, der indeholder følgende oplysninger:

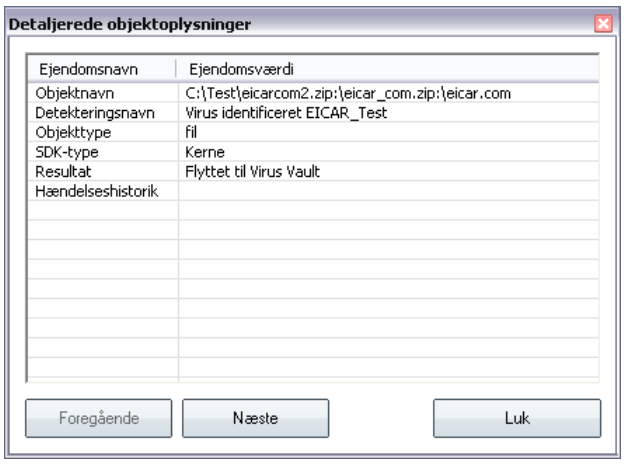
- ***Fil*** - fuld sti til det inficerede objekts oprindelige placering
- ***Infektioner*** - navn på den detekterede virus (*se Virus-opslagsværket online for yderligere oplysninger om specifikke vira*)
- ***Resultat*** - definerer den aktuelle status for det inficerede objekt, der blev detekteret under scanningen:
    - ***Inficeret*** - det inficerede objekt blev detekteret og efterladt på sin oprindelige placering (*for eksempel hvis du har slået automatisk helbredelse fra i en specifik scanningsindstilling*)
    - ***Helbredt*** - det inficerede objekt blev helbredt automatisk og efterladt på sin oprindelige placering
    - ***Flyttet til Virus Vault*** - det inficerede objekt blev flyttet til karantæne i ***Virus Vault***

- ***Slettet*** - det inficerede objekt blev slettet
- ***Tilføjet til PUP-undtagelser*** - fundet blev evalueret som en undtagelse og føjet til listen over PUP-undtagelser (*konfigureret i dialogen **PUP-undtagelser** i avancerede indstilliger*)
- ***Låst fil - ikke testet*** - det pågældende objekt er låst, og AVG er derfor ikke i stand til at scanne det
- ***Potentielt farligt objekt*** - objektet blev detekteret som potentielt farligt men ikke inficeret (*det kan for eksempel indeholde makroer*). Oplysningen skal kun betragtes som en advarsel
- ***Genstart påkrævet for at afslutte handlingen*** - det inficerede objekt kan ikke fjernes. For at fjerne det fuldstændigt skal du genstarte computeren

Betjeningsknapper

Der findes tre betjeningsknapper i denne dialog:

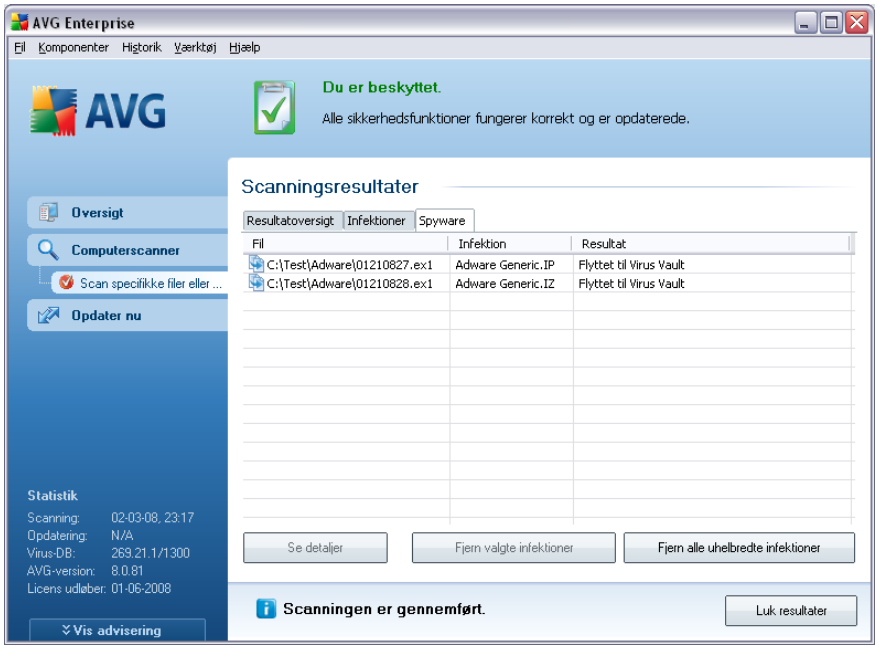
- ***Vis detaljer*** - knappen åbner et nyt dialogvindue med navnet ***Detaljerede oplysninger om scanningsresultat***:



I denne dialog finder du oplysninger om placeringen af det detekterede inficerede objekt (***Egenskabsnavn***). Med knapperne ***Forrige*** / ***Næste*** kan du vise oplysninger om specifikke fund. Brug knappen ***Luk*** til at lukke dialogen.

- ***Fjern valgte infektioner*** - brug knappen til at flytte de valgte fund til ***Virus Vault***
- ***Fjern alle uhelbredte infektioner*** - denne knap sletter alle fund, der ikke kan helbredes eller flyttes til ***Virus Vault***
- ***Luk resultater*** - lukker oversigten over detaljerede oplysninger og vender tilbage til dialogen ***Scanningsresultatoversigt***

14.7.3.Fanen Spyware



Fanen ***Spyware*** vises kun i dialogen ***Scanningsresultater***, hvis der blev detekteret spyware under scanningen. Fanen består af tre sektioner, der indeholder følgende oplysninger:

- ***Fil*** - fuld sti til det inficerede objekts oprindelige placering
- ***Infektioner*** - navn på den detekterede spyware (*se* ***Virusencyklopædien*** *online for yderligere oplysninger om specifikke vira*)
- ***Resultat*** - definerer den aktuelle status for det objekt, der blev detekteret under scanningen:
    - ***Inficeret*** - det inficerede objekt blev detekteret og efterladt på sin

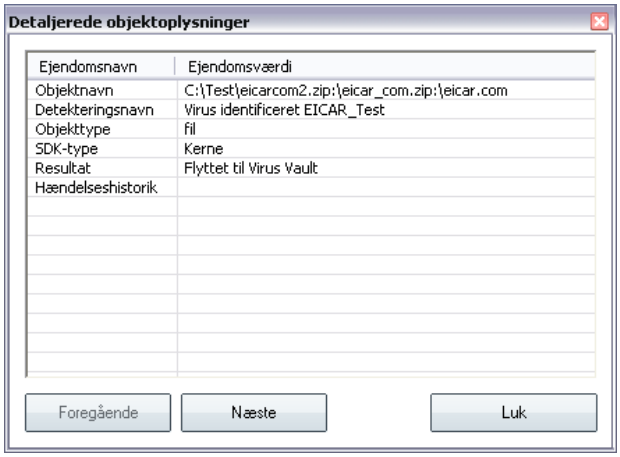
oprindelige placering (for eksempel hvis du har slået automatisk helbredelse fra i en specifik scanningsindstilling)

- ***Helbredt*** - det inficerede objekt blev helbredt automatisk og efterladt på sin oprindelige placering
- ***Flyttet til Virus Vault*** - det inficerede objekt blev flyttet til karantæne i ***Virus Vault***
- ***Slettet*** - det inficerede objekt blev slettet
- ***Tilføjet til PUP-undtagelser*** - fundet blev evalueret som en undtagelse og føjet til listen over PUP-undtagelser (*konfigureret i dialogen **PUP-undtagelser** i avancerede indstillinger*)
- ***Låst fil - ikke testet*** - det pågældende objekt er låst, og AVG er derfor ikke i stand til at scanne det
- ***Potentielt farligt objekt*** - objektet blev detekteret som potentielt farligt men ikke inficeret (det kan for eksempel indeholde makroer). Oplysningen er kun en advarsel
- ***Genstart påkrævet for at afslutte handlingen*** - det inficerede objekt kan ikke fjernes. For at fjerne det fuldstændig skal du genstarte computeren

Betjeningsknapper

Der findes tre betjeningsknapper i denne dialog:

- ***Vis detaljer*** - knappen åbner et nyt dialogvindue med navnet ***Detaljerede oplysninger om scanningsresultat***:



I denne dialog finder du oplysninger om placeringen af det detekterede inficerede objekt (***Ejendomsnavn***). Med knapperne ***Forrige*** / ***Næste*** kan du vise oplysninger om specifikke fund. Brug knappen ***Luk*** til at forlade denne dialog.

- ***Fjern valgte infektioner*** - brug knappen til at flytte de valgte fund til ***Virus Vault***
- ***Fjern alle uhelbredte infektioner*** - denne knap sletter alle fund, der ikke kan helbredes eller flyttes til ***Virus Vault***
- ***Luk resultater*** - lukker oversigten over detaljerede oplysninger og vender tilbage til dialogen ***Scanningsresultatoversigt***

14.7.4.Fanen Advarsler

Fanen ***Advarsler*** viser oplysninger om "mistænkelige" objekter (*typiske filer*), der detekteres under scanningen. Når ***Resident Shield*** detekterer disse filer, bliver adgangen til dem blokeret. Typiske eksempler på denne type fund er skjulte filer, cookies, mistænkelige registreringsdatabasenøgler, adgangskodebeskyttede dokumenter eller arkiver osv.

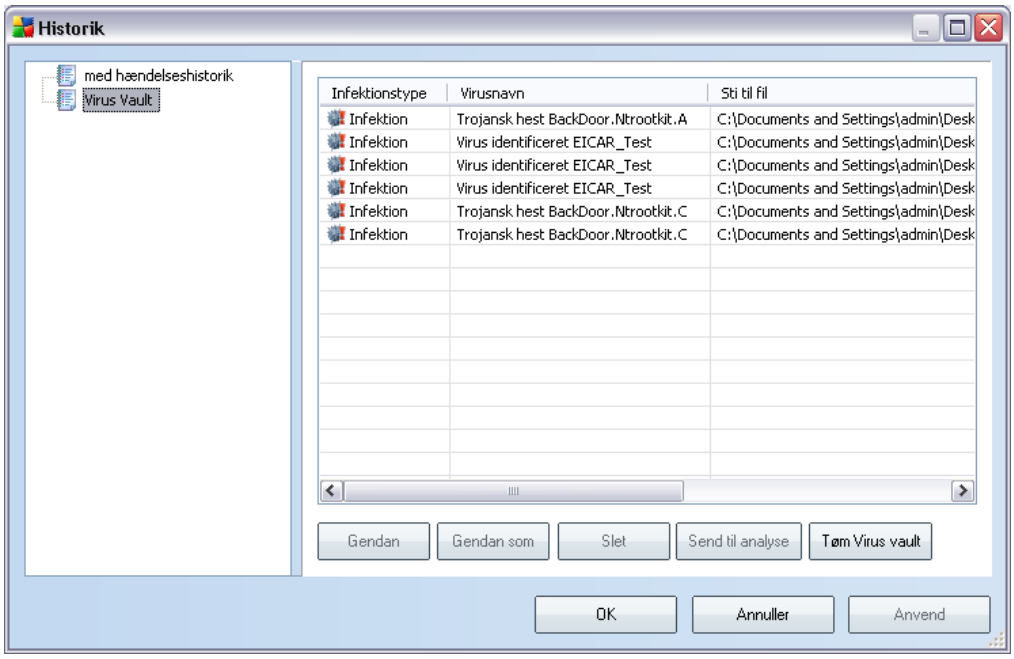
14.7.5.Fanen Rootkits

Fanen ***Rootkits*** viser oplysninger om rootkits, der detekteres under scanningen. Dens opbygning er grundlæggende den samme som ***fanen Infektioner*** eller ***fanen Spyware***.

14.7.6.Fanen Information

Fanen ***Information*** indeholder data om "fund", der ikke kan kategoriseres som infektioner, spyware osv. De kan heller ikke med vished kaldes farlige, men du bør være opmærksom på dem. Alle data på denne fane er kun med henblik på information.

14.8.Virus Vault



Virus Vault er et sikkert miljø til administration af mistænkelige/inficerede objekter, der er detekteret under AVG-test. Hvis et inficeret objekt detekteres under scanning, og AVG ikke automatisk kan helbrede det, bliver du spurgt om, hvad der skal gøres med det mistænkelige objekt. Den anbefalede løsning er at flytte objektet til ***Virus Vault*** for yderligere behandling.

Virus Vault-grænsefladen åbnes i et separat vindue og indeholder en oversigt over oplysninger om inficerede objekter:

- ***Infektionstype*** - skelner mellem fundtyper baseret på deres infektionsniveau (*alle anførte objekter kan være definitivt eller potentielt inficerede*)
- ***Virusnavn*** - angiver navnet på den detekterede infektion i henhold til Virusencyklopædien (online)

- ***Sti til fil*** - fuld sti til den detekterede inficerede fils oprindelige placering
- ***Oprindeligt objektnavn*** - alle detekterede objekter, der er anført i tabellen, er mærket med standardnavnet, der tildeles af AVG under scanningen. I tilfælde af, at bojektet havde et specifikt oprindeligt navn, som er kendt (*f. eks. et navn på en vedhæftet fil, der ikke svarer til den vedhæftede fils faktiske indhold*), bliver det oplyst i denne kolonne.
- ***Lagringsdato*** - dato og klokkeslæt den mistænkelige fil blev detekteret og fjernet til ***Virus Vault***

Betjeningsknapper

Følgende betjeningsknapper er til rådighed fra ***Virus Vault***-grænsefladen:

- ***Gendan*** - flytter den inficerede fil tilbage til sin oprindelige placering på disken
- ***Gendan som*** - i tilfælde af, at du beslutter at flytte det detekterede inficerede objekt fra ***Virus Vault*** til en udvalgt mappe, skal du bruge denne knap. Det mistænkelige, detekterede objekt bliver gemt med sit oprindelige navn. Hvis det oprindelige navn ikke er kendt, anvendes standardnavnet.
- ***Slet*** - fjerner den inficerede fil fuldstændig fra ***Virus Vault***
- ***Send til analyse*** - sender den mistænkelige fil til dybere analyse hos AVG's viruslaboratorium
- ***Tøm Vault*** - fjerner alle ***Virus Vault*** indhold helt

15. AVG Opdateringer

15.1. Opdateringsniveauer

Du kan vælge mellem to opdateringsniveauer:

- ***Definitionsopdatering*** indeholder nødvendige ændringer for pålidelig beskyttelse mod virus, spam og malware. Typisk inkluderer dette ikke ændringer af koden, og kun definitionsdatabasen bliver opdateret. Denne opdatering bør anvendes, så snart den er til rådighed.
- ***Programopdatering*** indeholder diverse programændringer, rettelser og forbedringer.

Ved planlægning af en opdatering er det muligt at vælge hvilket prioritetsniveau, der skal downloades og anvendes.

15.2. Opdateringstyper

Der skelnes mellem to opdateringertyper:

- ***Opdatering på forlangende*** er en øjeblikkelig opdatering af AVG, der kan udføres på ethvert tidspunkt, der er behov for det.
- ***Planlagt opdatering*** - i AVG er det også muligt at forudindstille en opdateringsplan. Den planlagte opdatering udføres derefter periodisk, i henhold til den valgte konfiguration. Når nye opdateringsfiler findes det angivne sted, downloades de enten direkte fra internettet eller fra netværksmappen. Hvis der ikke findes nye opdateringer, sker der intet.

15.3. Opdateringsproces

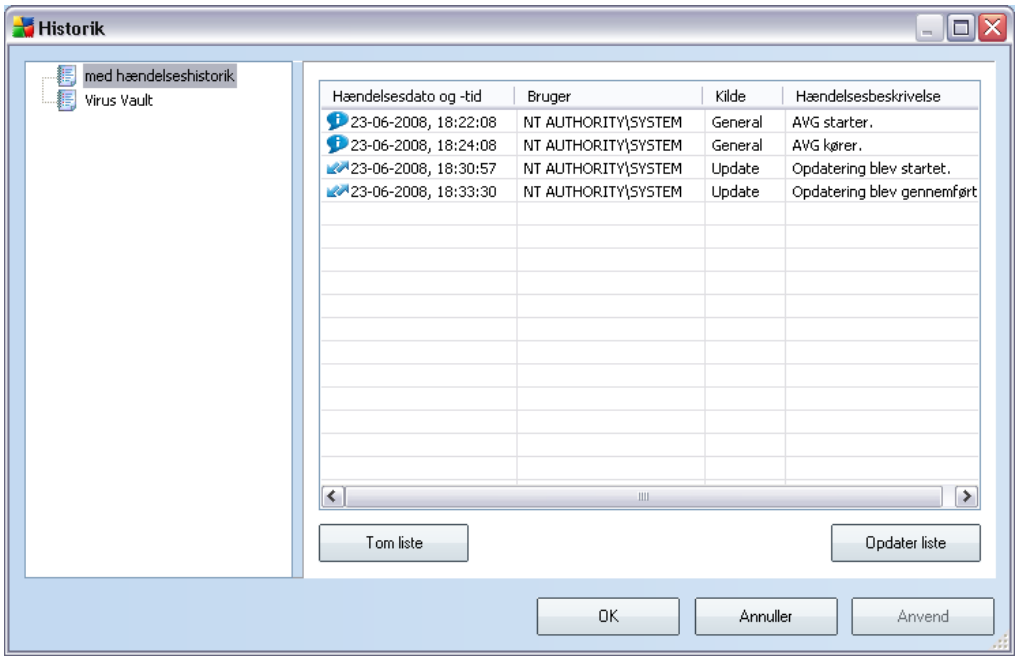
Opdateringsprocessen kan startes med det samme, når behovet opstår, med lynlinket ***Opdater nu***. Dette link er tilgængeligt til enhver tid fra alle dialoger i AVG-brugergrænsefladen. Det anbefales dog stadig på det kraftigste at udføre regelmæssige opdateringer som angivet i opdateringsplanen, der kan redigeres i Opdateringsadministrator-komponenten.

Når du har startet opdateringen, verificerer AVG først, om der er nye tilgængelige opdateringer. Hvis der er det, starter AVG med at downloade dem og kører selve opdateringsprocessen. Under opdateringsprocessen bliver du viderestillet til grænsefladen ***Opdater***, hvor du kan se processens forløb grafisk samt på en oversigt over relevante statistiske parametre (*opdateringsfilens størrelse, modtagne data,*

downloadhastighed, forløbet tid osv.).

***Bemærk**! Før AVG programopdateringen kører, oprettes et systemgendannelsespunkt. I tilfælde af at opdateringsprocessen mislykkes, og dit operativsystem går ned, kan du altid gendanne dit operativsystem i dets oprindelige konfiguration fra dette punkt. Denne indstilling er tilgængelig fra Start / Alle Programmer / Tilbehør / Systemværktøjer / Systemgendannelse. Anbefales kun for erfarne brugere!*

16. Hændelseshistorik



Der er adgang til dialogen ***Hændelseshistorik*** fra systemmenuen via punktet ***Historik/Log over hændelseshistorik***. I denne dialog findes en oversigt over vigtige hændelser, der er sket under brugen af **AVG 8.5 Anti-virus plus firewall**. ***Hændelseshistorik*** registrerer følgende typer hændelser:

- Information om opdateringer af AVG-applikationen
- Scanningsstart, -afslutning eller -stop (inklusive automatisk udførte test)
- Hændelser i forbindelse med virusdetektering (af Resident Shield eller scanning), inklusive forekomststed
- Andre vigtige hændelser

Betjeningsknapper

- ***Tøm liste*** - sletter alle poster i listen over hændelser
- ***Opdater liste*** - opdaterer alle poster i listen over hændelser

17. FAQ og teknisk support

Skulle du støde på problemer med AVG, enten salgsmæssigt eller teknisk, kan du se ***FAQ***-sektionen på AVG's websted på www.avg.com

Hvis du ikke finder hjælp på denne måde, kan du kontakte teknisk support-afdelingen via e-mail. Benyt kontaktformularen, der er adgang til fra systemmenuen via ***Hjælp / Få hjælp online***.