AVG Internet-sikkerhed 2011

Brugervejledning

Dokumentrevision 2011.21 (16.5.2011)

Indhold

1. Introduktion

Denne brugervejledning indeholder omfattende dokumentation til **AVG Internet-sikkerhed 2011**.

Tillykke med dit køb af AVG Internet-sikkerhed 2011!

AVG Internet-sikkerhed 2011 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 Internet-sikkerhed 2011** 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 Internet-sikkerhed 2011**-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.

Alle AVG produkter tilbyder

- Beskyttelse, som er relevant for måden, du bruger din computer og Internettet: netbank og shopping, surfing og søgning, chat og e-mail eller download af filer samt sociale netværker - AVG har et beskyttelsesprodukt, der passer til lige netop dig
- Problemfri beskyttelse, der anvendes af over 110 millioner mennesker verden over, og opretholdes af et globalt netværk af yderst erfarne forskere
- Beskyttelse som bakkes op af ekspertsupport døgnet rundt

2. AVG Installationskrav

2.1. Understøttede operativsystemer

AVG Internet-sikkerhed 2011 er udviklet til at beskytte arbejdsstationer med følgende operativsystemer:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 og x64, alle udgaver)
- Windows 7 (x86 og x64, alle udgaver)

(og muligvis senere servicepakker for specifikke operativsystemer)

***Bemærk**! ID-beskyttelse-komponenten understøttes ikke i Windows XP x64. På dette operativsystem kan du installere AVG Internet-sikkerhed 2011, men kun uden IDP-komponenten.*

2.2. Minimum og anbefalede hardwarekrav

Minimum hardwarekrav for **AVG Internet-sikkerhed 2011**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM
- 750 MB ledig plads på harddisk (af installationsgrunde)

Anbefalede hardwarekrav for **AVG Internet-sikkerhed 2011**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM
- 1400 MB ledig plads på harddisk (af installationsgrunde)

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 (http://www.avg.com/).

Inden du starter installation af AVG, anbefales det kraftigt, at du besøger AVG's websted (http://www.avg.com/) for at se, om der ligger nye installationsfiler. På denne måde kan du være sikker på at installere den nyeste version af AVG Internet-sikkerhed 2011.

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.

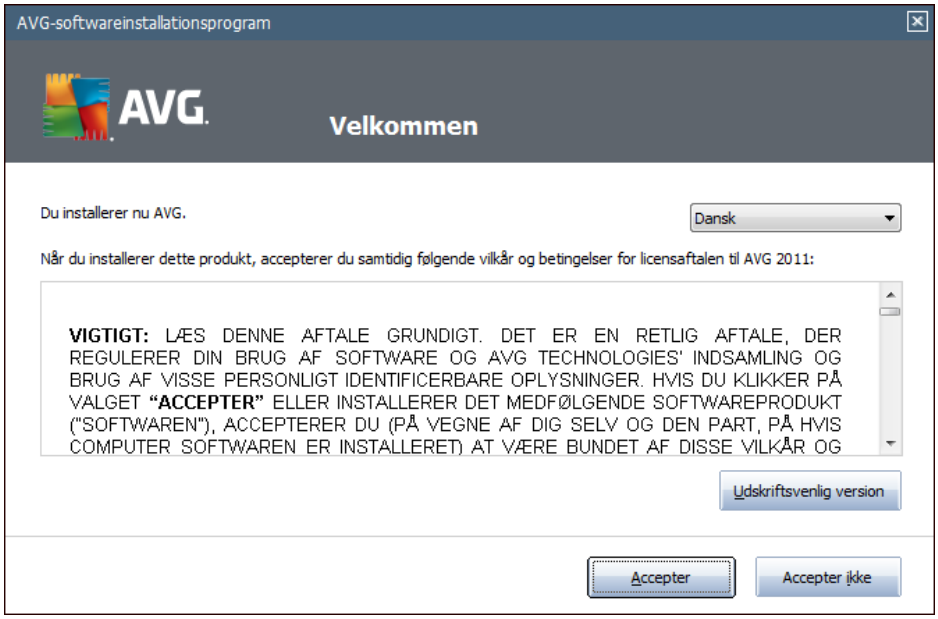
4. AVG Installationsproces

For at installere **AVG Internet-sikkerhed 2011** på din computer skal du hente 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 fra AVG's webside (http://www.avg.com/), sektionen ***Support Center/Download.***

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:

4.1. Velkommen

Installationen starter med dialogvinduet ***Velkommen***. Her kan du vælge det sprog, der skal bruges til installationsprocessen, og standardsproget for AVG-brugergrænsefladen. I øverste del af dialogvinduet findes en rullemenu med listen over sprog, der kan vælges:



OBS! *Her vælger du sprog til installationen. Det valgte sprog vil blive installeret som standardsprog for AVG-brugergrænsefladen sammen med engelsk, som installeres automatisk. Hvis du vil have installeret flere sprog til brugergrænsefladen, skal de angives i en af følgende opsætningsdialoger kaldet* ***Brugerdefinerede indstillinger****.*

Desuden indeholder denne dialog den fulde tekst i AVG-licensaftalen. Læs denne nøje igennem. For at bekræfte, at du har læst, forstået og accepterer aftalerne, skal du trykke på knappen ***Accepter***. Hvis du ikke er enig i licensaftalen skal du klikke på knappen ***Accepter ikke***, og installationsprocessen bliver afsluttet med det samme.

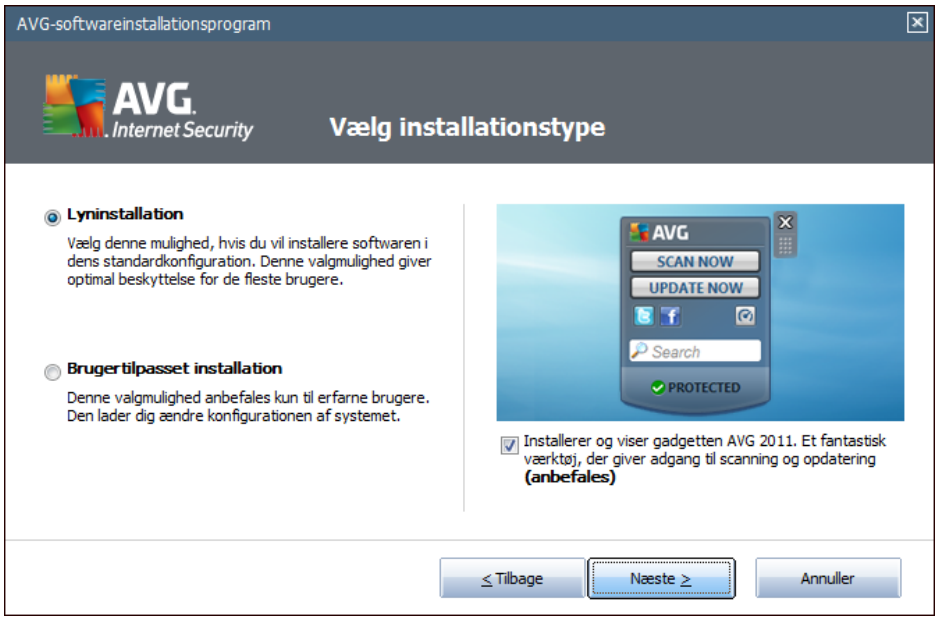
4.2. Aktiver din AVG-licens

I dialogen ***Aktivér din licens*** bliver du bedt om at udfylde dit licensnummer i det pågældende tekstfelt.

Salgsnummeret findes på CD-emballagen i boksen til **AVG Internet-sikkerhed 2011**. Licensnummeret findes i den bekræftelses-e-mail, du modtog, efter du købte **AVG Internet-sikkerhed 2011** 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.

4.3. Vælg installationstype



I dialogen ***Vælg installationstype*** kan du vælge mellem to installationsmuligheder: ***Lyninstallation*** og***Brugertilpasset installation***.

For de fleste brugere anbefales det at holde sig til den standard ***Hurtig installation***, 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. Hvis du har valgt muligheden ***Lyninstallation***, skal du trykke på knappen ***Næste*** for at fortsætte til næste dialog, ***Installér AVG Sikkerhedsværktøjslinje***.

Brugertilpasset installation bør kun anvendes af erfarne brugere, der har en god grund til at installere AVG uden standardindstillingerne, f.eks. for at passe til specifikke systemkrav. Når du har valgt denne mulighed, skal du trykke på knappen ***Næste*** for at fortsætte til dialogen ***Brugerdefinerede indstillinger***.

I højre side af dialogen findes afkrydsningsfeltet, der relaterer til ***AVG gadget*** (*understøttes i Windows Vista/Windows 7*). Hvis du vil installere denne gadget, skal du markere det pågældende afkrydsningsfelt. ***AVG gadget*** vil derefter være tilgængelig fra Windows Sidebar og give dig direkte adgang til de vigtigste funktioner i din **AVG Internet-sikkerhed 2011**, dvs. scanning og opdatering.

4.4. Brugerdefinerede indstillinger

I dialogen ***Brugerdefinerede indstillinger*** kan du konfigurere to installationsparametre:

Destinationsmappe

I afsnittet ***Destinationsmappe*** i dialogen er det meningen, at du skal angive placeringen, hvor **AVG Internet-sikkerhed 2011** 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.

Komponentvalg

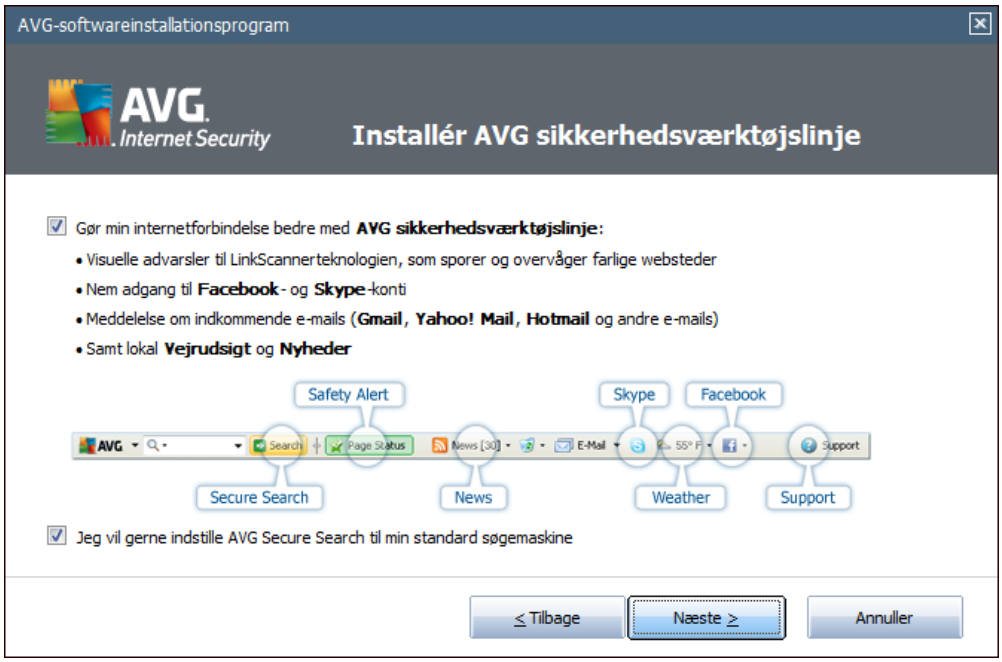
Afsnittet ***Valg af komponenter*** viser en oversigt over alle **AVG Internet-sikkerhed 2011**-komponenter, der kan installeres. Hvis standardindstillingerne ikke passer dig, kan du fjerne/tilføje specifikke komponenter.

Du kan imidlertid kun vælge mellem de komponenter, der medfølger i den AVG-udgave, du har købt!

Markér et element i listen ***Valg af komponenter***, hvorefter en kort beskrivelse af den pågældende komponent vises i højre side af dette afsnit. For detaljerede oplysninger om hver komponents funktioner henvises til kapitlet ***Komponentoversigt*** i denne dokumentation. For at gendanne standardkonfigurationen, der er forudindstillet af softwareleverabdøren, skal du bruge knappen ***Standard***.

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

4.5. Installér AVG Sikkerhedsværktøjslinje

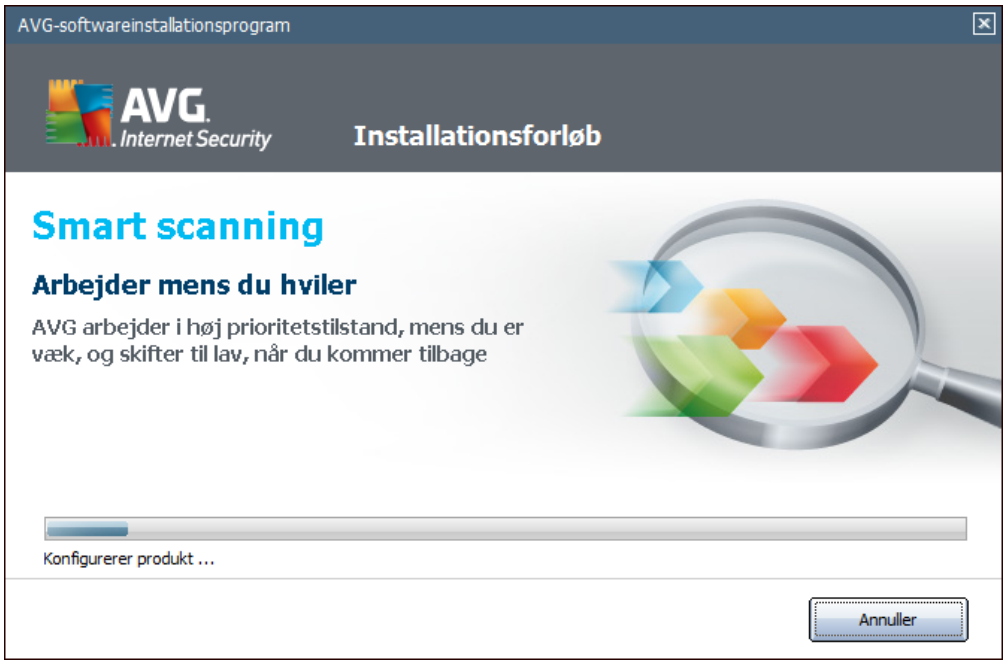


I dialogen ***Installér AVG Sikkerhedsværktøjslinje*** skal du bestemme, om du vil installere ***AVG Sikkerhedsværktøjslinje***. Hvis du ikke ændrer standardindstillingerne, vil denne komponent installeres automatisk i din webbrowser (*aktuelt understøttede browsere er Microsoft Internet Explorer v. 6.0 eller højere og Mozilla Firefox v. 3.0 eller højere*) for at give dig omfattende online beskyttelse, mens du surfer på internettet.

Du har også mulighed for at bestemme, om du vil vælge *AVG Secure Search (powered by Google)* som din standardsøgeudbyder. Hvis dette er tilfældet, skal det pågældende afkrydsningsfelt forblive markeret.

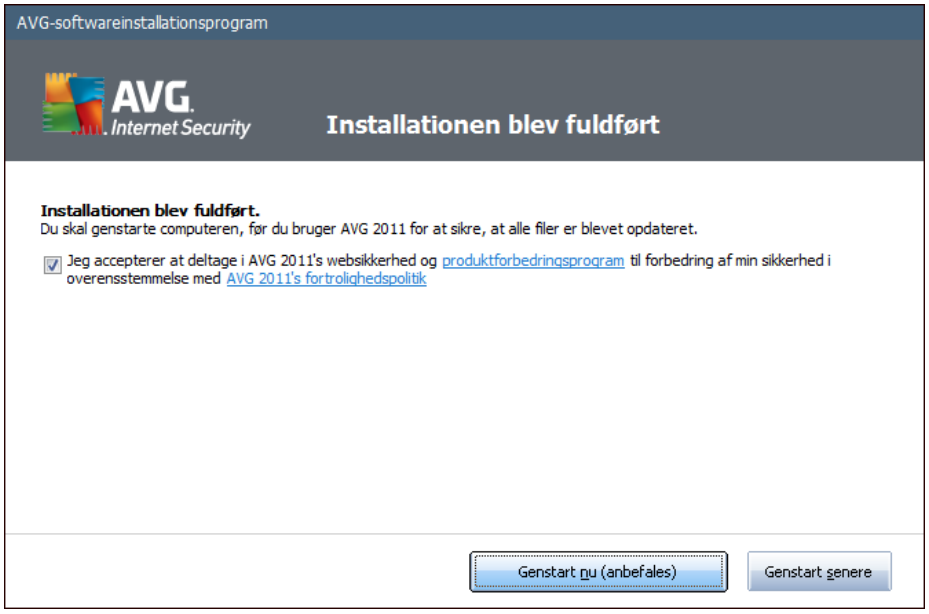
4.6. Installationsforløb

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



Når installationen er slut, bliver du viderestillet til den næste dialog.

4.7. Installationen blev fuldført



Dialogen ***Installationen blev fuldført*** bekræfter, at din **AVG Internet-sikkerhed 2011** er blevet installeret og konfigureret.

I denne dialog skal du angive dine kontaktoplysninger, så du kan modtage alle produktrelaterede oplysninger og nyheder. Under registreringsformularen finder du følgende to valgmuligheder:

- ***Ja, hold mig underrettet om sikkerhedsopdateringer og nyheder samt specielle tilbud på AVG 2011 via e-mail*** - markér afkrydsningsfeltet for at angive, at du vil informeres om nyt inden for Internetsikkerhed, og du vil modtage oplysninger om AVG-produktrelaterede tilbud, forbedringer og opgraderinger, osv.

- ***Jeg accepterer at deltage i AVG 2011's internetsikkerhed og produktforbedringsprogram ...*** - markér dette afkrydsningsfelt for at acceptere at deltage i Produktforbedringsprogrammet (*for oplysninger henvises til kapitlet AVG Avancerede indstillinger / Produktforbedringsprogram*), som indsamler anonyme oplysninger om detekterede trusler med henblik på at øge det overordnede internetsikkerhedsniveau.

For at fuldføre installationsprocessen skal du genstarte computeren: vælg om du vil ***Genstarte nu*** eller udsætte denne handling - ***Genstart senere***.

> ***Bemærk:*** *Hvis du bruger et AVG firmalicens og du tidligere har valgt at installere elementet Ekstern administration (se Brugerdefinerede indstillinger), vises dialogen "Installationen blev gennemført" med følgende grænseflade:*
>
> *Du skal angive AVG DataCenter-parametre - angiv forbindelsesstrengen til AVG DataCenter i formatet server:port. Hvis denne information ikke er tilgængelige i øjeblikket, skal du lade feltet stå tomt, og du kan indstille konfigurationen senere i dialogen* ***Avancerede indstilling / Ekstern administration*** *For yderligere oplysninger om AVG Ekstern administration, se brugervejledningen til AVG Business-udgave, der kan downloades fra AVG's websted (http://www.avg.com/).*

5. Efter installationen

5.1. Produktregistrering

Når installationen af **AVG Internet-sikkerhed 2011** er afsluttet, bedes du registrere dit produkt online på AVG's websted (http://www.avg.com/), ***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.

5.2. Adgang til brugergrænseflade

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

- dobbeltklik på ***AVG proceslinjeikon***
- dobbeltklik på AVG-ikonet på skrivebordet
- dobbeltklik på statuslinjen i nederste del af ***AVG gadget*** (*hvis installeret. Understøttes på Windows Vista/ Windows 7*)
- fra menuen ***Start/Programmer/AVG 2011/AVG Brugergrænseflade***
- fra ***AVG Sikkerhedsværktøjslinje*** gennem valgmuligheden ***Start AVG***

5.3. Scanning af hele computeren

Der er en potentiel risiko for, at en computervirus er blevet overført til din computer inden installationen af **AVG Internet-sikkerhed 2011**. Derfor bør du køre en ***Scanning af hele computeren*** for at sikre, at der ikke er infektioner på din pc.

For anvisninger om kørsel af en ***Scanning af hele computeren*** henvises til kapitlet ***AVG Scanning*** .

5.4. Eicar-test

For at bekræfte, at **AVG Internet-sikkerhed 2011** er blevet 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 ***Online Shield*** reagere med en advarsel. Denne notits demonstrerer, at AVG er korrekt installeret på din computer.

Fra websiden http://www.eicar.com kan du også downloade den komprimerede version af EICAR 'virus' (*f.eks. i form af eicar_com.zip*). ***Online Shield*** lade dig downloade denne fil og gemme den på din lokale harddisk, men derefter vil ***Resident Shield*** detektere 'virussen', når du forsøger at pakke den ud. **Hvis AVG ikke kan identificere EICAR-testfilen som en virus, skal du kontrollere programkonfigurationen igen!**

5.5. AVG standardkonfiguration

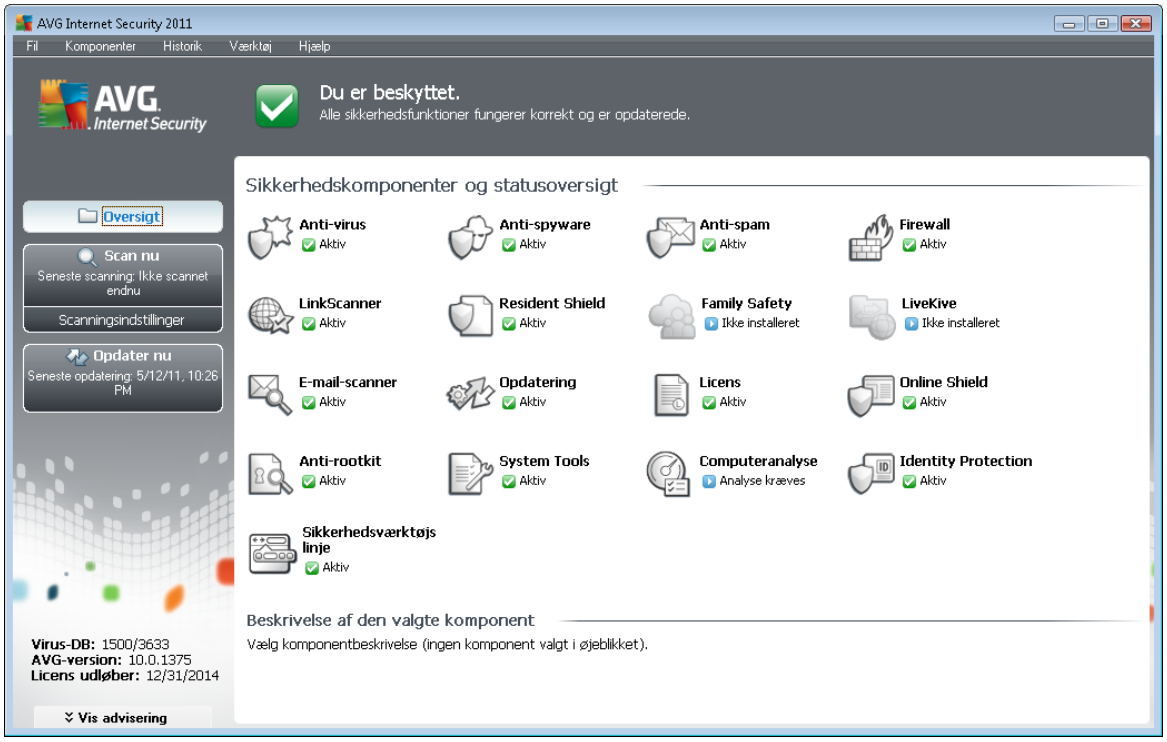
Standardkonfigurationen (*dvs. hvordan applikationen er sat op umiddelbart efter installationen*) af **AVG Internet-sikkerhed 2011** er konfigureret af softwareleverandøren, så alle komponenter og funktioner er indstillet til at opnå optimal ydelse.

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.

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.

6. AVG-brugerflade

AVG Internet-sikkerhed 2011 åbner 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 >>
- ***AVG gadget*** *(Windows Sidebar, understøttet i Windows Vista/7)* giver hurtig adgang til AVG scanning og opdatering - detaljer >>

6.1. Systemmenuen

Systemmenuen er standardnavigationen, der anvendes i alle Windows-applikationer. Den er placeret vandret i øverste del af hovedvinduet **AVG Internet-sikkerhed 2011**. Brug systemmenuen til at få adgang til specifikke komponenter, funktioner og tjenester i AVG.

Systemmenuen er opdelt i fem hovedsektioner:

6.1.1. Fil

- ***Afslut*** - lukker **AVG Internet-sikkerhed 2011**'s brugergrænseflade. AVG-applikationen fortsætter med at køre i baggrunden, og din computer er stadigvæk beskyttet!

6.1.2. 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*** sikrer at din computer er beskyttet mod virus, der forsøger at trænge ind i computeren - detaljer >>
- ***Anti-spyware*** sikrer, at din computer er beskyttet mod spyware og adware - detaljer >>
- ***Anti-spam*** kontrollerer alle indkommende e-mail-meddelelser og mærker uønsket e-mail som SPAM - detaljer >>
- ***Firewall*** kontrollerer, hvordan din computer udveklser data med andre computere på internettet eller lokale netværk - detaljer >>
- ***Linkscanner*** kontrollerer de søgeresultater, der vises i din internetbrowser - detaljer >>
- ***E-mail scanner*** kontrollerer al indkommende og udgående e-mail for virus - detaljer >>
- ***Familiesikkerhed*** hjælper med at overvåge dine børns online aktiviteter, og beskytter dem mod upassende websideindhold - detaljer>>
- ***LiveKive*** laver automatisk backup af dine data online - detaljer >>
- ***Resident Shield*** kører i baggrunden og scanner filer, når de kopieres, åbnes eller gemmes - detaljer >>
- ***Opdateringsadministrator*** kontrollerer alle AVG-opdateringer - detaljer >>
- ***Licens*** viser licensnummer, type og udløbsdato - detaljer >>
- ***Online Shield*** scanner alle data, der downloades af en internetbrowser - detaljer >>
- ***Anti-rootkit*** detekterer programmer og teknologier, der forsøger at camouflere malware -

detaljer >>

- ***Systemværktøjer*** indeholder en detaljeret sammenfatning af AVG-miljøet og operativsystemoplysninger - detaljer >>
- ***Computeranalyse*** giver oplysninger om computerens status - detaljer >>
- ***Identitetsbeskyttelse*** - antimalware-komponent, der fokuserer på at forhindre identitetstyve i at stjæle dine personlige digitale værdier - detaljer >>
- ***Sikkerhedsværktøjslinje*** lader dig bruge valgte AVG-funktioner direkte fra din webbrowser - detaljer >>
- ***Ekstern administration*** vises kun i AVG Business Editions, hvis du i løbet af installationsprocessen angav, at du ønskede denne komponent installeret

6.1.3. 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
- ***Online Shield-fund*** - åbn en dialog med en oversigt over trusler detekteret af ***Online 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 Internet-sikkerhed 2011**-handlinger
- ***Firewall*** - åbner Firewall-indstillingsinterfacet på fanen ***Logge*** med en detaljeret oversigt over alle Firewall-handlinger

6.1.4. Værktøj

- ***Scan computer*** - skifter til AVG scanningsgrænsefladeog starter en scanning af hele computeren.
- ***Scan udvalgte mapper*** - skifter til AVG scanningsgrænsefladeog 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 Internet-sikkerhed 2011**.

- ***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 Internet-sikkerhed 2011**-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.

6.1.5. Hjælp

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

- ***Find hjælp online*** - åbner AVG's websted (http://www.avg.com/) på kundesupportcentrets side

- ***Dit AVG-site*** - åbner AVG's websted (http://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 registreringssiden på AVG's websted (http://www.avg.com/). Udfyld dine registreringsdata. Kun kunder, der registrerer deres AVG-produkt kan modtage gratis teknisk support.

***Bemærk**: Hvis du bruger prøveversionen af* **AVG Internet-sikkerhed 2011**, *vises de to sidstnævnte elementer som **Køb nu** og **Aktivér**, så du kan købe den fulde version af programmet med det samme. Hvis* **AVG Internet-sikkerhed 2011** *er installeret med et salgsnummer, vises elementerne som **Registrér** og **Aktivér**. For flere oplysninger henvises til sektionen Licens i denne dokumentation.*

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

6.2. 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 Internet-sikkerhed 2011**. Herunder er en oversigt over ikoner, der kan være afbilledet 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 AVG. 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 indikeer, 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.

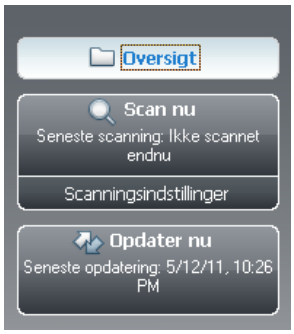
Hvis AVG ikke er indstillet til optimal ydelse, vises en ny knap kaldet Reparér (eller Reparér alle, hvis problemet involverer mere end en komponent) ved siden af sikkerhedsstatusoplysningerne. Tryk på knappen for at starte en automatisk kørsel af programgennemsyn og konfiguration. Der findes en nemmere måde at indstille AVG til optimal ydelse og nå det maksimale sikkerhedsniveau!

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.*

6.3. 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*** >>
- ***Scan nu*** - som standard viser knappen oplysninger (*scanningstype, dato for sidste kørsel*) om den sidst kørte scanning. Du kan enten starte kommandoen ***Scan nu*** for at starte samme scanning igen, eller følge linket ***Scanningsindstillinger***for at åbne AVG scanningsgrænsefladen, hvor du kan kører scanninger, planlægge scanninger eller redigere deres parametre - se kapitlet ***AVG Scanning*** >>
- ***Opdatér nu*** - linket viser datoen for sidste kørsel af opdateringsprocessen. Tryk på knappen for at åbne opdateringsgrænsefladen, og køre AVG-opdateringsprocessen 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.

6.4. 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 Internet-sikkerhed 2011** 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*** sikrer, at din computer er beskyttet mod spyware og adware - detaljer >>
- ***Anti-spam*** kontrollerer alle indkommende e-mail-meddelelser og mærker uønsket e-mail som SPAM - detaljer >>
- ***Firewall*** kontrollerer, hvordan din computer udveklser data med andre computere på internettet eller lokale netværk - detaljer >>
- ***Linkscanner*** kontrollerer de søgeresultater, der vises i din internetbrowser - detaljer >>
- ***E-mail scanner*** kontrollerer al indkommende og udgående e-mail for virus - detaljer >>
- ***Resident Shield*** kører i baggrunden og scanner filer, når de kopieres, åbnes eller gemmes - detaljer >>
- ***Familiesikkerhed*** hjælper med at overvåge dine børns online aktiviteter, og beskytter dem mod upassende websideindhold - detaljer>>
- ***LiveKive*** laver automatisk backup af dine data online - detaljer >>
- ***Opdateringsadministrator*** kontrollerer alle AVG-opdateringer - detaljer >>
- ***Licens*** viser licensnummer, type og udløbsdato - detaljer >>
- ***Online Shield*** scanner alle data, der downloades af en internetbrowser - detaljer >>
- ***Anti-rootkit*** detekterer programmer og teknologier, der forsøger at camouflere malware - detaljer >>
- ***Systemværktøjer*** indeholder en detaljeret sammenfatning af AVG-miljøet og operativsystemoplysninger - detaljer >>
- ***Computeranalyse*** giver oplysninger om computerens status - detaljer >>
- ***Identitetsbeskyttelse*** - antimalware-komponent, der fokuserer på at forhindre identitetstyve i at stjæle dine personlige digitale værdier - detaljer >>
- ***Sikkerhedsværktøjslinje*** lader dig bruge valgte AVG-funktioner direkte fra din webbrowser - detaljer >>
- ***Ekstern administration*** vises kun i AVG Business Editions, hvis du i løbet af installationsprocessen angav, at du ønskede denne komponent installeret

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 på systembakkeikonet.

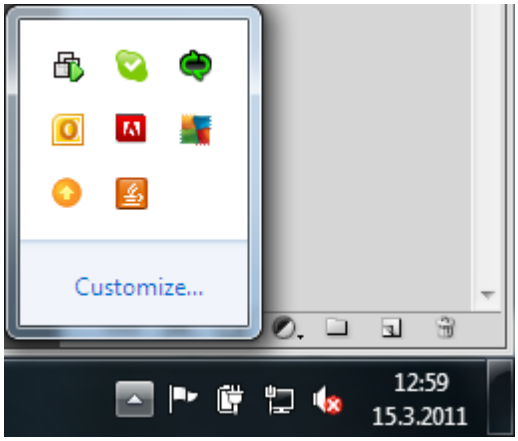
6.5. Statistik

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

- ***Virus-DB*** - informerer om den aktuelle installerede version af virusdatabasen
- ***AVG-version*** - informerer om den installerede AVG-version *(nummeret har formatet 10.0. xxxx, hvor 10.0 er produktlinjeversionen, og xxxx står for buildnummeret)*
- ***Licens udløber*** - angiver udløbsdatoen for din AVG-licens

6.6. Systembakkeikon

Systembakkeikonet (*på Windows' proceslinje*) angiver den aktuelle status for **AVG Internet-sikkerhed 2011**. 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***. Et ikon med et udråbstegn angiver et problem (*en 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, forekomst af 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
- ***Scanninger*** - klik for at åbne kontekstmenuen for
- ***Firewall*** - klik for at åbne kontekstmenuen for Firewall-indstillingsmuligheder, hvor du kan redigere de vigtigste parametre:Firewall-status (*Firewall aktiveret/Firewall deaktiveret/ Nødtilstand*), Skift til gamingtilstandog Firewall-profiler
- ***Kør computeranalyse*** - klik for at starte Computeranalyse-komponenten
- ***Kørende scanninger*** - dette element vises kun, hvis der er en scanning igang på computeren. For denne scanning kan du indstille prioriteten, eller stoppe eller afbryde den igangværende scanning. Desuden er følgende handlinger tilgængelige: *Indstil prioritet for alle scanninger, Afbryd alle scanninger midlertidigt* eller *Stop alle scanninger*.
- ***Opdater nu*** - kører en omgående opdatering
- ***Hjælp*** - åbner hjælpefilen på startsiden

6.7. AVG gadget

AVG gadget vises på Windows skrivebordet (*Windows Sidebar*). Denne applikation understøttes kun i operativsystemerne Windows Vista og Windows 7. ***AVG gadget*** giver øjeblikkelig adgang til de vigtigste **AVG Internet-sikkerhed 2011**-funktioner, dvs. scanning og opdatering:

AVG gadget indeholder følgende genvejsmuligheder:

- ***Scan nu*** - klik på linket ***Scan nu*** for at starte ***scanning af hele computeren*** direkte. Du kan se forløbet af scanningen i gadgettens brugergrænseflade. En kort statistisk oversigt viser oplysninger om antallet af scannede elementer, detekterede trusler og helbredte

trusler. I løbet af scanningen kan du altid midlertidigt stoppe , eller afbryde scanningsprocessen. For detaljerede data, der relaterer til scanningsresultaterne, se den standard ***Scanningsresultatoversigt***-dialog, som kan åbnes direkte fra gadgetten via indstillingen ***Vis detaljer*** (de respektive scanningsresultater vil blive vist under ***Sidebar-scanning***).

- ***Opdatér nu*** - klik på linket ***Opdatér nu*** for at starte AVG-opdateringen direkte fra gadgetten:

- ***Twitter-link*** - åbner en ny ***AVG gadget***-grænseflade, der viser en oversigt over de seneste AVG feeds på Twitter. Følg linket ***Vis alle AVG Twitter-feeds*** for at åbne internetbrowseren i et nyt vindue, hvorefter du vil blive taget direkte til Twitter-websiden med AVG-relaterede nyheder:

- ***Facebook-link***  - åbner din internetbrowser på Facebook-websiden, på siden med ***AVG-fællesskab***

- ***LinkedIn***  **-** denne indstilling er kun tilgængelig i netværksinstallationen (*dvs. forudsat at du har installeret AVG vha. en af AVG's Business Editions-licensers*), og den åbner din internetbrowser på websiden ***AVG SMB Community*** i det sociale netværk LinkedIn

- ***Computeranalyse***  - åbner brugergrænsefladen i komponenten ***Computeranalyse***

- ***Søgeboks*** - indtast et søgeord og få søgeresultaterne med det samme i et nyt vindue med din standard webbrowser

7. AVG Komponenter

7.1. Anti-virus

7.1.1. Antivirusprincipper

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.

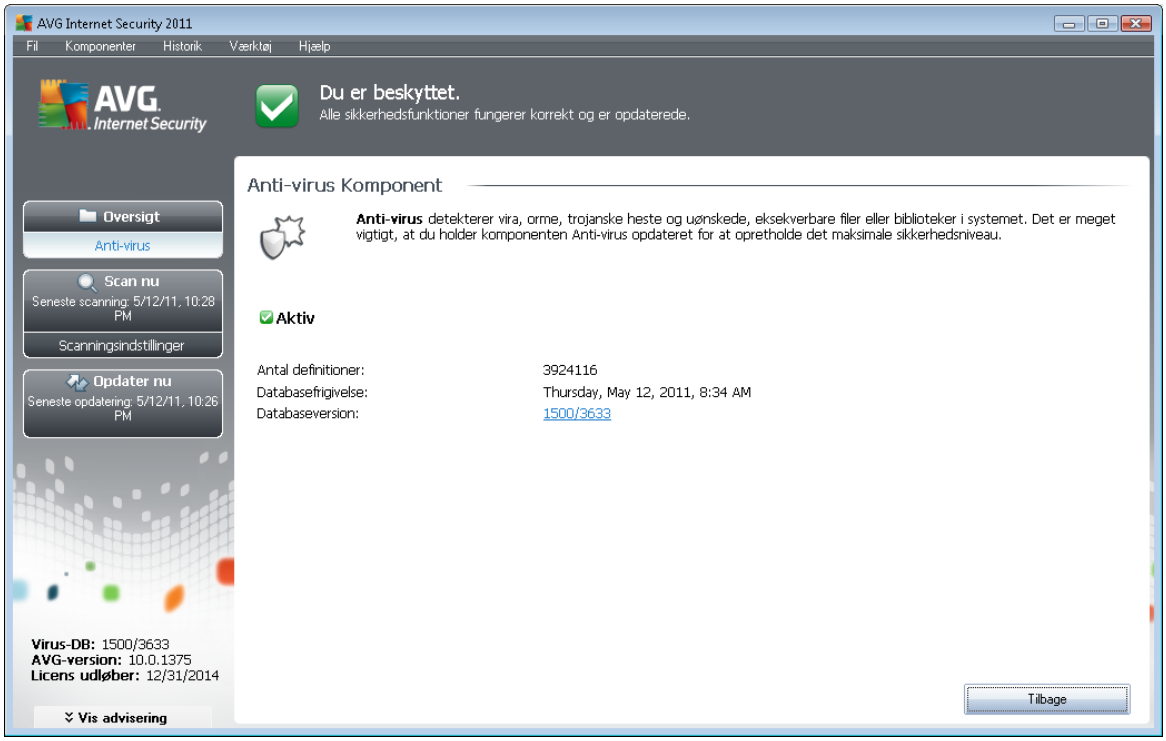
Den vigtige funktion ved antivirusbeskyttelse er, at ingen kendt virus kan køre på computeren.

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.

7.1.2. 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:

- ***Antallet af definitioner*** - nummeret angiver antallet af vira, der er defineret i den opdaterede version af virusdatabasen
- ***Databasefrigivelse*** - angiver hvornår og på hvilket tidspunkt virusdatabasen blev opdateret
- ***Databaseversion*** - definerer nummeret på den aktuelt installerede virusdatabaseversion. Dette nummer forøges for hver opdatering af virusdatabasen

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

7.2. Anti-spyware

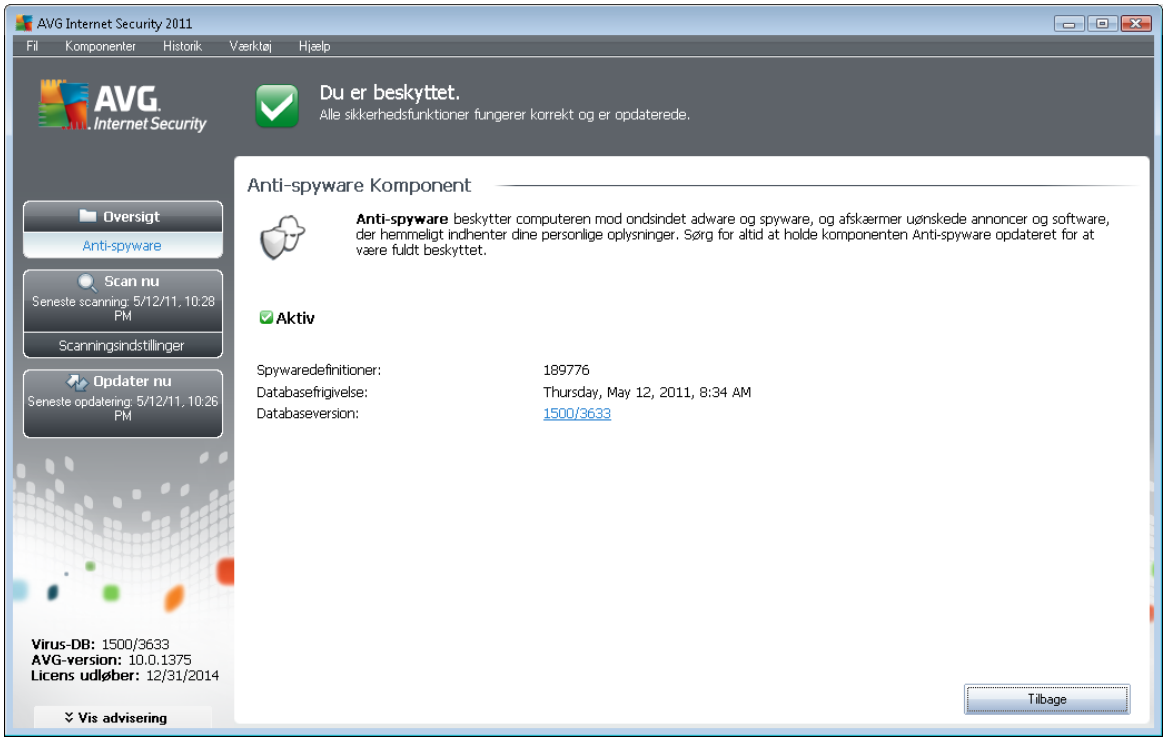
7.2.1. Anti-Spyware principper

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 Internet-sikkerhed 2011** 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.

7.2.2. Anti-spyware-grænseflade



Anti-spyware-komponentens grænseflade indeholder en kort oversigt over komponentens funktionalitet, oplysninger om komponentens aktuelle status samt nogle ***Anti-spyware***-statistikker:

- ***Spywaredefinitioner*** - tallet er det antal spywareeksempler, der er defineret i den seneste version af spywaredatabasen
- ***Databasefrigivelse*** - 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*).

7.3. Anti-spam

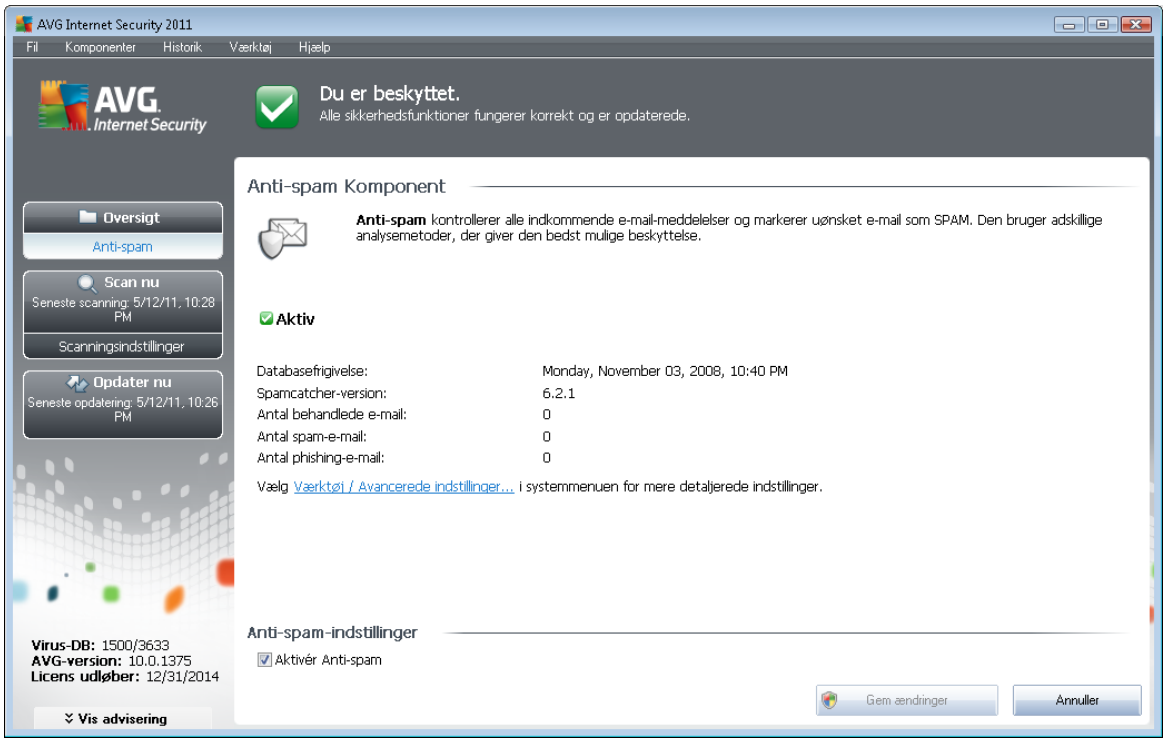
Spam er uopfordret e-mail, for det meste annoncering af et produkt eller en service, der masseudsendes til et enormt antal e-mail-adresser ad gangen, og fylder modtagernes indbakker op. Spam er ikke legitim, kommerciel e-mail, som forbrugeren har givet tilladelse til. Spam er ikke kun irriterende, men er ofte en kilde til svindel, vira og anstødeligt indhold.

7.3.1. Anti-spam-principper

AVG Anti-spam kontrollerer alle indkommende e-mail-meddelelser og markerer uønsket e-mail som spam.***AVG Anti-spam*** kan modificere emnet i den e-mail (*der er blevet identificeret som spam*) ved at tilføje en bestemt tekststreng. Så kan du lettere filtrere dine e-mail i din e-mail-klient.

AVG Anti-spam-komponenten anvender flere forskellige analysemetoder til behandling af hver e-mail-meddelelse, hvilket sikrer den maksimale beskyttelse imod uønskede e-mail-meddelelser. ***AVG anti-spam*** bruger en regelmæssigt opdateret database til detektering af spam. Det er også muligt at bruge RBL-servere (*offentlige databaser over "kendt spammer"-e-mailadresser*) og manuelt føje e-mailadresser til din Hvidliste (*marker aldrig som spam*) og Sortliste (*marker altid som spam*).

7.3.2. Anti-spam-grænseflade



I ***Anti-spam***-komponentens dialog finder du en kort tekst, der beskriver komponentes funktionalitet, oplysninger om dens aktuelle status og følgende statistikker:

- ***Databasefrigivelse*** - angiver hvornår og på hvilket tidspunkt spamdatabasen blev opdateret og udgivet
- ***Spamcatcher-version*** - definerer nummeret på den seneste version af anti-spam-enginen

- ***Antallet af behandlede e-mails*** - angiver, hvor mange e-mail-meddelelser er blevet scannet siden sidste kørsel af antispam-programmet
- ***Antallet af spam-e-mails*** - blandt alle scannede e-mails, hvor mange meddelelser blev markeret som spam
- ***Antallet af phishing-e-mails*** - blandt alle scannede e-mails, hvor mange meddelelser blev angivet som forsøg på phishing

Dialogen ***Anti-spam*** indeholder også linket ***Værktøjer/Avancerede indstillinger***. Brug linket for at komme til miljøet for avanceret konfiguration af alle **AVG Internet-sikkerhed 2011**-komponenter.

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.*

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

7.4. Firewall

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.

Anbefaling: *Det anbefales generelt ikke at bruge mere end én firewall på en enkeltstående computer. Computerens sikkerhed forbedres ikke, hvis du installerer flere firewalls. Det er mere sandsynligt, at der vil opstå konflikter mellem de to applikationer. Derfor anbefaler vi, at du kun bruger én firewall på computeren og deaktiverer alle andre, hvorved risikoen for mulige konflikter og eventuelle problemer i den forbindelse bliver elimineret.*

7.4.1. Firewall-principper

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.

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

Hvad AVG 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
- Skifte profil automatisk, når der oprettes forbindelse til forskellige netværk eller bruges forskellige netværksadaptere

7.4.2. 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***:
    - ***Direkte tilsluttet internettet*** egnet til almindelige stationære computere, der er sluttet direkte til internettet, eller bærbare computere, der opretter forbindelse til internettet uden for det sikre firmanetværk. Vælg denne indstilling, hvis du opretter forbindelse hjemmefra, eller du er på et lille firmanetværk uden central styring. Vælg også denne indstilling, når du er ude at rejse og opretter forbindelse med din notebook fra forskellige ukendte og muligvis farlige steder (*internetcafé, hotelværelse osv.*). Der oprettes mere restriktive regler, da det antages, at disse computere ikke har ekstra beskyttelse og derfor kræver maksimal beskyttelse.

- ***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.

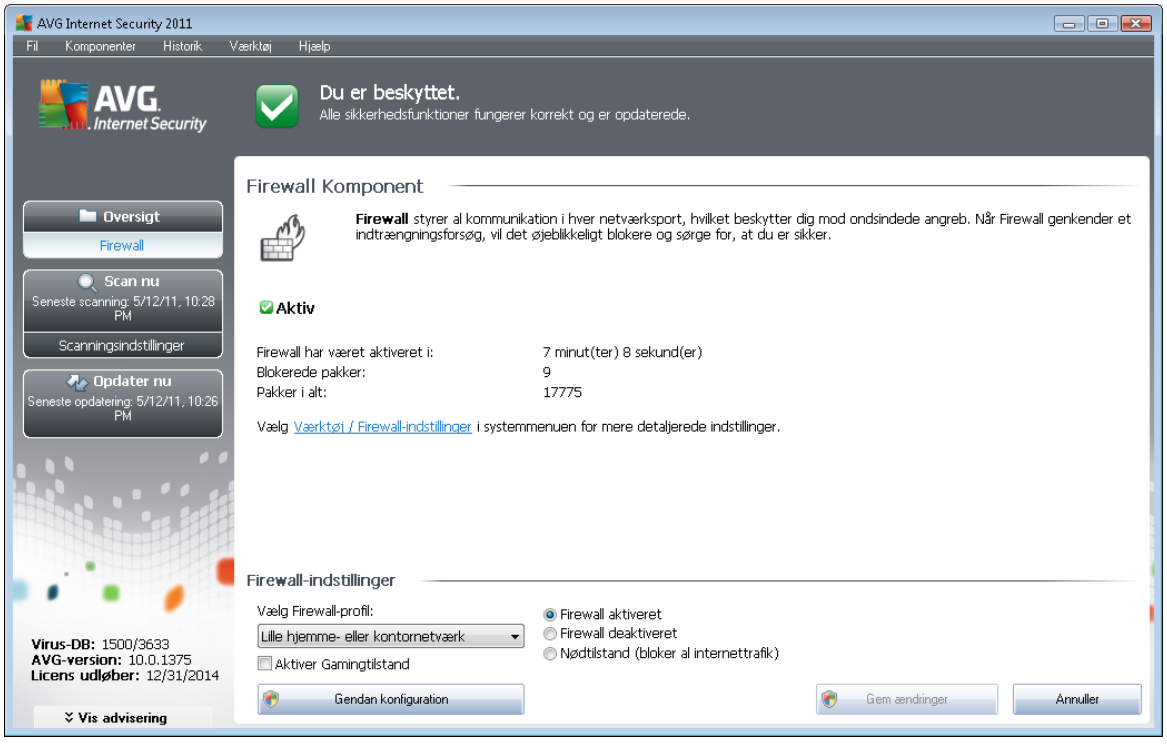
Profilskift

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.

7.4.3. Firewall-grænseflade



Firewallens grænseflade indeholder nogle grundlæggende oplysninger om komponentens funktionalitet, dens status 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

- ***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 manuelt ved redigering af profiler i dialogen ***Profiler*** i ***Firewall-indstillinger***.
- ***Aktivér gamingtilstand*** - Markér denne indstilling for at sikre, at når der køres fuldskærmsapplikationer (*spil, præsentationer, film, etc.*), vil ***Firewall*** ikke vise dialoger, der spørger dig, om du vil tillade eller blokere kommunikation for ukendte applikationer. 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:*** Når gamingtilstanden er slået til, bliver alle planlagte opgaver (scanninger, opdateringer) udsat, indtil programmet lukkes.
- ***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

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 / Firewall-indstillinger*** *og redigere Firewall-konfigurationen i dialogen* ***Firewall-indstillinger****, der åbnes.*

Betjeningsknapper

- ***Gendan konfiguration*** - tryk på denne knap for at overskrive den aktuelle ***Firewall***-konfiguration, og gendanne standardkonfigurationen baseret på en automatisk detektion.
- ***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*)

7.5. Linkscanner

7.5.1. Linkscanner-principper

LinkScanner beskytter dig mod det stigende antal "Her i dag, væk i morgen"-trusler på internettet. Disse trusler kan være skjult på en hvilken som helst type webside, fra myndigheder til store, velkendte filialer til små virksomheder, og de forbliver sjældent på disse sider i mere end 24 timer. ***LinkScanner*** beskytter dig ved at analysere websiderne bag alle linkene på et websted, du besøger, og sørger for, at de er sikre på det eneste tidspunkt, det betyder noget for dig, nemlig når du klikker på linket.

LinkScanner-teknologien består af to funktioner, ***Søgeskjold*** og ***Surfskjold***:

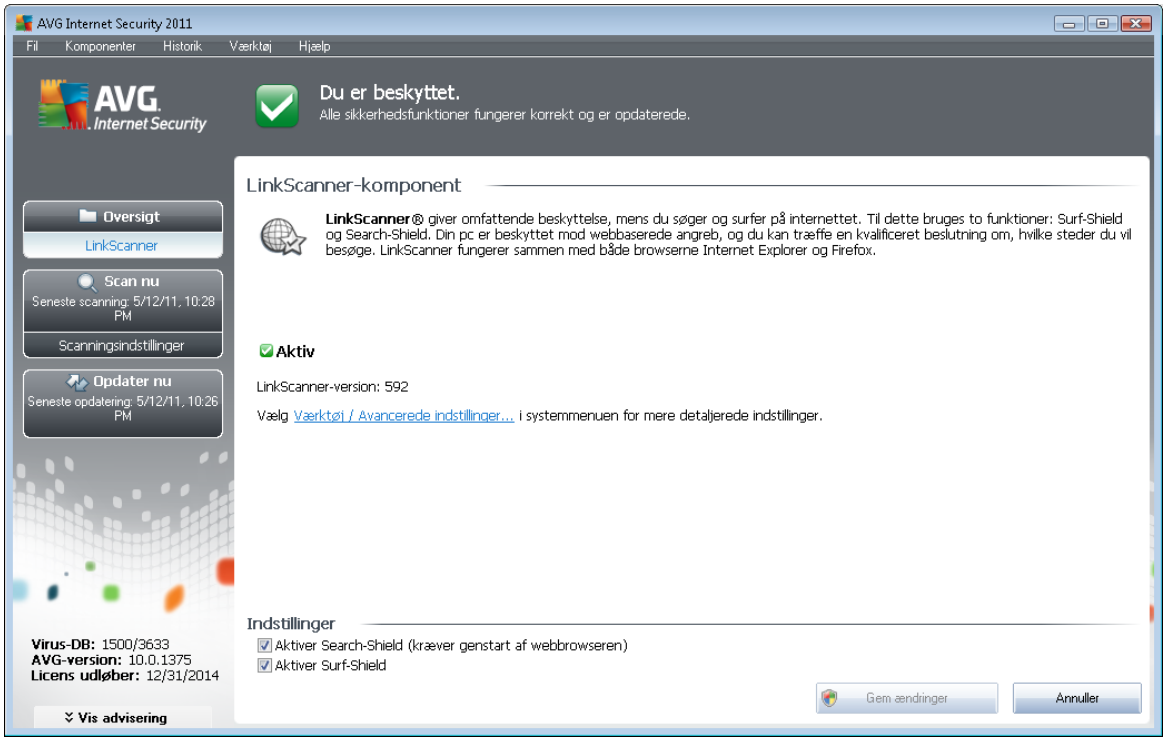
- ***Søgeskjold*** indeholder en liste over websteder (*URL-adresser*), der er kendt som farlige. Når du søger med Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg eller SlashDot, kontrolleres alle søgeresultaterne iht. denne liste, og der vises et resultatikon (*for Yahoo-søgeresultater vises kun resultatikoner for "websted med exploit"*).

- ***Surfskjold*** scanner indholdet på de websteder, du besøger, uanset webstedets adresse. Selvom et websted ikke detekteres af ***Søgeskjold*** (*f.eks. hvis der oprettes et nyt ondsindet websted, eller hvis et tidligere rent websted nu indeholder malware*), bliver det detekteret og blokeret af ***Surfskjold***, når du prøver at besøge det.

Bemærk: *LinkScanner er ikke beregnet til serverplatforme!*

7.5.2. Linkscanner-grænseflade

LinkScanner-komponentens grænseflade indeholder en kort beskrivelse af komponentens funktionalitet og oplysninger om dens aktuelle status. Desuden kan du finde oplysninger om det nyeste versionsnummer af ***LinkScanner***-databasen (*LinkScanner-version*).



LinkScanner-indstillinger

I den nederste del af dialogen kan du redigere adskillige indstillinger:

- ***Aktiver Søgeskjold*** - (*slået til som standard*): vejledende ikoner på søgninger udført i Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, or SlashDot: efter forudgående kontrol af indholdet på de websteder, der returneres af søgemaskinen.

- ***Aktiver 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*).

7.5.3. Søgeskjold

Når du søger på internettet med ***Søgeskjold*** aktiveret, vil alle søgeresultater, der returneres fra de mest populære søgemaskine (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, and SlashDot*) blive evalueret for farlige eller mistænkelige. Ved at kontrollere disse link og markere de dårlige link, advarer ***AVG LinkScanner*** 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 (*dette ikon vil ikke vises for sikre Yahoo! JP søgeresultater*).

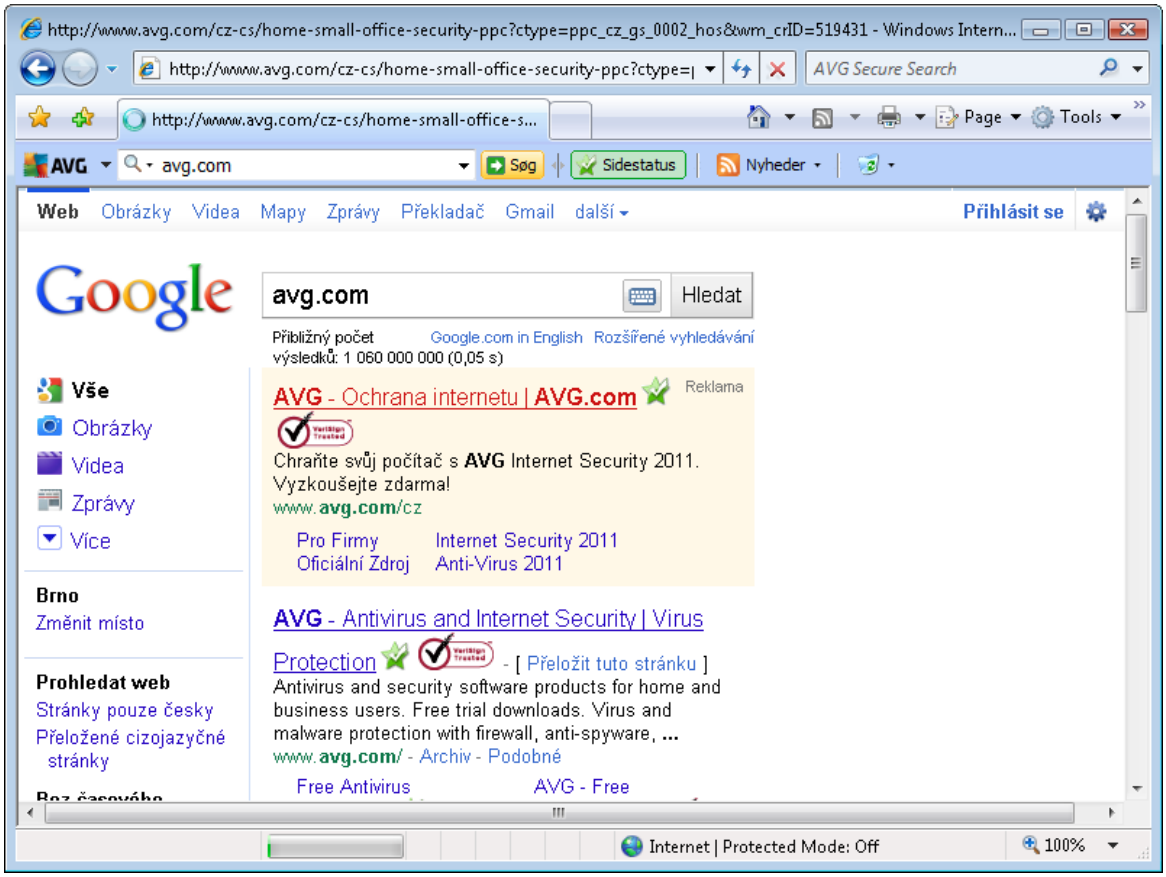
Siden, der linkes til, indeholder ingen trusler men er mistænkelig (*tvivlsom oprindelse eller motiv og anbefales derfor ikke til e-handel osv.*).

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.

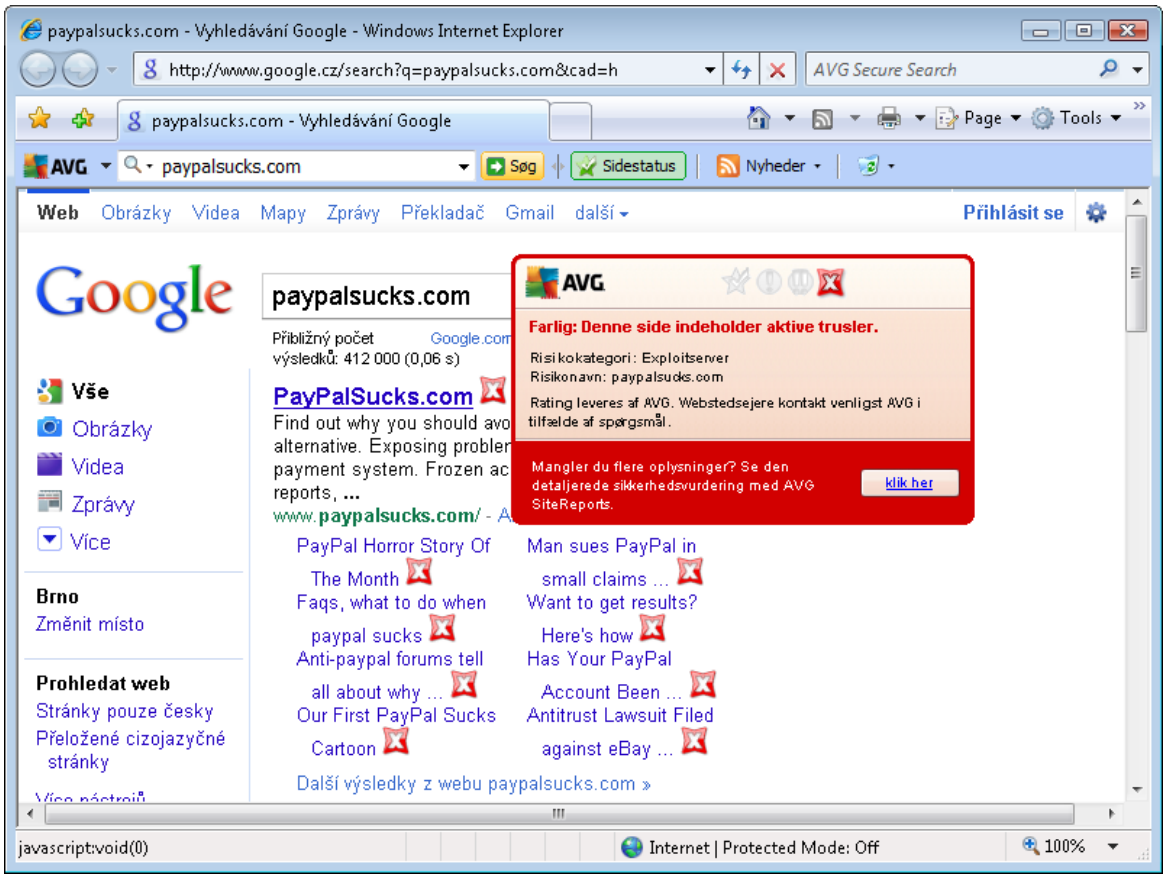
Hvis musen holdes over et individuelt ratingikon, vises detaljer om det pågældende link. Oplysninger omfatter yderligere oplysninger om truslen (*hvis der er nogen*):



7.5.4. 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 Linkscanner*** ikke din browser at vise farlige websider, der indeholder exploits eller andre alvorlige trusler.

Hvis du støder på et ondsindet websted, vil ***AVG Link Scanner*** advare dig i din webbrowser med et skærmbillede lignende dette:



Det er meget risikabelt at åbne et sådant websted, og det kan ikke anbefales!

7.6. Resident Shield

7.6.1. Resident Shield-principper

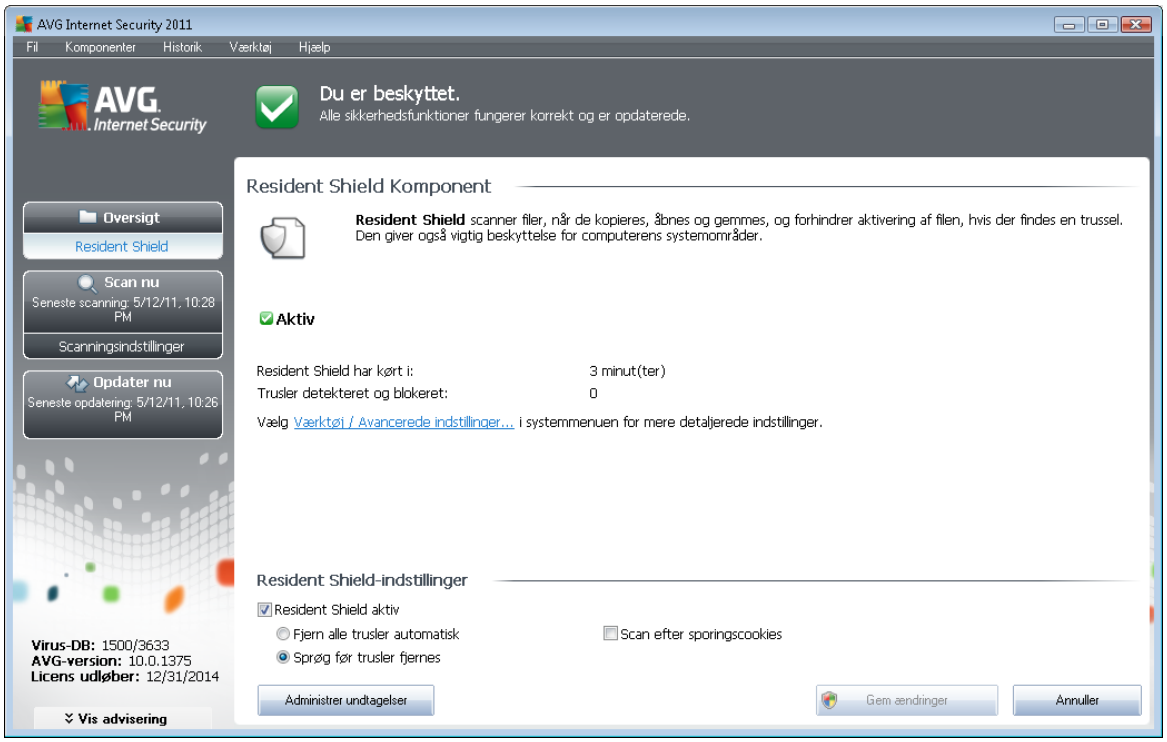
Resident Shield-komponenten yder konstant beskyttelse til din computer. Den scanner hver eneste fil, der åbnes, gemmes eller kopieres, og beskytter computerens systemområder. Hvis ***Resident Shield*** opdager en virus i en fil, der aktiveres, stoppes den igangværende operation, og virussen får ikke lov til at aktivere sig selv. Normalt bemærker du ikke engang processen, da den kører "i baggrunden", og du bliver kun orienteret, når der findes trusler. Samtidig blokerer ***Resident Shield*** mod, at truslen aktiveres, og fjerner den. ***Resident Shield*** bliver indlæst i hukommelsen på din computer under opstart af systemet.

Hvad Resident Shield kan gøre:

- Scan efter bestemte typer af mulige trusler
- Scan fjernbare medier (*flashdisk osv.*)
- Scan filer med specifikke filtypenavne eller uden filtypenavn
- Tillad undtagelser fra scanning - specifikke filer eller mapper, der aldrig skal scannes

Advarsel! Resident Shield indlæses i computerens hukommelse under opstarten, og det er vigtigt, at du altid har det slået til!

7.6.2. Resident Shield-grænseflade



I tillæg til en oversigt over ***Resident Shield***'s funktion og oplysninger om komponentens status viser ***Resident Shield***-grænsefladen også nogle statistiske data:

- ***Resident Shield har kørt i*** - indeholder den forløbne tid, siden komponenten blev startet sidst

- ***Trusler detekteret og blokeret*** - detekterede infektioner, der blev forhindret i at køre/åbne (*denne værdi kan om nødvendigt nulstilles, f.eks. til statistiske formål - Nulstil værdi*)

Resident Shield-indstillinger

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 Værktøjer/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 ***Scanne efter sporings-cookies***. 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:

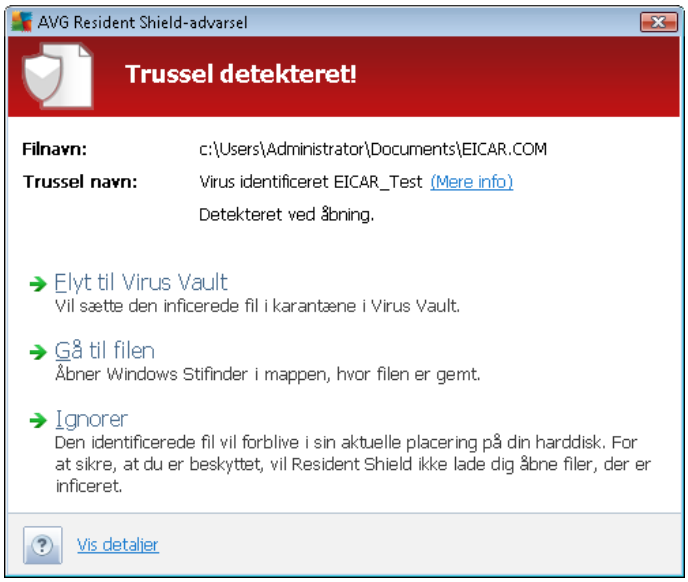
- ***Administrer undtagelser*** - åbner dialogen ***Resident Shield - Udeladte elementer***, hvor du kan definere mapper og filer, der ikke skal medtages i ***Resident Shield***-scanningen

- ***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*)

7.6.3. 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:



I denne advarselsdialog vil du finde data om den fil, der blev detekteret og defineret som inficeret (*Filnavn*), navnet på den genkendte infektion (*Trusselnavn*), og et link til ***Virus-opslagsværket***, hvor du kan finde detaljerede oplysninger om den detekteres infektion, hvis den kendes (*Mere info*).

Du skal desuden vælge, hvilken handling, der nu skal foretages - følgende valgmuligheder er tilgængelige:

Bemærk, at ved særlige betingelser (hvilken type fil er inficeret, og hvor den er placeret), er ikke alle valgmulighederne altid tilgængelige!

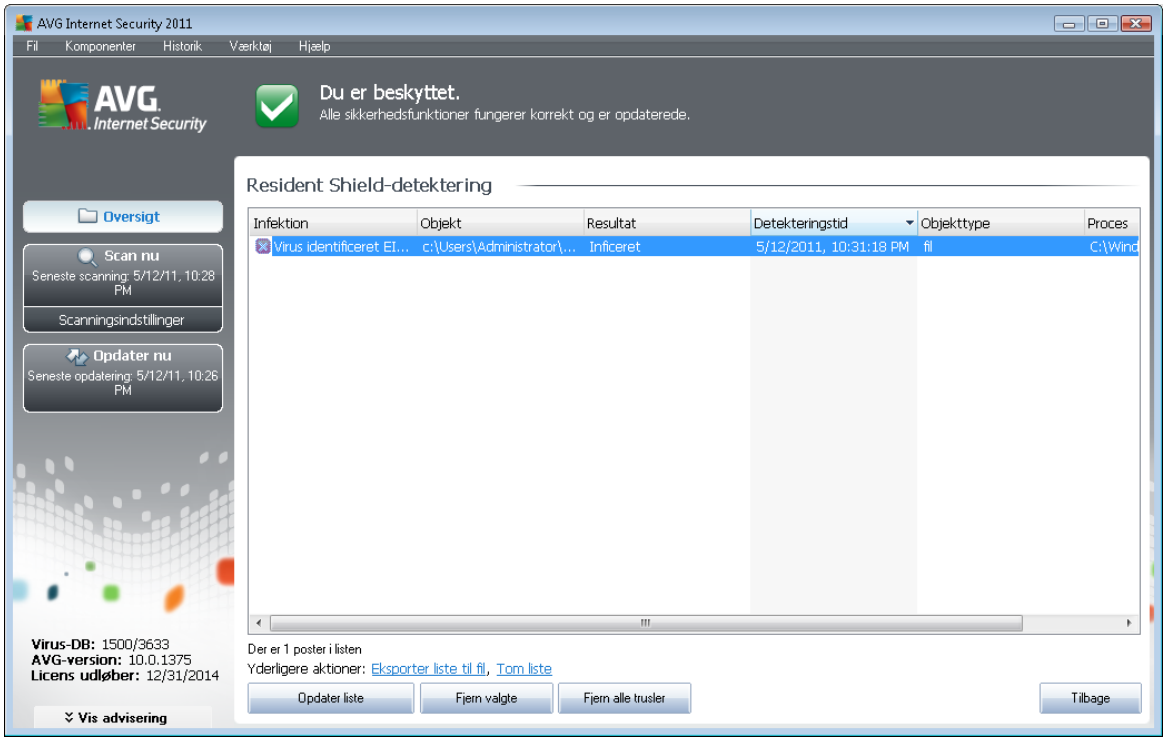
- ***Fjern trussel som superbruger*** - marker feltet, hvis du tror, at du muligvis ikke har tilstrækkelige rettigheder til at fjerne truslen som almindelig bruger. Superbrugere har udvidede adgangsrettigheder, og hvis truslen er placeret i en bestemt systemmappe, skal du muligvis bruge dette afkrydsningsfelt til at fjerne den.
- ***Helbred*** - denne knap vises kun, hvis den detekterede infektion kan helbredes. Derefter fjernes den fra filen, og filen gendannes til den oprindelige tilstand. Hvis selve filen er en virus, skal du bruge denne funktion til at slette den (*dvs. flytte den til **Virus Vault***)
- ***Flyt til Virus Vault*** - virussen flyttes til AVG ***Virus Vault***
- ***Gå til fil*** - denne mulighed sender dig til den nøjagtige placering af det mistænkelige objekt (*åbner et nyt vindue i Windows stifinder*)
- ***Ignorer*** - vi anbefaler på det kraftigste IKKE at anvende denne valgmulighed, medmindre du har en meget god grund til at gøre det!

Bemærk: *Det kan ske, at størrelsen på det detekterede objekt overstiger pladsbegrænsningen i*

Virus Vault. I dette tilfælde vises advarsels-popups, der informerer dig om problemet, når du forsøger at flytte det inficerede objekt til Virus Vault. Størrelsen på Virus Vault kan dog tilpasses. Den er defineret som en justerbar procentdel af den faktiske størrelse på din harddisk. For at øge størrelsen på din Virus Vault skal du gå til Virus Vault-dialogen i AVG Avancerede indstillinger via indstillingen 'Begræns størrelse på Virus Vault'.

I nederste del af dialogen findes linket ***Vis detaljer*** - klik på det for at åbne et popup-vindue med detaljerede oplysninger om den proces, der var igang, da infektionen blev detekteret, og processens identifikation.

Hele oversigten over alle trusler detekteret af ***Resident Shield*** kan findes i dialogen ***Resident Shield-detektering***, der er tilgængelig fra systemmenupunktet ***Historik / Resident Shield-fund***:



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
- ***Detekteringstid*** - dato og klokkeslæt, da objektet blev detekteret
- ***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***. Med knappen ***Tilbage*** skifter du tilbage til den standard ***AVG-brugergrænseflade*** (*komponentoversigt*).

7.7. Familiesikkerhed

AVG Familiesikkerhed hjælper dig med at beskytte dine børn mod upassende websteder, medieindhold og online søgninger, og viser dig rapporter omkring deres online aktivitet. Du kan indstille det passende beskyttelsesniveau for hvert barn, og overvåge dem særskilt via unikke login.

Komponenten er kun aktiv, når ***AVG Familiesikkerhed***-produktet er installeret på din maskine. Hvis ***AVG Familiesikkerhed***-produktet ikke er installeret, skal du klikke på det pågældende ikon i **AVG Internet-sikkerhed 2011** brugergrænsefladen for at komme til produktwebstedet, hvor du kan finde alle de nødvendige oplysninger.

7.8. AVG LiveKive

AVG LiveKive sikkerhedskopierer automatisk alle fine filer, fotos og musik et sikkert sted, hvor du kan dele dem med familie og venner, og få adgang til dem fra enhver enhed med internetforbindelse, inklusive iPhones og Android-enheder.

Komponenten er kun aktiv, når ***AVG LiveKive***-produktet er installeret på din maskine. Hvis ***AVG LiveKive***-produktet ikke er installeret, skal du klikke på det pågældende ikon i **AVG Internet-sikkerhed 2011** brugergrænsefladen for at komme til produktwebstedet, hvor du kan finde alle de nødvendige oplysninger.

7.9. E-mail Scanner

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.

7.9.1. E-mail Scanner-principper

Personlig e-mail-scanner scanner automatisk indkommende/udgående e-mail. Du kan bruge den med e-mail-klienter, der ikke har deres eget plugin i AVG (*men kan også bruges til at scanne e-mail-meddelelser for e-mail-klienter, som AVG understøtter med et specifikt plugin, dvs. Microsoft Outlook og The Bat*). Den skal primært bruges sammen med e-mail-programmer som Outlook Express, Mozilla, Incredimail, osv.

Under AVG-installation AVG oprettes der automatiske servere til kontrol af e-mail: en til at

kontrollere indkommende e-mail og en anden til at kontrollere udgående e-mail. Ved hjælp af disse to servere kontrolleres e-mail automatisk på port 110 og 25 (*standardporte til at sende/modtage e-mail*).

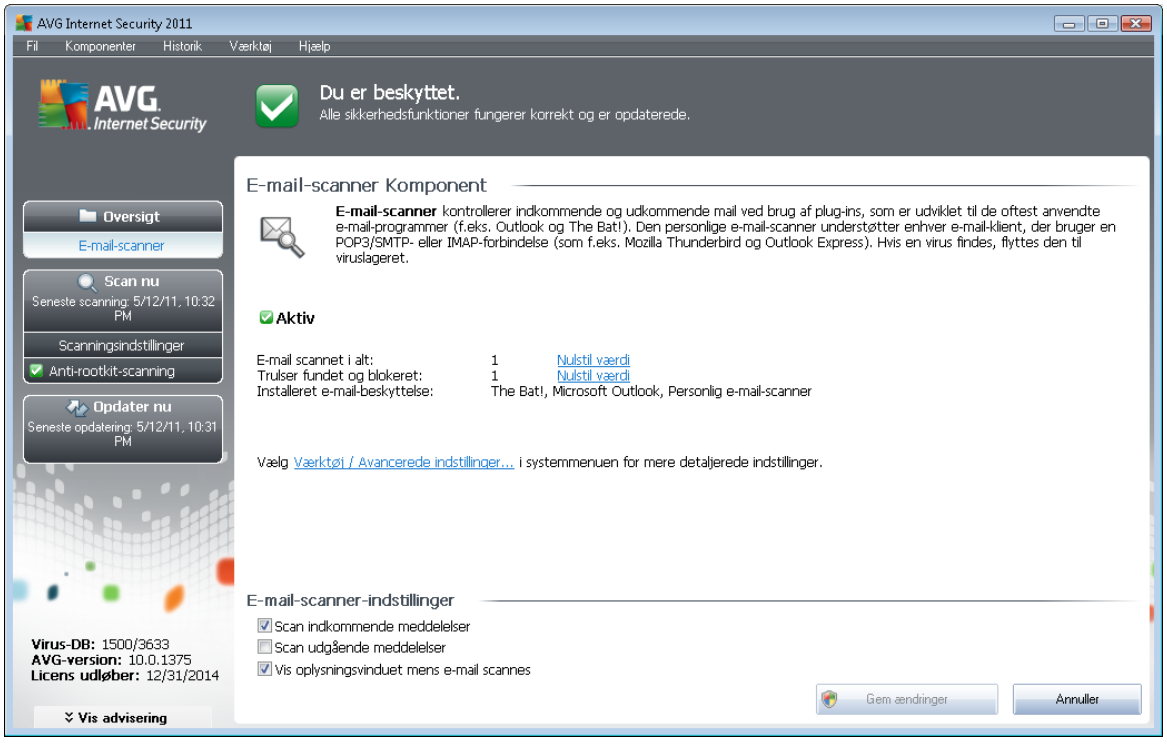
E-mail-scanner fungerer som en grænseflade mellem e-mail-klient og e-mail-servere på internettet.

- ***Indkommende mail:*** Men en meddelelse modtages fra serveren, tester ***E-mail-scanner***-komponenten den for vira, fjerner inficerede vedhæftede filer, og tilføjer certificering. Når vira detekteres, bliver de omgående sat i karantæne i ***Virus Vault***. Derefter videresendes meddelelsen til e-mail-klienten.

- ***Udgående mail:*** Meddelelsen sendes fra e-mail-klienten til E-mail-scanner, som tester meddelelsen og dens vedhæftede filer for vira og derefter sender meddelelsen til SMTP-serveren (*scanning af udgående e-mail er deaktiveret som standard og kan konfigureres manuelt*).

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

7.9.2. E-mail Scanner-grænseflade



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

- ***E-mail scannet i alt*** - hvor mange e-mail-meddelelser er blevet scannet siden ***E-mail scanner*** sidst blev kørt (*denne værdi kan om nødvendigt 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

E-mail-scanner-indstillinger

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 elementet for at angive, at alle e-mail, der leveres til din konto, skal scannes for vira. Som standard er dette element 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 informationsvinduet, mens e-mailen scannes*** - markér elementet for at bekræfte, at du vil informeres via informationsdialogen, der vises over AVG ikonet på systembakken under scanning af din post via ***E-mail scanner***-komponenten. Som standard er dette element slået til, og det anbefales ikke at ændre denne indstilling!

Der er adgang til den avancerede konfiguration af ***E-mail scanner***-komponenten via punktet ***Værktøjer/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.*

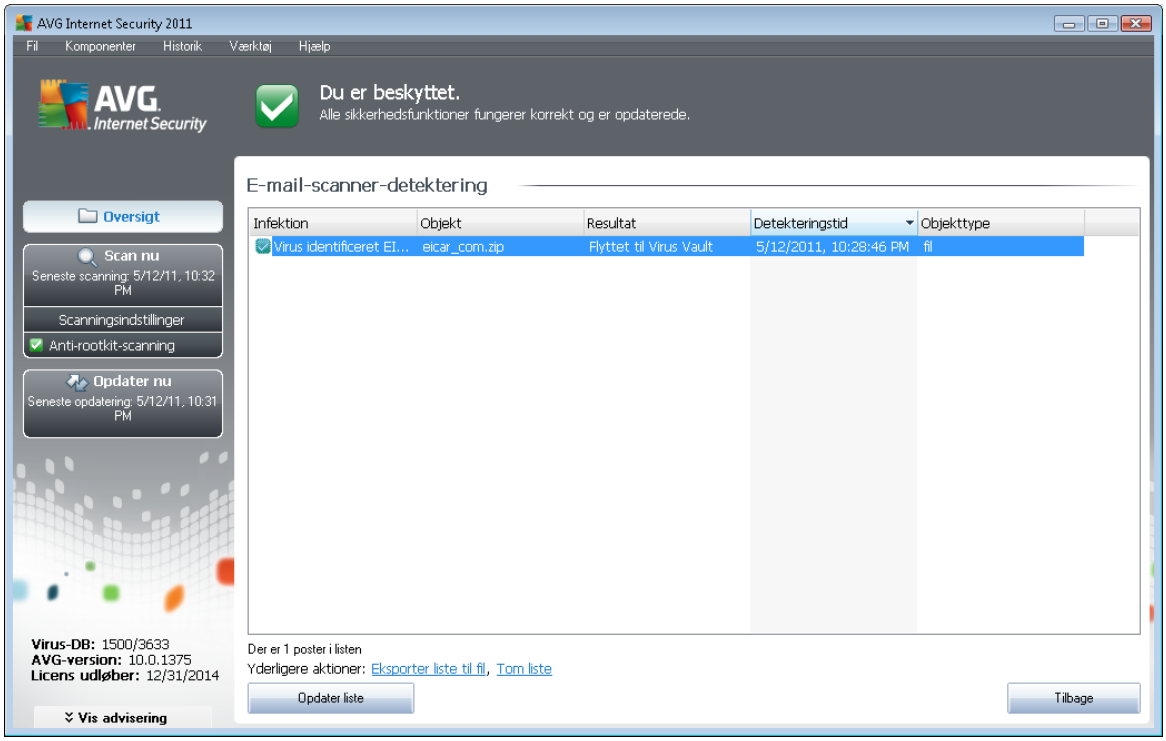
Betjeningsknapper

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*)

7.9.3. 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
- ***Detekteringstid*** - dato og klokkeslæt, da det mistænkelige objekt blev detekteret
- ***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***).

Betjeningsknapper

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

- ***Opdater liste*** - opdaterer listen over detekterede trusler

- ***Tilbage*** - tager dig tilbage til den sidst viste dialog

7.10. Opdateringsadministrator

7.10.1. Opdateringsadministrator-principper

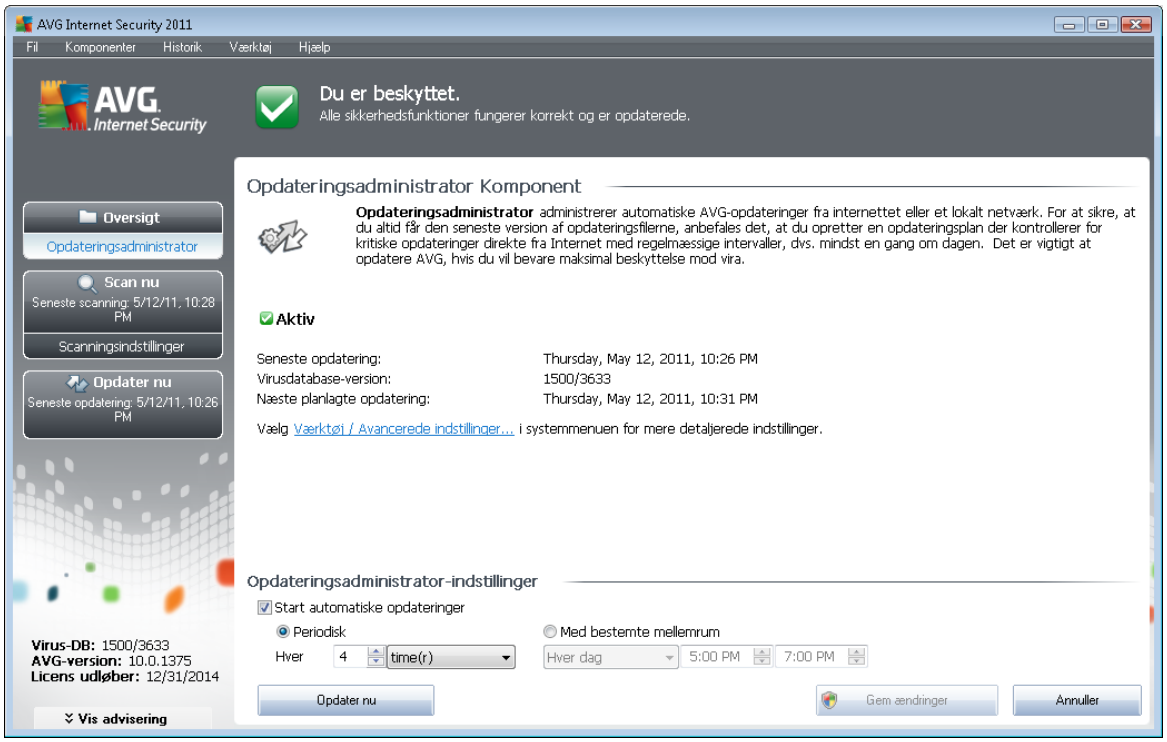
Ingen sikkerhedssoftware kan garantere reel beskyttelse mod forskellige typer af trusler, med mindre den opdateres regelmæssigt! Virusskribenter er altid på udkig efter nye sikkerhedshuller, de kan udnytte, i både software og operativsystemer. Nye vira, nye malware og nye hackingforsøg forekommer dagligt. 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!*

7.10.2. Opdateringsadministrator-grænseflade



Grænsefladen til ***Opdateringsadministrator*** viser oplysninger om komponentens funktionalitet og dens aktuelle status, og viser de relevante statistiske data:

- ***Seneste opdatering*** - angiver datoen og tidspunktet for den sidste databaseopdatering
- ***Virusdatabaseversion*** - definerer nummeret på den aktuelt installerede virusdatabaseversion. Dette nummer forøges for hver opdatering af virusdatabasen
- ***Næste planlagte opdatering*** - angiver datoen og tidspunktet for den næste databaseopdatering

Opdateringsadministrator-indstillinger

I den nederste del af dialogboksen finder du sektionen ***Indstillinger for opdateringsadministrator***, hvor du kan udføre nogle ændinger 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
- ***Med et specifikt tidsinterval*** - angiv den nøjagtige dag og tidspunkt, hvor opdateringen skal køres

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!

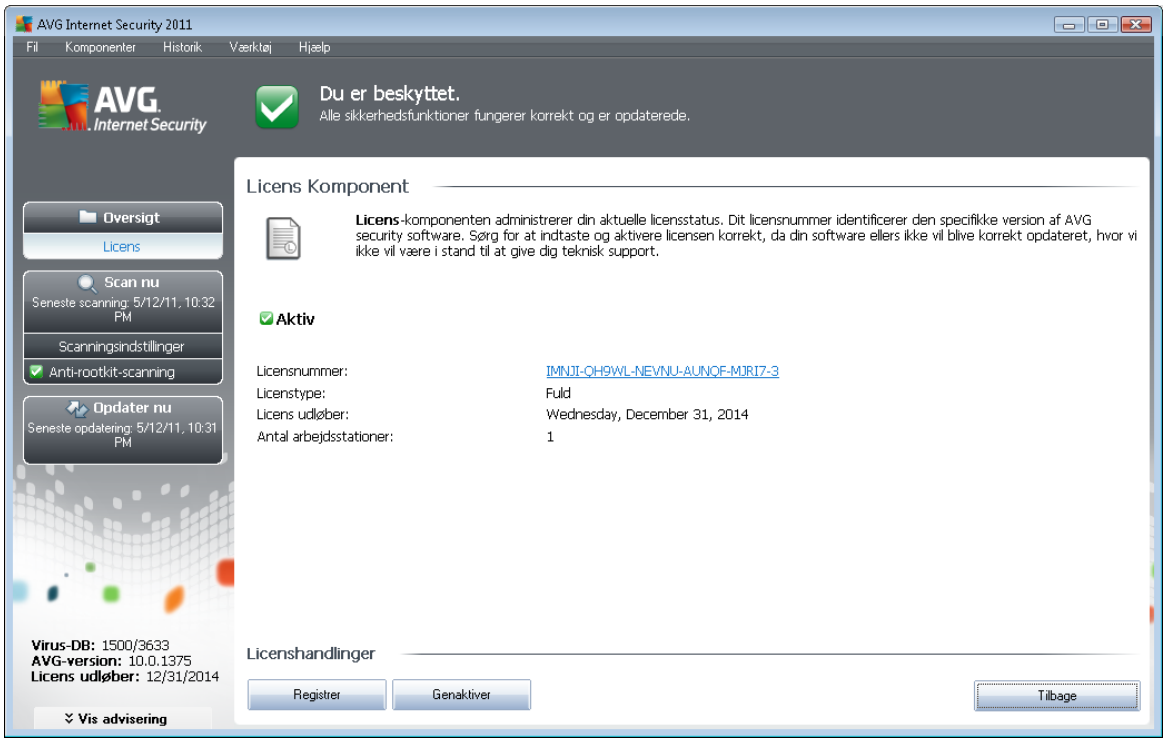
Bemærk: *-softwareleverandøren har konfigureret alle AVG-komponenter til den optimale ydeevne. Medmindre du har en god grund til at gøre det, bør du ikke ændre AVG's konfiguration. Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal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

7.11. Licens



I ***Licens***-komponentens grænseflade finder du en kort tekst, der beskriver komponentens funktionalitet, oplysninger om dens aktuelle status og følgende oplysninger:

- ***Licensnummer*** - angiver en forkortet udgave af dit licensnummer (*af sikkerhedsmæssige årsager mangler de sidste fire tegn*). Når du indtaster licensnummeret, skal du være fuldstændig præcis og indtaste det nøjagtig som vist. Derfor anbefaler vi på det kraftigste altid at bruge "kopier og sæt ind"-metoden til alle ændringer af licensnummeret.

- ***Licenstype*** - angiver den installerede produkttype.

- ***Licens udløber*** - denne dato bestemmer licensens gyldighedsperiode. Hvis du vil fortsætte med at anvende **AVG Internet-sikkerhed 2011** 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 Internet-sikkerhed 2011** på.

Betjeningsknapper

- ***Registrer*** - opretter forbindelse til registreringssiden på AVG's websted (http://www.avg.com/). Udfyld dine registreringsdata. Kun kunder, der registrerer deres AVG-produkt kan modtage gratis teknisk support.

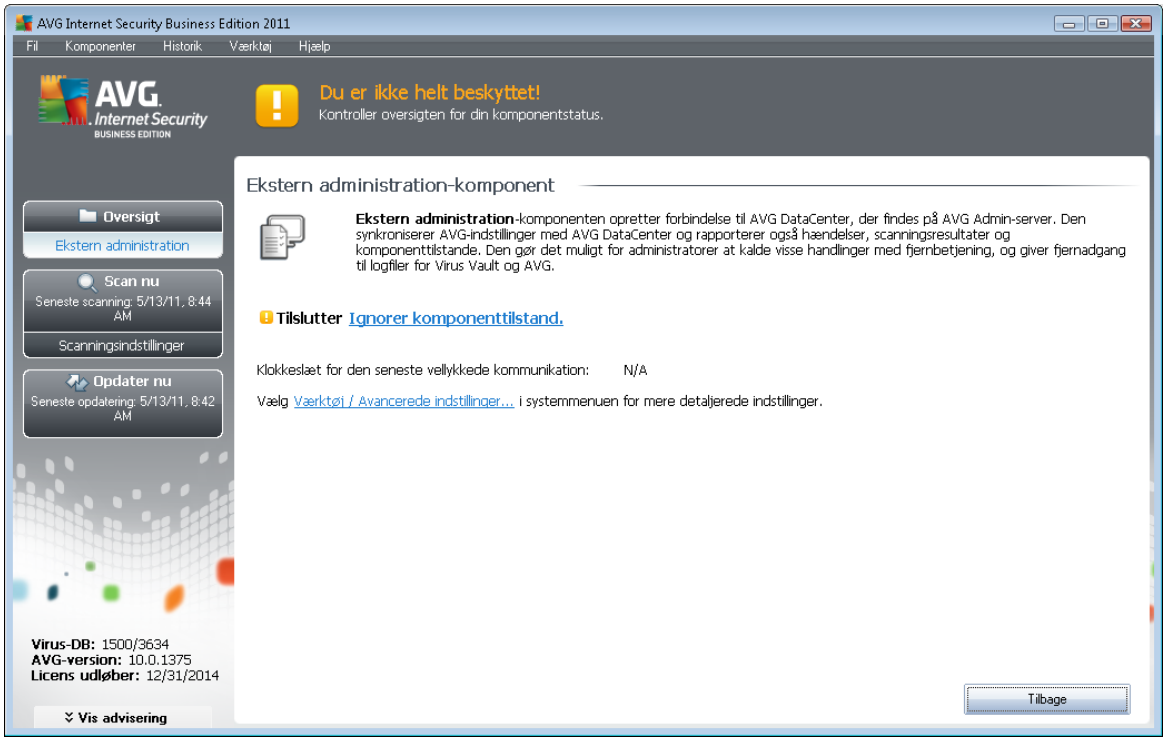
- ***Genaktiver*** - åbner dialogen ***Aktiver AVG*** med de data, du har indtastet i dialogen ***Personliggør AVG*** under installationsprocessen. I denne dialog kan du indtaste dit

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*).

Bemærk: *Hvis du bruger prøveversionen af* **AVG Internet-sikkerhed 2011***, vises knapperne som* ***Køb nu*** *og* ***Aktivér****, så du kan købe den fulde version af programmet med det samme. Hvis* **AVG Internet-sikkerhed 2011** *er installeret med et salgsnummer, vises knapperne som* ***Registrér*** *og* ***Aktivér****.*

- ***Tilbage*** - tryk på denne knap for at vende tilbage til den normale ***AVG-brugergrænseflade*** (*komponentoversigt*).

7.12. Ekstern administration



Komponenten ***Ekstern administration*** vises kun i brugergrænsefladen **AVG Internet-sikkerhed 2011**, hvis du har installeret Business-udgaven af dit produkt (*se komponentens* ***Licens***). I dialogen ***Ekstern administration*** vil du kunne se, om komponenten er aktiv og tilsluttet serveren. Alle indstillinger for komponenten ***Ekstern administration*** skal foretages i ***Avancerede indstillinger / Ekstern administration***.

For en detaljeret beskrivelse af komponentens indstillinger og funktioner i systemet AVG Ekstern administration henvises til den specifikke dokumentation, der specifikt omhandler dette emne. Denne dokumentation kan downloades på AVG's websted (www.avg.com), i sektionen ***Supportcenter / Download / Dokumentation***.

Betjeningsknapper

- ***Tilbage*** - tryk på denne knap for at vende tilbage til den normale AVG-brugergrænseflade (*komponentoversigt*).

7.13. Online Shield

7.13.1. Online Shield-principper

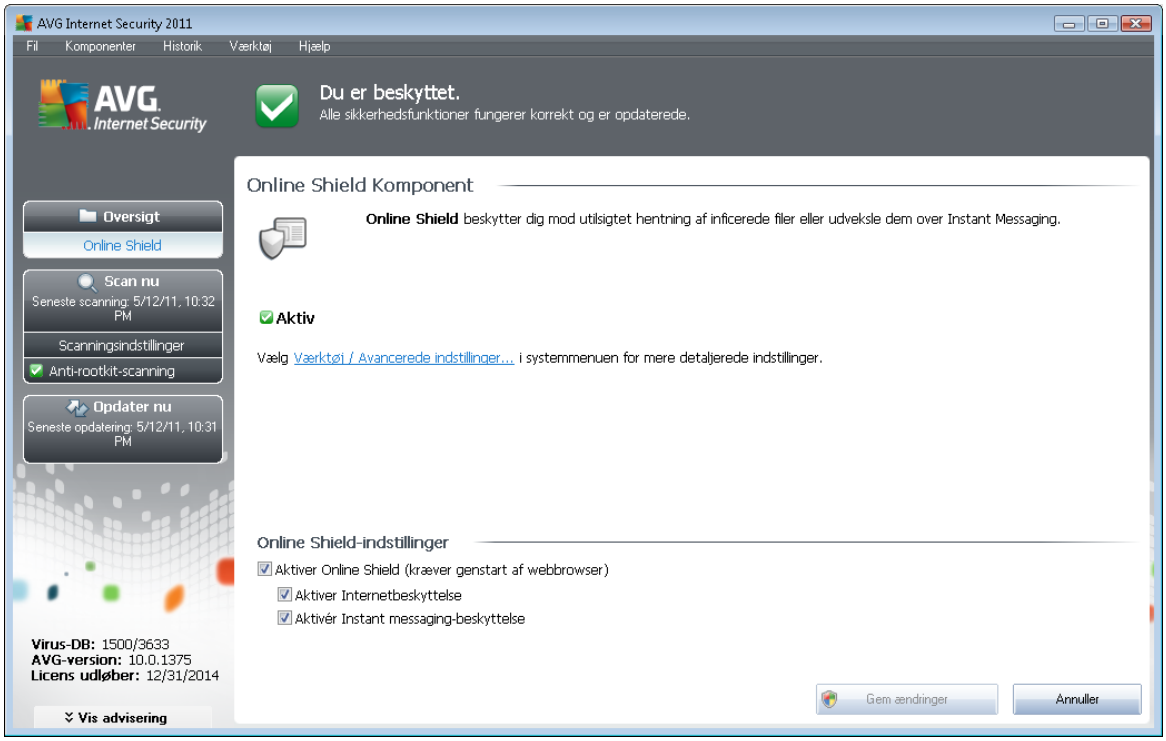
Online Shield er en form for indbygget realtidsbeskyttelse. Det scanner indholdet på besøgte websider (*og evt. filer på dem*), før de vises i din webbrowser eller downloades til din computer.

Online 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 Online Shield er ikke beregnet til serverplatforme!*

7.13.2. Online Shield-grænseflade

Online Shield-komponentens grænseflade beskriver opførslen for denne beskyttelsestype. Du kan desuden finde oplysninger om komponentens aktuelle status. I den nederste del af dialogen kan du finde de elementære redigeringsmuligheder for denne komponents funktionalitet:



Online Shield-indstillinger

Først og fremmest har du mulighed for omgående at slå ***Web Shield*** til/fra ved at markere elementet ***Aktivér Online Shield***. Denne indstilling er slået til som standard, og ***Online 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 ***Online Shield*** kører, aktiveres yderligere to konfigurationsmuligheder:

- ***Aktiver internetbeskyttelse*** - denne indstilling bekræfter, at ***Online Shield*** skal udføre en scanning af indhold på websiden.
- ***Aktivér Instant messaging-beskyttelse*** - markér dette element, hvis du ønsker, at ***Online Shield*** skal verificere, at instant messaging-kommunikation (*f.eks. ICQ, MSN Messenger, ...*) er virusfri.

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 ***Online 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*)

7.13.3. Online Shield-detektering

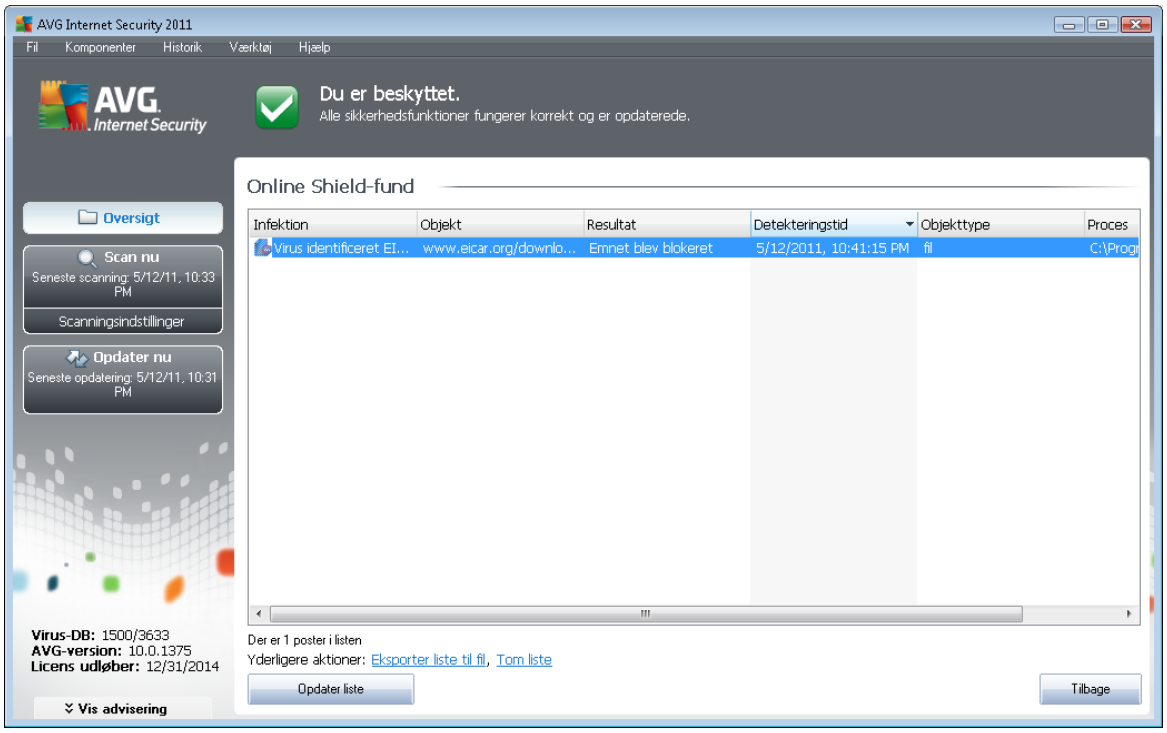
Online Shield scanner indholdet på besøgte websider og eventuelle filer på dem, før de vises i din webbrowser eller downloades til din computer. Hvis en trussel detekteres, bliver du omgående advaret med følgende dialog:

I denne advarselsdialog vil du finde data om den fil, der blev detekteret og defineret som inficeret (*Filnavn*), navnet på den genkendte infektion (*Trusselnavn*), og et link til ***Virus-opslagsværket***, hvor du kan finde detaljerede oplysninger om den detekteres infektion (*hvis den kendes*). Dialogboksen undeholder følgende knapper:

- ***Vis detaljer*** - klik på knappen ***Vis detaljer*** for at åbne et nyt popup-vindue, hvor du vil finde oplysninger om den proces, der var i gang, da infektionen blev detekteret, samt processens identifikation.

- ***Luk*** - klik på knappen for at lukke advarselsdialogen.

Den mistænkelige webside bliver ikke åbnet, og trusseldetekteringen bliver logget i listen over ***Online Shield-fund*** - denne oversigt over detekterede trusler er tilgængelig via systemmenuen ***Historik / Online Shield-fund***.



For hvert detekteret objekt findes følgende oplysninger:

- ***Infektion*** - beskrivelse af (*muligvis også navn på*) det detekterede objekt

- ***Objekt*** objektkilde (*webside*)

- ***Resultat*** - handling udført med det detekterede objekt

- ***Detekteringstid*** - dato og klokkeslæt, hvor truslen blev detekteret og blokeret

- ***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 ***Online Shield***. Med knappen ***Tilbage*** skifter du tilbage til den standard ***AVG-brugergrænseflade*** (*komponentoversigt*).

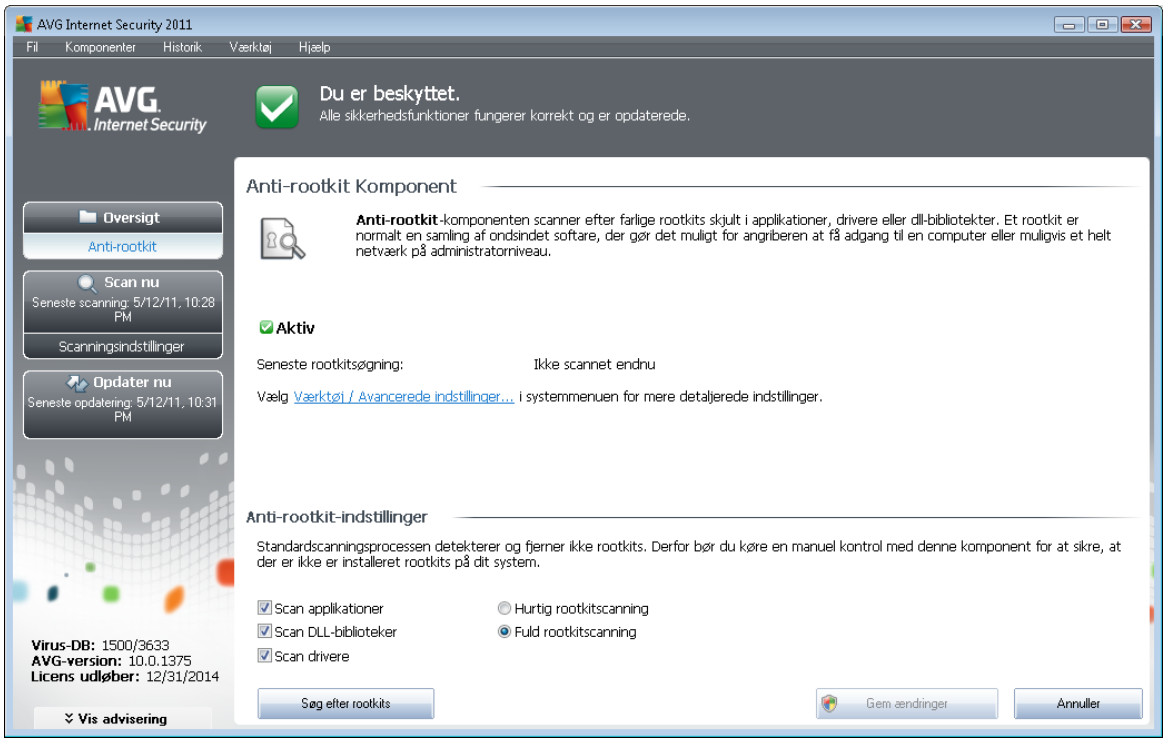
7.14. Anti-rootkit

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.

7.14.1. Anti-rootkit-principper

AVG 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. ***AVG Anti-rootkit*** kan detektere rootkits baseret på det foruddefineret sæt af regler. Bemærk, at alle rootkits detekteres (*ikke kun de inficerede*). Hvis ***AVG Anti-rootkit*** finder et rootkit, betyder det ikke nødvendigvis, at rootkit'et er inficeret. Nogle gange bruges rootkits som drivere, eller de er en del af rigtige applikationer.

7.14.2. Anti-rootkit-grænseflade



Brugergrænsefladen ***Anti-rootkit*** giver en kort beskrivelse af komponentens funktionalitet, informerer om komponentens aktuelle status og giver oplysninger om sidste gang, ***Anti-rootkit***-testen blev kørt

(***Seneste rootkitsøgning***). Dialogen ***Anti-rootkit*** indeholder også linket ***Værktøjer/Avancerede indstillinger***. Brug linket for at komme til miljøet for avanceret konfiguration af ***Anti-rootkit***-komponenten.

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.*

Anti-rootkit-indstillinger

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 alle igangværende processer, indlæste drivere og systemapper (*typisk c:\Windows*)
- ***Fuld rootkitscanning*** - scanner alle igangværende processer, indlæste drivere, systemmapper (*typisk c:\Windows*), samt alle lokale drev (*inklusive flashdrev, men ikke floppydrev/CD-drev*)

Betjeningsknapper

- ***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

7.15. Systemværktøjer

Systemværktøjer henviser til værktøjer, der giver en detaljeret oversigt over **AVG Internet-sikkerhed 2011** miljøet og operativsystemet. Komponenten viser en oversigt over:

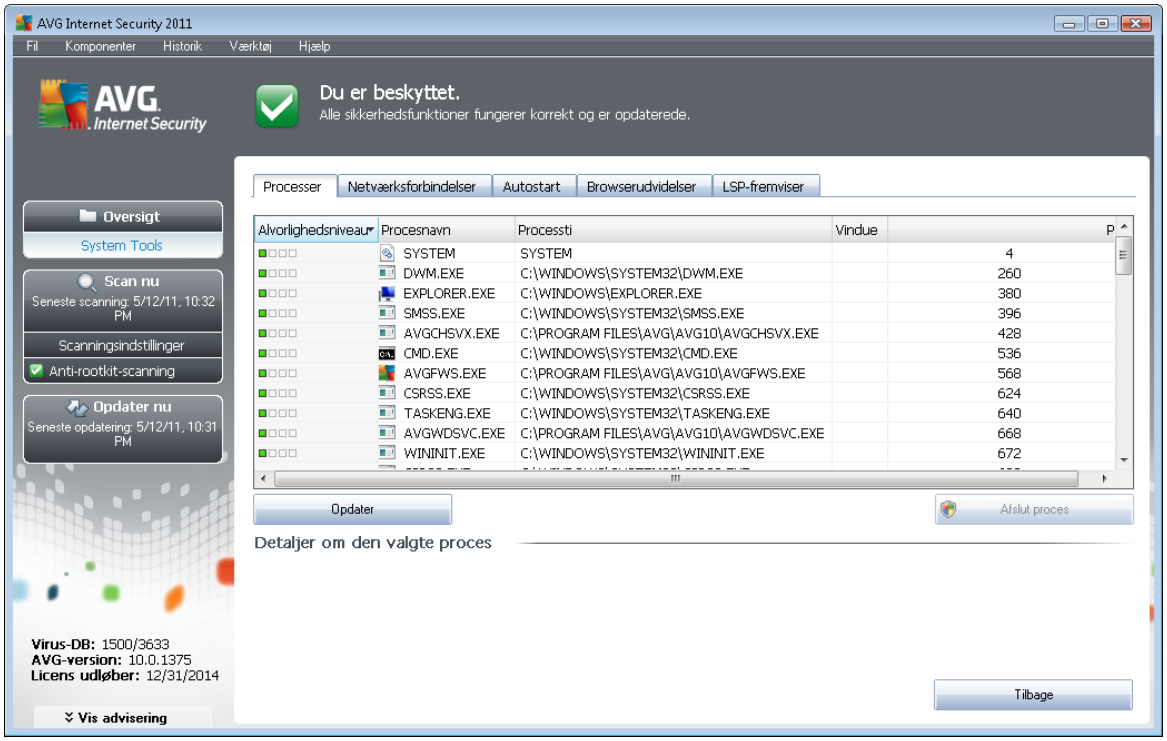
- Processer - liste med de processer (*dvs. kørende applikationer*), som aktuelt er aktive på

din computer

- Netværksforbindelser - liste med de aktuelt aktive forbindelser
- Autostart - liste med alle de applikationer, der igangsættes under opstart af Windows
- Browserudvidelser - liste med plugins (*dvs. applikationer*), som installeres i din internetbrowser
- LSP-fremviser - liste med LSP-udbydere (*Layered Service Providers*)

Specifikke oversigter kan også redigeres, men det anbefales kun for meget erfarne brugere!

7.15.1. Processer



Dialogen ***Processer*** indeholder en liste over processer (*dvs. kørende applikationer*), der aktuelt er aktive på din computer. Listen er opdelt i flere kolonner:

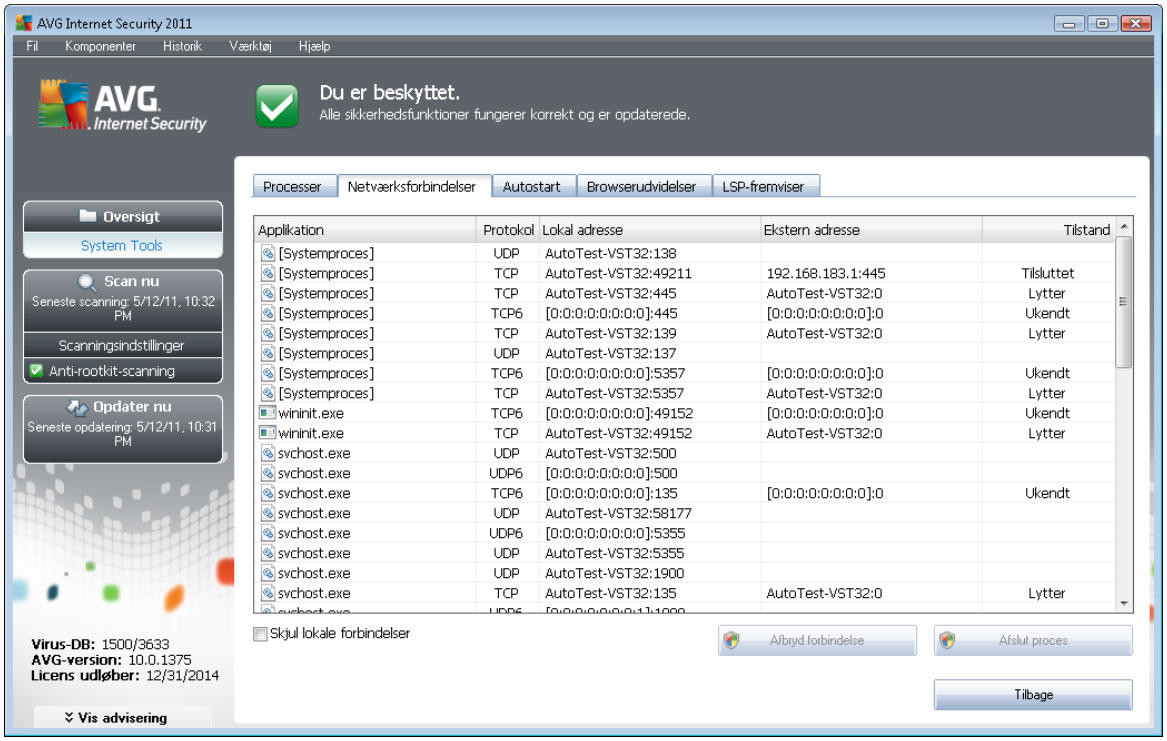
- ***Alvorlighedsniveau*** - grafisk identifikation af den pågældende proces' alvorlighed på en firetrins skala fra mindre vigtig (■□□□) op til kritisk (■■■■)
- ***Procesnavn*** - navn på den kørende proces
- ***Processti*** - fysisk sti til den kørende proces
- ***Vindue*** - indikerer om muligt navnet på applikationsvinduet
- ***PID*** - procesidentifikationsnummer er en unik, intern procesidentifikation i Windows

Betjeningsknapper

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

- ***Opdater*** - opdaterer listen over processer i henhold til den aktuelle status
- ***Afslut proces*** - du kan vælge en eller flere applikationer og derefter afslutte dem ved at trykke på denne knap. ***Det anbefales kraftigt, at du ikke afslutter applikationer, medmindre du er helt sikker på, at de udgør en virkelig trussel!***
- ***Tilbage*** - skifter tilbage til den almindelige AVG-brugergrænseflade (*komponentoversigt*)

7.15.2. Netværksforbindelser



Dialogen ***Netværksforbindelser*** indeholder en liste over aktuelt aktive forbindelser. Listen er opdelt i følgende kolonner:

- ***Program*** - navnet på det program, der er knyttet til forbindelsen (*med undtagelse af Windows 2000, hvor oplysningerne ikke er tilgængelige*)
- ***Protokol*** - overførselsprotokoltypen der anvendes til forbindelsen:
  - TCP - protokol, der anvendes sammen med Internetprotokol (IP) til at overføre oplysninger via internettet
  - UDP - alternativ til TCP-protokollen

- ***Lokal adresse*** - IP-adresse på den lokale computer og det anvendte portnummer
- ***Ekstern adresse*** - IP-adresse på den eksterne computer og det portnummer, der er oprettet forbindelse til. Hvis det er muligt, slår den også værtsnavnet på den eksterne computer op.
- ***Tilstand*** - indikerer den mest sandsynlige aktuelle tilstand (*Tilsluttet, Server bør lukke, Lytter, Aktiv lukning afsluttet, Passiv lukning, Aktiv lukning*

For kun at anføre eksterne forbindelser skal du markere afkrydsningsfeltet ***Skjul lokale forbindelser*** i den nederste sektion af dialogen under listen.

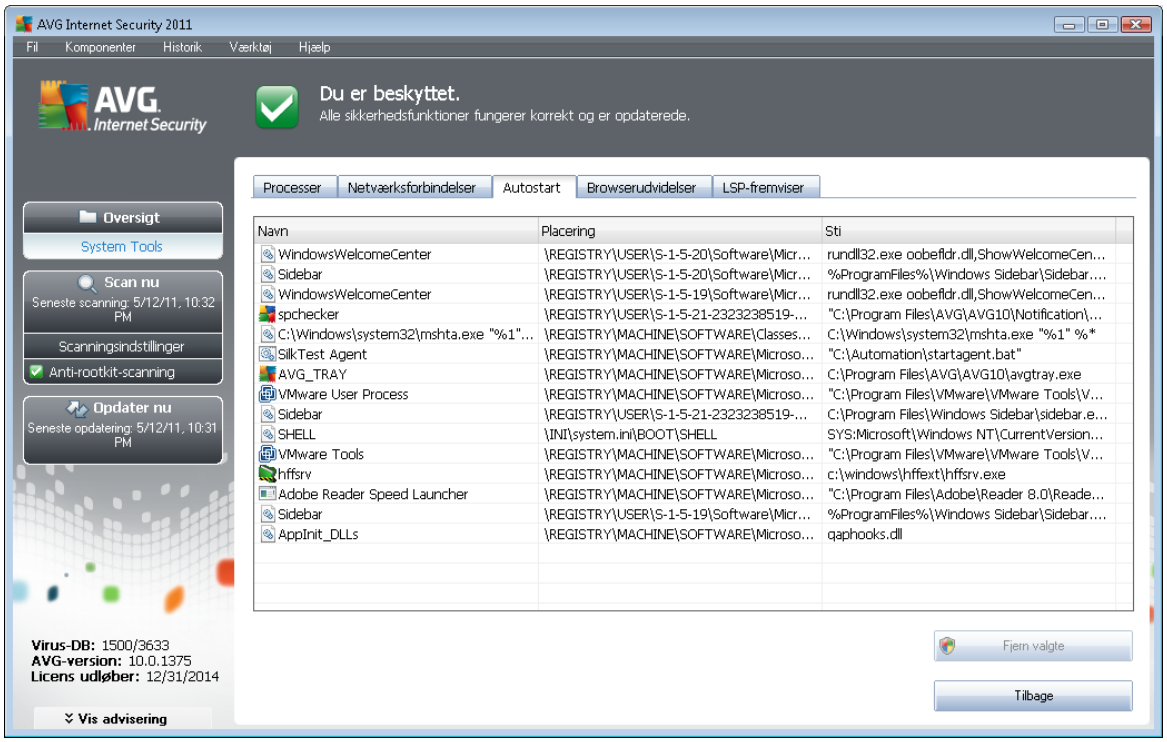
Betjeningsknapper

De tilgængelige betjeningsknapper er:

- ***Afslut forbindelse*** - lukker en eller flere valgte forbindelser i listen
- ***Afslut proces*** - lukker en eller flere applikationer, der er knyttet til de valgte forbindelser i listen
- ***Tilbage*** - skift tilbage til den almindelige ***AVG-brugerfalde*** (komponentoversigt).

Undertiden er det kun muligt at afslutte applikationer, der aktuelt er i tilsluttet tilstand. Det anbefales kraftigt, at du ikke afslutter forbindelser, medmindre du er helt sikker på, at de udgør en virkelig trussel!

7.15.3. Autostart

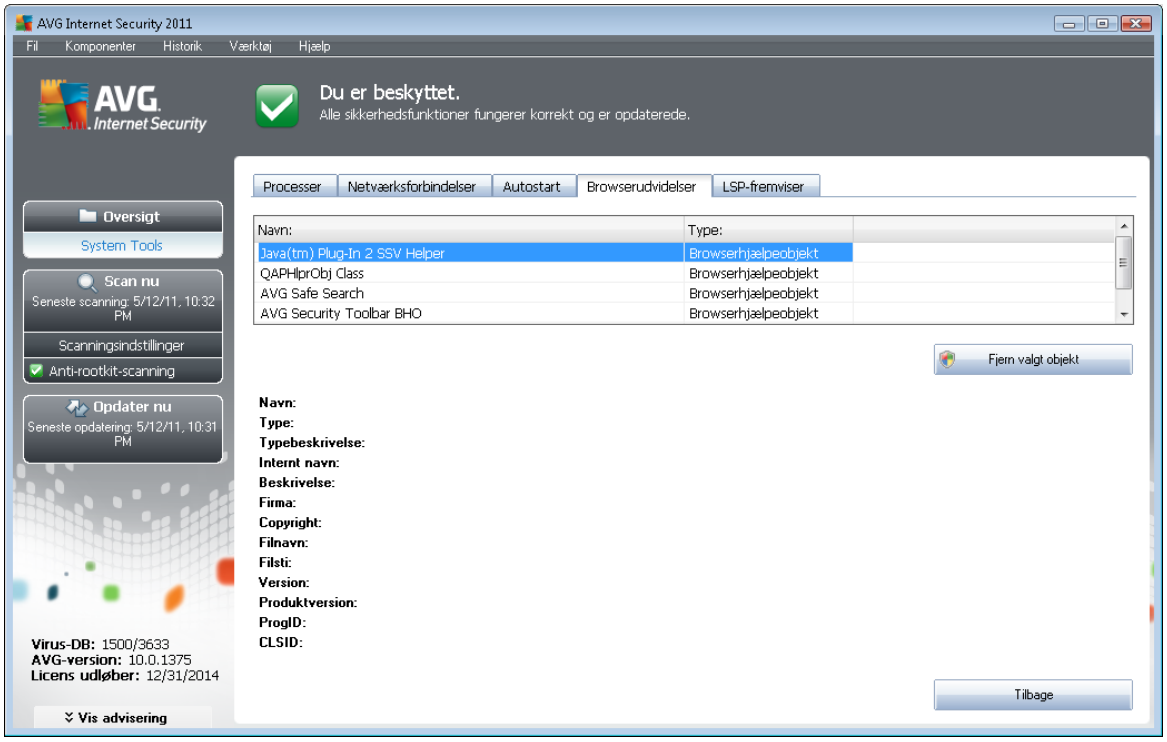


Dialogen ***Autostart*** viser en liste over alle applikationer, der køres under opstart af Windows. Meget ofte føjer malware-applikationer automatisk sig selv til opstartpunktet i registreringsdatabasen.

Du kan slette en eller flere poster ved at vælge dem og trykke på knappen ***Fjern valgte.*** Med knappen ***Tilbage*** skifter du tilbage til den standard AVG-brugergrænseflade (*komponentoversigt*).

Det anbefales kraftigt, at du ikke sletter applikationer, medmindre du er helt sikker på, at de udgør en virkelig trussel!

7.15.4. Browserudvidelser



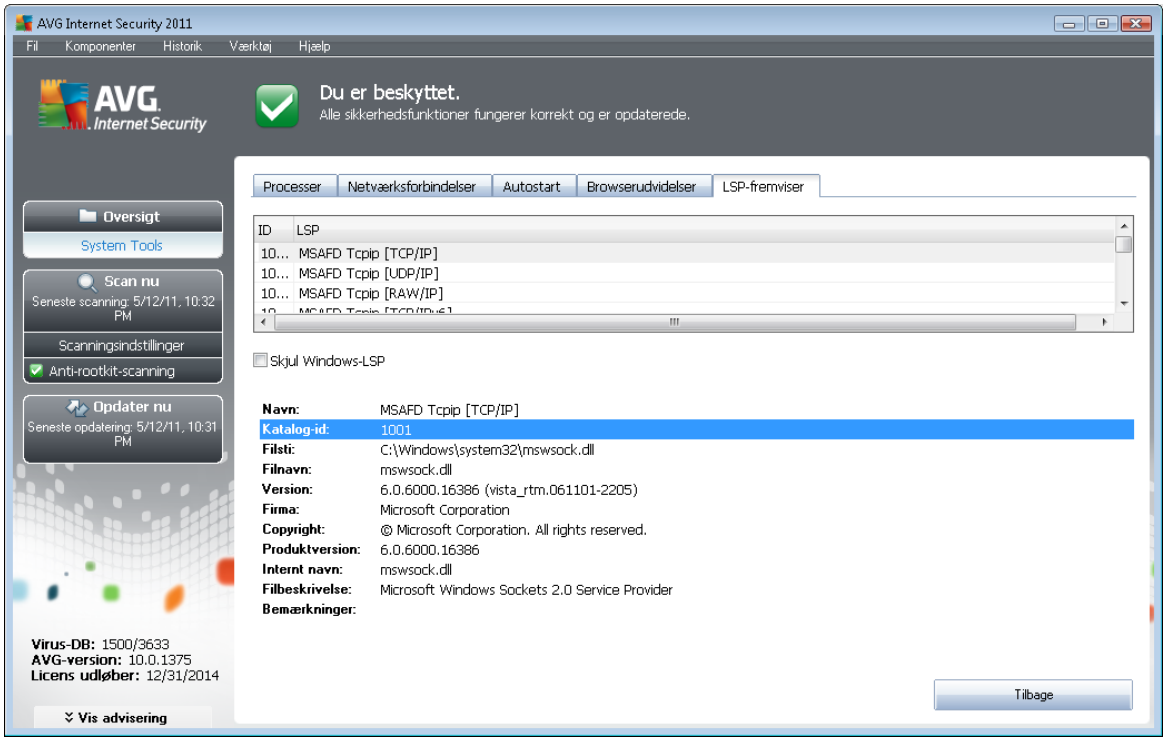
Dialogen ***Browserudvidelser*** indeholder en liste over plugins (*dvs. applikationer*), der er installeret i din internetbrowser. Listen kan indeholde almindelige applikations-plug-ins samt potentielle malware-programmer. Klik på et objekt i listen for at få detaljerede oplysninger om det valgte plugin, der vises i dialogens nederste sektion.

Betjeningsknapper

Betjeningsknapperne, der er tilgængelige på fanen ***Browserudvidelse***, er:

- ***Fjern valgt objekt*** - fjerner det plugin, der i øjeblikket er fremhævet i listen. ***Det anbefales kraftigt, at du ikke sletter plugins, medmindre du er helt sikker på, at de udgør en virkelig trussel!***
- ***Tilbage*** - skifter tilbage til den almindelige ***AVG-brugerflade*** (komponentoversigt)

7.15.5. LSP-fremviser



Dialogen ***LSP-fremviser*** viser en liste over LSP-udbydere (Layered Sercice Provider).

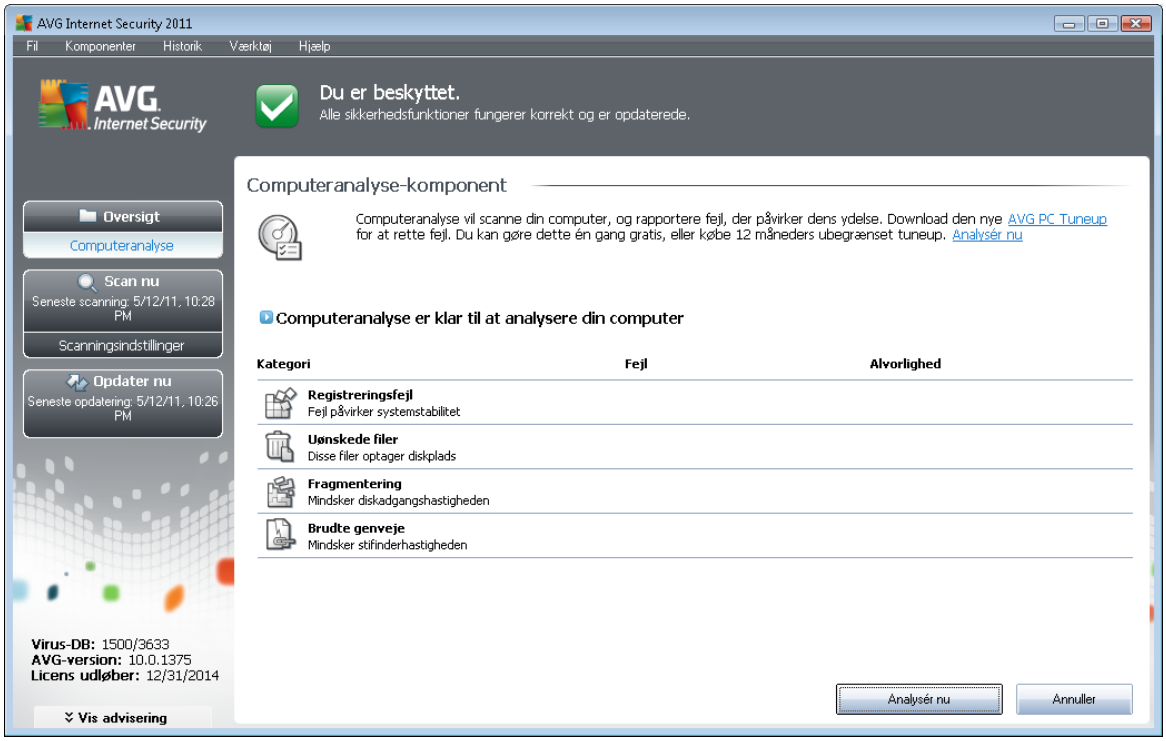
En ***Layered Service Provider*** (LSP) er en systemdriver, der er kædet ind i Windows' netværksservices. Den har adgang til alle de data, der kommer ind i og forlader computeren, inklusive muligheden for at ændre disse data. Nogle LSP'er er nødvendige for at Windows kan etablere tilslutning til andre computere, herunder internettet. Imidlertid kan visse malware-applikationer også installere sig selv som en LSP, og dermed få adgang til alle de data, din computer transmitterer. Derfor kan denne oversigt muligvis hjælpe dig til at kunne kontrollere alle mulige LSP-trusler.

Det er under visse omstændigheder muligt at reparere brudte LSP'er (*f.eks. hvis filen er blevet fjernet, men registreringsdatabase-elementerne forbliver uberørte*). Der vises en ny knap til rettelse af problemet, når en reparerbar LSP findes.

For at inkludere Windows LSP'er i listen, skal du fjerne markeringen i afkrydsningsfeltet ***Skjul Windows LSP.*** Med knappen ***Tilbage*** skifter du tilbage til den standard ***AVG-brugergrænseflade*** (*komponentoversigt*).

7.16. Computeranalyse

Komponenten ***Computeranalyse*** kan scanne din computer for systemproblemer, og give dig en gennemsigtig oversigt over, hvad der nedsætter din computers overordnede ydelse. I komponentens brugergrænseflade kan du se et diagram, der opdelt i fire linjer, som henviser til de respektive kategorier: registreringsdatabasefejl, junkfiler, fragmentering og brudte genveje



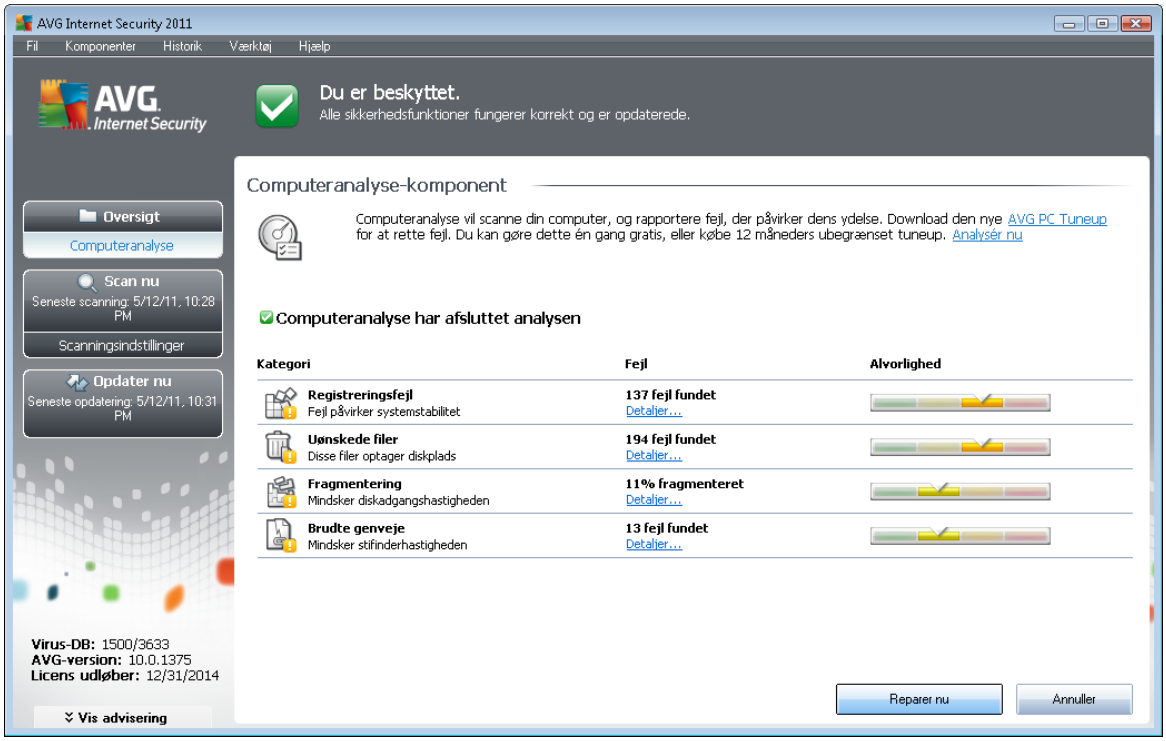
- ***Registerfejl*** vil vise dig antallet af fejl i Windows registreringsdatabase. Da det kræver avanceret kendskab at reparere registreringsdatabasen, fraråder vi at forsøge selv at reparere den.

- ***Uønskede filer*** vil vise dig antallet af filer, du højst sandsynligt kan undvære. Disse vil typisk være mange slags midlertidige filer, og filer i Papirkurven.

- ***Fragmentering*** vil beregne procentdelen af din harddisk, der er fragmenteret, dvs. har været brugt i lang tid, så de fleste filer nu er spredt på forskellige dele af den fysiske disk. Du kan bruge et defragmenteringsværktøj til at løse dette.

- ***Brudte genveje*** vil informere dig om genveje, der ikke længere virker, fører til ikke-eksisterende placeringer, osv.

For at starte analyse af systemet skal du trykke på knappen ***Analyser nu***. Du vil kunne se analyseforløbet, og resultaterne vises direkte i diagrammet:



Resultatoversigten viser antallet af detekterede systemproblemer (***Fejl***), der er opdelt iht. de respektive testede kategorier. Analyseresultaterne vises også grafisk i kolonnen ***Alvorlighed***.

Betjeningsknapper

- ***Analyser nu*** (*vises inden analysen starter*) - tryk på denne knap for øjeblikkeligt at starte analysen af din computer
- ***Reparér nu***(*vises når analysen er fuldført*) - tryk på knappen for at komme til AVG's websted (http://www.avg.com/) på siden med detaljerede og opdaterede oplysninger, der relaterer til komponenten ***Computeranalyse***
- ***Annullér*** - tryk på denne knap for at stoppe den igangværende analyse, eller for at vende tilbage til den standard AVG-brugergrænseflade (*komponentoversigt*), når analysen er fuldført

7.17. ID-beskyttelse

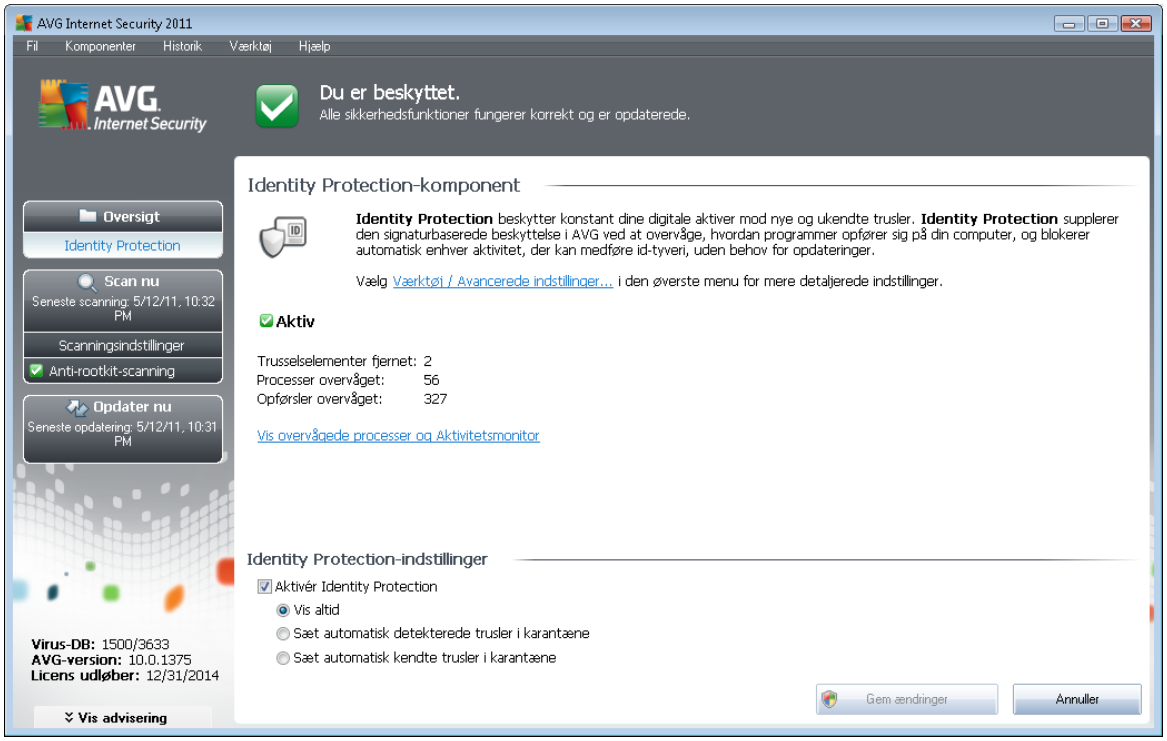
AVG Identitetsbeskyttelse er et antimalware-produkt, som fokuerer på at forhindre indentitetstyve i at sjæle dine adgangskoder, bankkontooplysninger, kreditkortnumre og andre personlige digitale værdier fra alle former for ondsindet software (*malware*), som er rettet mod din pc. Det sørger for, at alle programmer, der kører på din pc, fungerer korrekt. ***AVG Identitetsbeskyttelse*** opdager og blokerer kontinuerligt mistænkelig adfærd og beskytter din computer mod al ny malware.

7.17.1. ID-beskyttelse-principper

AVG Identetsbeskyttelse er en antimalware-komponent, som beskytter dig mod alle former for malware (*spyware, botter, identitetstyveri, ...*) ved hjælp af adfærdsteknologi og yder dag nul-beskyttelse mod nye vira. Efterhånden som malware bliver sofistikeret og kommer i form af normale programmer, som kan åbne din pc for identitetstyveri fra den eksterne angriber, sikrer ***AVG Identitetsbeskyttelse*** dig mod denne nye eksekveringsbaserede malware. Det er en supplerende beskyttelse til ***AVG Antivirus***, som beskytter dig mod filbaserede og kendte vira ved hjælp af signaturmekanismer og scanning.

Vi anbefaler på det kraftigste, at du har installeret begge komponenterne AVG Antivirus- og AVG Identitetsbeskyttelse for at have komplet beskyttelse af din pc.

7.17.2. ID-beskyttelse-grænseflade



Identitetsbeskyttelse-komponentens grænsefade indeholder en kort beskrivelse af komponentens grundlæggende funktionalitet, dens status og nogle statistiske data:

- ***Fjernede malware-elementer*** - indeholder antallet af applikationer detekteret som malware og fjernet
- ***Overvågede processer*** - antal aktuelt kørende applikationer, der overvåges af IDP
- ***Overvågede opførsler*** - antal specifikke handlinger, der kører i de overvågede applikationer

Herunder finder du linket ***Vis overvågede processer og Aktivitetsmonitor***, som vil tage dig til brugergrænsefladen til komponenten ***Systemværktøjer***, hvor du vil finde en detaljeret oversigt med alle overvågede processer.

Identity Protection-indstillinger

I den nederste del af dialogen finder du sektionen ***Identitetsbeskyttelse-indstillinger***, hvor du kan redigere nogle af komponentens grundlæggende funktioner:

- ***Aktivér Identitetsbeskyttelse*** - (*slået til som standard*): Marker for at aktivere IDP-komponenten og åbne yderligere redigeringsmuligheder.

I visse tilfælde kan ***Identitetsbeskyttelse*** rapportere, at en ligitim fil er mistænkelig eller farlig. Fordi ***Identitetsbeskyttelse*** detekterer trusler baseret på deres opførsel. Dette sker normalt, når et program forsøger at overvåge tastetryk, installere andre programmer, eller en ny driver installeres på computeren. Derfor skal du vælge en af nedenstående indstillinger, der specificerer ***Identitetsbeskyttelse***-komponentens opførsel ved detektering af en mistænkelig aktivitet:

  - ***Vis altid*** - hvis en applikation detekteres som malware, vil du blive spurgt, om den skal blokeres (*denne valgmulighed er slået til som standard og det anbefales ikke at ændre den, medmindre du har en reel grund til det*
  - ***Sæt automatisk detekterede trusler i karantæne*** - alle applikationer, der detekteres som malware, bliver blokeret automatisk
  - ***Sæt automatisk kendte trusler i karantæne*** - kun applikationer, der med absolut vished detekteres som malware, vil blive blokeret

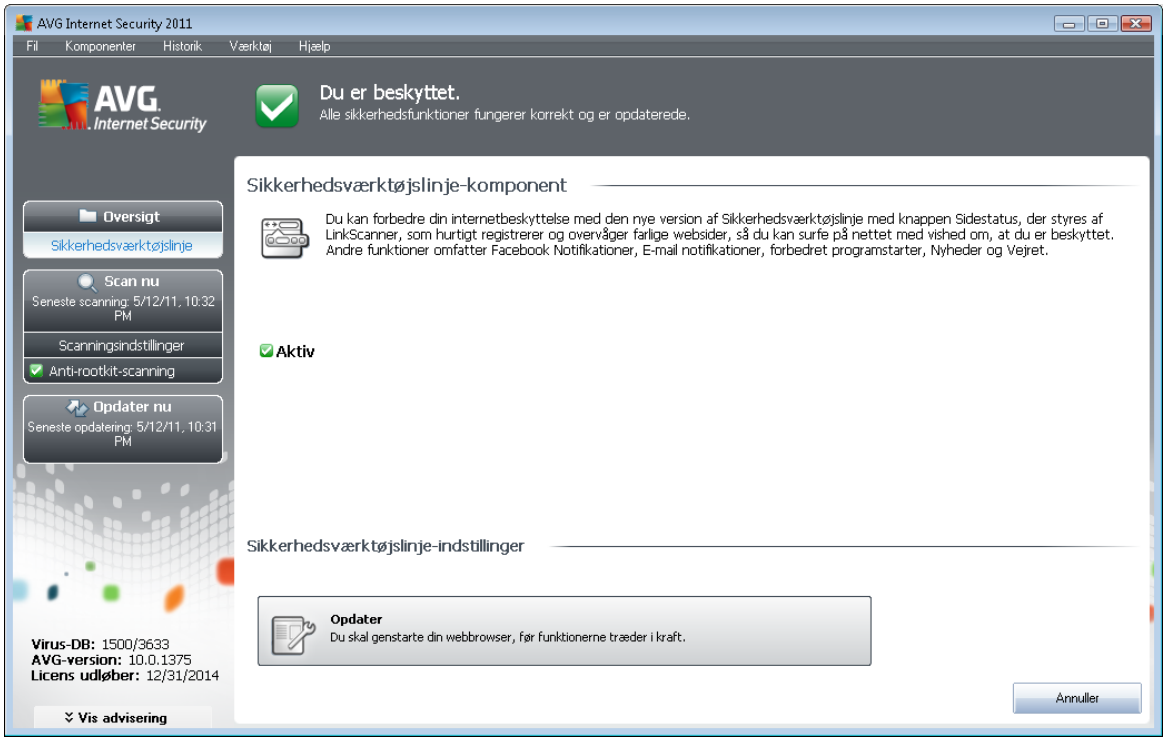
Betjeningsknapper

Følgende betjeningsknapper er tilgængelige i ***Identitetsbeskyttelse***-grænsefladen:

- ***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*)

7.18. Sikkerhedsværktøjslinje

Sikkerhedsværktøjslinjen er en valgfri webbrowserværktøjslinje, der tilbyder øget AVG-beskyttelse og forskellige funktioner og værktøjer, mens du surfer på nettet. På nuværende tidspunkt understøttes ***Sikkerhedsværktøjslinjen*** af webbrowserne Internet Explorer (*6.0 eller højere)*, og Mozilla Firefox *(3.0 eller højere*):



Alle indstillinger for ***Sikkerhedsværktøjslinje***-komponenten er tilgængelige direkte i ***Sikkerhedsværktøjslinjen*** i webbrowseren.

8. AVG Sikkerhedsværktøjslinje

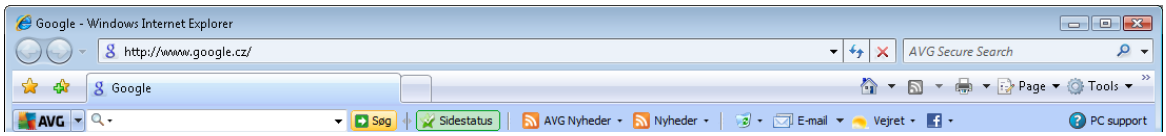
AVG Sikkerhedsværktøjslinje er et nyt værktøj, der arbejder sammen med ***LinkScanner*-komponenten.** ***AVG Sikkerhedsværktøjslinjen*** kan bruges til at styre***LinkScanner*'s** funktioner og til at tilpasse dens opførsel.

Hvis du vælger at installere værktøjslinjen under installationen af **AVG Internet-sikkerhed 2011**, vil den automatisk blive føjet til din webbrowser (*Internet Explorer 6.0 eller højere, og Mozilla Firefox 3.0 eller højere*). Andre internetbrowsere understøttes ikke på nuværende tidspunkt.

Bemærk! *Hvis du bruger en ny, alternativ internetbrowser (f.eks. Avant), kan du opleve uventet adfærd.*

8.1. AVG Sikkerhedsværktøjslinje-grænseflade

AVG Sikkerhedsværktøjslinje er designet til at fungere med ***MS Internet Explorer*** (*version 6.0 eller højere*) og ***Mozilla Firefox*** (*version 3.0 eller højere*). Når du har besluttet, at du vil installere ***Sikkerhedsværktøjslinje*** (*under AVG installationsprocessen blev du bedt om at beslutte, om du ville installere komponenten eller ej*), bliver komponenten placeret i din webbrowser lige under adresselinjen:



AVG Sikkerhedsværktøjslinje består af følgende:

8.1.1. AVG logoknap

Denne knap giver adgang til generelle værktøjslinjepunkter. Klik på logoknappen for at blive viderestillet til AVG's websted. 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*** - åbner **AVG Internet-sikkerhed 2011** ***brugergrænsefladen***
- ***AVG Info*** - åbner en kontekstmenu med følgende links, der fører til vigtige sikkerhedsoplysninger, der relaterer til **AVG Internet-sikkerhed 2011**:
  - *Om trusler* - åbner AVG's websted på den side, der indeholde de vigtigste data om de værste trusler, anbefaler til fjernelse af virus, AVG-opdateringsoplysninger, adgang til Virusdatabase og flere relevante oplysninger
  - *AVG Nyheder* - åbner websiden med de seneste pressemeddelelser vedrørende AVG
  - *Aktuelt trusselsniveau* - åbner viruslaboratoriets webside med en grafisk visning af det aktuelle trusselsniveau på nettet

- *AVG trusselslaboratorier* - åbner websiden AVG-webstedsrapporter, hvor du kan søge efter specifikke trusler efter navn, og få detaljerede oplysninger om hver trussel

- ***Indstillinger*** - åbner en konfigurationsdialog, hvor du kan justere dine ***AVG Sikkerhedsværktøjslinje***-indstillinger, så de passer til dine behov - se følgende kapitel ***Indstillinger for AVG Sikkerhedsværktøjslinje***

- ***Slet historik*** - lader dig i ***AVG Sikkerhedsværktøjslinje*** slette hele historikken, eller kun slette søgehistorikken, browserhistorikken, downloadhistorikken eller cookies.

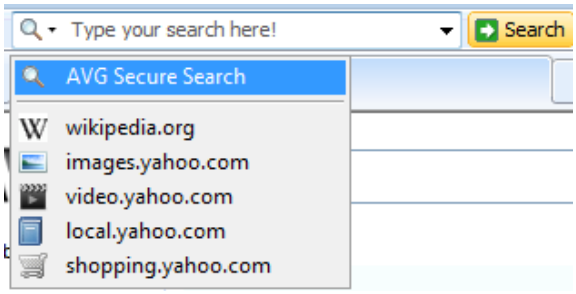
- ***Opdater*** - søger efter nye opdateringer til din ***AVG Sikkerhedsværktøjslinje***

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

8.1.2. AVG Secure Search (powered by Google)-styret søgefelt

AVG Secure Search (powered by Google)-feltet er en nem og sikker måde at søge på nettet ved hjælp af AVG Secure Search (powered by Google). Indtast et ord eller en sætning i søgefeltet og tryk på ***Søg***-knappen eller ***Enter***-tasten for at starte søgningen direkte på AVG Secure Search (powered by Google)-serveren, uanset hvilken side der aktuelt vises. Søgefeltet viser også en liste over din søgehistorik. Søgninger foretaget med søgefeltet analyseres ved hjælp af ***Søgeskjold***-beskyttelsen.

Du kan i søgefeltet også skifte til Wikipedia, eller en anden specifik søgetjeneste - se billedet:



8.1.3. Sidestatus

Direkte i værktøjslinjen viser denne knap evalueringen af den aktuelt viste webside, baseret på kriterierne for ***Surfskjold***-komponenten:

- - Siden der linkes til er sikker

- - Siden er noget mistænkelig.

- - Siden indeholder link til definitivt farlige sider.

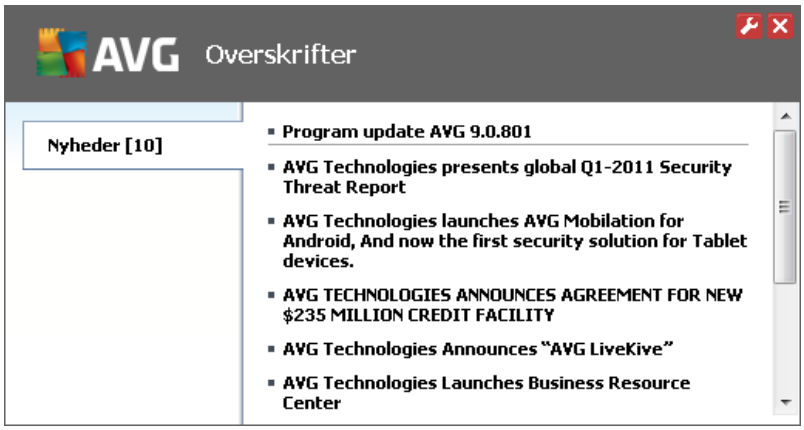
- - Siden der linkes til indeholder aktive trusler! For din egen sikkerhed får du ikke tilladelse til at besøge denne side.

-  - siden er ikke tilgængelig og kunne derfor ikke scannes.

Klik på knappen for at åbne et informationspanel med detaljerede data om den specifikke webside.

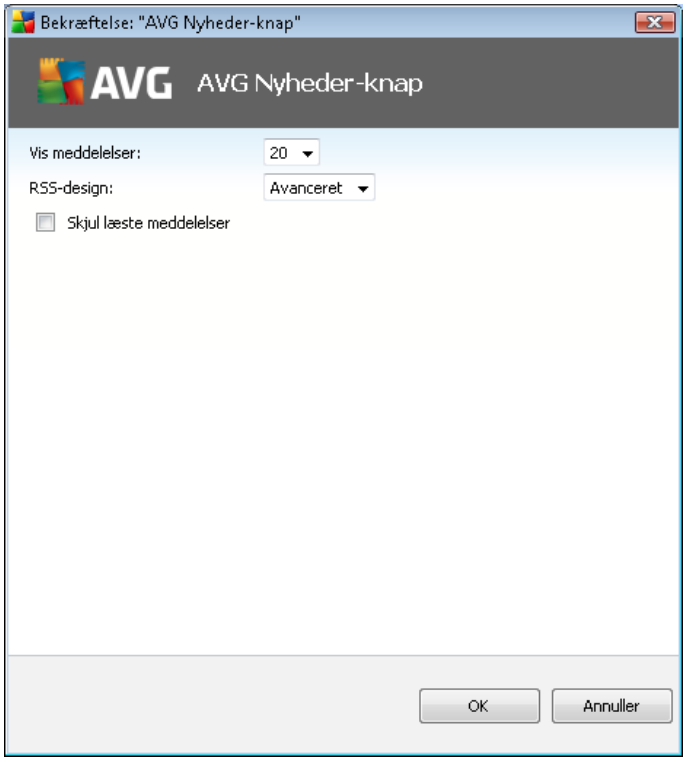
8.1.4. AVG Nyheder

Direkte fra ***AVG Sikkerhedsværktøjslinje*** åbner denne knap en oversigt over de seneste ***Nyhedsoverskrifter***, der relaterer til AVG, både fra pressen og firmapressemeddelelser:



Øverst til højre kan du se to røde kontrolknapper:

-  - knappen åbner redigeringsvinduet, hvor du kan angive parametre for knappen ***AVG Nyheder***, som vises i ***AVG Sikkerhedsværktøjslinje***:

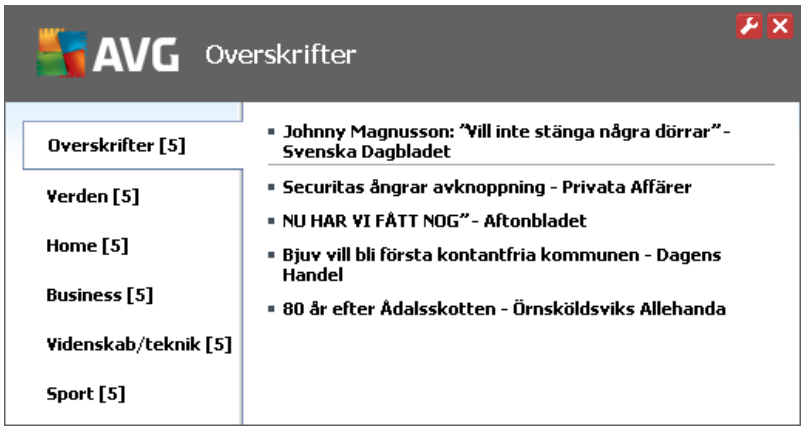


- o ***Vis meddelelser*** - skift det ønskede antal meddelelser, der skal vises ad gangen
- o ***RSS design*** - vælg mellem Avanceret/Grundlæggende tilstand for den aktuelle visning af nyhedsoversigten (*Avanceret tilstand er valgt som standard - se billedet herover*)
- o ***Skjul læste meddelelser*** - markér dette element for at bekræfte, at hver læst meddelelse ikke skal vises mere, så du kan se nye meddelelser

- - klik på denne knap for at lukke den aktuelt åbne nyhedsoversigt

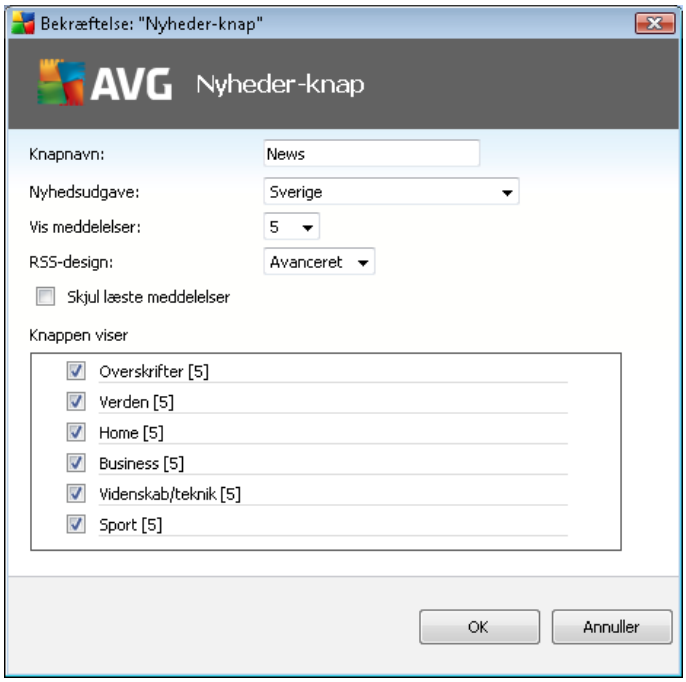
8.1.5. Nyheder

Ligeledes vil denne knap direkte fra ***AVG Sikkerhedsværktøjslinje*** åbne en oversigt over de seneste nyheder fra valgte medier, der er opdelt i flere sektioner:



Øverst til højre kan du se to røde kontrolknapper:

-  - knappen åbner redigeringsvinduet, hvor du kan angive parametre for knappen ***Nyheder*** , som vises i ***AVG Sikkerhedsværktøjslinje***:



o ***Knapnavn*** - du har mulighed for at ændre knapnavnet, som vises i ***AVG Sikkerhedsværktøjslinje***

o ***Nyhedsudgave*** - vælg et land fra listen for at få vist nyheder fra det valgte område
o ***Vis meddelelser*** - angiv det ønskede antal meddelelser, der skal vises ad gangen
o ***RSS-design*** - skift mellem valgmuligheden Grundlæggende/Avanceret for at vælge designet på

nyhedsoversigten (***avanceret design er indstillet som standard, se billedet herover***)

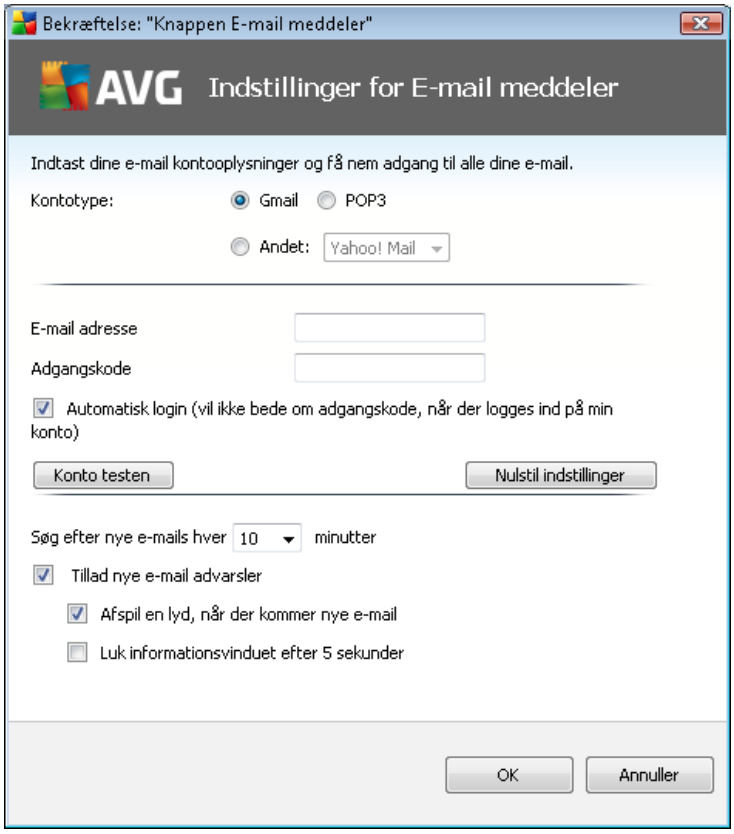
- ***Skjul læste meddelelser*** - markér dette element for at bekræfte, at hver læst meddelelse ikke længere skal vises i nyhedsoversigten, og skal erstattes af en ny overskrift
- ***Knappen viser*** - i dette felt kan du angive, hvilken type nyheder der skal vises i ***AVG Sikkerhedsværktøjslinjens*** nyhedsoversigt
  - - klik på denne knap for at lukke den aktuelt åbne nyhedsoversigt

8.1.6. Slet historik

Med denne knap kan du slette historikken for din browser ligesom via valgmuligheden ***AVG logo -> Slet historik***.

8.1.7. E-mail meddeler

Med knappen ***E-mail meddeleler*** kan du aktivere muligheden for at blive informeret om nye e-mail direkte i ***AVG Sikkerhedsværktøjslinje***-grænsefladen. Knappen åbner følgende redigeringsvindue, hvor du kan definere parametre for din e-mailkonto og e-mailvisningsregler Følg instruktionerne i dialogen:



- ***Kontotype*** - angiv den protokoltype, din e-mailkonto anvender. Du kan vælge mellem følgende alternativer: *Gmail*, *POP3*, eller vælge servernavnet fra rullemenuen i elementet *Andet* (*på nuværende tidspunkt kan du bruge denne mulighed, hvis din konto er på Yahoo! JP Mail eller Hotmail*). Hvis du ikke er sikker på, hvilken e-mailservertype, din konto bruger, kan du forsøge at finde oplysningerne fra din e-mailudbyder, eller din internetudbyder.

- ***Login*** - I afsnittet herunder findes det nøjagtige format på din *e-mailadresse*, og den pågældende *adgangskode*. Lad valgmuligheden *Automatisk login* være markeret, så du ikke behøver udfylde dataene hver gang.

- ***Test konto*** - Brug denne knap til at teste de indtastede oplysninger.

- ***Nulstil indstillinger*** - Fjerner hurtigt de e-mailadresseoplysninger, der er indtastet herover.

- ***Søg efter nye e-mails hver ... minutter*** - Angiv tidsintervallet, der skal bruges til at søge efter nye e-mails (*i intervallet 5-120 minutter*), og angiv om og hvordan du vil informeres om nye e-mails.

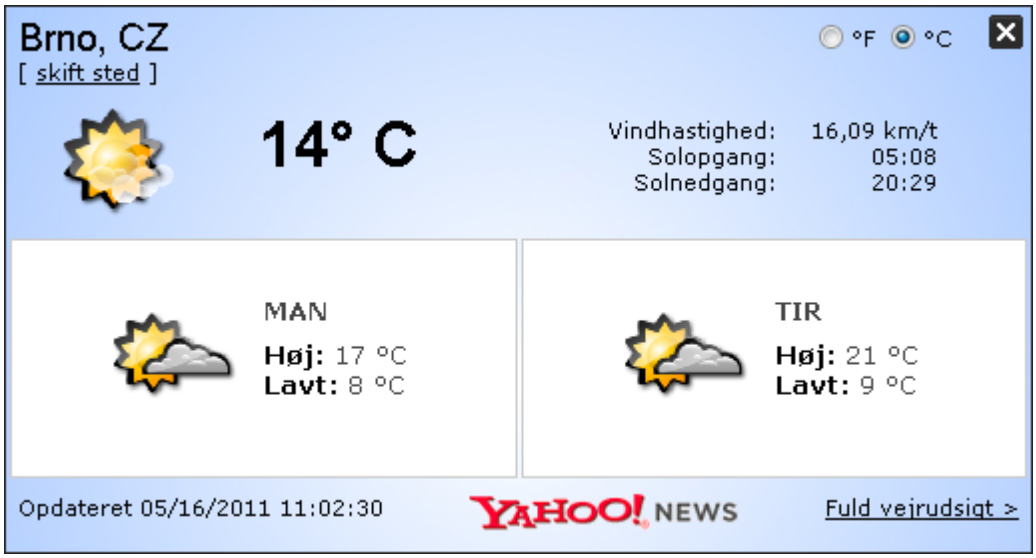
- ***Tillad nye e-mailadvarsler*** - Fjern markeringen for at deaktivere visuelle informationsmeddelelser om nye indkommende e-mailmeddelelser.

    - ***Afspil en lyd, når der kommer nye e-mail*** - Fjern markeringen for at deaktivere lydafspilning ved modtagelse af nye e-mailmeddelelser.

    - ***Luk informationsvinduet efter 5 sekunder*** - Markér dette for automatisk at lukke det visuelle informationsvindue om nye indkommende e-mailmeddelelser efter 5 sekunder.

8.1.8. Vejrudsigt

Knappen ***Vejret*** viser oplysninger om den aktuelle temperatur (*opdateres hver 3-6 time*) i den valgte destination direkte i ***AVG Sikkerhedsværktøjslinje***-grænsefladen. Klik på knappen for at åbne et ny informationspanel med en detaljeret vejroversigt:



Find herefter redigeringsmulighederne:

- ***Skift område***- klik på teksten ***Skift område***for at se en ny dialog kaldet ***Find dit område***. Indtast navnet på det ønskede område i tekstfeltet, og bekræft ved at klikke på knappen ***Søg***. Vælg derefter det ønskede område i listen over alle områder med samme navn. Til

sidst vil informationspanelet vises igen med oplysninger om vejret for det valgte område.

- ***Fahrenheit / Celsius-omregner*** - øverst til højre i informationspanelet kan du vælge mellem Fahrenheit og Celsius. Baseret på dit valg vises temperaturoplysningerne i den valgte måleenhed.

- ***Fuld vejrudsigt*** - hvis du er interesseret i en komplet og detaljeret vejrudsigt, kan du bruge linket ***Fuld vejrudsigt*** til komme til det særlige vejrwebsted på.

8.1.9. Facebook

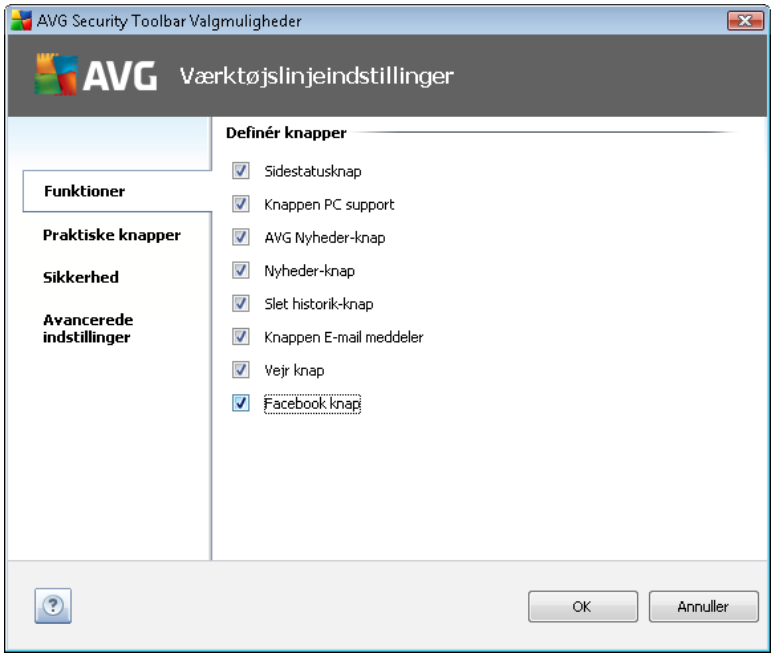
Med ***Facebook***-knappen kan du oprette forbindelse til Facebook-netværket direkte fra ***AVG Sikkerhedsværktøjslinje***. Klik på knappen for at få vist login-invitationen. Klik igen for at åbne dialogen ***Facebook login*** . Indtast dine adgangsdata, og tryk på knappen ***Tilslut***. Hvis du endnu ikke har en Facebook-konto, kan du oprette en direkte vha. linket ***Opret Facebook-konto***.

Når du er kommet gennem Facebook-registreringsforløbet, vil du blive spurgt, om du vil tillade applikationen ***AVG Social Extension***. Denne applikationsfunktion er meget vigtig for værktøjslinjen - Facebook-forbindelse, og det anbefales derfor at tillade denne funktion, så husk at tillade den. Facebook-forbindelsen vil derefter være aktiveret, og knappen ***Facebook*** i ***AVG Sikkerhedsværktøjslinje*** indeholder nu de standard Facebook-menupunkter.

8.2. AVG Sikkerhedsværktøjslinje-indstillinger

Al konfiguration af ***AVG Sikkerhedsværktøjslinje***-parametre er tilgængelig i ***AVG Sikkerhedsværktøjslinje***-panelet. Redigeringsgrænsefladen åbnes med elementet *AVG / Indstillinger* i værktøjslinjemenuen i en ny dialog med navnet ***Værktøjslinjeindstillinger***, der er inddelt i fire sektioner:

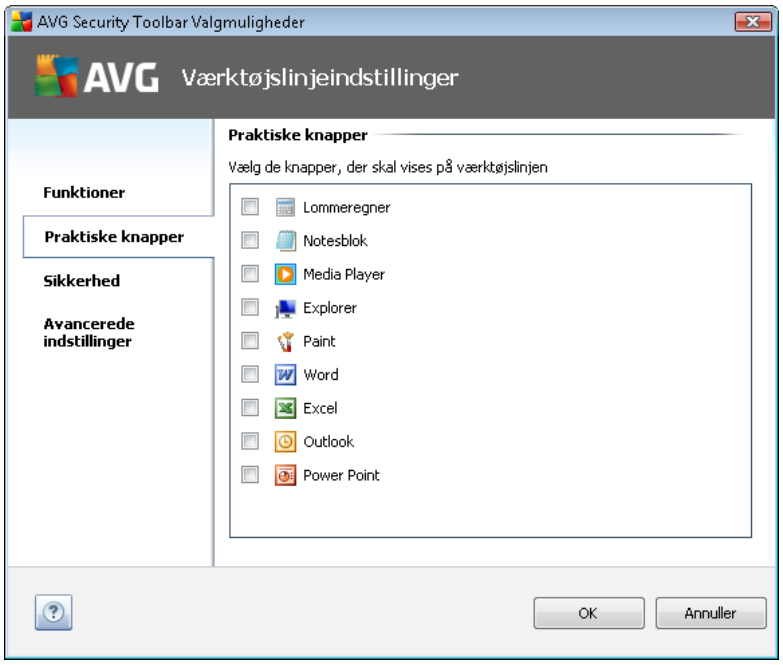
8.2.1. Fanen Generelt



På denne fane kan du angive værktøjslinjebetjeningsknapper, der skal vises eller skjules i panelet ***AVG Sikkerhedsværktøjslinje***. Markér en valgmulighed, hvis du vil have vist den pågældende knap. Desuden vil du finde en beskrivelse af funktionen af hver værktøjslinjeknap:

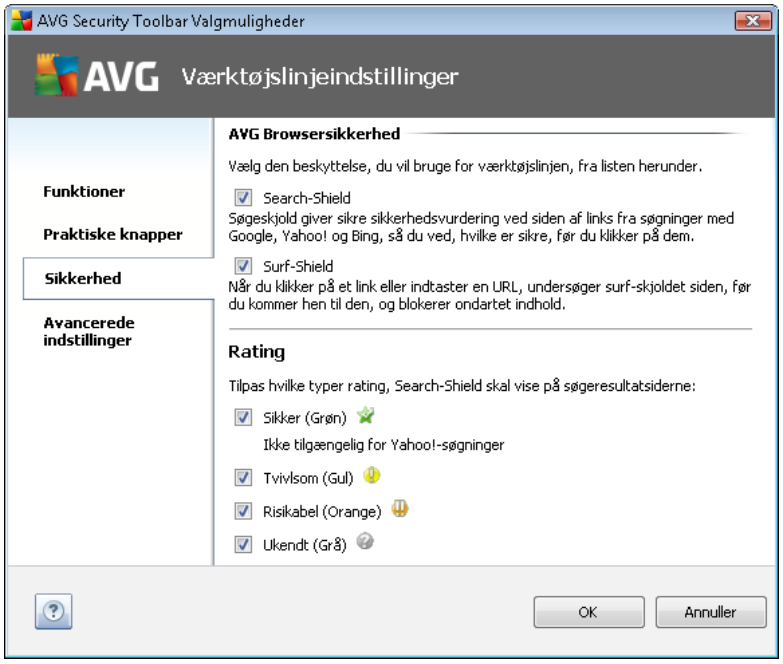
- ***Knappen Sidestatus -*** knappen giver mulighed for at få vist oplysninger om den aktuelt åbne sides sikkerhedsstatus i ***AVG Sikkerhedsværktøjslinje***
- ***Knappen AVG Nyheder*** - knappen åbner en webside med de seneste AVG relaterede pressemeddelelser
- ***Knappen Nyheder*** - knappen viser en struktureret oversigt over aktuelle nyheder fra den daglige presse
- ***Slet historik-knap*** - med denne knap kan du bruge funktionerne Slet komplet historik eller Slet søgehistorik, Slet browserhistorik, Slet downloadhistorik, eller Slet cookies direkte fra AVG Sikkerhedsværktøjslinje-panelet
- ***Knappen E-mail meddeler*** - knappen lader dig se nye indkommende e-mails i grænsefladen ***AVG Sikkerhedsværktøjslinje***
- ***Knappen Vejret*** - knappen giver øjeblikkelige oplysninger om vejrsituationen i et valgt område
- ***Knappen Facebook*** - knappen giver direkte forbindelse til det sociale netværk Facebook

8.2.2. Fanen Nyttige knapper



Med fanen ***Nyttige knapper*** kan du vælge programmer fra en liste og vise deres ikon i værktøjslinjegrænsefladen. Ikonet fungerer derefter som lynlink til øjeblikkelig start af det pågældende program.

8.2.3. Fanen Sikkerhed

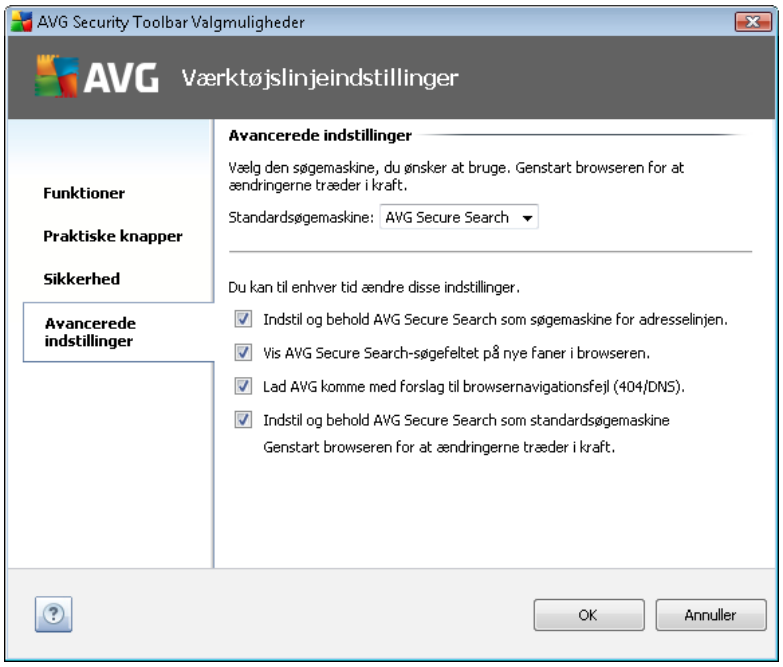


Fanen ***Sikkerhed*** er inddelt i to sektioner, ***AVG Browsersikkerhed*** og ***Rating***, hvor du kan markere bestemte afkrydsningsfelter for at tildele ***AVG Sikkerhedsværktøjslinje*** funktionalitet, du vil bruge:

- ***Browsersikkerhed*** - marker dette element for at aktivere eller slukke tjenesten ***Søgeskjold*** og/eller ***Surfskjold***
- ***Rating*** - vælg grafiske symboler, der bruges til rating af søgeresultater af ***Søgeskjold***-komponenten, som du vil bruge:
  - o siden er sikker
  - o siden er noget mistænkelig
  - o siden indeholder link til definitivt farlige sider
  - o siden indeholder aktive trusler
  - o siden er ikke tilgængelig og kunne derfor ikke scannes

Marker den pågældende indstilling for at bekræfte, at du vil informeres om det specifikke trusselsniveau. Visning af det røde mærke, der er tildelt sider med aktive og farlige trusler, kan imidlertid ikke slås fra. ***Det anbefales igen at bevare standardkonfigurationen, der er indstillet af programleverandøren, medmindre du har en god grund til at ændre den.***

8.2.4. Fanen Avancerede indstillinger



På fanen ***Avancerede indstillinger*** skal du først vælge, hvilken søgemaskine du vil bruge som standard. Du kan vælge mellem *AVG Secure Search (powered by Google), Baidu, WebHledani*, *Yandex og Yahoo! JP*. Når du har ændret den standard søgemaskine, skal du genstarte internetbrowseren, før ændringen træder i kraft.

Du kan desuden aktivere eller deaktivere specifikke ***AVG Security Toolbar***-indstillinger *(den viste overskrift henviser til de standard AVG Secure Search (powered by Google)-indstillinger)*:

- ***Indstil og behold AVG Secure Search (powered by Google) som søgeudbyder for adresselinjen*** - hvis den er markeret, giver denne indstilling mulighed for at indtaste et søgeord direkte i adresselinjen i din internetbrowser, og Google-tjenesten bruges automatisk til at søge efter relevante websteder.

- ***Lad AVG komme med forslag ved browsernavigationsfejl (404/DNS)*** - hvis du under søgning på internettet støder på en side, der ikke eksisterer, eller en side der ikke kan vises (404 fejl), vil du automatisk blive viderestillet til en webside, hvor du kan vælge fra en oversigt over alternative emnerelaterede sider.

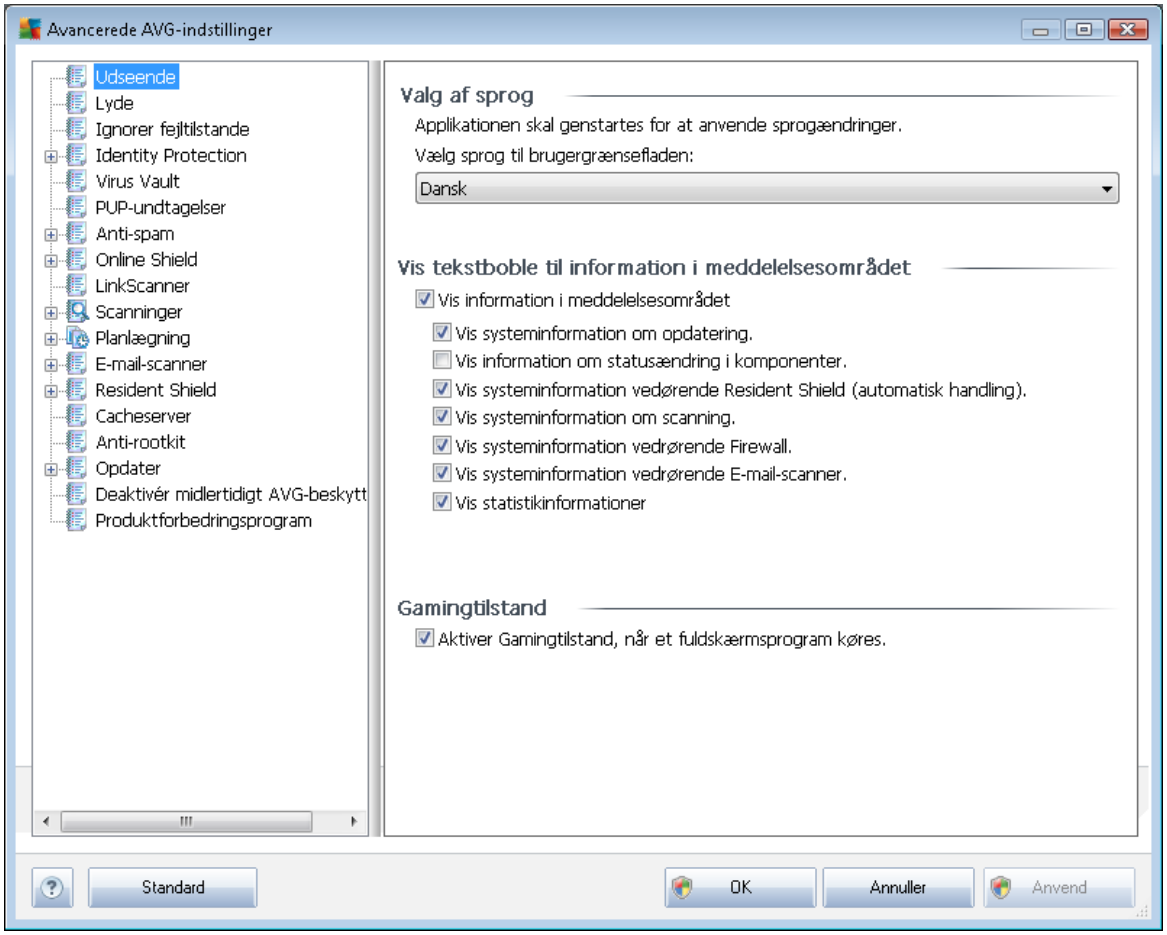
- ***Indstil og behold AVG Secure Search (powered by Google) som standard søgeudbyder*** - Google er den standard søgemaskine for internetsøgning i ***AVG Sikkerhedsværktøjslinje***, og ved at aktivere denne indstilling kan den også blive standardsøgemaskine i din webbrowser.

9. AVG Avancerede indstillinger

Den avancerede konfigurationsdialog for **AVG Internet-sikkerhed 2011** åbner i et nyt vindue kaldet ***Avancerede AVG-indstillinger***. Vinduet er inddelt i to sektioner: Venstre del indeholder et navigationstræ til programmets konfigurationsindstillinger. Vælg den komponent, du vil ændre konfigurationen af (*eller den specifikke del*), for at åbne redigeringsdialogen i vinduets højre sektion.

9.1. Udseende

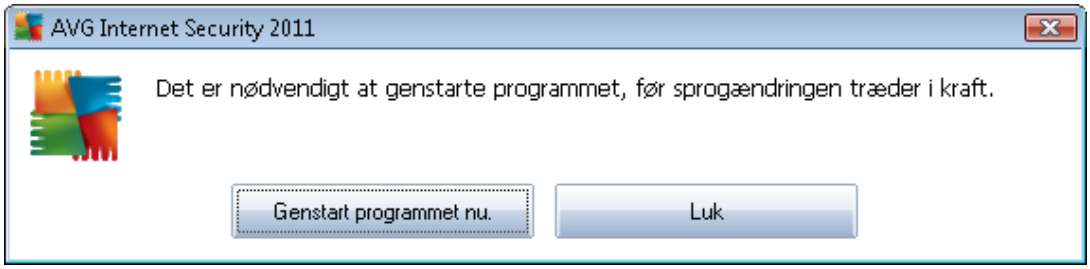
Det første element i navigationstræet, ***Udseende***, refererer til de generelle indstillinger for AVG-brugergrænsefladen og nogle få elementære indstillinger for applikationens opførsel:



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 valgte at installere under installationsprocessen (*se kapitlet Brugerdefineret indstilling*) samt engelsk (*som installeres som standard*). 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 ***OK***-knappen for at bekræfte
- Et nyt dialogvindue vises for at informere dig om, at applikationen skal genstartes, før sprogændringen i AVG-brugergrænsefladen træder i kraft:



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 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 Resident Shield (automatisk handling)*** - afgør om oplysninger vedrørende lagring, kopiering og åbning af filer skal vises eller tilsidesættes (*denne konfiguration vises kun, hvis Resident Shield-funktionen Automatisk fjernelse af infektioner er slået til*).
  - ***Vis bakketekstbobler om scanning*** - bestem, om oplysninger ved automatisk kørsel, forløb og resultater af planlagt scanning skal vises;

- ***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.

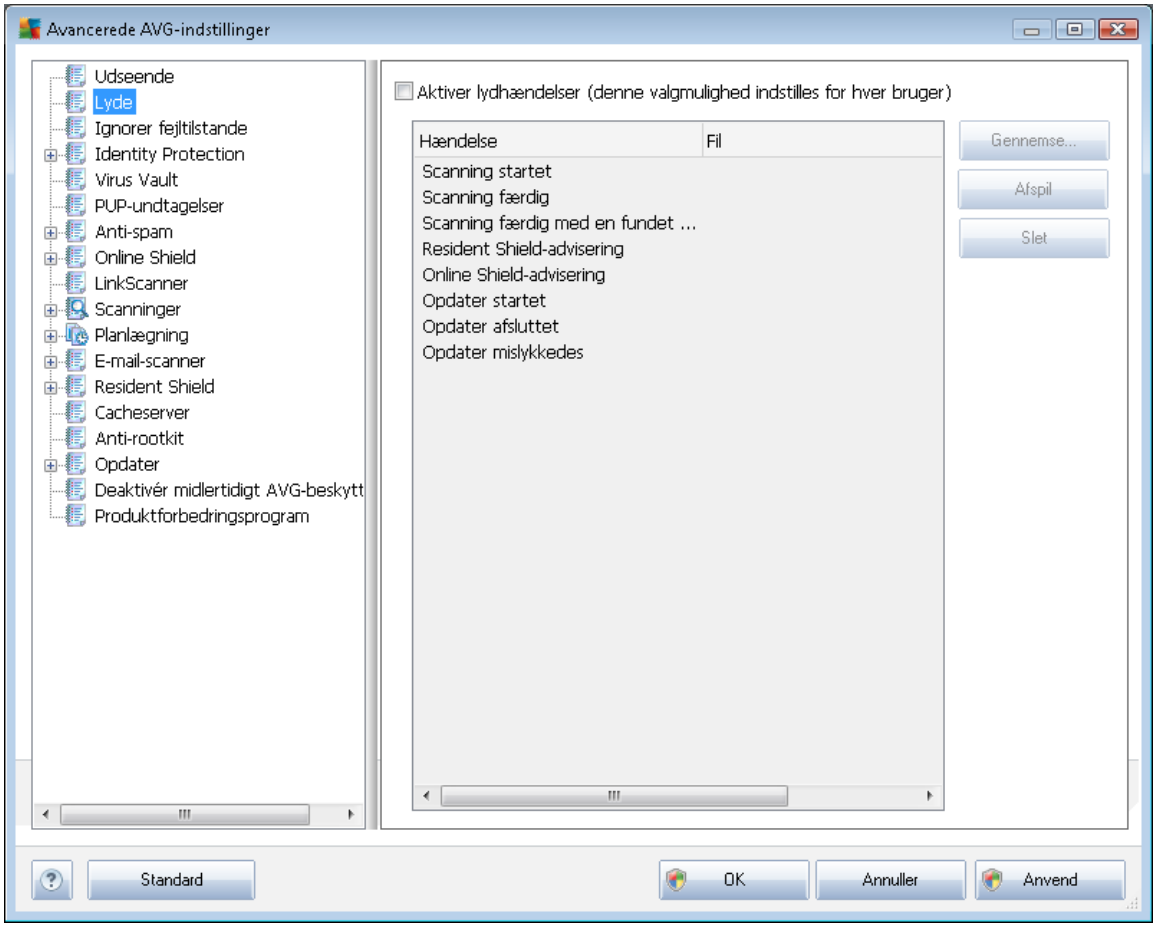
- ***Vis statistikinformationer*** - hold denne indstilling markeret for at tillade regelmæssig visning af statistikinformationsmeddelelser i systembakken.

Gamingtilstand

Denne VG-funktion er designet til fuldskærmsapplikationer, hvor mulige AVG-informationsballoner (*vises f.eks. når en planlagt scanning er startet*) ville forstyrre (de kunne minimere applikationen eller gøre grafikken korrupt*d*). Hold afkrydsningsfeltet for ***Aktiver gamingtilstand, når et fuldskærmsprogram køres.*** markeret for at undgå denne situation (*standardindstilling*).

9.2. Lyde

I dialogen ***Lyde*** kan du angive, om du vil informeres om bestemte AVG-handlinger med lydsignaler. Hvis du vil det, skal du markere indstillingen ***Aktiver lydhændelser*** (*slået fra som standard*) for at aktivere listen over AVG-hændelser:

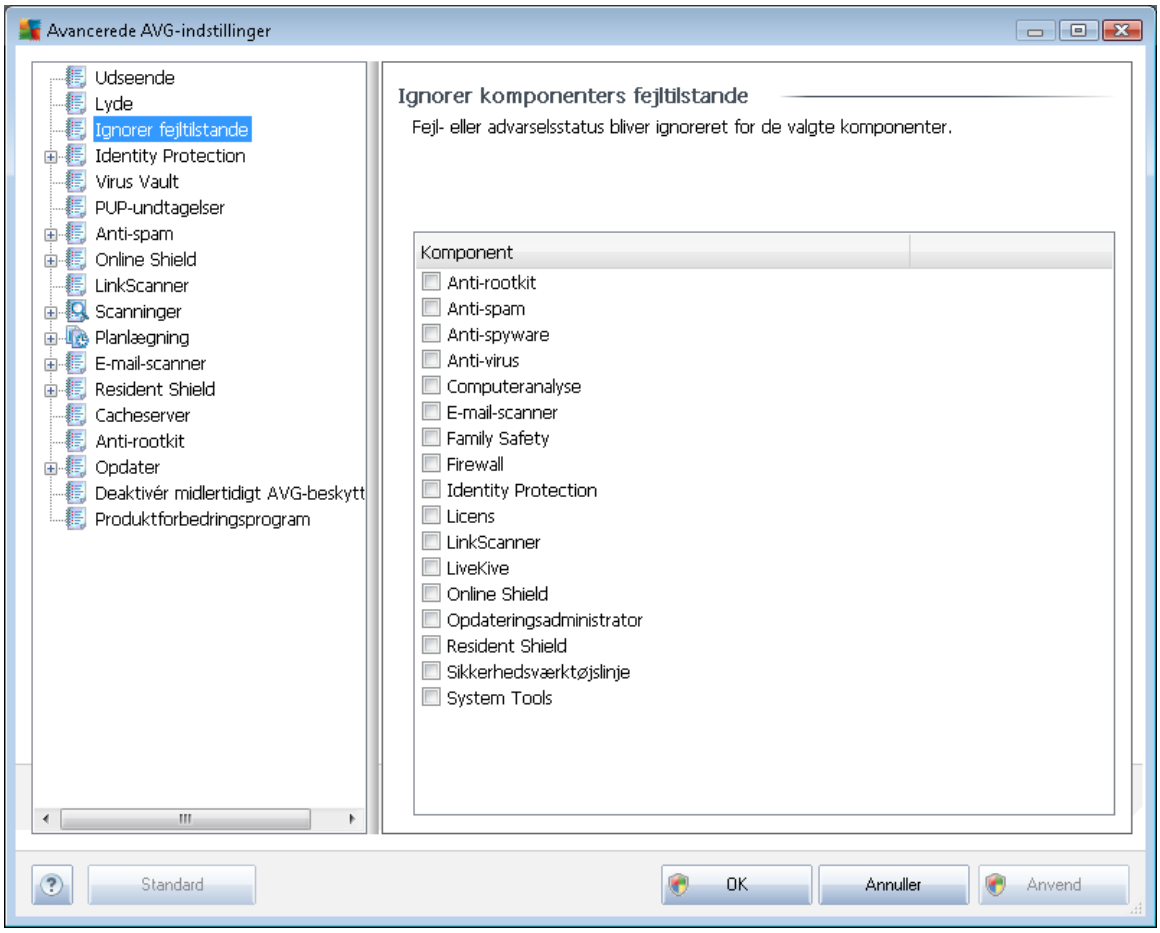


Vælg derefter den pågældende hændelse i listen, og gennemse (***Gennemse***) din disk efter en passende lyd, du vil tildele denne hændelse. For at lytte til den valgte lyd skal du fremhæve hændelsen i listen og trykke på knappen ***Afspil***. Brug knappen ***Slet*** til at fjerne den tildelte lyd fra en bestemt hændelse.

Bemærk! *Kun *.wav-lyde understøttes!*

9.3. 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, vises ikonet med et gult udråbstegn,
- tekstbeskrivelse af det eksisterende problem i sektionen ***Info om sikkerhedsstatus*** i AVG's hovedvindue

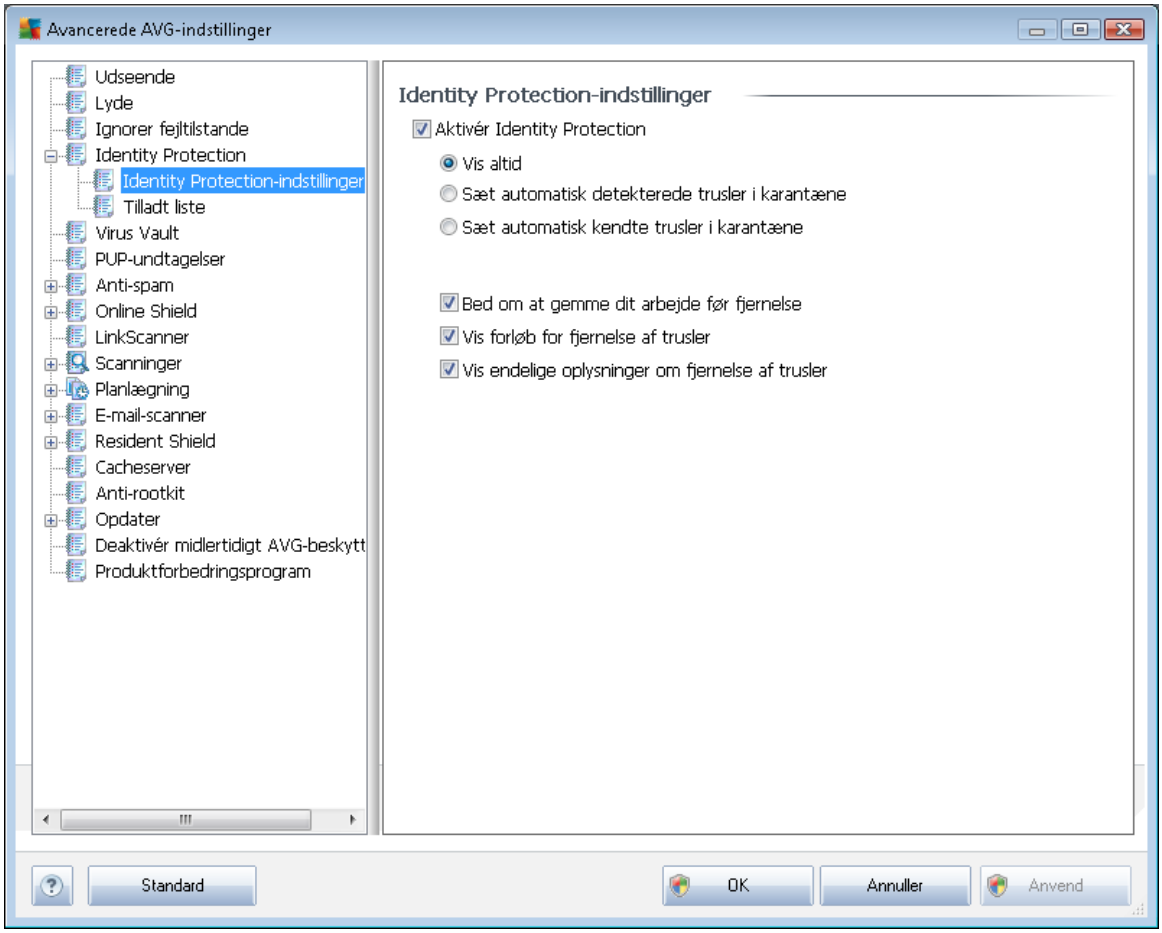
Der kan være en situation, hvor du af en årsag vil slå en komponent fra midlertidigt (*dette anbefales ikke, du bør forsøge at holde alle komponenter aktive permanent og i standardkonfigurationen, men det kan forekomme*). I dette tilfælde rapporterer systembakkeikonet automatisk komponentens fejltilstand. 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.

9.4. Identitetsbeskyttelse

9.4.1. Identitetsbeskyttelsesindstdillinger

I dialogen ***Identitetsbeskyttelse-indstillinger*** kan du slå de elementære funktioner i ***Identitetsbeskyttelse***-komponenten til og fra:



Aktivér Identitetsbeskyttelse (*slået til som standard*) – fjern markeringen for at slå ***Identitetsbeskyttelse***-komponenten fra.

Vi anbefaler kraftigt ikke at gøre dette, medmindre du er nødt til det!

Når ***Identitetsbeskyttelse*** er aktiveret, kan du angive, hvad der skal gøres, når en trussel detekteres:

- ***Vis altid*** (*aktiveret som standard*) - når en trussel detekteres, vil du blive spurgt, om den skal sættes i karantæne for at sørge for, at ingen af de programmer, du ønsker at køre,

bliver fjernet.

- ***Sæt automatisk detekterede trusler i karantæne*** - markér dette afkrydsningsfelt for at definere, at du vil have alle detekterede mulige trusler flyttet i sikkerhed i ***AVG Virus Vault*** med det samme. Hvis du bevarer standardindstillingerne, bliver du, når en trussel detekteres, spurgt, om den skal flyttes i karantæne, for at sikre at ingen applikationer, du ønsker at køre, bliver fjernet.

- ***Sæt automatisk kendte trusler i karantæne*** - hold dette element markeret, hvis du ønsker, at alle programmer, der detekteres som potentiel malware, automatisk og øjeblikkeligt flyttes til ***Virus Vault***.

Du kan desuden tildele specifikke elementer for at aktivere flere ***Identitetsbeskyttelse***-funktioner:

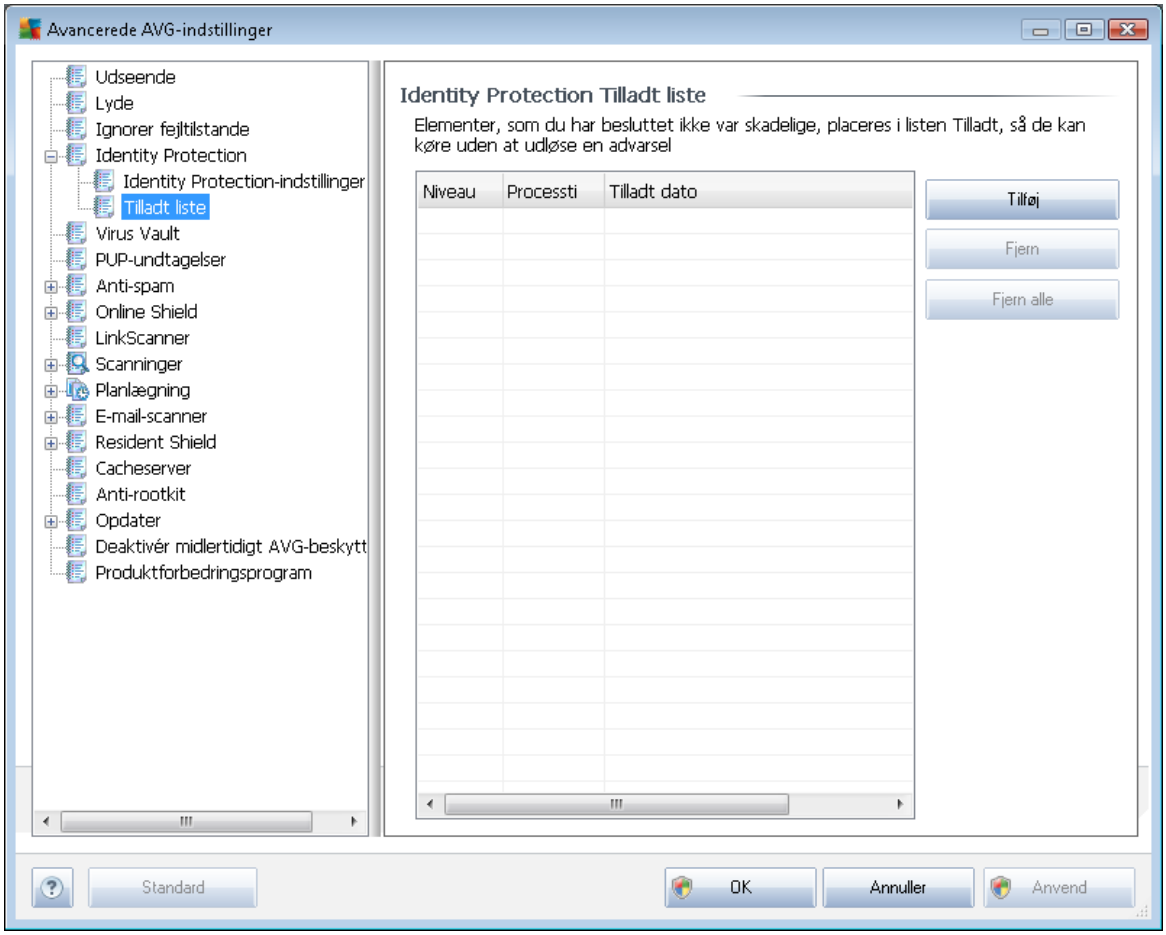
- ***Spørg om at gemme dit arbejde før fjernelse*** - (*slået til som standard*) - hold dette element markeret, hvis du ønsker at blive advaret, før programmet, der detekteres som potentiel malware, sættes i karantæne. Hvis du var i gang med at arbejde med programmet, kan dit projekt gå tabt og du skal gemme det først. Dette element er som standard aktiveret, og vi anbefaler at holde det aktiveret.

- ***Vis fremskridt ved fjernelse af malware*** - (*slået til som standard*) - med dette element slået til, når der detekteres en potentiel malware, åbnes en ny dialog, der viser fremskridtet af den malware, der flyttes til karantæne.

- ***Vis endelig detalje ved fjernelse af malware***- (*slået til som standard*) - med dette element slået til viser ***Identitetsbeskyttelse*** detaljerede oplysninger om hvert objekt, der flyttes til karantæne (*alvorlighedsniveau, placering, osv.*).

9.4.2. Tilladt liste

Hvis du i dialogen ***Identitetsbeskyttelse-indstillinger*** besluttede at lade elementet ***Sæt automatisk detekterede trusler i karantæne*** være umarkeret, bliver du, hver gang en potentielt farlig malware detekteres, spurgt, om den skal fjernes. Hvis du tildeler den mistænkelige applikation (*detekteret på baggrund af sin adfærd*) sikker status, og du bekræfter, at den skal beholdes på din computer, bliver applikationen føjet til den såkaldte ***Identitetsbeskyttelse Tilladte liste***, og den bliver ikke rapporteret som potentielt farlig igen:



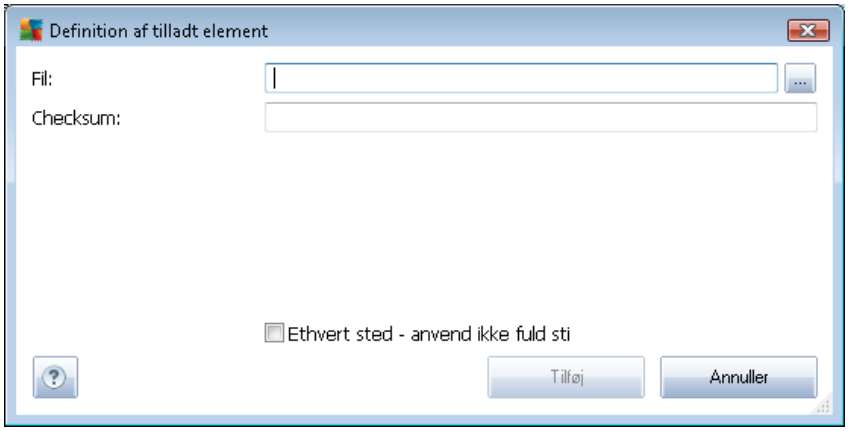
Identitetsbeskyttelse Tilladte liste indeholder følgende oplysninger om hver applikation:

- ***Niveau*** - grafisk identifikation af den pågældende proces' alvorlighed på en firetrins skala fra mindre vigtig (■□□□) op til kritisk (■■■■)
- ***Processti*** - sti til placeringen af applikationens (*proces*) eksekverbare fil
- ***Dato tilladt*** - dato, da du manuelt tildelte applikationen sikker status

Betjeningsknapper

Betjeningsknapperne, der er tilgængelige i dialogen ***Identitetsbeskyttelse Tilladt liste***, er som følger:

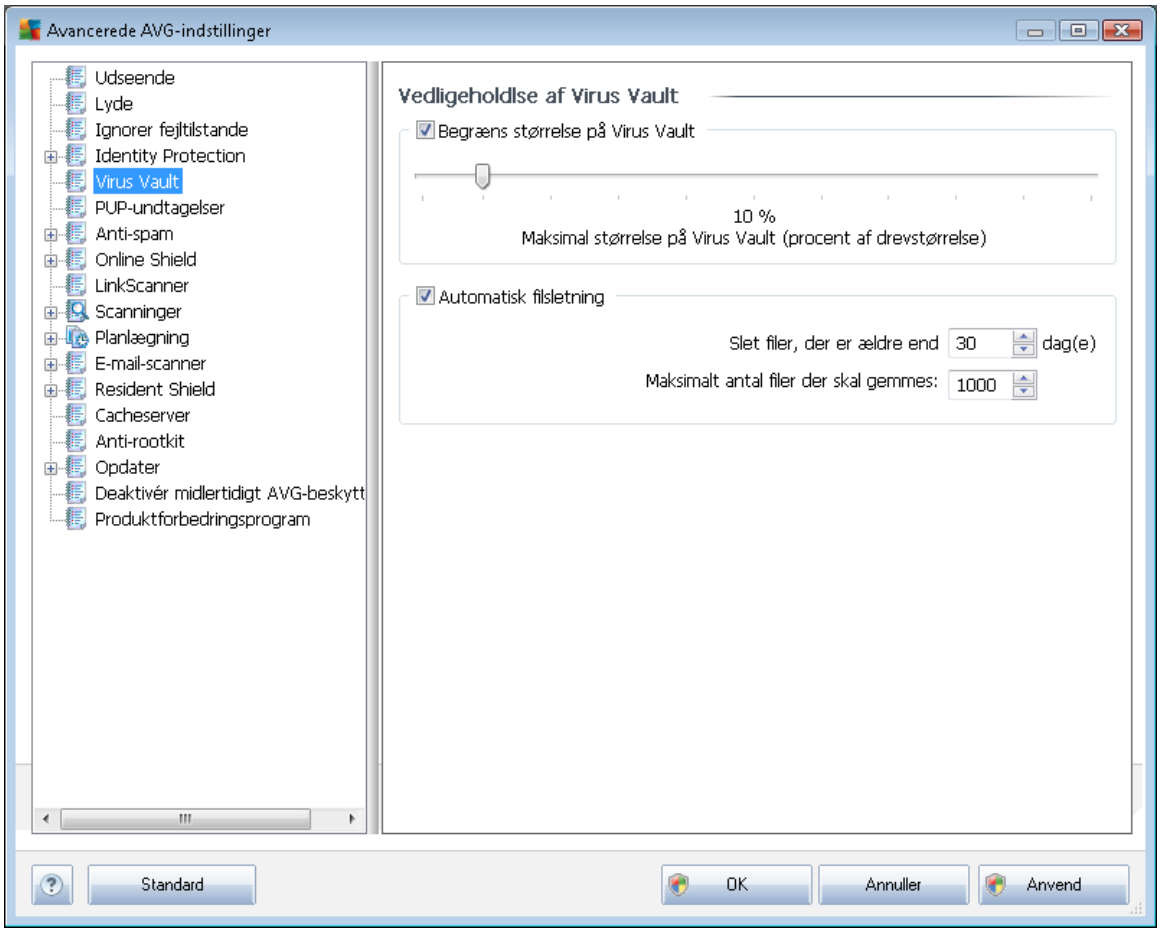
- ***Tilføj*** - tryk på denne knap for at føje en ny applikation til den tilladte liste. Følgende dialog vises:



- ***Fil*** - indtast de fulde sti til filen (*applikationen*), som du vil markere 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.
- ***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

- ***Fjern*** - tryk for at fjerne den valgte applikation fra listen
- ***Fjern alle*** - tryk for at fjerne alle anførte applikationer

9.5. Virus Vault

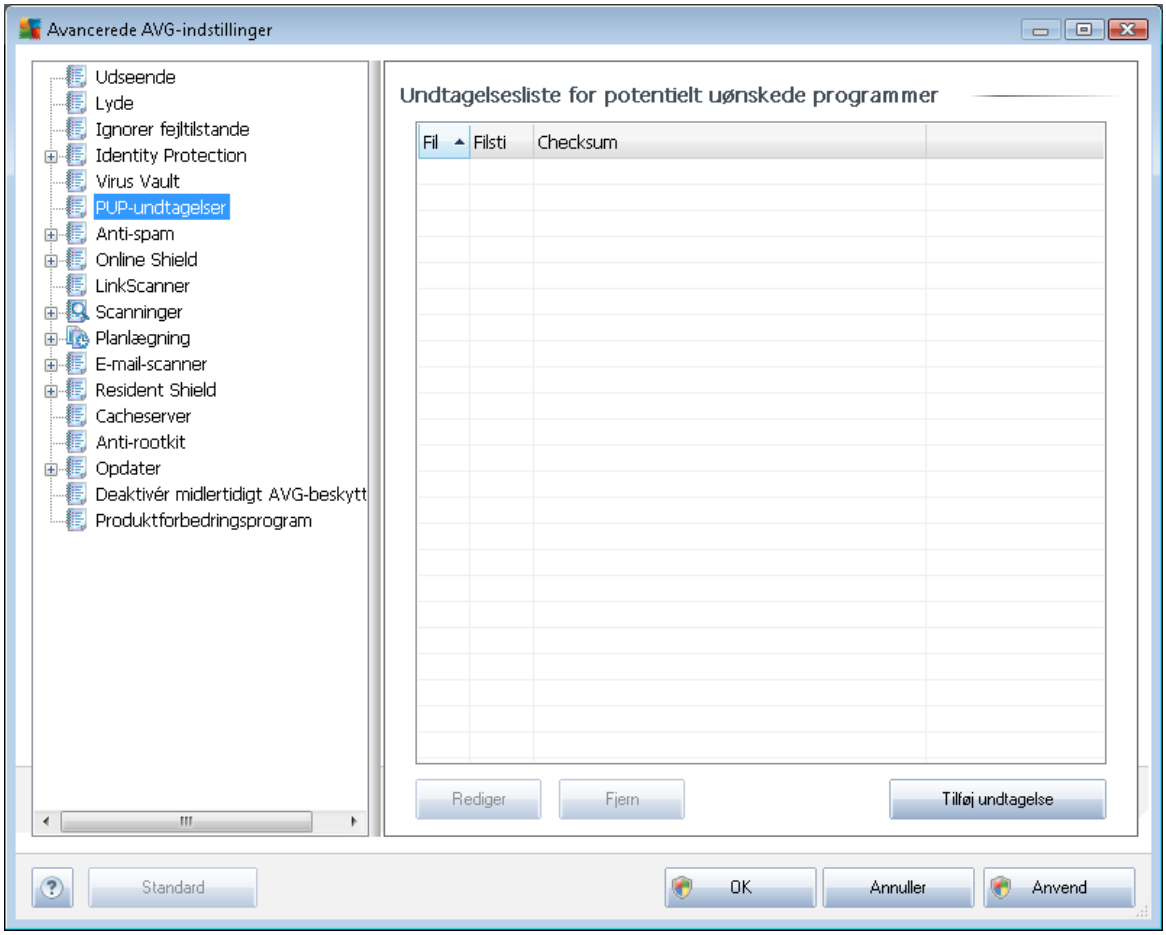


I dialogboksen ***Virus Vault-vedligeholdelse*** kan du definere adskillige parametre vedrørende administration af objekter, der opbevares i ***Virus Vault***:

- ***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***)

9.6. PUP-undtagelser

AVG Internet-sikkerhed 2011 kan analysere og detektere eksekverbare applikationer og DLL-biblioteker, der er potentielt uønskede i systemet. I visse 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:



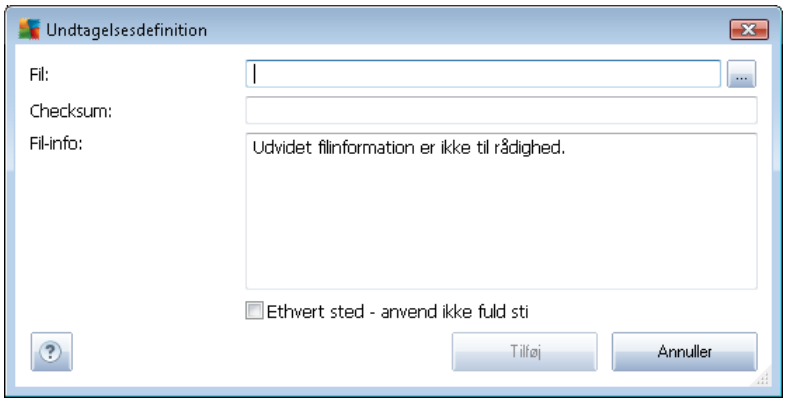
Dialogen ***Potentielt uønsket program-undtagelser*** viser en liste over allerede definerede og aktuelt gyldige undtagelser fra potentielt uønskede programmer. Du kan redigere listen, slette eksisterende elementer eller tilføje nye undtagelser. Følgende oplysninger kan findes i listen for hver enkelt undtagelse:

- ***Fil*** - indeholder navnet på den pågældende applikation
- ***Filsti*** - viser applikationens placering
- ***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.

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

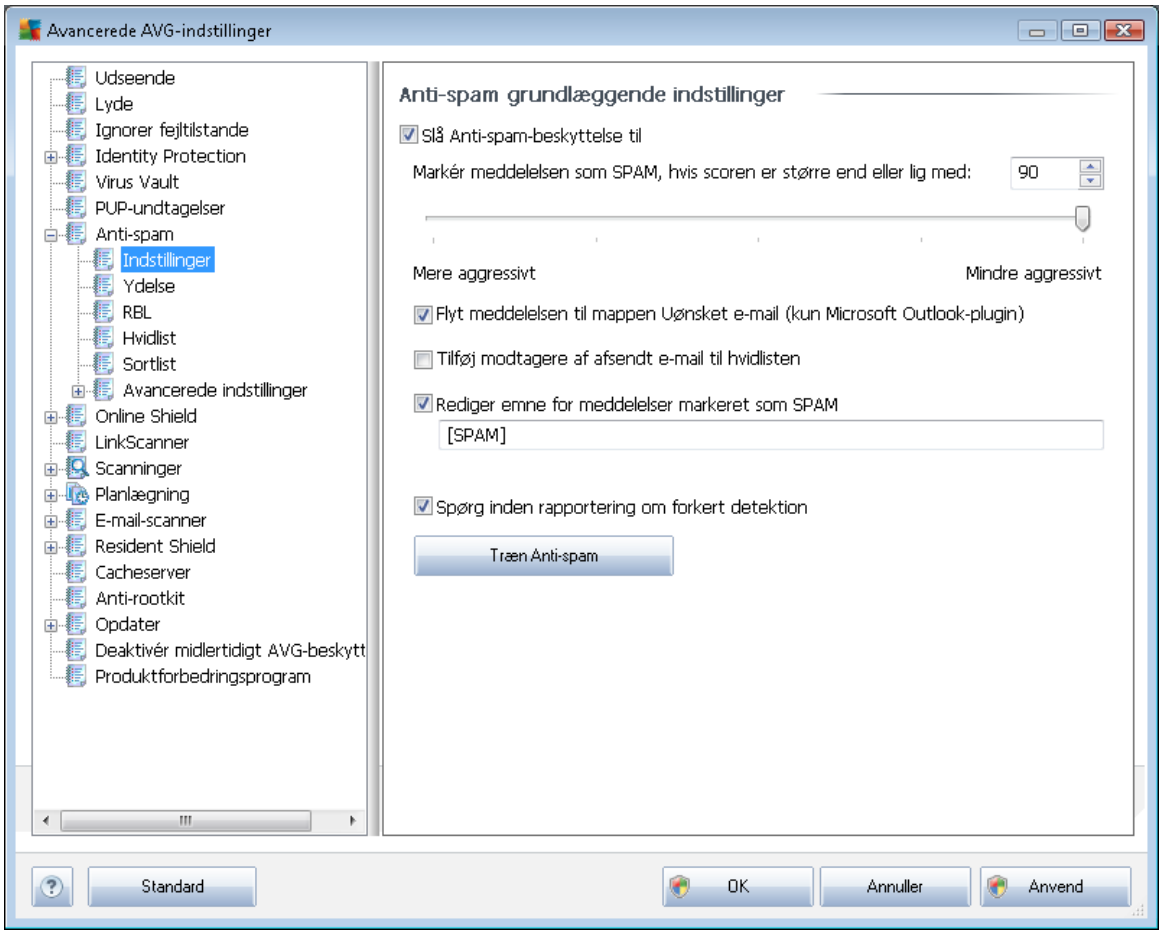
- ***Tilføj undtagelse*** - åbn en redigeringsdialog, hvor du kan definere parametre for den nye undtagelse, der skal oprettes:



  - ***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. Hvis afkrydsningsfeltet er markeret, angives den definerede fil som en undtagelse, uanset hvor den er placeret (*du skal dog alligevel udfylde den fulde sti til den specifikke fil. Filen vil derefter blive brugt som et unikt eksempel på, at der er mulighed for, at to filer med samme navn vises i dit system*.

9.7. Anti-spam

9.7.1. Indstillinger



I dialogen ***Anti-spam-basisindstillinger*** kan du markere/afmarkere afkrydsningsfeltet ***Aktiver Anti-spam-beskyttelse*** for at tillade/forbyde anti-spam-scanning af e-mail-kommunikation. Denne indstilling er slået til som standard, og som altid anbefales det at beholde denne konfiguration, medmindre du har en god grund til at ændre den.

Derefter kan du også vælge en mere eller mindre aggressiv scoringsbedømmelse. ***Anti-spam***-filtret tildeler hver meddelelse en score (*dvs. hvor tæt meddelelsens indhold ligner SPAM*) baseret på flere dynamiske scanningsteknikker. Du kan justere indstillingen ***Marker meddelelse som spam, hvis score er større end*** ved enten at indtaste værdien eller ved at flytte skyderen mod venstre eller højre (*værdiintervallet er begrænset til 50-90*).

Generelt anbefaler vi at tærsklen indstilles mellem 50 - 90, eller hvis du er meget i tvivl, til 90. Her er en generel vurdering af scoringstærsklen:

- ***Værdi 80-90*** - E-mail-meddelelser, der sandsynligvis er spam, vil blive filtreret fra. Visse ikke-spam meddelelser kan også blive filtreret ud.
- ***Værdi 60-79*** - Betragtes som en ret aggressiv konfiguration. E-mail-meddelelser, der muligvis er spam, vil blive filtreret fra. Ikke-spam meddelelser vil sandsynligvis også blive filtreret fra.

- ***Værdi 50-59*** - Meget aggressiv konfiguration. Ikke-spam e-mail-meddelelser vil sandsynligvis bliver filtreret fra sammen med ægte spam-meddelelser. Dette tærskelværdi-interval anbefales ikke til normal brug.

I dialogen ***Anti-spam-basisindstillinger*** kan du yderligere definere, hvordan de detekterede spam e-mail-meddelelser skal behandles:

- ***Flyt meddelelse til mappen Uønsket e-mail*** - marker dette afkrydsningsfelt, for at angive, at alle detekterede spam-meddelelser automatisk skal flyttes til mappen med uønsket e-mail i din e-mail-klient.

- ***Tilføj modtagere af sendte e-mail til hvidlisten*** - marker dette afkrydsningsfelt for at bekræfte, at alle modtagere af sendte e-mail er pålidelige, og alle e-mail-meddelelser, der modtages fra deres e-mail-konti kan leveres.

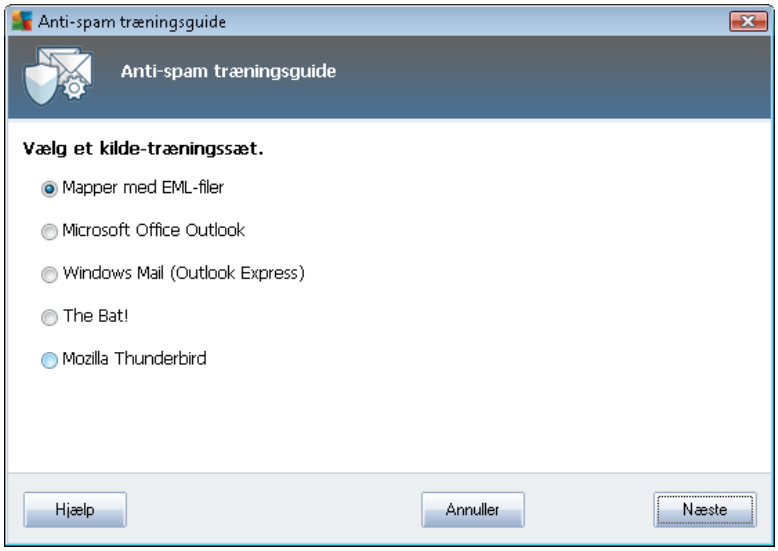
- ***Modificer emnet for meddelelser mærket som SPAM*** - marker dette afkrydsningsfelt, hvis du vil have at alle meddelelser, der detekteres som spam, skal mærkes med et bestemt ord eller tegn i e-mailens emnelinje. Den ønskede tekst kan indtastes i det aktiverede tekstfelt.

- ***Spørg inden rapportering om forkert detektion*** - forudsat at du under installationsprocessen accepterede at deltage i ***Produktforbedringsprogrammet***. I så fald har du tilladt rapportering af detekterede trusler til AVG. Rapporteringen sker automatisk. Du kan dog markere dette afkrydsningsfelt for at bekræfte, at du vil spørges, inden detekteret spam rapporteres til AVG for at sikre, at meddelelsen skal klassificeres som spam.

Betjeningsknapper

Træn Anti-spam-knap åbn ***guiden Anti-spam-træning*** beskrevet detaljeret i næste kapitel.

Den første dialog i ***Guiden Anti-spam-træning*** beder dig om at vælge kilden for de e-mail-meddelelser, du vil anvende til træning. Normalt bruger du enten e-mail, der er forkert mærket som SPAM eller spam-meddelelser, der ikke er blevet genkendt.



Du kan vælge mellem følgende indstillinger:

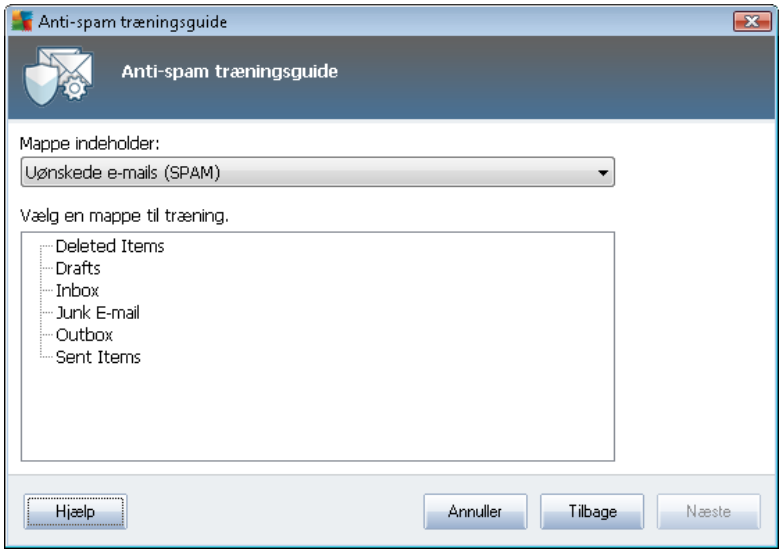
- ***En specifik e-mail-klient*** - hvis du bruger en af de anførte e-mail-klienter (*MS Outlook, Outlook Express, The Bat!,*), skal du helt enkelt vælge den pågældende indstilling.
- ***Mappe med EML-filer*** - hvis du bruger et andet e-mail-program, skal du først gemme meddelelserne i en specifik mappe (*i .eml-format*) eller sørge for, at du kender placeringen af e-mail-klientens meddelelsesmapper. Vælg derefter ***Mappe med EML-filer***, som gør det muligt for dig at finde den ønskede mappe i næste trin

For at gøre træningen hurtigere og nemmere er det en god i dé at sortere e-mailene i mapperne på forhånd, så den mappe, du vil anvende til træning, kun indeholder træningsmeddelelserne (enten ønskede eller uønskede). Det er dog ikke nødvendigt, da du kan filtrere e-mailene senere.

Vælg den ønskede indstilling, og klik på ***Næste*** for at fortsætte guiden.

Dialogen der vises i dette trin, afhænger af dit forudgående valg.

Mapper med EML-filer



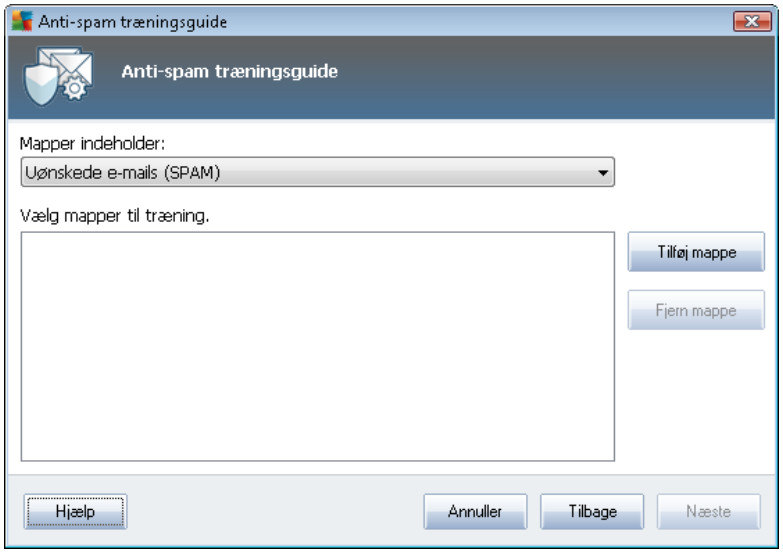
I denne dialog skal du vælge mappen med de meddelelser, du vil anvende til træning. Tryk på knappen ***Tilføj mappe*** for at finde mappen med .eml-filer (*gemte e-mail-meddelelser*). Den valgte mappe vises derefter i dialogen.

I rullemenuen ***Mapper indeholder*** kan du indstille en af de to muligheder - afhængigt af om den valgte mappe indeholder ønskede (*HAM*) eller uønskede (*SPAM*)-meddelelser. Bemærk, at du kan filtrere meddelelserne i næste trin, så mappen behøver ikke kun at indholde trænings-e-mail. Du kan også fjerne uønskede valgte mapper fra listen ved at klikke på knappen ***Fjern mappe***.

Klik på ***Næste*** og fortsæt til ***Indstillinger for meddelelsesfiltrering***, når du er færdig.

Specifik e-mail-klient

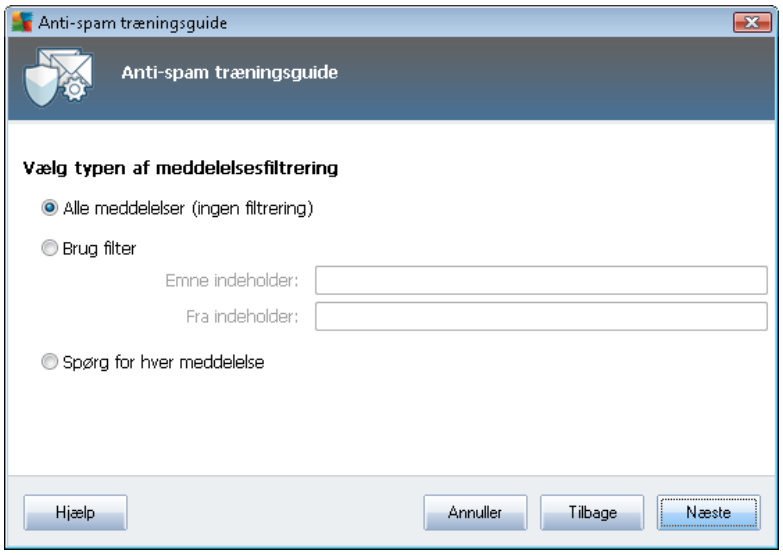
Når du bekræfter en af indstillingerne, vises en ny dialog.



Bemærk: *For Microsoft Office Outlook bliver du først bedt om at vælge MS Office Outlook-profilen.*

I rullemenuen ***Mapper indeholder*** kan du indstille en af de to muligheder - afhængigt af om den valgte mappe indeholder ønskede (*HAM*) eller uønskede (*SPAM*)-meddelelser. Bemærk, at du kan filtrere meddelelserne i næste trin, så mappen behøver ikke kun at indholde trænings-e-mail. Der vises allerede et navigationstræ for den valgte e-mail-klient i dialogens hovedsektion. Find den ønskede mappe i træet og marker den med musen.

Klik på ***Næste*** og fortsæt til ***Indstillinger for meddelelsesfiltrering***, når du er færdig.



I denne dialog kan du indstille filtrering af e-mail-meddelelser.

Hvis du er sikker på, at den valgte mappe kun indeholder meddelelser, du vil anvende til træning, skal du vælge indstillingen ***Alle meddelelser (ingen filtrering)***.

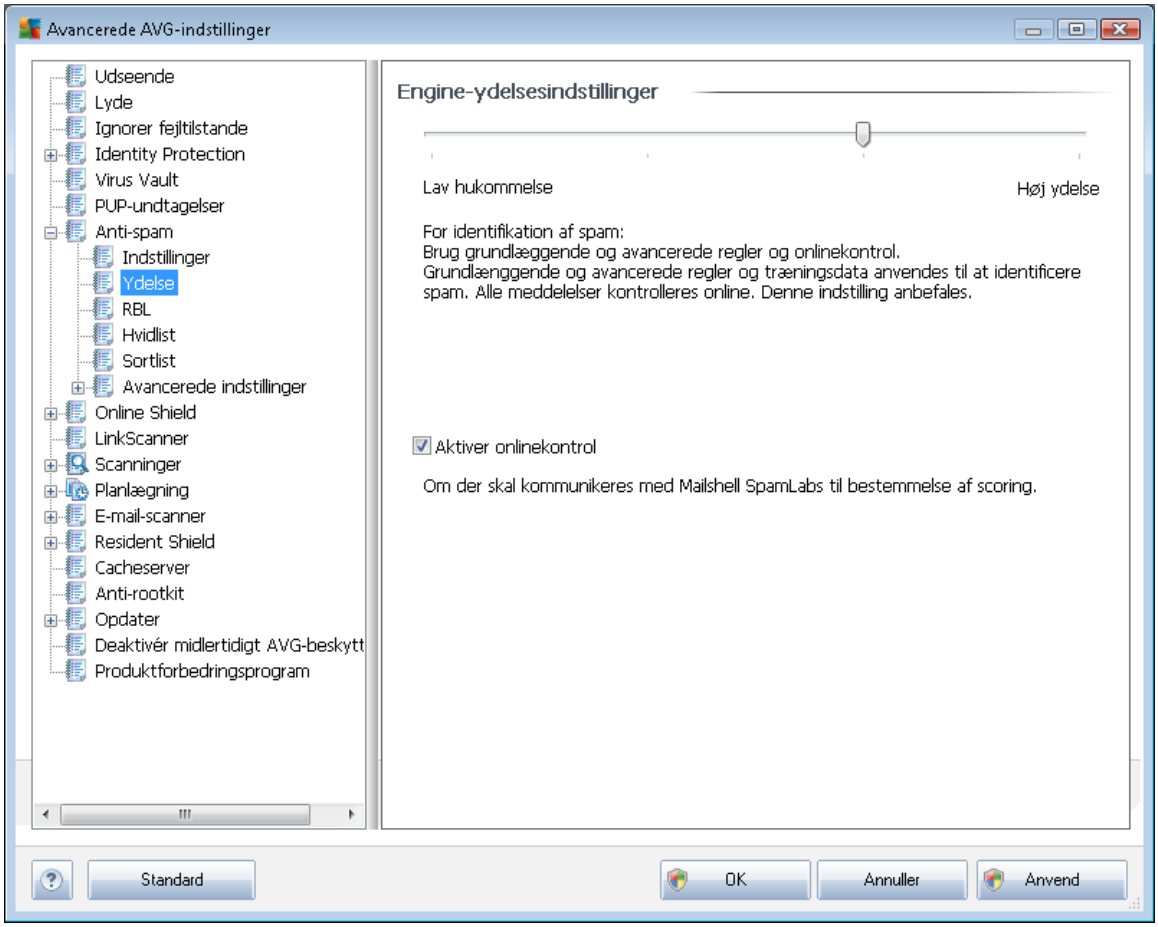
Hvis du er usikker på meddelelserne i mappen, og du vil have guiden til at spørge dig om hver enkelt meddelelse (så du kan bestemme om den skal anvendes til træning eller ej), skal du vælge indstillingen ***Spørg for hver meddelelse***.

Vælg indstillingen ***Brug filter*** for mere avanceret filtrering. Du kan udfylde et ord (*navn*) en del af et ord eller en frase, der skal søges efter i e-mailens emne og/eller afsenderfeltet. Alle meddelelser, der svarer nøjagtig til det indtastede kriterium, anvendes til træningen uden yderligere forespørgsler.

OBS!: *Hvis du udfylder begge tekstfelter, anvendes adresser, der kun svarer til en af de to betingelser, også!*

Klik på ***Næste***, når du har valgt den ønskede indstilling. Følgende dialog er kun med henblik på information, og fortæller dig at guiden er klar til at behandle meddelelserne. Klik på knappen ***Næste*** igen for at starte træningen. Træningen starter i overensstemmelse med de tidligere valgte betingelser.

9.7.2. Ydelse



Dialogboksen ***Engine-ydelsesindstillinger*** (*åbnes via elementet* ***Ydelse*** *i venstre navigationsområde*) indeholder ydelsesindstillinger for ***Anti-spam***-komponenten. Flyt skyderen til venstre elller højre for at ændre scanningens ydelsesniveau mellem tilstandene ***Lav hukommelse*** / ***Høj ydelse***.

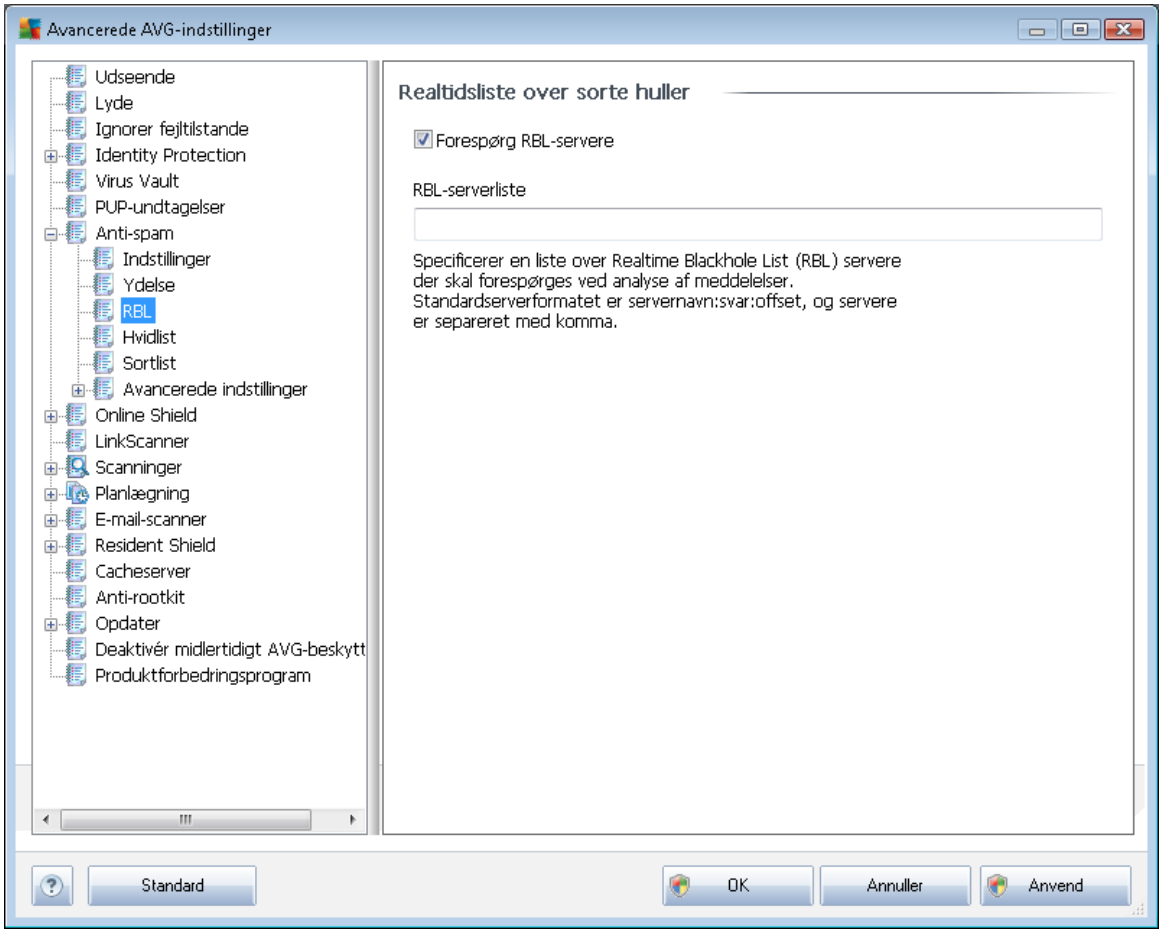
- ***Lav hukommelse*** - under scanningsprocessen for at identificere spam anvendes ingen regler. Kun træningsdata bruges til identifikation. Denne tilstand anbefales ikke til almindelig brug, medmindre computerhardwaren er virkelig dårlig.
- ***Høj ydelse*** - denne tilstand forbruger en stor mængde hukommelse. Under scanningsprocessen for at identificere spam anvendes følgende funktioner: regler og spam-databasecache, grundlæggende og avancerede regler, spammer-IP-adresser og spammerdatabaser.

Elementet ***Aktiver onlinekontrol*** er slået til som standard. Det medfører mere præcis detektering af spamvia kommunikation med Mailshell-serverne, dvs. de scannede data bliver sammenlignet med Mailshell-databaser online.

Det anbefales generelt at bevare standardindstillingerne og kun ændre dem, hvis du har en god grund til det. Ændringer i denne konfiguration bør kun udføres af superbrugere!

9.7.3. RBL

Elementet ***RBL*** åbner en redigeringsdialogboks med navnet ***Realtime Blackhole List***:



I denne dialog kan du aktivere/deaktivere funktionen ***Forespørg RBL-servere***.

RBL-serveren (*Realtime Blackhole List*) er en DNS-server med en omfattende database over kendte spam-afsendere. Når denne funktion er aktiveret, vil alle e-mail meddelelser blive verificeret mod RBL-serverdatabasen og blive markeret som spam, hvis de er identiske med poster i databasen. RBL-serverdatabaserne indeholder helt opdaterede spam-fingeraftryk, så du opnår den bedste og mest præcise detektering af spam. Denne funktion er specielt nyttig for brugere, der modtager store mængder spam, der ikke normalt detekteres af Anti-spam-enginen.

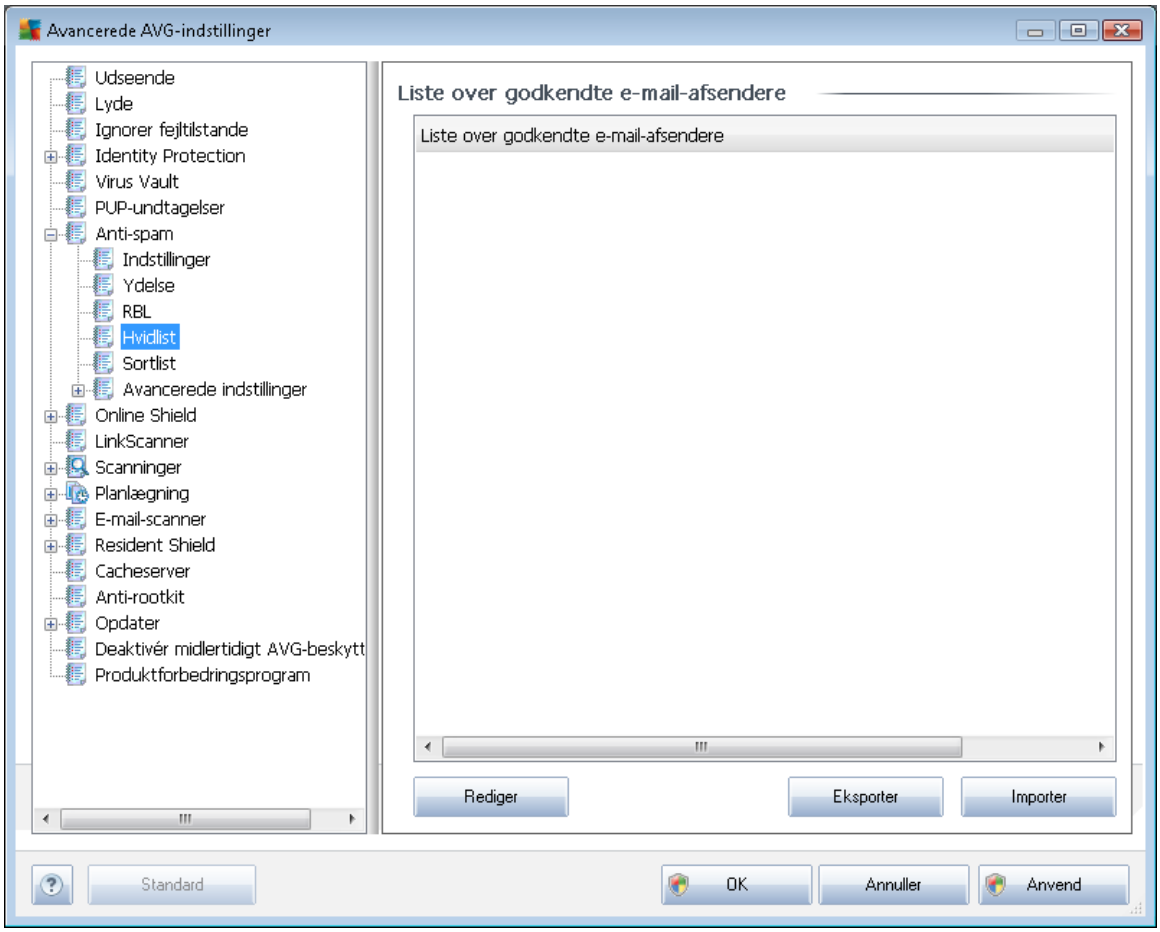
I ***RBL-serverlisten*** kan du definere specifikke RBL-serverplaceringer.

Bemærk:*Aktivering af denne funktion kan gøre e-mail-modtagelsen langsommere på nogle systemer og konfigurationer, da hver enkelt meddelelse skal verificeres i RBL-serverdatabasen.*

Der sendes ingen personlige data til serveren!

9.7.4. Hvidliste

Punktet ***Hvidliste*** åbner dialogen ***Liste over godkendte e-mail-afsendere*** med en global liste over godkendte afsenderes e-mail-adresser og domænenavne, hvis meddelelser aldrig mærkes som spam.



I redigeringsgrænsefladen kan du sammensætte en liste over afsendere, som du er sikker på aldrig vil sende dig uønskede meddelelser (spam). Du kan også sammensætte en liste med domænenavne (*f.eks. avg.com*), som du ved ikke genererer spammeddelelser.

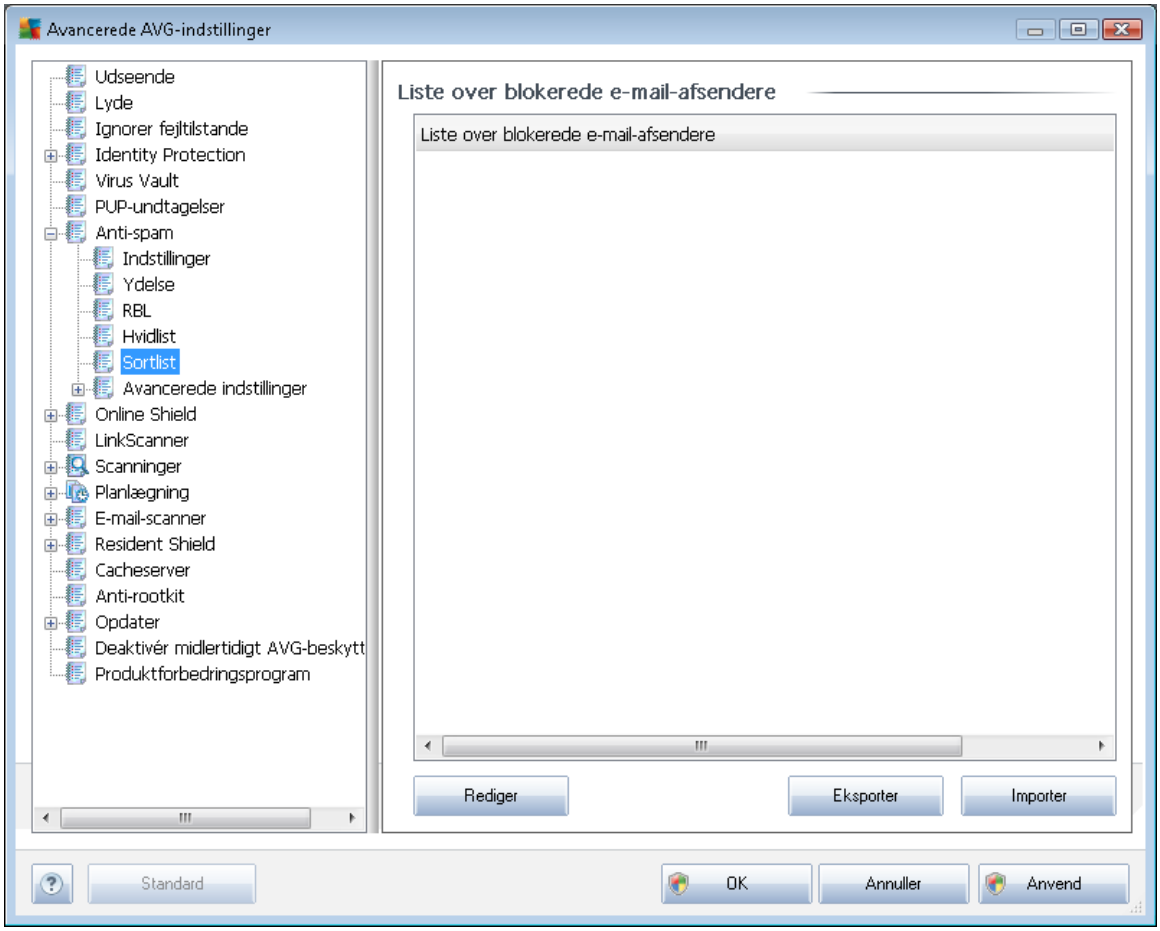
Når du først har klargjort en liste over afsendere og/eller domænenavne, kan du indtaste dem med en af følgende metoder: ved at indtaste hver e-mail-adresse direkte eller ved at importere hele listen over adresser på en gang. Følgende betjeningsknapper er til rådighed:

- ***Rediger*** - klik på denne knap for at åbne en dialogboks, hvori du manuelt kan indtaste en adresseliste (*kopier/sæt ind-metoden fungerer også*). Indsæt et element (*afsender, domænenavn*) pr. linje.
- ***Eksporter*** - hvis du bestemmer dig for at eksportere posterne, kan du gøre dette ved at klikke på denne knap. Alle poster gemmes som en almindelig tekstfil.
- ***Importer*** - hvis du allerede har en tekstfil med e-mail-adresser/domænenavne, kan du

importere listen ved at klikke på denne knap. Indholdet i denne fil må kun indholde ét element (*adresse, domænenavn*) pr. linje.

9.7.5. Sortliste

Punktet ***Sortliste*** åbner en dialog med en global liste over blokerede afsenderes e-mail-adresser og domænenavne, hvis meddelelser altid mærkes som spam.



I redigeringsgrænsefladen kan du sammensætte en liste over afsendere, som du forventer vil sende dig uønskede meddelelser (spam). Du kan også kompilere en liste over fulde domænenavne (*f.eks. spammingcompany.com*), som du forventer eller modtager spam-meddelelser fra. Alle e-mail adresser fra de angivne adresser/domæner vil blive identificeret som spam.

Når du først har klargjort en liste over afsendere og/eller domænenavne, kan du indtaste dem med en af følgende metoder: ved at indtaste hver e-mail-adresse direkte eller ved at importere hele listen over adresser på en gang. Følgende betjeningsknapper er til rådighed:

- ***Rediger*** - klik på denne knap for at åbne en dialogboks, hvori du manuelt kan indtaste en adresseliste (*kopier/sæt ind-metoden fungerer også*). Indsæt et element (*afsender, domænenavn*) pr. linje.
- ***Eksporter*** - hvis du bestemmer dig for at eksportere posterne, kan du gøre dette ved at

klikke på denne knap. Alle poster gemmes som en almindelig tekstfil.

- ***Importer*** - hvis du allerede har en tekstfil med e-mail-adresser/domænenavne, kan du importere listen ved at klikke på denne knap.

9.7.6. Avancerede indstillinger

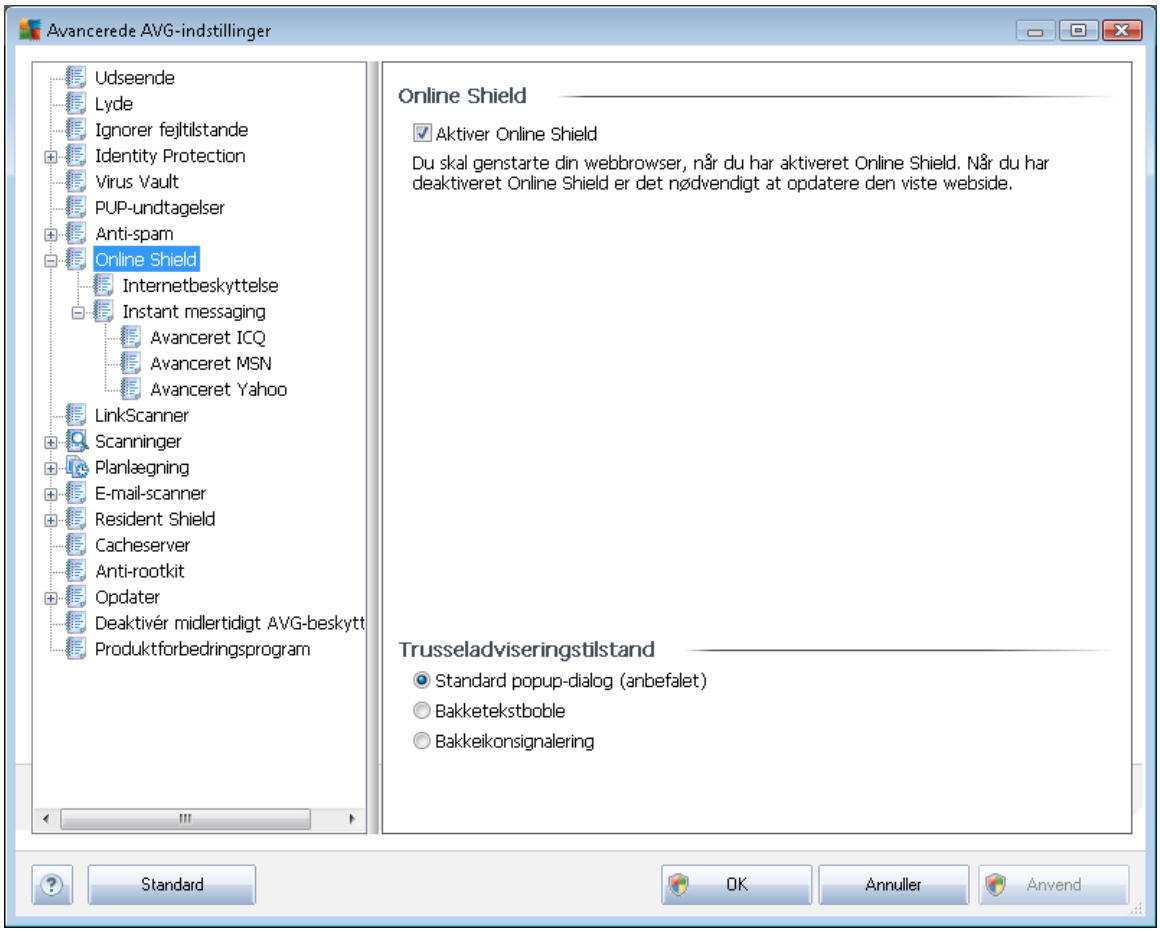
Grenen Avancerede indstillinger indeholder udvidede indstillingsmuligheder for Anti-spam-komponenten. Disse indstillinger er beregnet til erfarne brugere, typisk netværksadministratorer, der har behov for at konfigurere antispam-beskyttelsen i detaljer for at beskytte e-mail-servere bedst muligt. Derfor er der ingen ekstra hjælp tilgængelig for de enkelte dialoger. Der er imidlertid en kort beskrivelse af hver enkelt indstilling direkte i brugergrænsefladen.

Vi anbefaler på det kraftigste, at ingen indstillinger ændres, medmindre du er fuldt fortrolig med de avancerede indstillinger i Spamcatcher (MailShell Inc.). Eventuelle forkerte ændringer kan medføre dårlig ydelse eller forkert komponentfunktionalitet.

Hvis du stadig mener, det er nødvendigt at ændre ***Anti-spam***-konfigurationen på det meget avancerede niveau, skal du følge vejledningen, der findes i selve brugergrænsefladen. Generelt findes der i hver dialog en enkelt specifik funktion, og du kan redigere den - beskrivelsen af den findes altid i selve dialogen:

- ***Cache*** - fingeraftryk, domæneomdømme, LegitRepute
- ***Træning*** - maksimalt antal ord, automatisk træningstærskel, vægt
- ***Filtrering*** - sprogliste, landeliste, godkendte IP'er, blokerede IP'er, blokerede lande, blokerede tegnsæt, spoofede afsendere
- ***RBL*** - RBL-servere, multihit, tærskel, timeout, maksimat antal IP'er
- ***Internetforbindelse*** - timeout, proxyserver, proxygodkendelse

9.8. Online Shield



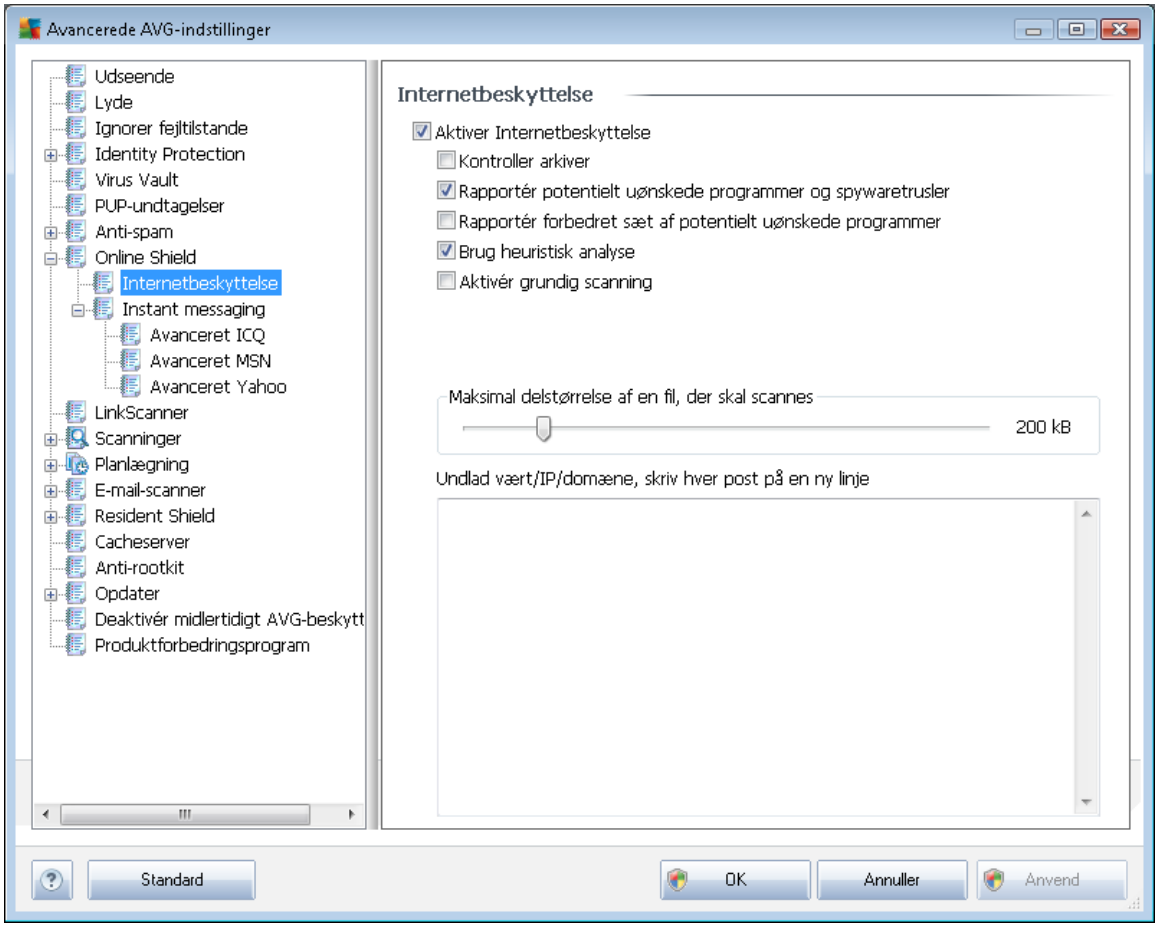
I dialogen ***Online Shield*** kan du aktivere/deaktivere hele ***Online Shield***-komponenten med indstillingen ***Aktivér Online Shield*** (*aktiveret som standard*). Fortsæt til de efterfølgende dialogbokse anført i navigationstræet for yderligere avancerede indstillinger af denne komponent:

- ***Internetbeskyttelse***
- ***Instant messaging***

Trusseladviseringstilstand

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.

9.8.1. Internetbeskyttelse



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

- ***Aktiver internetbeskyttelse*** - denne indstilling bekræfter, at ***Online 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*** - (*slået fra som standard*): scan indholdet i arkiver, der muligvis er en del af www-siden, der skal vises.
    - ***Rapporter potentielt uønskede programmer og spywaretrusler*** - (*aktiveret som standard*): markér for at aktivere programmet ***Anti-spyware*** og scanne efter spyware og efter vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.
    - ***Rapportér forbedret sæt af potentielt uønskede programmer*** - (*slået fra som standard*): markér for at detektere udvidede pakker af spyware: programmer, der er

fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.

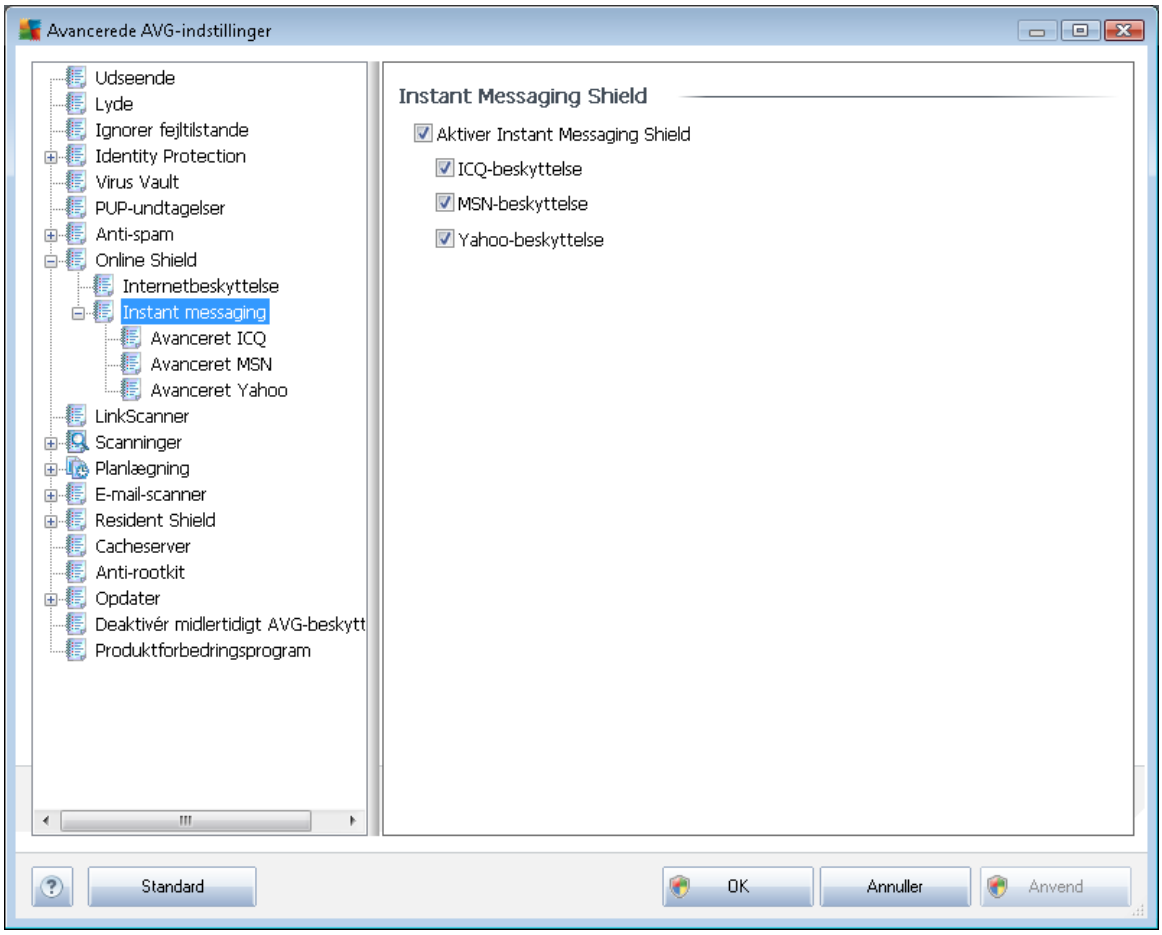
- **Brug heuristisk analyse** - (*slået til som standard*): scan indholdet på siden, der skal vises, vha. heuristisk analyse (*dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø*).

- **Aktivér grundig scanning** (*slået fra som standard*) - i særlige situationer (*hvor der er mistanke om, at computeren er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som egentlig ikke kan blive inficeret, men bare for at være sikker. Husk at denne metode er ret tidskrævende.

- **Maksimal delstørrelse af en fil, der skal scannes** - 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 ***Online Shield***. Selvom den downloadede fil er større end angivet, og derfor ikke scannes med Online Shield, er du stadig beskyttet. Hvis filen er inficeret, detekterer ***Resident Shield*** det øjeblikkeligt.

- **Udeluk 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 ***Online Shield***. Derfor bør du kun udelade værter, som du kan være fuldstændig sikker på aldrig leverer provide farligt indhold.

9.8.2. Instant messaging

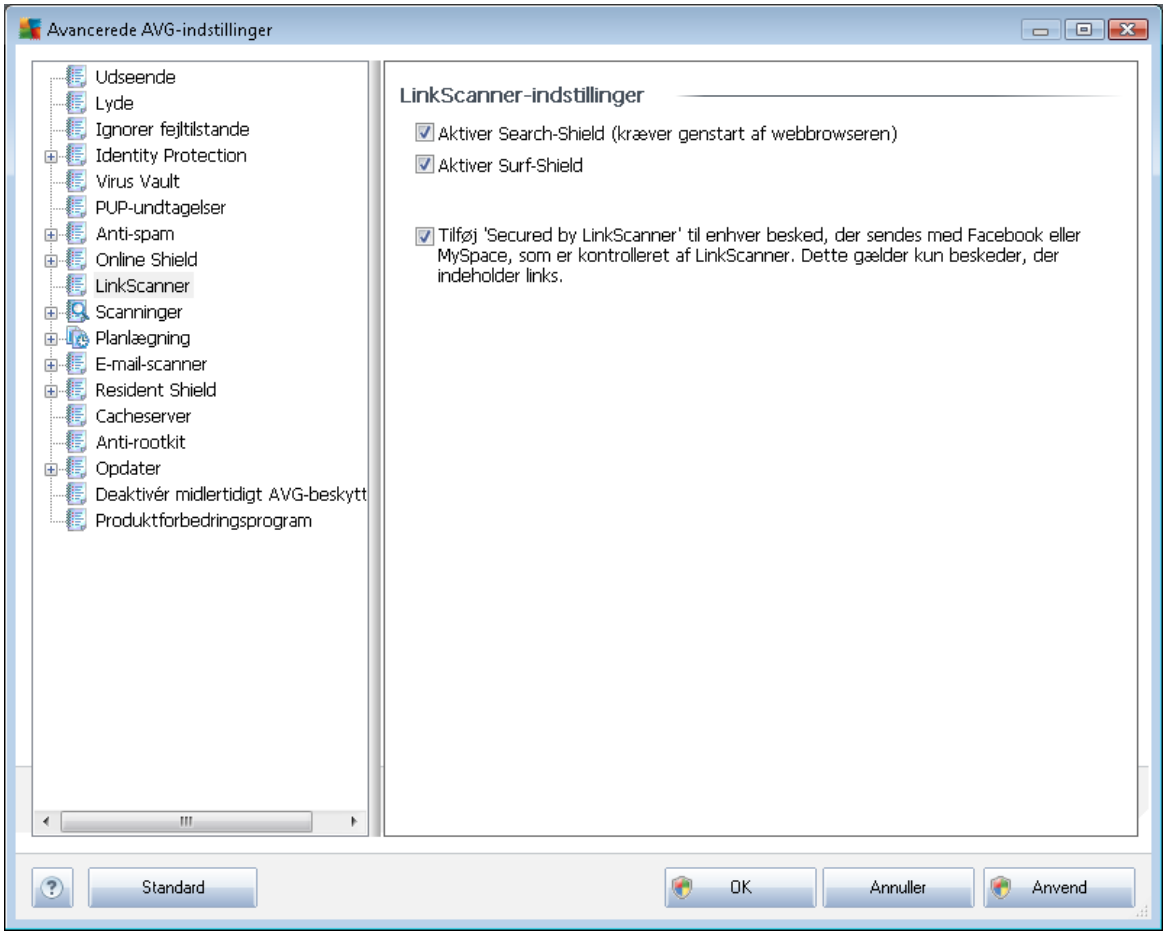


I dialogen ***Instant Messaging Shield*** kan du redigere ***Online Shield***-komponentens indstillinger vedrørende scanning af instant messaging. I øjeblikket understøttes følgende tre instant messaging-programmer: ***ICQ***, ***MSN*** og ***Yahoo*** - marker det pågældende punkt for hver af dem, hvis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

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

9.9. Linkscanner

I dialogen ***LinkScanner*-indstillinger** kan du slå de elementære funktioner i ***LinkScanner*** til og fra:



- ***Aktiver Søgeskjold*** - (*slået til som standard*): vejledende ikoner på søgninger udført i Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, or SlashDot efter forudgående kontrol af indholdet på de websteder, der returneres af søgemaskinen.

- ***Aktiver 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*).

- ***Tilføj 'Secured by LinkScanner' ...*** - markér dette element for at bekræfte, at du ønsker at tilføje certificeringstekst om ***Link Scanner***-kontrol i alle meddelelser, der indeholder aktive hyperlinks, som er blevet sendt fra de sociale netværker Facebook og MySpace.

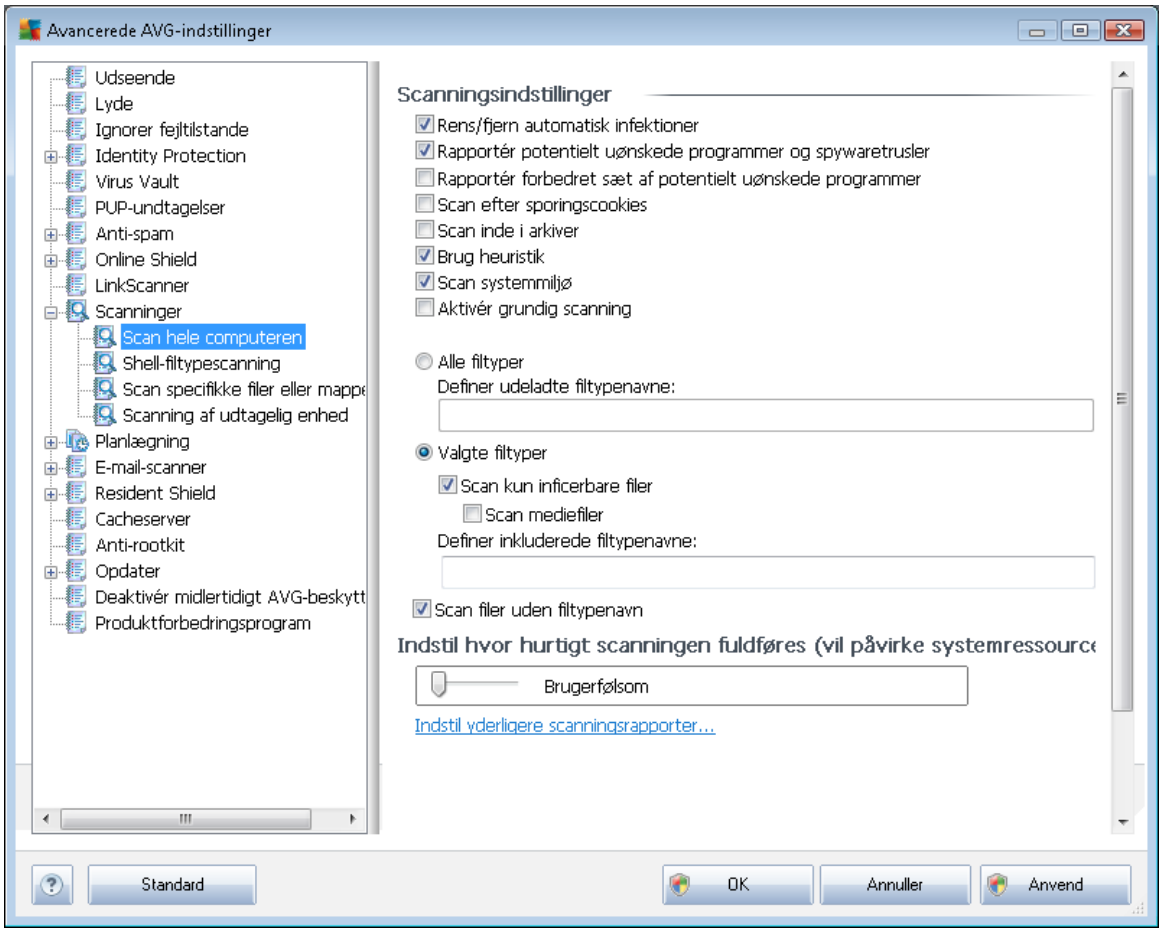
9.10. Scanninger

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

- ***Scanning af 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

9.10.1. Scan hele computeren

Valgmuligheden ***Scanning af 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*** (*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, vil det inficerede objekt flyttes til ***Virus Vault***.

- ***Rapporter potentielt uønskede programmer og spywaretrusler*** (*aktiveret som standard*) - markér for at aktivere programmet ***Anti-spyware*** ***og scanne efter spyware og efter vira.*** Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*) - markér for at detektere udvidede pakker af spyware: programmer, der er fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.

- ***Scan efter sporingscookies*** (*slået fra 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 fra som standard*) - disse parametre definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i arkiver, f.eks. ZIP, RAR, ...

- ***Brug heuristik*** (*slået til som standard*) - Heuristisk analyse (*dynamisk emulering af det scannede objektsinstruktioner 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.

- ***Aktivér grundig scanning***(*slået fra som standard*) - i særlige situationer (*hvor der er mistanke om, at computeren er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som egentlig ikke kan blive inficeret, men bare for at være sikker. Husk at denne metode er ret tidskrævende.

Derudover skal de beslutte, om du vil have scannet

- ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en kommaseparet (*når den gemmes, ændres kommaerne til semikolon*) liste over filtypenavne, som ikke skal scannes;

- ***Udvalgte filtyper*** - du kan angive, at du kun vil scanne filer, som er mulige at inficere (*filer som ikke kan blive inficeret, bliver ikke scannet, for eksempel visse almindelige tekstfiler, eller andre ikke eksekverbare filer*), herunder mediefiler (*video- og lydfiler - hvis du lader dette felt stå tomt, reducerer det scanningen yderligere, fordi disse filer ofte er ret store, og det ikke er særlig sandsynligt, at de er inficerede med virus*). Igen kan du angive, hvilke filer, der altid skal scannes, ud fra filtypenavnene.

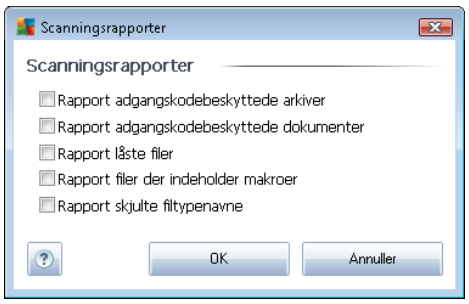
- Du kan også vælge at ***Scanne filer uden filtypenavn*** - denne indstilling er slået til som standard, og det anbefales, at du bevarer den sådan, medmindre du har en virkelig god grund til at ændre den. Filer uden filtypenavn er ret mistænkelige og bør altid scannes.

Indstil hvor hurtigt scanningen fuldføres

I sektionen ***Indstil hvor hurtigt scanningen fuldføres*** kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne indstillingsværdi sat til *brugerfølsomt* niveau 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.

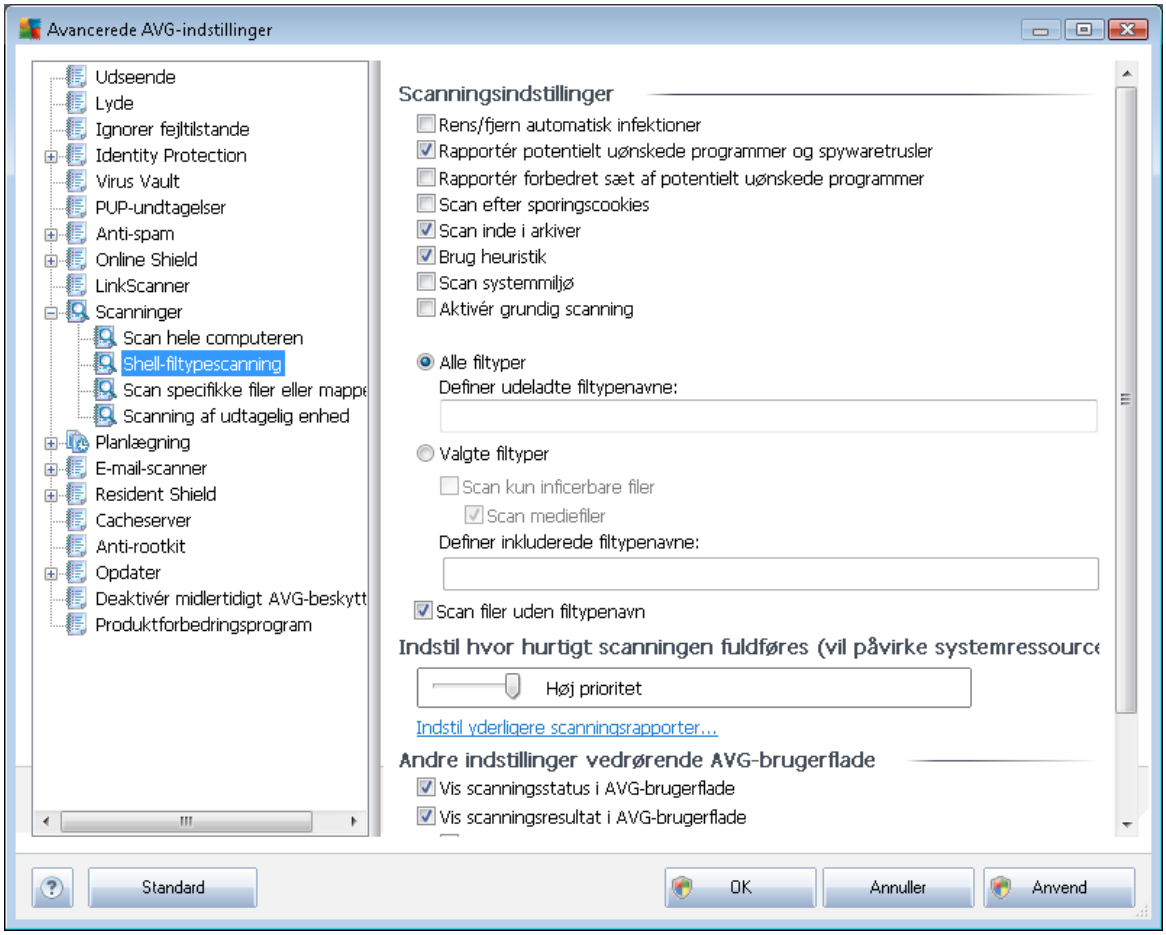
Indstil yderligere scanningsrapporter...

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:



9.10.2. Shell-udvidelsesscanning

I lighed med det tidligere element ***Scanning af 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***:



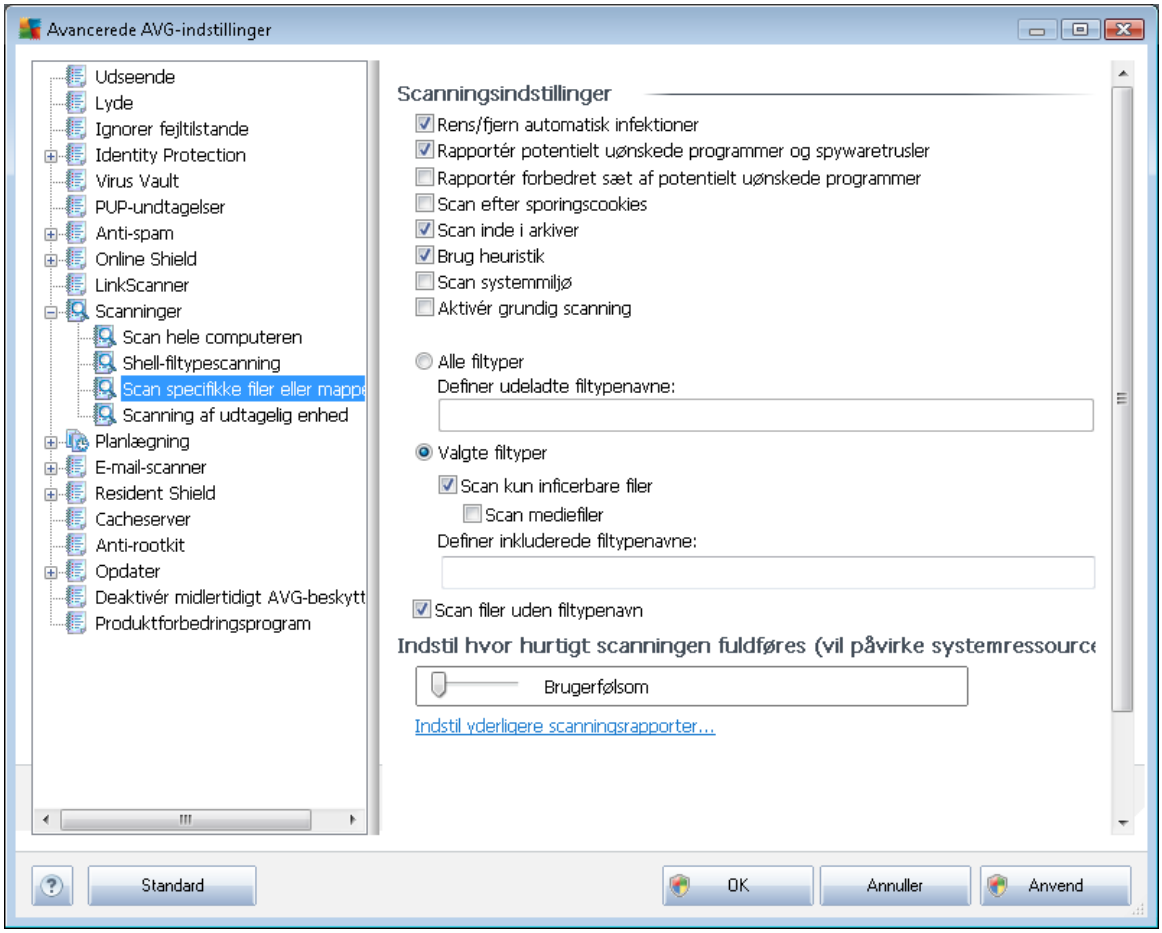
Parameterlisten er magen til listerne for ***Scanning af hele computeren***. Standardindstillingerne varierer dog (*for eksempel kontrollerer Scanning af hele computeren ikke arkiver, men scanner systemmiljøet, mens det med Shell-udvidelsesscanning er omvendt*).

Bemærk: *For at se en beskrivelse af specifikke parametre henvises til kapitlet* ***AVG Avancerede indstillinger / Scanninger / Scanning af hele computeren***.

Sammenlignet med dialogen ***Scanning af hele computeren*** indeholder dialogen ***Shell-udvidelsesscanning*** også sektionen kaldet ***Andre indstillinger for AVG-brugergrænsefladen***, hvor du kan angive, om scanningsforløbet og scanningsresultaterne skal være tilgængelige fra AVG-brugergrænsefladen. Du kan også angive, at scanningsresuultatet kun vises, hvis der detekteres infektion under scanningen.

9.10.3. 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***:

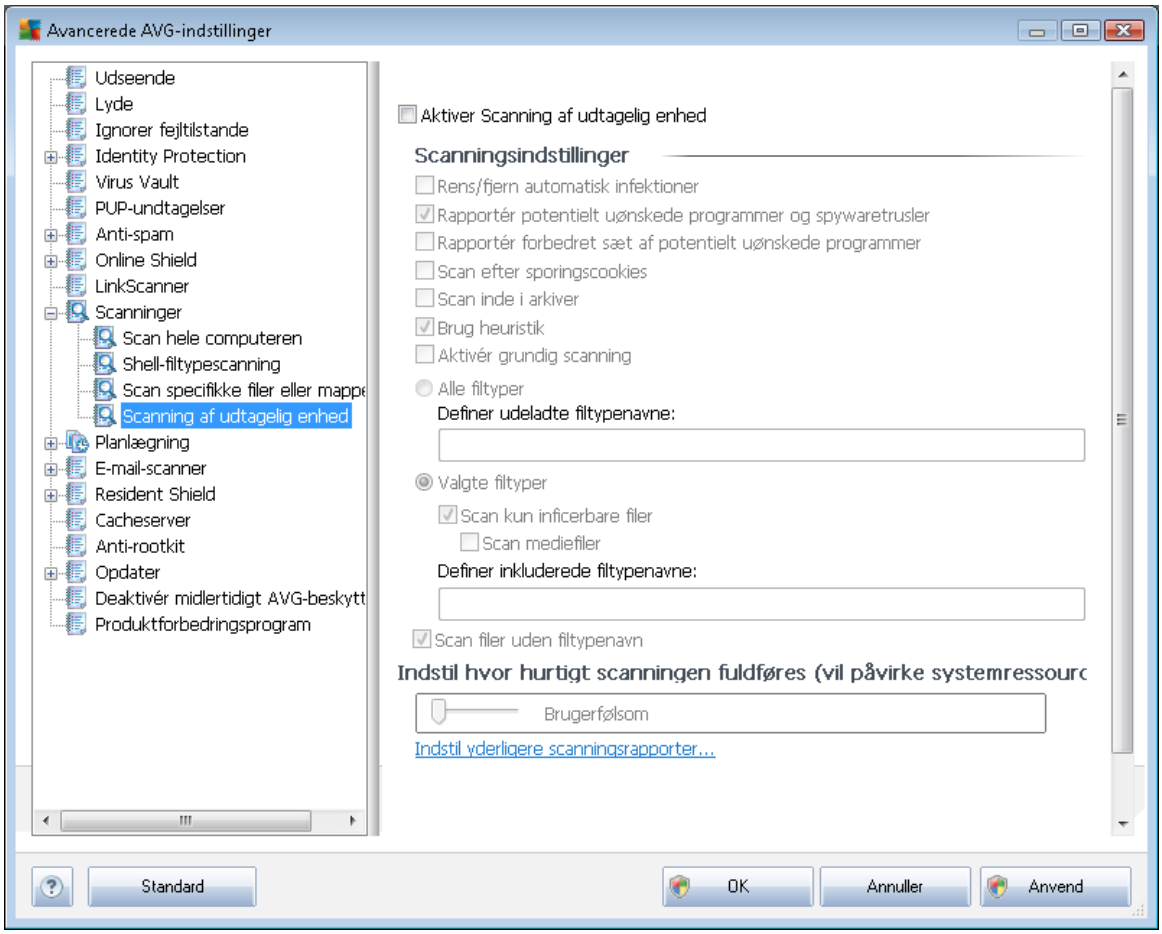


Alle parametre indstillet i denne konfigurationsdialog gælder kun for de områder, der er udvalgt til scanning med ***Scanning af specifikke filer eller mapper***!

Bemærk: *For at se en beskrivelse af specifikke parametre henvises til kapitlet* ***AVG Avancerede indstillinger / Scanninger / Scanning af hele computeren***.

9.10.4. Scanning af udtagelig enhed

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



Scanning af flytbar enhed køres automatisk, når du tilslutter en flytbar enhed til din computer. Som standard er denne scanning slået fra. Det er imidlertid vigtigt at scanne flytbare 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 flytbar enhed***

Bemærk: *For at se en beskrivelse af specifikke parametre henvises til kapitlet* ***AVG Avancerede indstillinger / Scanninger / Scanning af hele computeren****.*

9.11. Planlægning

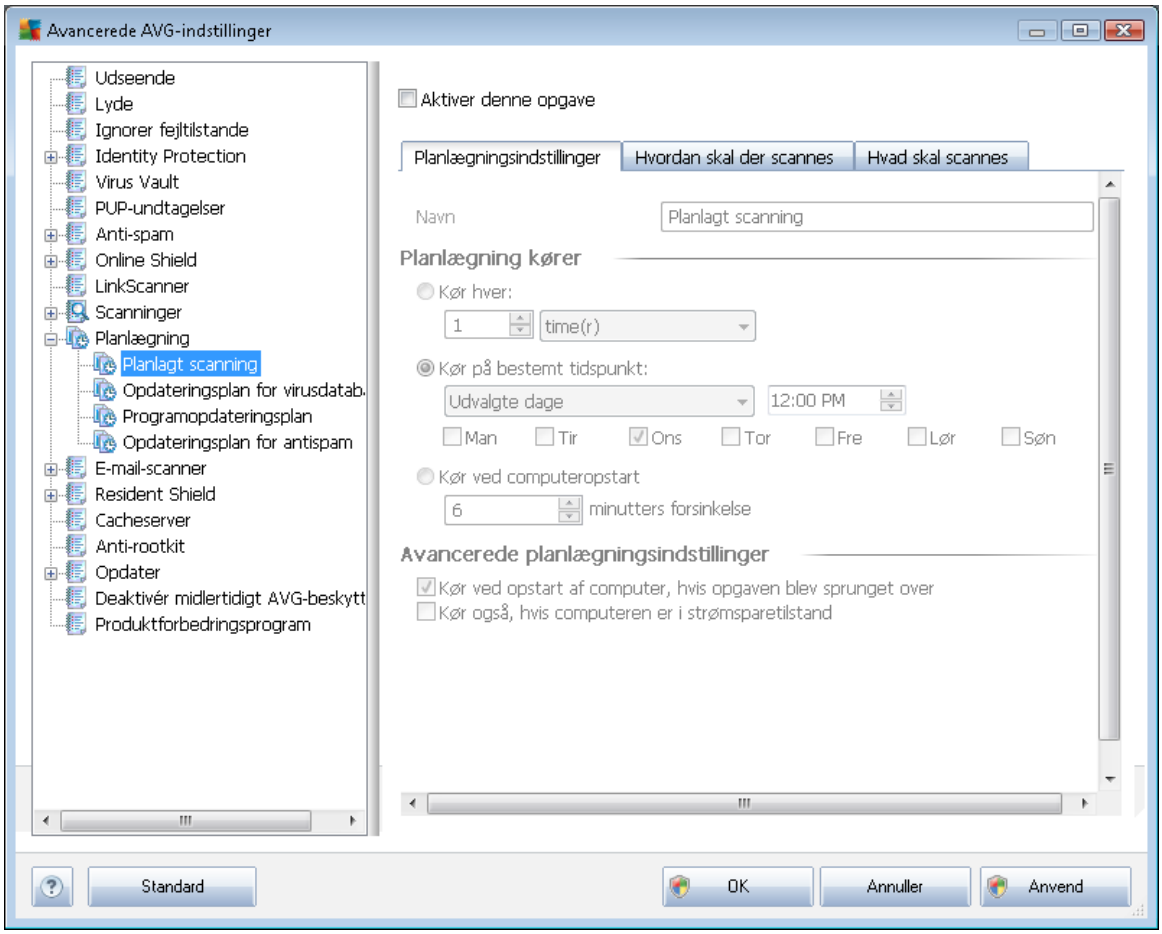
I sektionen ***Planlægning*** kan du redigere standardindstillingerne for:

- Planlagt scanning
- Opdateringsplan for virusdatabase

- Programopdateringsplan
- Anti-spam-opdateringsplan

9.11.1. Planlagt scanning

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



I tekstfeltet ***Navn*** (*deaktiveret for alle standardplaner*) står derefter navnet, der er tildelt netop denne plan af programleverandøren. For nyoprettede planer (*du kan tilføje en ny plan ved at højreklikke med musen over elementet* ***Planlagt scanning*** *i venstre navigationstræ*) kan du angive dit eget navn, og i så fald vil det være muligt at redigere tekstfeltet. Prøv altid 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:

Planlægning kører

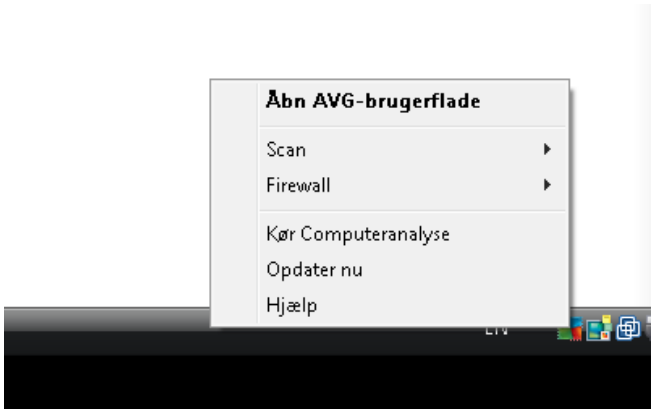
Her kan du angive tidsintervaller for kørsel af den nyplanlagte scanning. Timingen kan enten defineres med gentaget kørsel af scanningen efter et vist tidsrum (***Kør hver ...***) eller ved at definere en nøjagtig dato og klokkeslæt (***Kør med bestemte mellemrum ...***), eller muligvis ved at definere en hændelse, der knyttes til kørsel af scanningen (***Hændelsesbaseret ved opstart af computeren***).

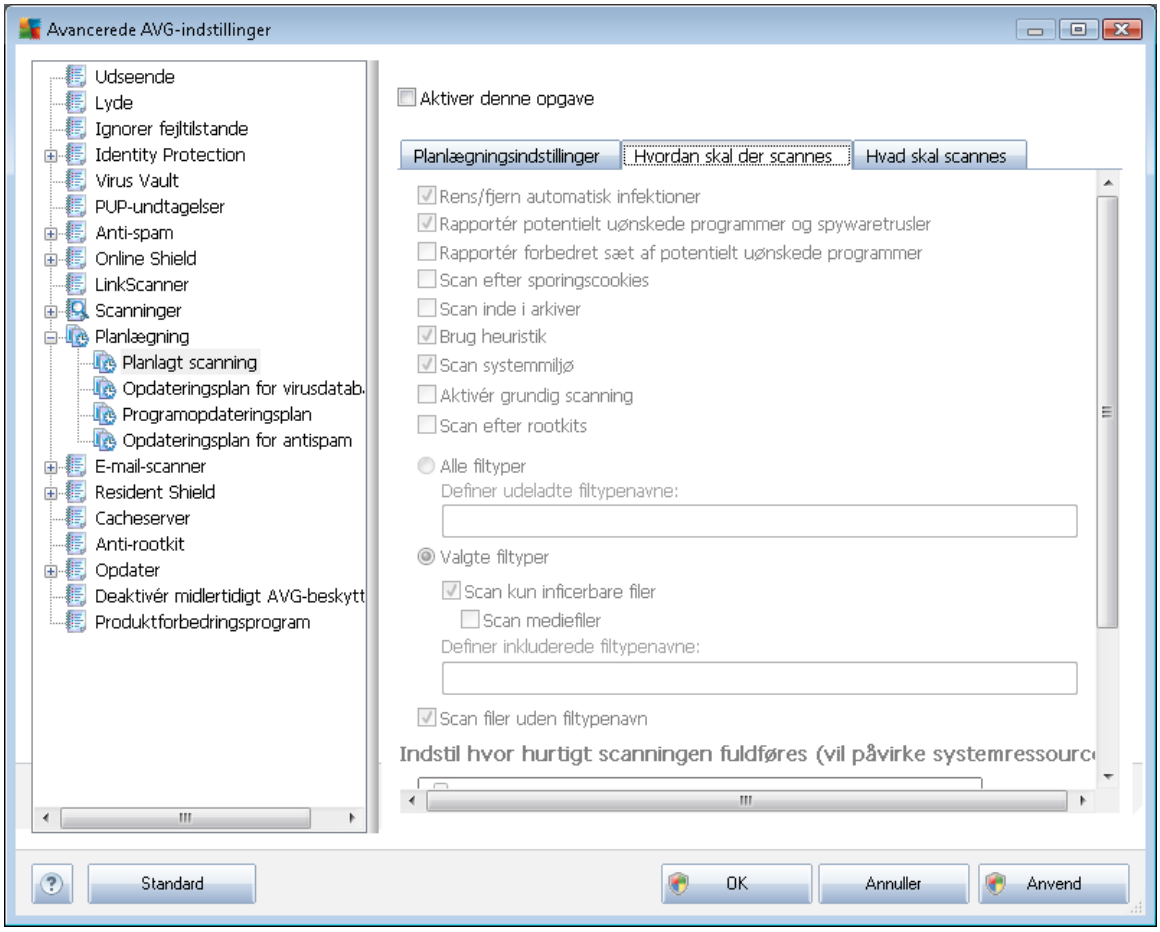
Avancerede planlægningsindstillinger

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 lommelygte*), der informerer om, at der køres en planlagt scanning. Højreklik på AVG ikonet for den igangværende scanning for at åbne en kontekstmenu, hvor du kan stoppe scanningen midlertidigt eller afbryde den, og ændre prioriteten på den aktuelt kørende scanning:





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, vil det inficerede objekt flyttes til ***Virus Vault***.

- ***Rapporter potentielt uønskede programmer og spywaretrusler*** *(slået til som standard):* markér for at aktivere programmet ***Anti-spyware*** og scanne efter spyware og efter vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*): markér for at detektere udvidede pakker af spyware: programmer, der er fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.

- ***Scan efter sporingscookies*** (*slået fra 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 fra som standard*): Denne parameter definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i et arkiv, f.eks. ZIP, RAR, osv.

- ***Brug heuristik*** (*slået til som standard*): Heuristisk analyse (*dynamisk emulering af det scannede objektsinstruktioner 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;

- ***Aktivér grundig scanning*** (*slået fra som standard*) - i særlige situationer (*hvor der er mistanke om, at computeren er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som egentlig ikke kan blive inficeret, men bare for at være sikker. Husk at denne metode er ret tidskrævende.

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

Derudover skal de beslutte, om du vil have scannet

- ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en kommasepareret (*når den gemmes, ændres kommaerne til semikolon*) liste over filtypenavne, som ikke skal scannes;

- ***Udvalgte filtyper*** - du kan angive, at du kun vil scanne filer, som er mulige at inficere (*filer som ikke kan blive inficeret, bliver ikke scannet, for eksempel visse almindelige tekstfiler, eller andre ikke eksekverbare filer*), herunder mediefiler (*video- og lydfiler - hvis du lader dette felt stå tomt, reducerer det scanningen yderligere, fordi disse filer ofte er ret store, og det ikke er særlig sandsynligt, at de er inficerede med virus*). Igen kan du angive, hvilke filer, der altid skal scannes, ud fra filtypenavnene.

- Du kan også vælge at ***Scanne filer uden filtypenavn*** - denne indstilling er slået til som standard, og det anbefales, at du bevarer den sådan, medmindre du har en virkelig god grund til at ændre den. Filer uden filtypenavn er ret mistænkelige og bør altid scannes.

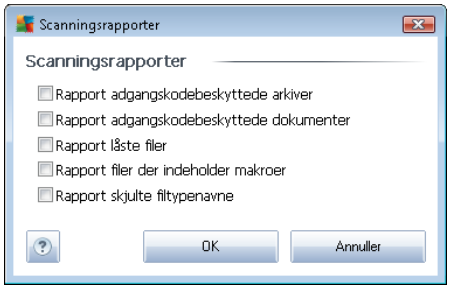
Indstil hvor hurtigt scanningen fuldføres

I sektionen ***Indstil hvor hurtigt scanningen fuldføres*** kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne indstillingsværdi sat til *brugerfølsomt* niveau 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.

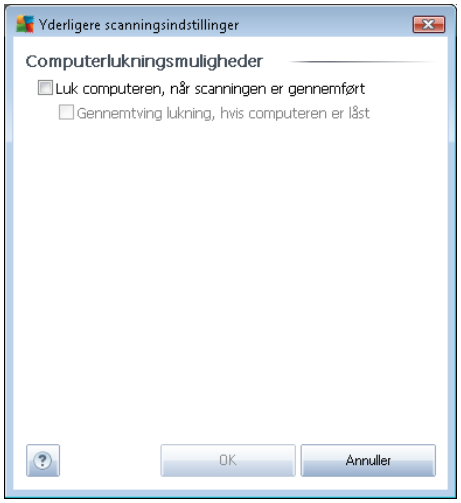
Indstil yderligere scanningsrapporter

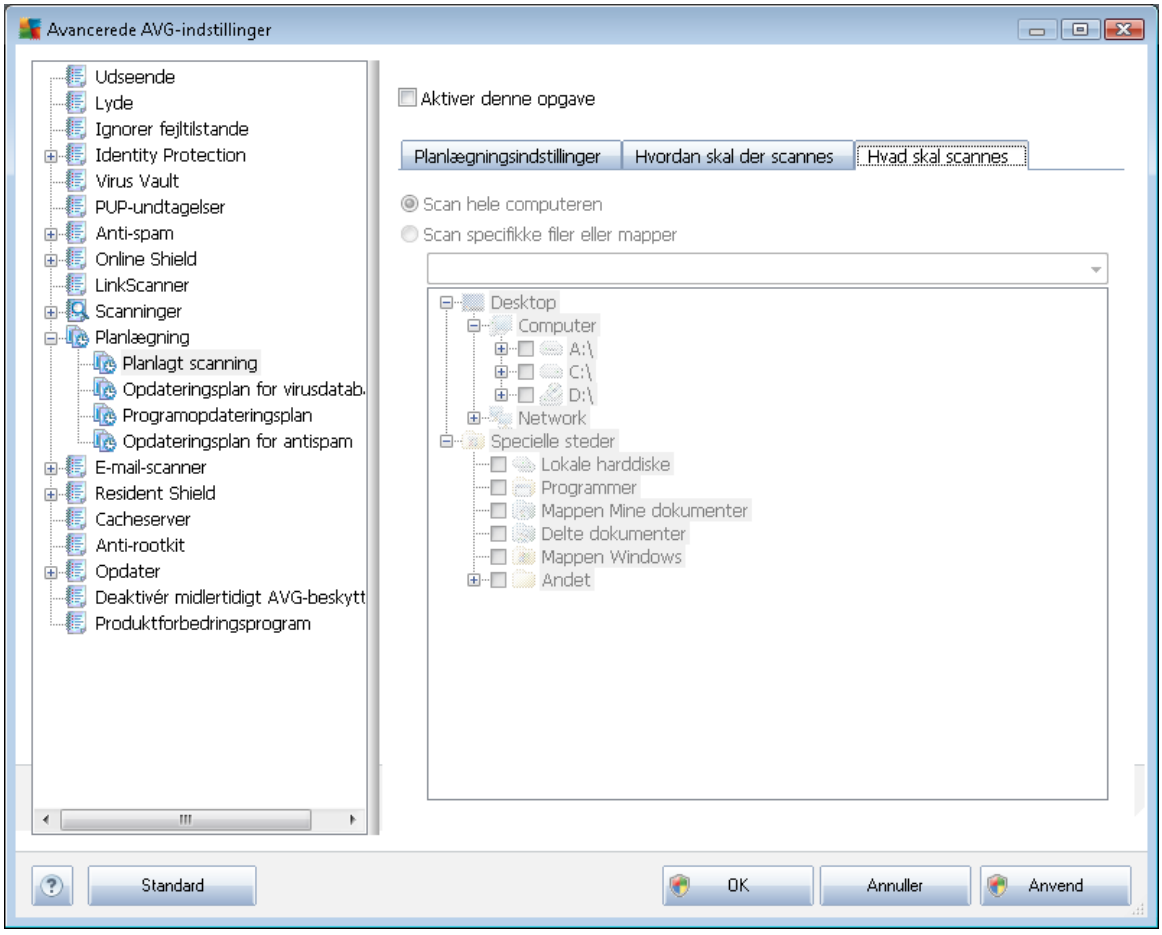
Klik på linket ***Indstil yderligere scanningsrapporter ...*** for at åbne det selvstændige dialogvindue ***Scanningsrapporter***, hvor du kan markere adskillige punkter for at definere, hvilke scanningsfund, der skal rapporteres:



Yderligere scanningsindstillinger

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***).

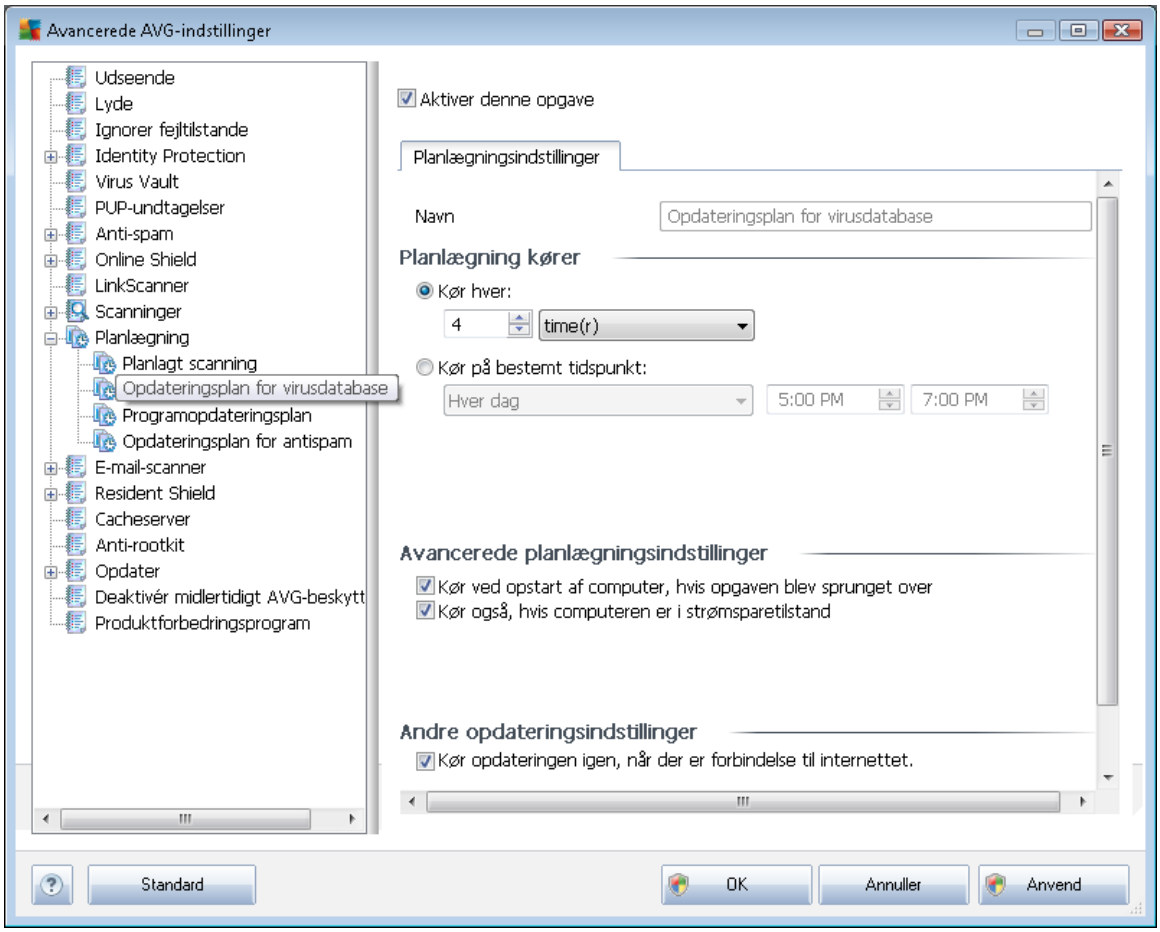




På fanen ***Hvad skal scannes*** kan du definere, om du vil planlægge scanning af hele computeren eller scanning af specifikke filer eller mapper. Hvis du vælger scanning af specifikke filer eller mapper, aktiveres træstrukturen nederst i denne dialogboks, og du kan angive mapper, der skal scannes.

9.11.2. Opdateringsplan for virusdatabase

Hvis det ***virkelig er nødvendigt***, kan du afmarkereelementet ***Aktiver denne opgave*** for midlertidigt at deaktivere den planlagte opdatering af virusdatabasen, og slå den til igen på et senere tidspunkt:



Den grundlæggende opdateringsplanlægning for virusdatabasen er beskrevet under ***Opdateringsadministrator***-komponenten. I denne dialog kan du konfigurere nogle detaljerede parametre for opdateringsplanlægningen for virusdatabasen. I tekstfeltet ***Navn*** (*deaktiveret for alle standardplaner*) står navnet, der af programleverandøren er tildelt netop denne plan.

Planlægning kører

I dette afsnit angiver du tidsintervallerne for den nyplanlagte kørsel af virusdatabaseopdateringen. Timingen kan enten defineres af den gentagne opdateringskørsel efter en bestemt tidsperiode (***Kør hver...***) eller ved at definere en nøjagtig dato og klokkeslæt (***Kør på specifikt klokkeslæt...***).

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.

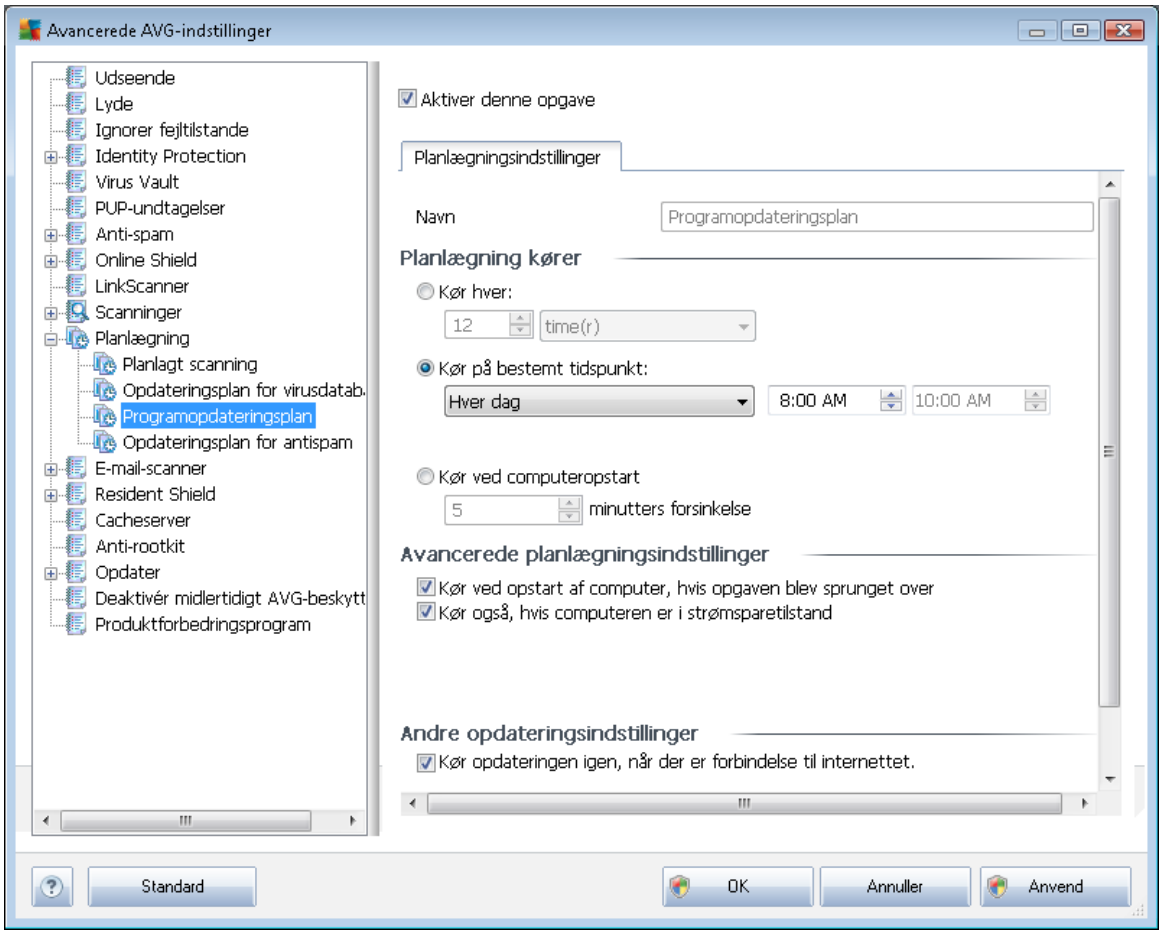
Andre opdateringsindstillinger

Marker til sidst indstillingen ***Kør opdateringen igen, så snart der er forbindelse til internettet*** for at sikre, at opdateringen bliver kørt igen, så snart internetforbindelsen er genoprettet, hvis internetforbindelsen bliver afbrudt, og opdateringen mislykkes.

Når den planlagte opdatering køres 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***).

9.11.3. Programopdateringsplan

Hvis det ***virkelig er nødvendigt***, kan du afmarkereelementet ***Aktiver denne opgave*** for midlertidigt at deaktivere den planlagte opdatering af programmet, og slå den til igen på et senere tidspunkt:



I tekstfeltet ***Navn*** (*deaktiveret for alle standardplaner*) står navnet, der af programleverandøren er tildelt netop denne plan.

Planlægning kører

Her kan du angive 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

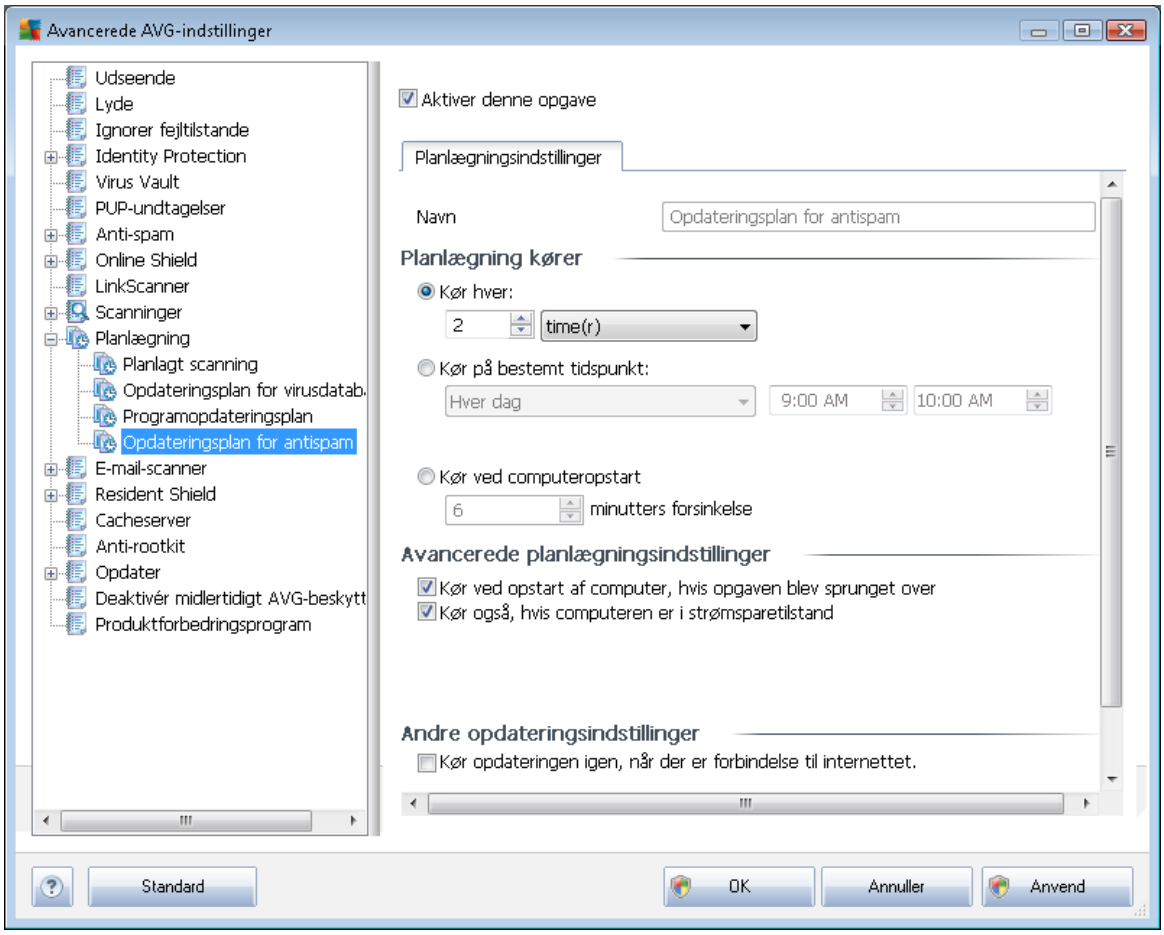
Marker indstillingen ***Kør opdateringen igen, så snart der er forbindelse til internettet*** for at sikre, at opdateringen bliver kørt igen, så snart internetforbindelsen er genoprettet, hvis internetforbindelsen bliver afbrudt, og opdateringen mislykkes.

Når den planlagte opdatering køres 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***).

Bemærk: *Hvis der forekommer et tidsmæssigt sammenfald af en planlagt programopdatering og en planlagt scanning, tager opdateringsprocessen prioritet og scanningen vil blive afbrudt.*

9.11.4. Anti-spam opdateringsplan

Hvis det ***virkelig er nødvendigt***, kan du afmarkere elementet ***Aktiver denne opgave*** for midlertidigt at deaktivere den planlagte opdatering af ***Anti-spam***, og slå det til igen senere:



Grundlæggende ***Anti-spam***-opdateringsplanlægning er beskrevet i ***Opdateringsstyring***-komponenten. I denne dialog kan du konfigurere nogle detaljerede parametre for opdateringsplanlægningen. I tekstfeltet ***Navn*** (*deaktiveret for alle standardplaner*) står navnet, der af programleverandøren er tildelt netop denne plan.

Planlægning kører

Her kan du angive 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.

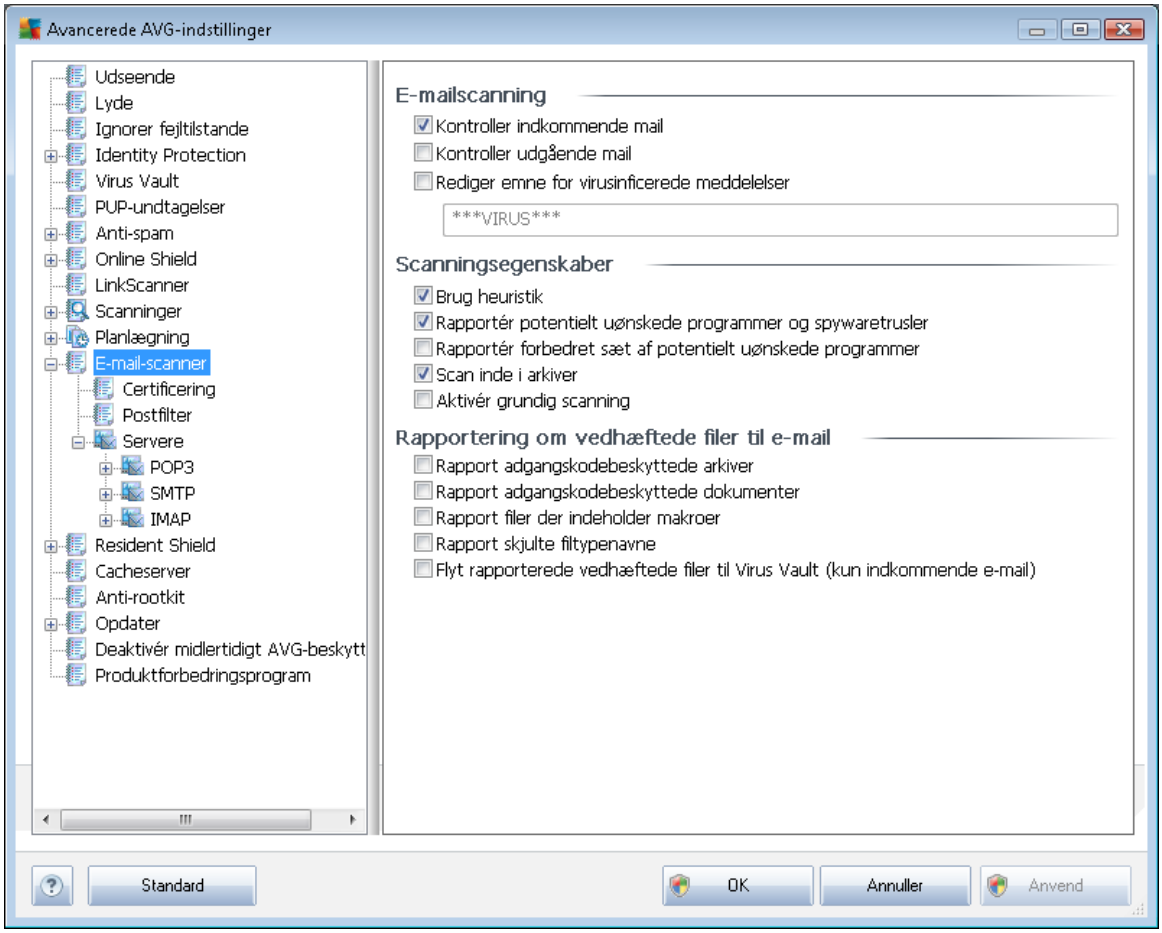
Andre opdateringsindstillinger

Marker indstillingen ***Kør opdateringen igen, så snart der er forbindelse til internettet*** for at sikre, at opdateringen bliver kørt igen, så snart internetforbindelsen er genoprettet, hvis internetforbindelsen bliver afbrudt, og ***Anti-spam***-opdateringen mislykkes.

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***).

9.12. E-mail-scanner

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



E-mailscanning

I denne sektion kan du foretage disse grundlæggende indstillinger for indkommende og/eller udgående e-mail:

- ***KOntrollér indkommende e-mail*** (*slået til som standard*) - markér for at aktivere/deaktivere scanning af alle e-mail-meddelelser, der leveres til din e-mail-klient
- ***Kontrollér udgående e-mail*** (*slået fra som standard*) - markér for at aktivere/deaktivere scanning af e-mails, der sendes fra din konto
- ***Rediger emne for virusinficerede meddelelser*** (*slået fra som standard*) - hvis du vil advares om, at den scannede e-mail-meddelelse blev detekteret som inficeret, skal du markere dette element og udfylde den ønskede tekst i tekstfeltet. Denne tekst vil derefter blive føjet til "Emne"-linjen i alle detekterede e-mail-meddelelser, , så de nemmere kan identificeres og filtreres. Standardværdien er ***VIRUS***, som vi anbefaler at beholde.

Scanningsegenskaber

I denne sektion kan du specificere, hvordan e-mail-meddelelserne scannes:

- ***Brug heuristik*** (*slået til som standard*) – markér for at anvende detekteringsmetoden heuristik ved scanning af e-mail-meddelelser. Hvis denne indstilling er slået til, kan du filtrere e-mail med vedhæftede filer efter den vedhæftede fils egentlige indhold, så der ikke kun tages højde for filtypenavnet. Filtreringen kan indstilles i dialogen ***Postfilter***.
- ***Rapporter potentielt uønskede programmer og spywaretrusler*** (*aktiveret som standard*) - markér for at aktivere programmet ***Anti-spyware*** og scanne efter spyware og efter vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.
- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*) - markér for at detektere udvidede pakker af spyware: programmer, der er fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.
- ***Scan inde i arkiver*** (*slået til som standard*) - marker for at scanne indholdet i arkiver, der er vedhæftet til e-mail-meddelelser.
- ***Aktivér grundig scanning*** (*slået fra som standard*) - i særlige situationer (*hvor der er mistanke om, at computeren er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som egentlig ikke kan blive inficeret, men bare for at være sikker. Husk at denne metode er ret tidskrævende.

Rapportering om vedhæftede filer til e-mail

I denne sektion kan du indstille yderligere rapporter om potentielt farlige eller mistænkelige filer. Bemærk, at der ikke vises en advarselsdialog, der tilføjes kun i certificeringstekst i slutningen af e-mail-meddelelsen, og alle sådanne rapporter bliver anført i dialogen E-mail scanner-detaktering:

- ***Rapporter adgangskodebeskyttede arkiver*** – arkiver (*ZIP, RAR osv.*) der er beskyttet med adgangskode er ikke mulige at scanne for vira. Marker feltet for at rapportere dem som potentielt farlige.

- ***Rapporter adgangskodebeskyttede dokumenter*** – dokumenter beskyttet med adgangskode er ikke mulige at scanne for vira. Marker feltet for at rapportere dem som potentielt farlige.

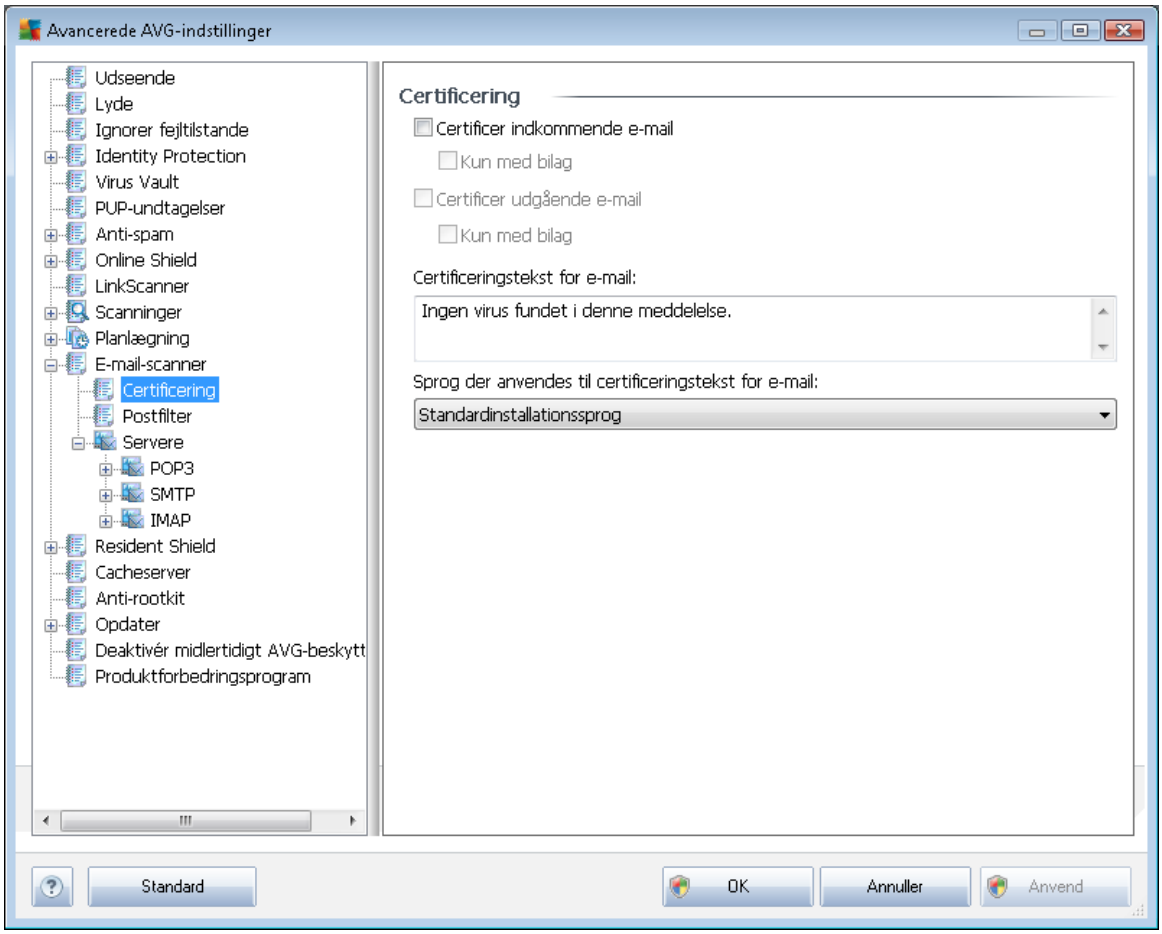
- ***Rapporter filer med makroer***– en makro er en foruddefineret række trin, der er beregnet til at gøre bestemte opgaver nemmere for en bruger (*MS Word-makroer er almindeligt kendte*). Som sådan kan en makro indeholde potentielt farlige instruktioner, og det er muligvis relevant for dig at markere feltet for at sikre, at filer med makroer bliver rapporteret som mistænkelige.

- ***Rapporter skjulte filtypenavne*** – skjulte filtypenavne kan f.eks. få en mistænkelig eksekverbar fil "something.txt.exe" til at se ud som en harmløs almindelig tekstfil "something.txt". Marker feltet for at rapportere dem som potentielt farlige.

- ***Flyt rapporterede vedhæftede filer til Virus Vault*** - 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***.

9.12.1. Certificering

I dialogen ***Certificering*** kan du angive teksten og sproget på certificeringne af både indkommende og udgående mail:



Certificeringsteksten består af to dele, brugerdelen og systemdelen - se følgende eksempel: den første linje viser brugerdelen, resten er genereret automatisk:

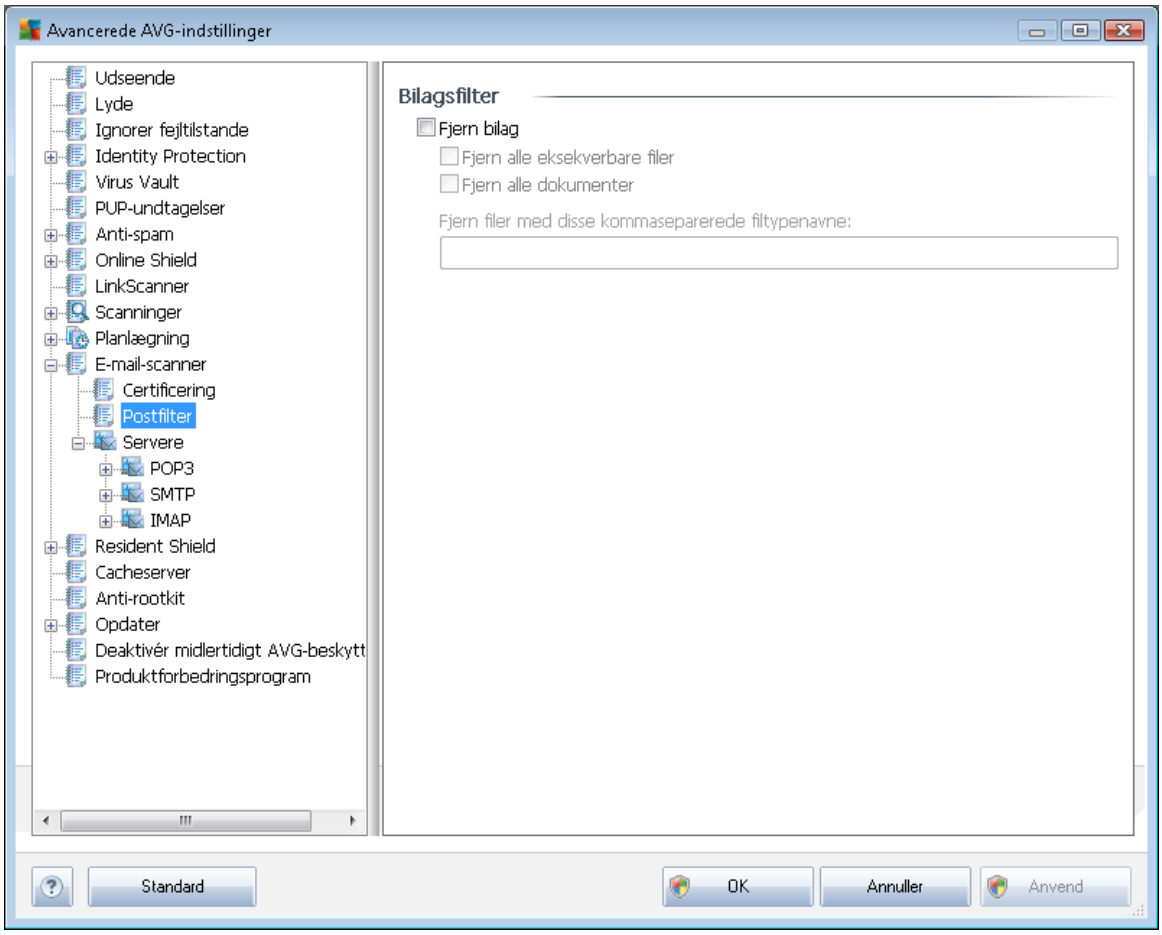
Ingen virus fundet i denne meddelelse.

Kontrolleret af AVG.

Version: x.y.zz / Virusdatabase: xx.y.z - Udgivelsesdato: 12/9/2010

Hvis du vælger at bruge certificering for enten indkommende eller udgående e-mails, kan du i denne dialog også angive den nøjagtige certificeringstekst for brugerdelen (***E-mail certificeringstekst***), og vælge det sprog, der skal bruges til den automatisk genererede systemdel af certificeringen (***Sprog der anvendes til certificeringstekst for e-mail***).

9.12.2. Postfilter

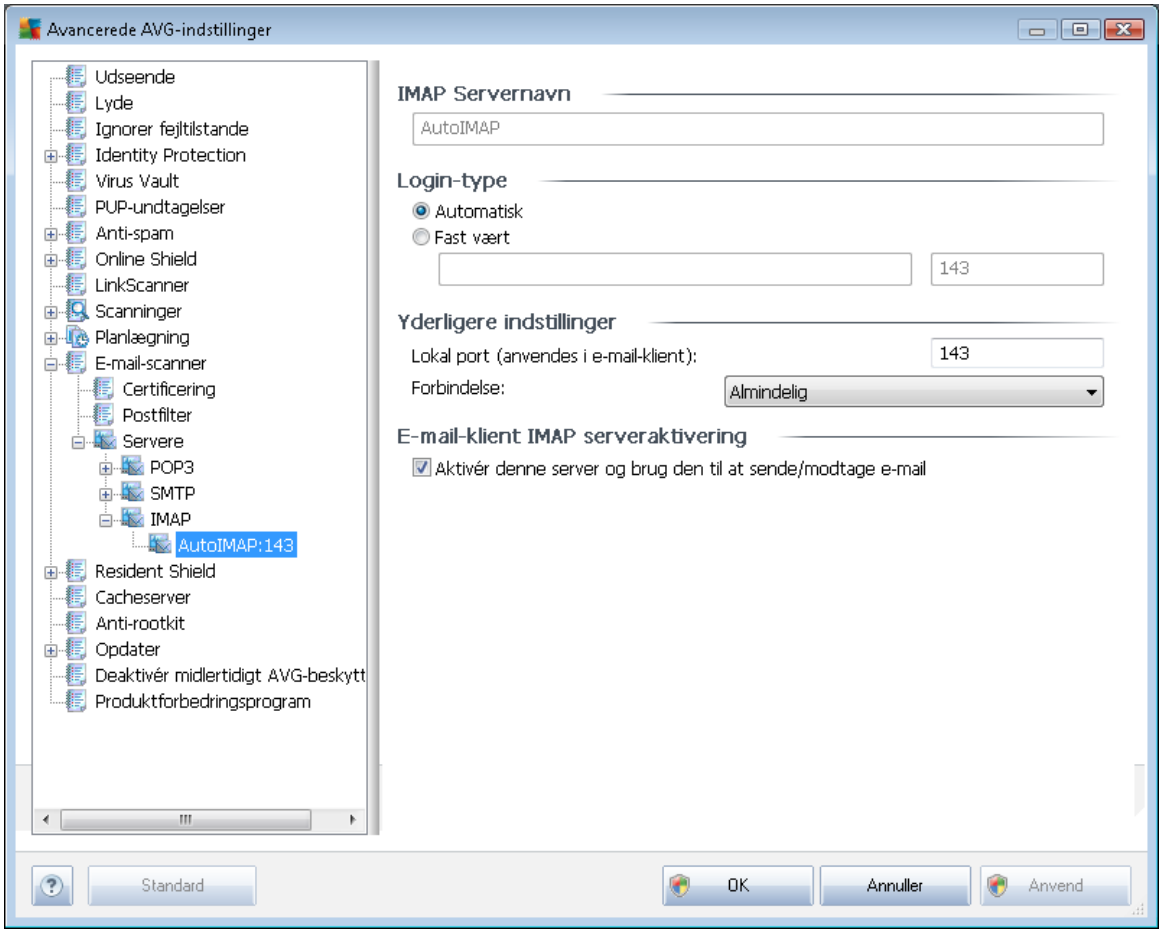


I dialogboksen ***Filter for vedhæftede filer*** kan du indstille parametre for scanning af vedhæftede filer i e-mail-meddelelser . Som standard er indstillingen ***Fjern vedhæftede filer*** slået fra. Hvis du beslutter at aktivere den, bliver alle vedhæftede filer i e-mail, der detekteres som inficerede 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, *.docx, *.xls, *.xlsx filer vil blive slettet
- ***Fjern filer med disse kommaseparerede filtypenavne*** - fjerner alle filer med de definerede filtypenavne

9.12.3. Servere

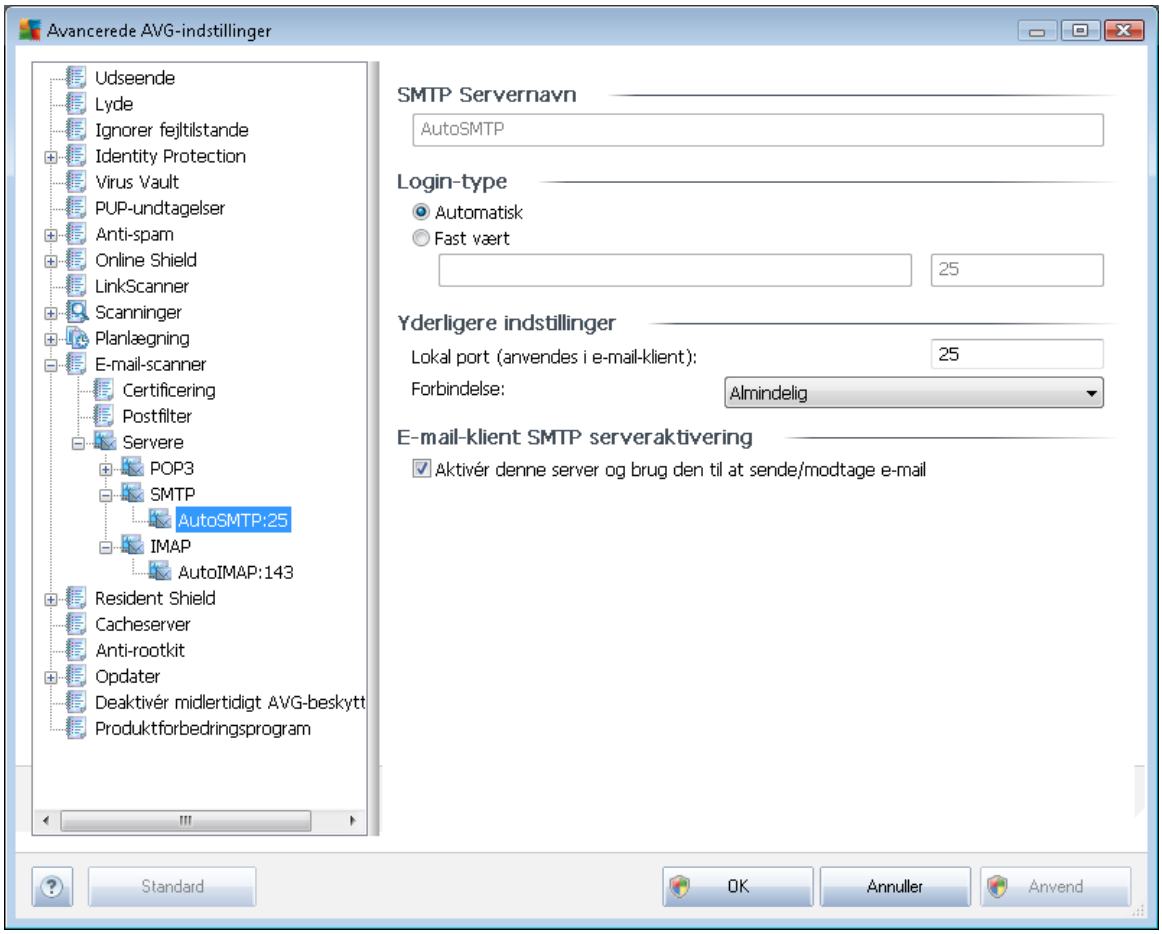
I sektionen ***Servere*** kan du redigere parametre for ***E-mail-scanner***-komponentservere, eller sætte en ny server op ved hjælp af knappen ***Tilføj ny server***.



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*** - i dette felt kan du angive navnet på de nye tilføjede servere (*for at tilføje en POP3-server skal du højreklikke på musen over POP3-elementet i venstre navigationsmenu*). For automatisk oprettet "AutoPOP3"-server er dette felt deaktiveret.
- ***Logintype*** - definerer metoden til at bestemme mailserveren, der anvendes til indkommende 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. Loginnavnet forbliver uændret. Som navn kan du anvende et domænenavn (*for eksempel pop.acme.com*) samt 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.
    - ***Forbindelse*** - in 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*** - marker/afmarker dette element for at aktivere eller deaktivere den angivne POP3-server

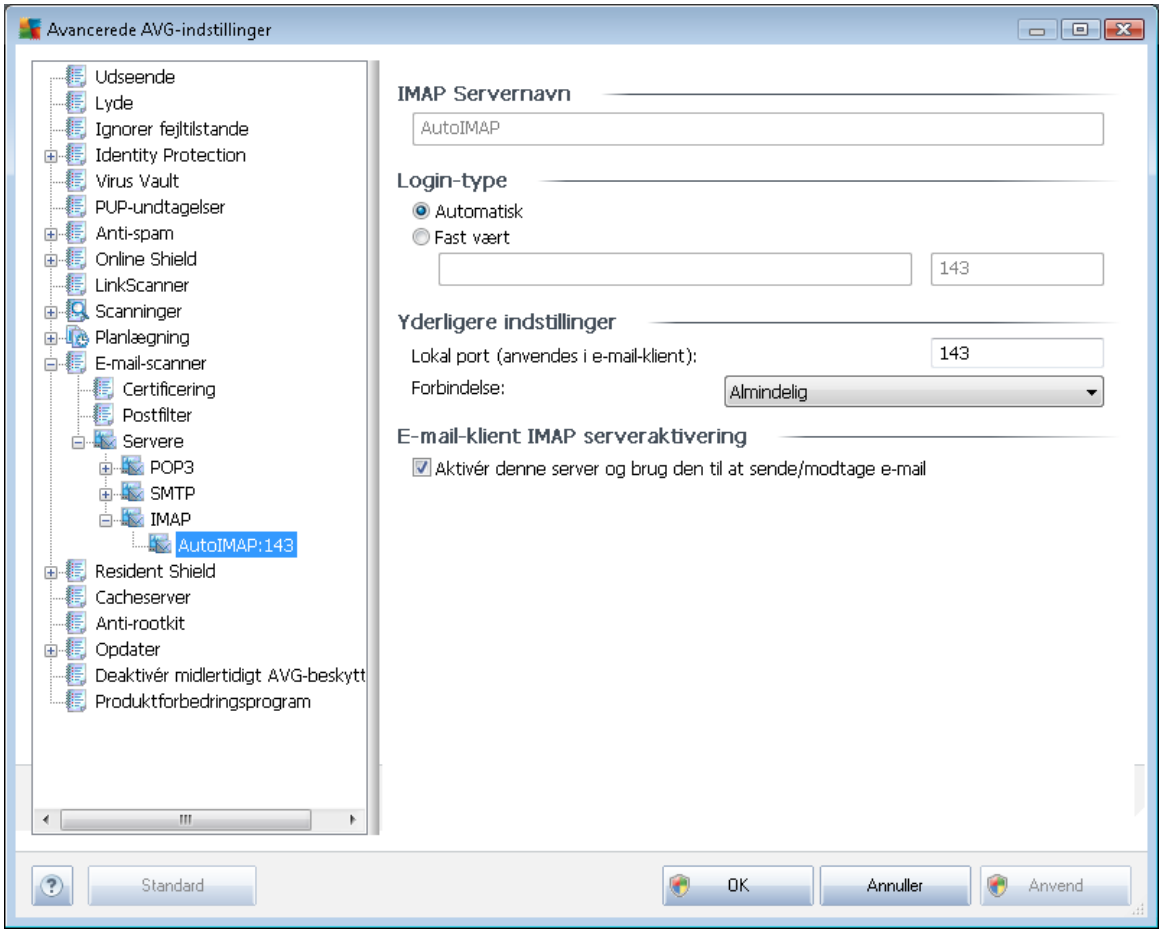


I denne dialogboks (*åbnes via* ***Servere / SMTP***) kan du konfigurere en ny ***E-mail scanner***-server vha. SMTP-protokollen for udgående e-mail:

- ***SMTP-servernavn*** - i dette felt kan du angive navnet på de nye tilføjede servere (*for at tilføje en SMTP-server skal du højreklikke på musen over SMTP-elementet i venstre*

navigationsmenu). For automatisk oprettet "AutoSMTP"-server er dette felt deaktiveret.

- ***Logintype*** - 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 smtp.acme.com:8200*). Standardporten for SMTP-kommunikation er 25.
- ***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 SMTP-kommunikation i dit e-mail-program.
    - ***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.
- ***Aktivering af e-mail klients SMTP-server*** - indsæt/fjern markering i dette felt for at aktivere/deaktivere SMTP-serveren, der er angivet herover



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

- ***IMAP-servernavn*** - i dette felt kan du angive navnet på de nye tilføjede servere (*for at tilføje en IMAP-server skal du højreklikke på musen over IMAP-elementet i venstre navigationsmenu*). For automatisk oprettet "AutoIMAP"-server er dette felt deaktiveret.

- ***Logintype*** - 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 imap.acme.com:8200*). Standardporten for IMAP-kommunikation er 143.

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

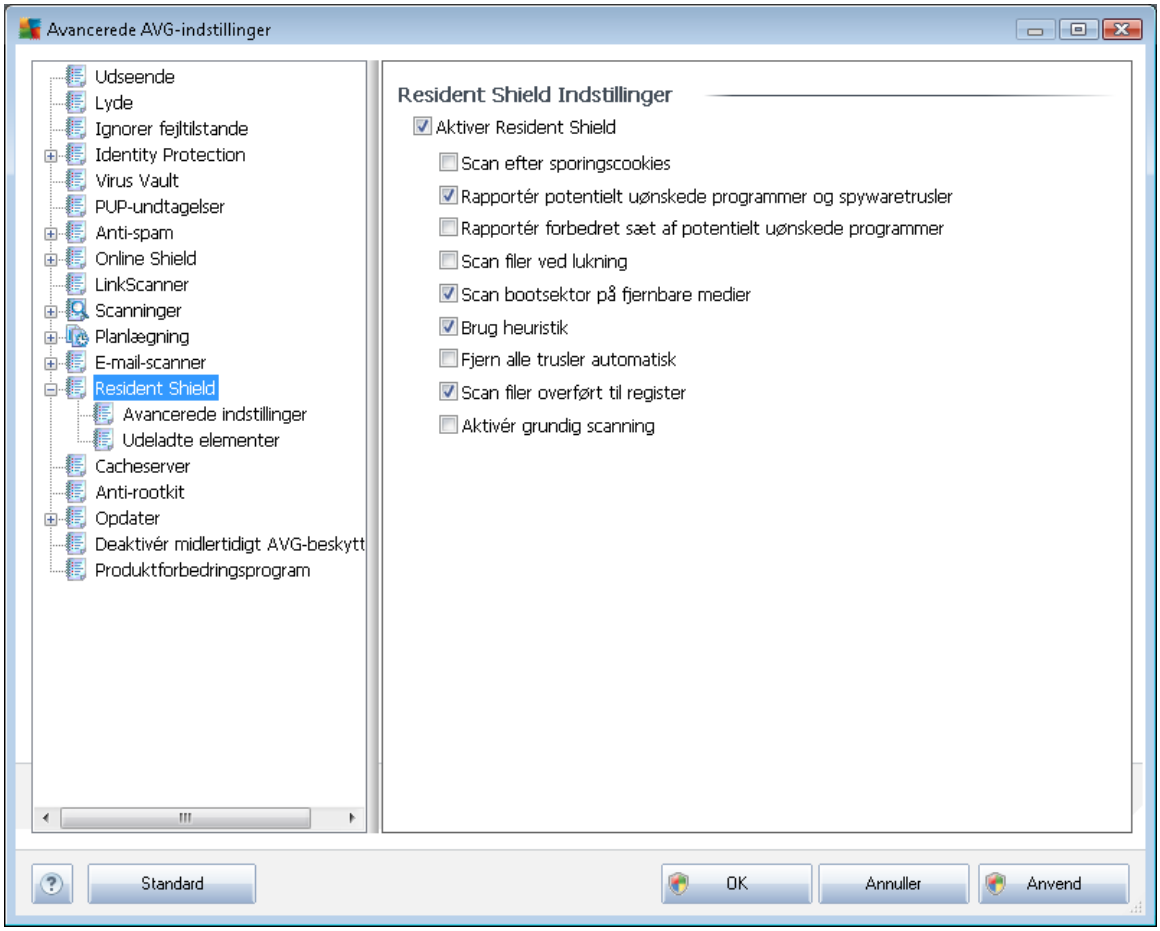
- **Lokal port** - angiver den port, hvor kommunikation fra din mailapplikation forventes. Du skal derefter angive denne port som port for IMAP-kommunikation i dit e-mail-program.

- **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.

- ***Aktivering af e-mail klients IMAP-server*** - indsæt/fjern markering i dette felt for at aktivere/deaktivere IMAP-serveren, der er angivet herover

9.13. 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 vælge hvilke funktioner i ***Resident Shield***, der skal være aktiveret:

- ***Scan efter sporingscookies*** (*slået fra som standard*) - 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*)

- ***Rapporter potentielt uønskede programmer og spywaretrusler*** - (*aktiveret som standard*): markér for at aktivere programmet ***Anti-spyware*** og scanne efter spyware og efter vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*) - markér for at detektere udvidede pakker af spyware: programmer, der er fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.

- ***Scan ved lukning*** (*slået fra som standard*) - 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 bootsektor 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*)

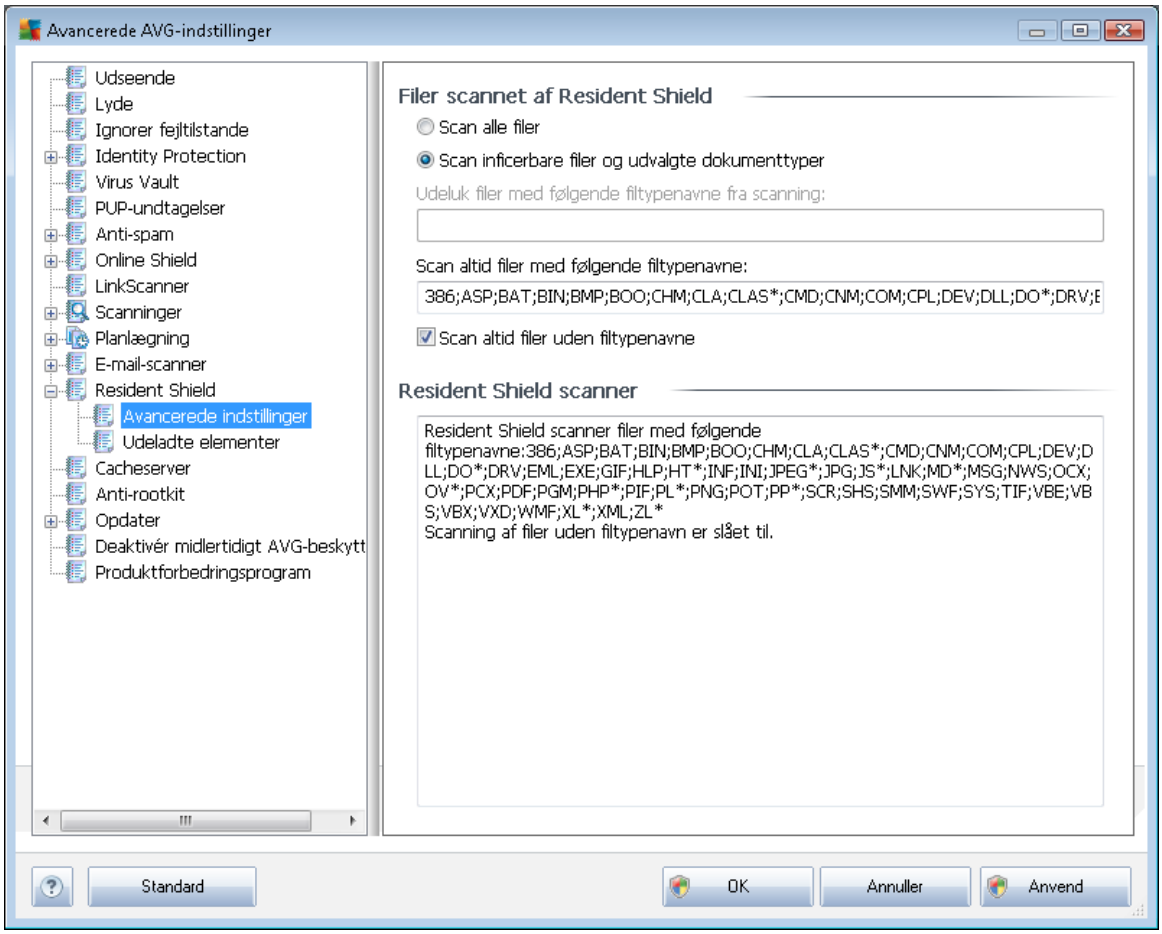
- ***Fjern alle trusler automatisk*** (*slået fra som standard*) - enhver detekteret infektion vil automatisk blive helbredt, hvis der findes en kur, og alle infektioner, som ikke kan helbredes, vil blive fjernet.

- ***Scan filer overført til register*** (*slået til som standard*) - denne parameter angiver, at AVG scanner alle eksekverbare filer, der er føjet til startgisteret for at undgå, at en kendt infektion eksekveres ved næste computeropstart.

- ***Aktivér grundig scanning*** (*slået fra som standard*) - i bestemte situationer (*i ekstreme nødstilfælde*) kan du markere denne valgmulighed for at aktivere de mest dybdegående algoritmer, som vil undersøge alle potentielt truende objekter. Husk at denne metode er ret tidskrævende.

9.13.1. Avancerede indstillinger

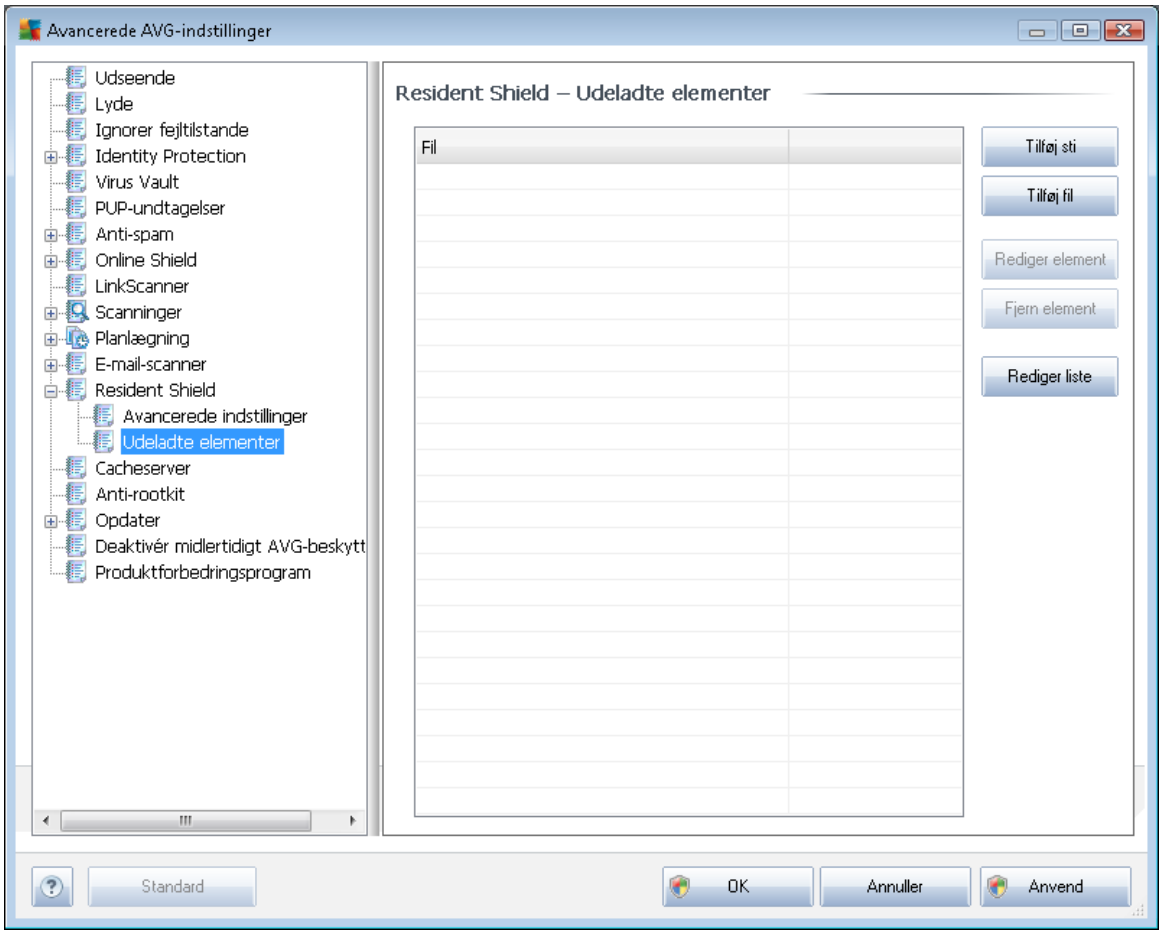
I dialogen ***Filer scannet med Resident Shield*** er det muligt at konfigurere, hvilke filer, der bliver scannet (*med specifikke filtypenavne*):



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.

Sektionen herunder, som kaldes ***Resident Shield scanner*** further sammenfatter de aktuelle indstillinger og viser en detaljeret oversigt over, hvad ***Resident Shield*** vil scanne.

9.13.2. Udeladte elementer



Dialogen ***Resident Shield - Udeladte elementer*** giver mulighed for at definere filer og/eller mapper, der skal undtages fra ***Resident Shield***-scanningen.

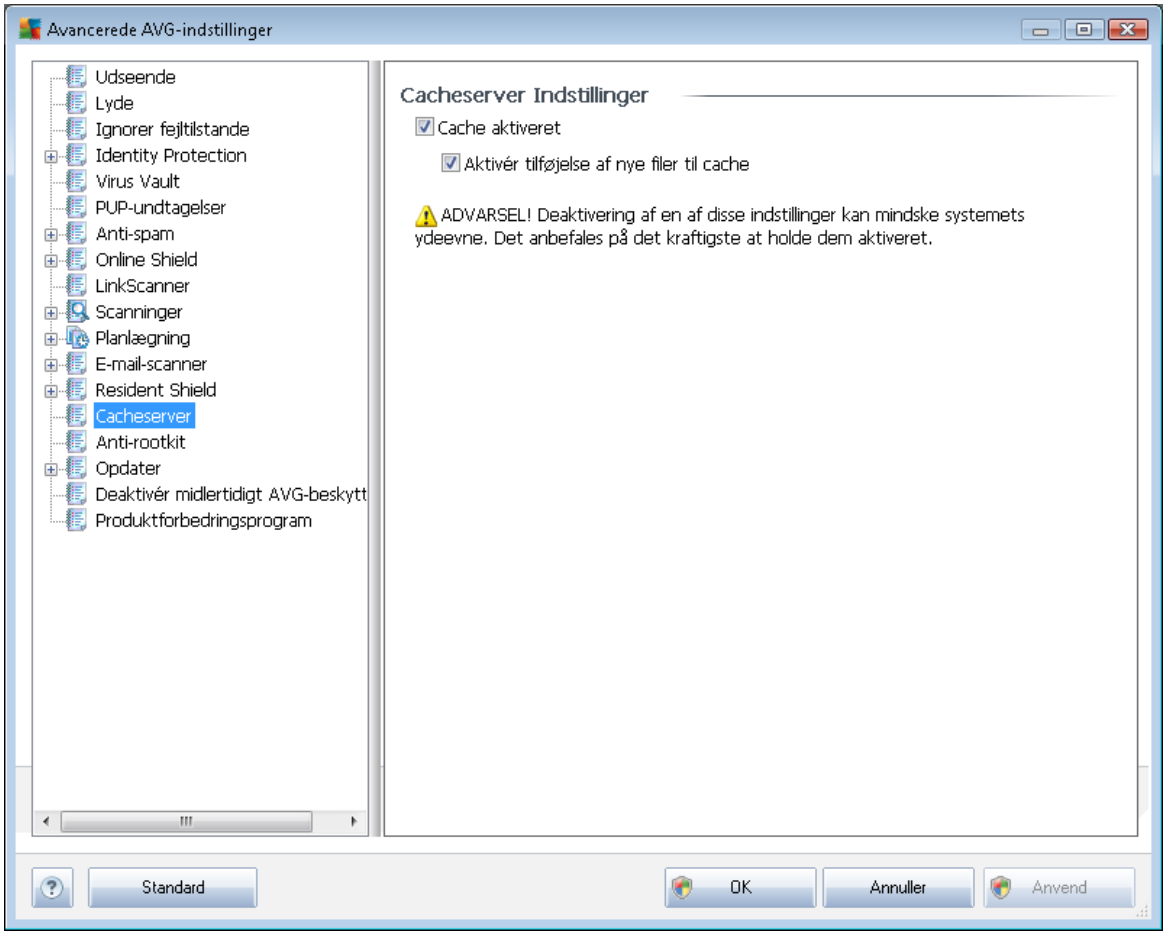
Hvis det ikke er nødvendigt, anbefales det ikke at udelukke nogen elementer!

Dialogboksen undeholder følgende betjeningsknapper:

- ***Tilføj sti*** – angiv en mappe (mapper), der skal undtages fra scanningen, ved at vælge dem én for én i navigationstræet for det lokale drev
- ***Tilføj fil*** – angiv filer, der skal udelukkes fra scanningen, ved at vælge dem én efter én i navigationstræet for det lokale drev
- ***Rediger element*** – giver mulighed for at redigere den angivne sti til en valgt fil eller mappe
- ***Fjern element*** – giver mulighed for at fjerne stien til et valgt element på listen

9.14. Cacheserver

Cacheserver er en proces, der er designet til at gøre scanninger hurtigere (*scanning af udvalgte områder, scanning af hele computeren, Resident Shield-scanning*). Den indsamler og gemmer oplysninger om pålidelige filer (*systemfiler med digital signatur, osv.*): Disse filer betragtes derefter som sikre, og springes over under scanning.



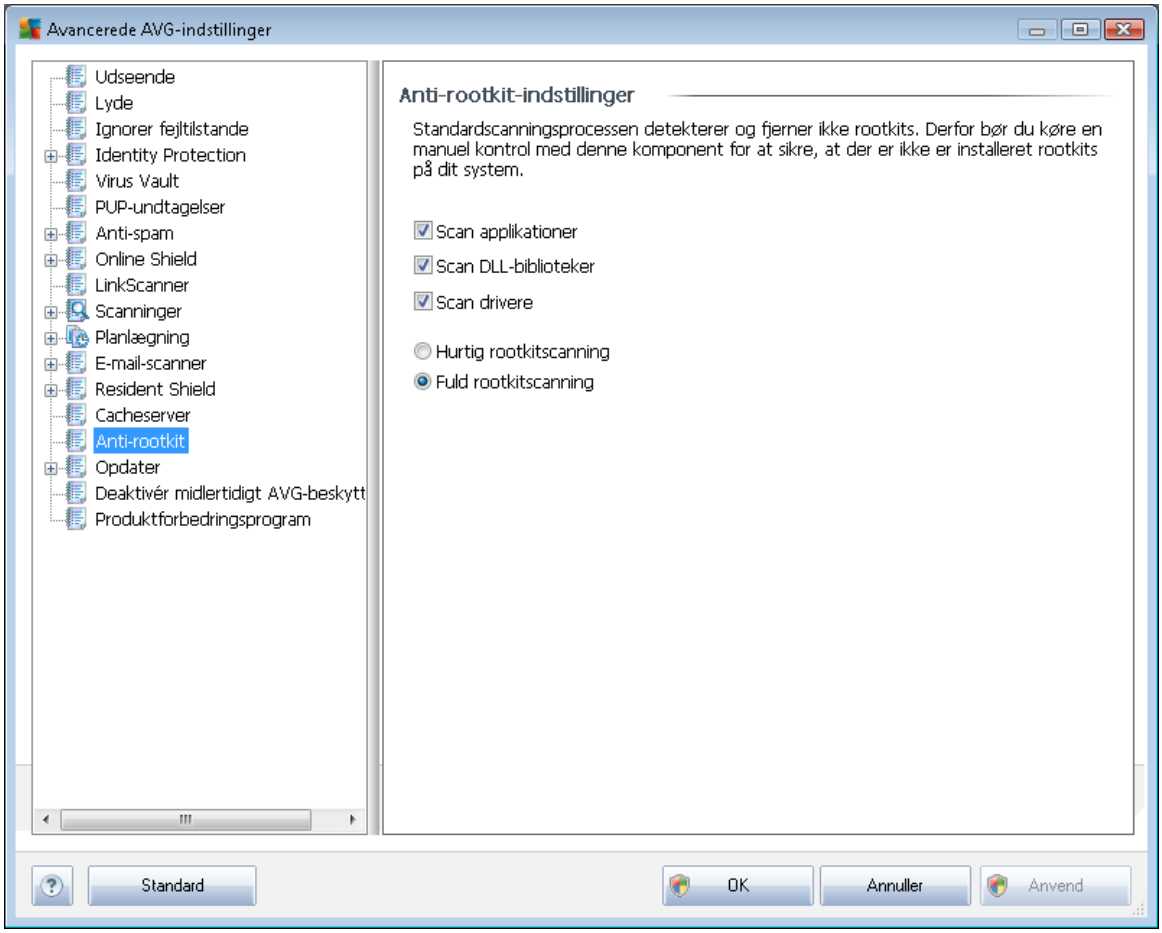
Indstillingsdialogen tilbyder to valgmuligheder:

- ***Cache aktiveret*** (*aktiveret som standard*) - markér dette felt for at slå ***cacheserver*** fra og tømme cachehukommelsen. Vær opmærksom på, at scanningen kan være langsommere, og den samlede computerydelse kan reduceres, da hver enkelt fil i brug vil blive scannet for vira og spyware først.

- ***Aktivér tilføjelse af nye filer til cache*** (*aktiveret som standard*) – fjern markeringen i dette felt for at stoppe tilføjelse af flere filer til cachehukommelsen. Filer, der allerede er gemt i cachen, vil beholdes og bruges, indtil caching slås fra helt, eller indtil næste opdatering af virusdatabasen.

9.15. 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:

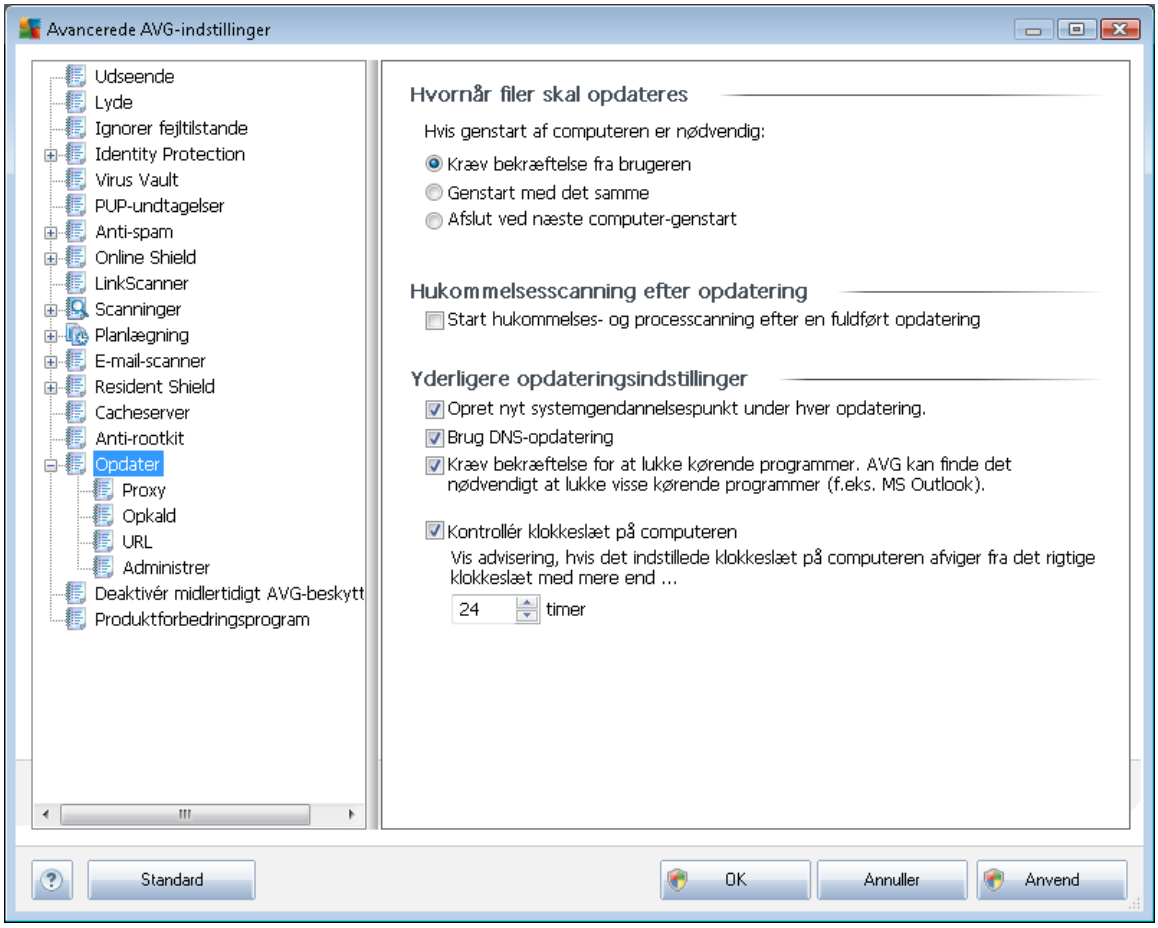
- ***Scan applikationer***
- ***Scan DLL-biblioteker***
- ***Scan drivere***

Derudover kan du vælge rootkitscanningstilstanden:

- ***Hurtig rootkitscanning*** - scanner alle igangværende processer, indlæste drivere og systemapper (*typisk c:\Windows*)
- ***Fuld rootkitscanning*** - scanner alle igangværende processer, indlæste drivere,

systemmapper (*typisk c:\Windows*), samt alle lokale drev (*inklusive flashdrev, men ikke floppydrev/CD-drev*)

9.16. 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 blandt tre alternative indstillinger, der skal bruges i tilfælde af, at opdateringsprocessen kræver genstart af computeren. Opdateringsfærdiggørelsen kan planlægges til næste computergenstart, eller du kan genstarte med det samme:

- ***Kræver bekræftelse fra brugeren*** *(som standard)* - du vil blive bedt om at acceptere den nødvendige computergenstart for at færdiggøre opdateringsprocessen
- ***Genstart med det samme*** - computeren genstartes automatisk, så snart opdateringsprocessen er færdig, og du behøver ikke at godkende det

- ***Udfør ved næste genstart af computeren***- færdiggørelsen af opdateringsprocessen vil blive udsat indtil næste computergenstart. Vær opmærksom på, at denne indstilling kun anbefales, hvis du er sikker på, at din computer genstartes regelmæssigt, mindst én gang om dagen!

Hukommelsesscanning efter opdatering

Marker dette afkrydsningsfelt for at definere, at du vil køre en ny hukommelsesscanning efter hver gennemført opdatering. Den senest downloadede opdatering kan have indeholdt nye virusdefinitioner, og de kan anvendes i scanningen med det samme.

Yderligere opdateringsindstillinger

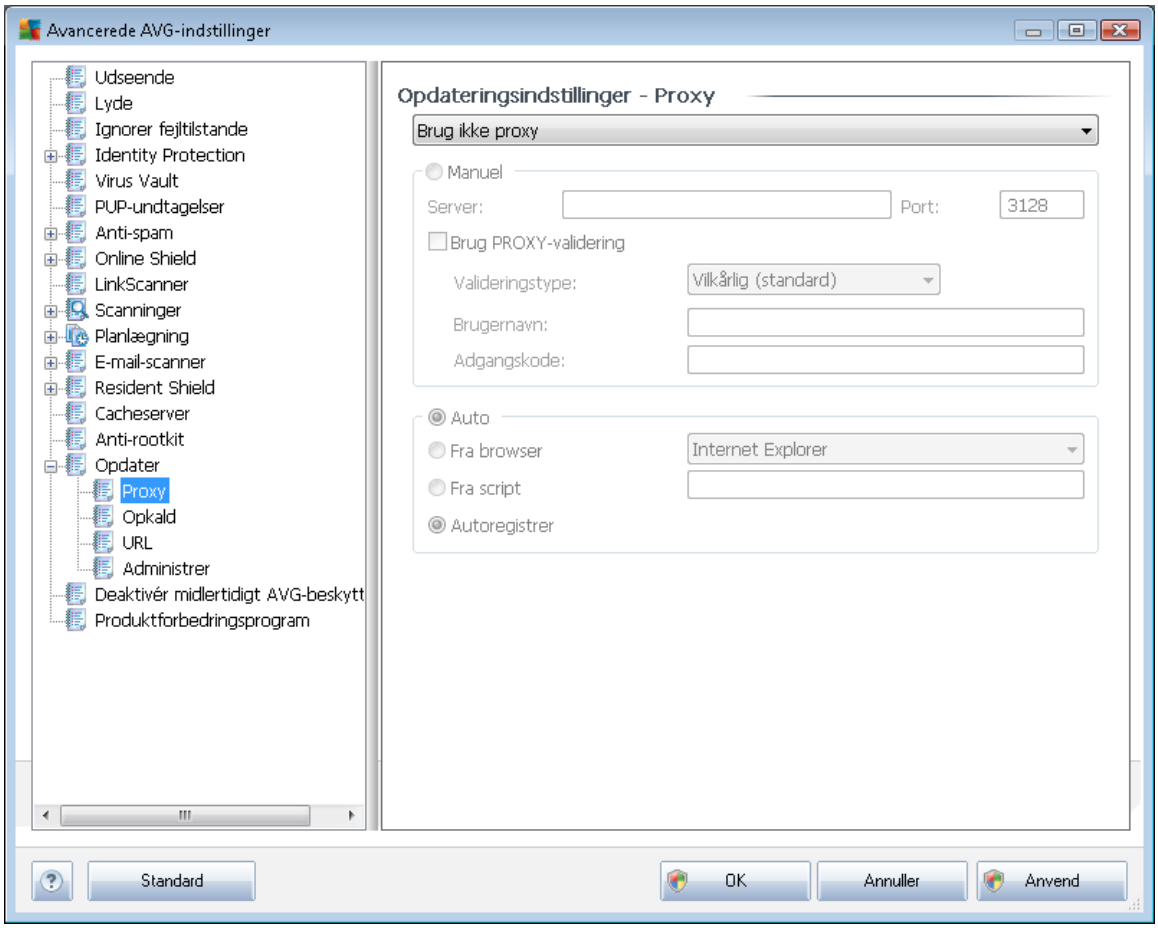
- ***Opret nyt systemgendannelsespunkt i løbet af hver programopdatering*** - før hver AVG programopdatering oprettes et systemgendannelsespunkt. I tilfælde af at opdateringsprocessen mislykkes, og dit operativsystem går ned, kan du altid gendanne dit operativsystem i dets oprindelige konfiguration fra 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*** (*slået til som standard*) - når dette element er markeret, vil din **AVG Internet-sikkerhed 2011** søge efter oplysninger om den seneste virusdatabaseversion og seneste programversion på DNS-serveren, så snart opdateringen startes. Derefter vil kun de mindste uundværlige opdateringsfiler opdateres og anvendes. På denne måde minimeres den samlede mængde downloadede data, og opdateringsprocessen kører hurtigere.

- ***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.

9.16.1. 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*** - standardindstillinger
- ***Prøv at tilslutte med proxy og tilslut direkte, hvis det mislykkes***

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*)

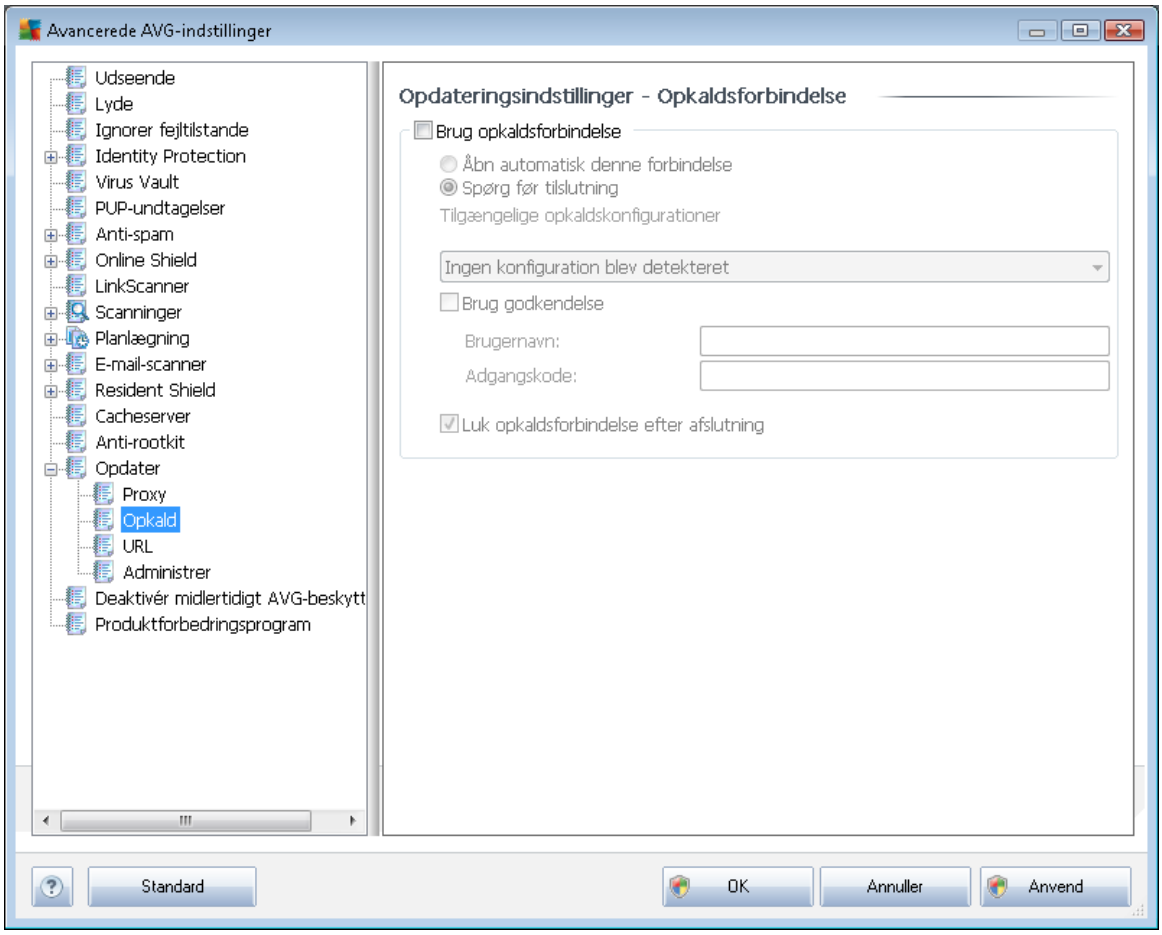
Proxyserveren kan også have specifikke regler defineret for hver bruger. Hvis din proxyserver er konfigureret på denne måde, skal du markere indstillingen ***Brug PROXY-validering*** for at verificere, at dit brugernavn og din adgangskode er gyldige til at oprette forbindelse til internettet via proxyserveren.

Automatisk konfiguration

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

- ***Fra browser*** - konfigurationen bliver læst fra din standardinternetbrowser
- ***Fra script*** - konfigurationen bliver læst fra et downloadet script, hvor funktionen returnerer proxyadressen
- ***Autodetektering*** - konfigurationen bliver detekteret automatisk, direkte fra proxyserveren

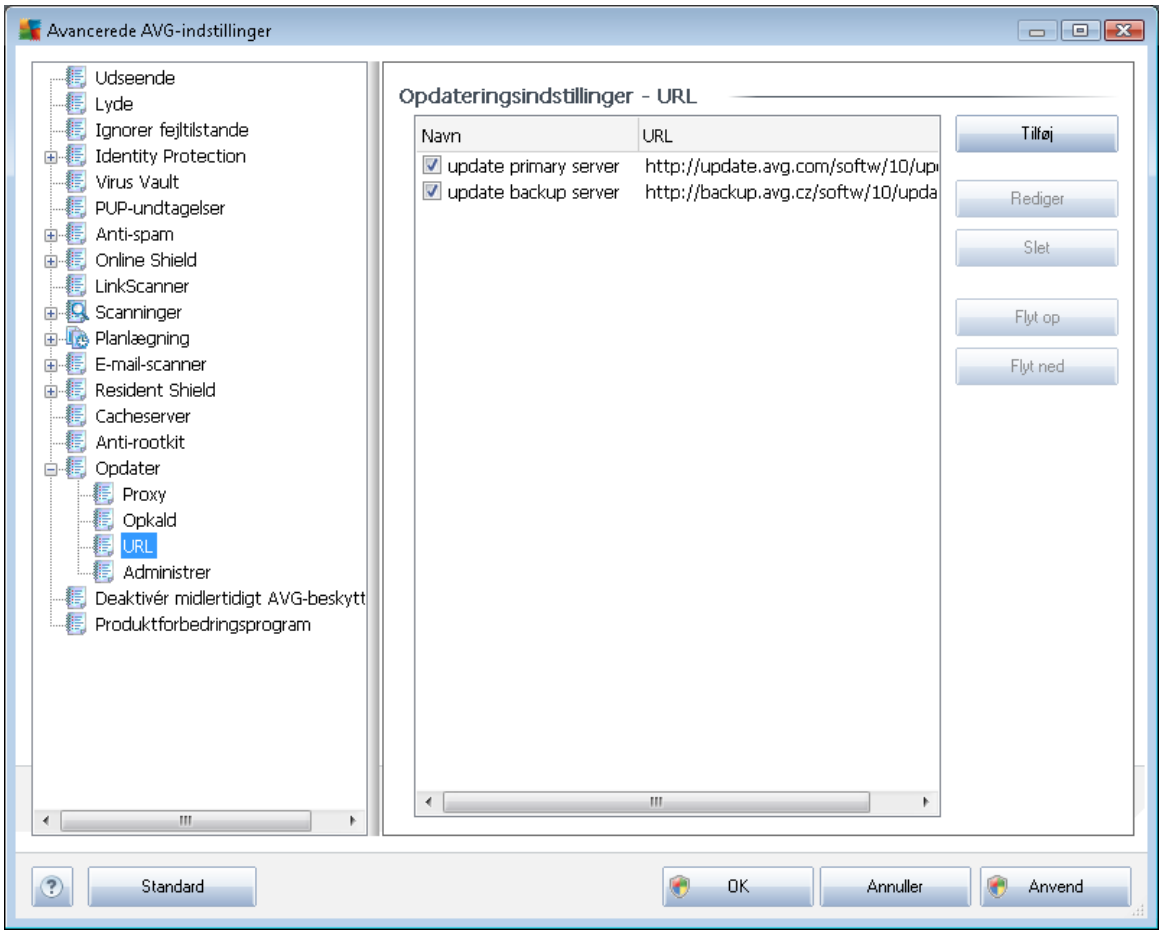
9.16.2. Opkald



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***).

9.16.3. URL

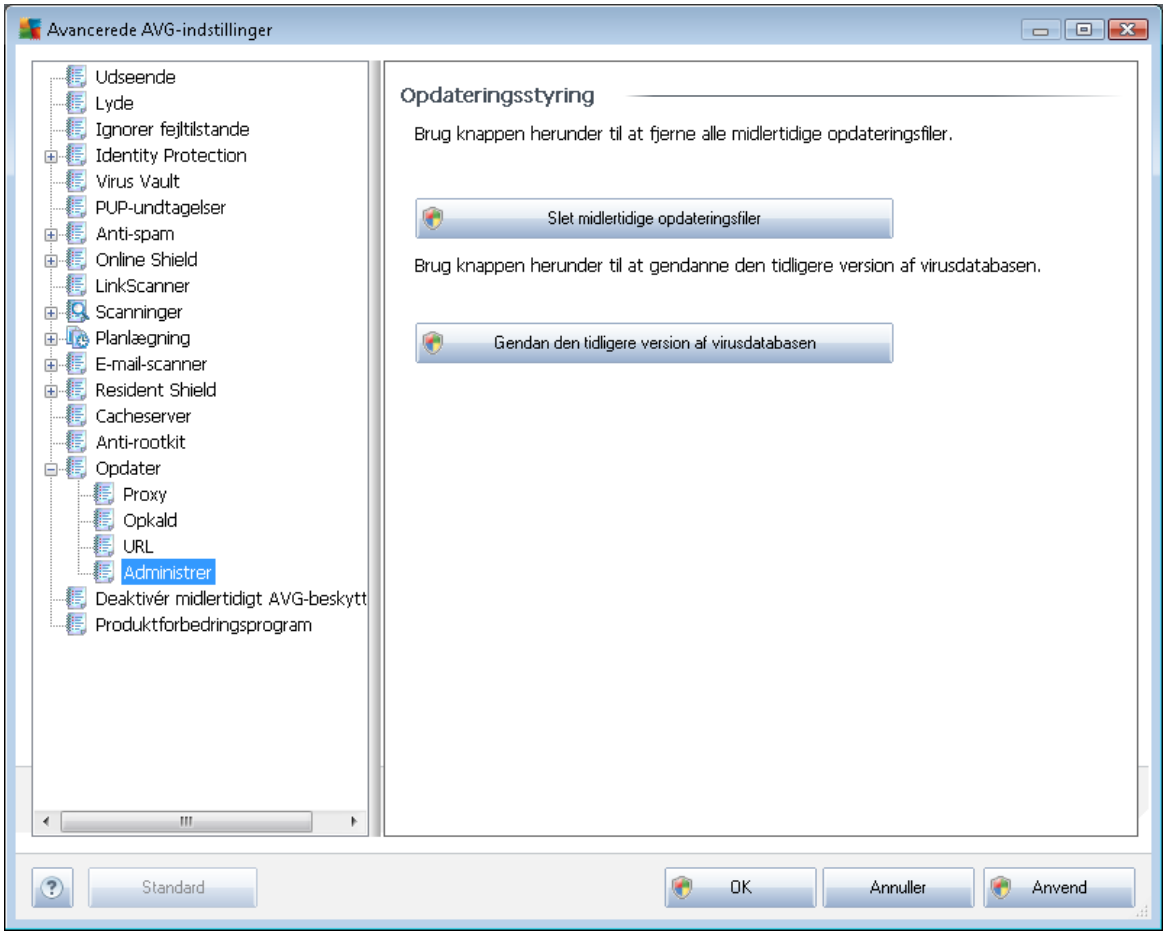


Dialogboksen ***URL*** indeholder en liste over internet-adresser, hvorfra opdateringsfilerne kan downloades. Listen og dens elementer kan ændres vha. nedenstående betjeningsknapper:

- ***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
- ***Flyt op***- flytter den valgte URL én position opad på listen
- ***Flyt ned*** - flytter den valgte URL én position nedad på listen

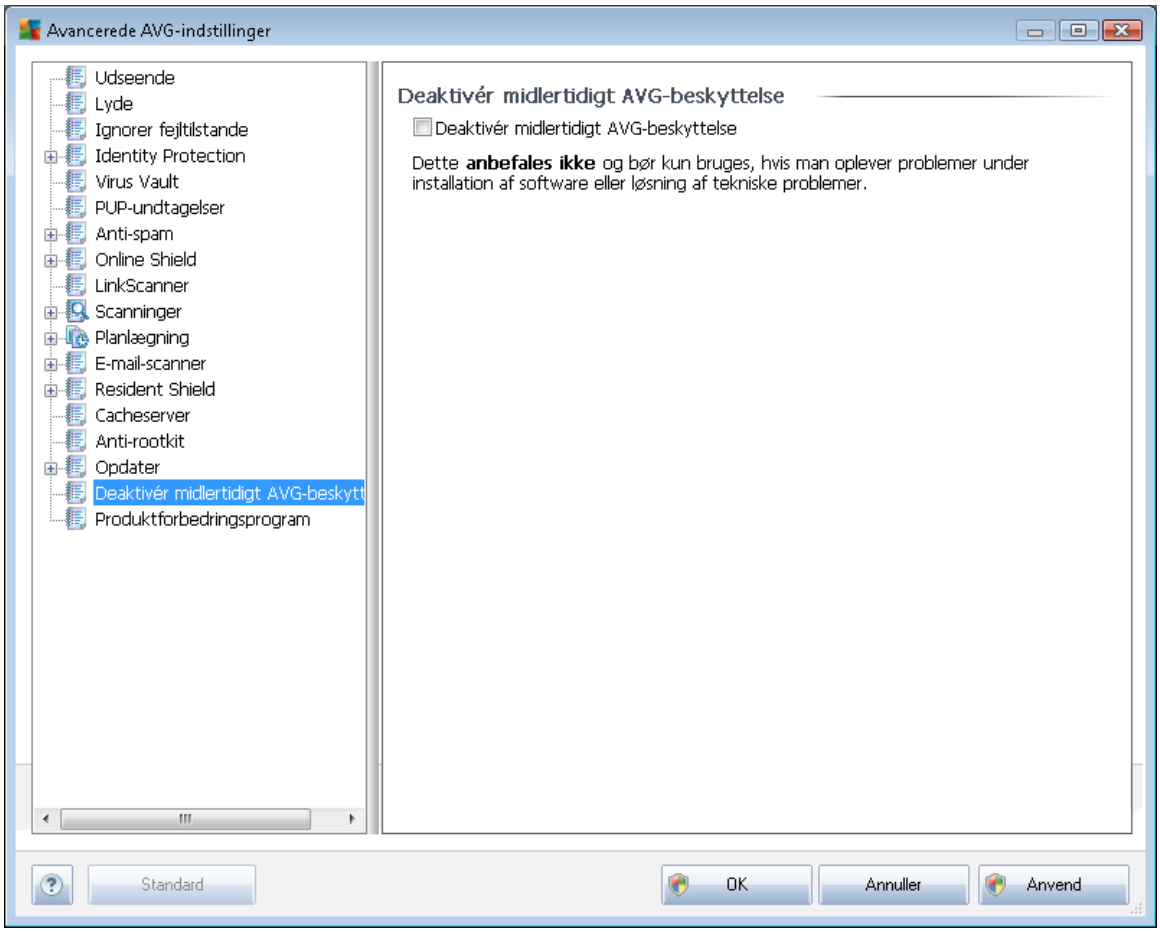
9.16.4. Administrer

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*)

9.17. Deaktivér midlertidigt AVG-beskyttelse



I dialogen ***Deaktivér midlertidigt AVG-beskyttelse*** har du mulighed for at deaktivere hele beskyttelsen fra din **AVG Internet-sikkerhed 2011** med det samme.

Husk at du kun bør bruge denne valgmulighed, når det er absolut nødvendigt!

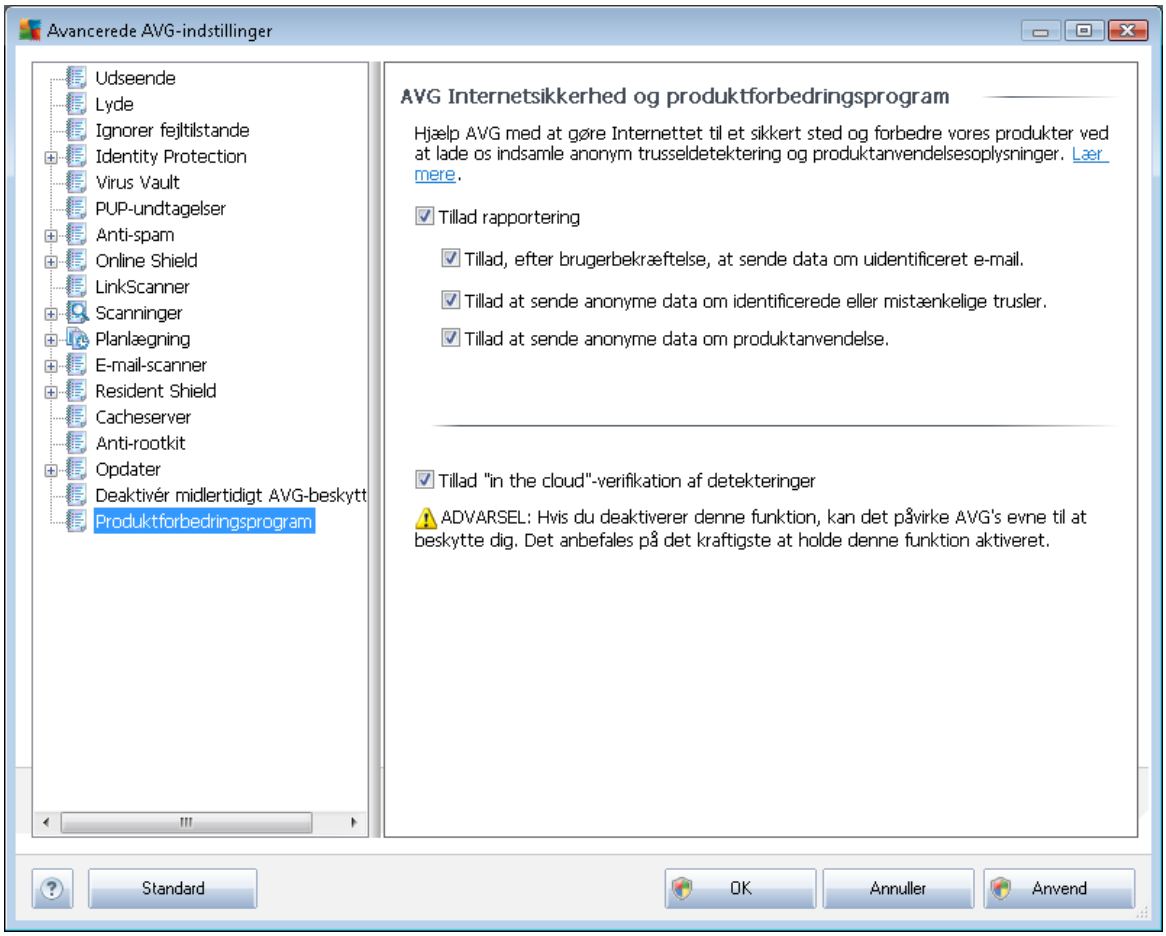
I de fleste tilfælde er det ***ikke nødvendigt*** at deaktivere AVG, inden du installerer ny software eller drivere, selv ikke hvis installationsprogrammet eller softwareguiden anbefaler, at kørende programmet og applikationer slukkes først for at sikre, at der ikke forekommer unødvendige afbrydelser under installationsprocessen. Skulle der opstå problemer under installationen, kan du forsøge først at deaktivere komponenten ***Resident Shield***. Hvis du midlertidigt har deaktiveret AVG, skal du genaktivere den, så snart du er færdig. Hvis du er tilsluttet internettet eller et netværk, mens antivirus-softwaren er deaktiveret, vil din computer være i fare for angreb.

9.18. Produktforbedringsprogram

Dialogen ***AVG Internet-sikkerhed og produktforbedringsprogram*** inviterer dig til at deltage i AVG's produktforbedring, og til at hjælpe os med at øge det overordnede Internet-sikkerhedsniveau. Markér valgmuligheden ***Tillad rapportering*** for at aktivere rapportering af detekterede trusler til AVG. Det hjælper os med at indsamle aktuelle oplysninger om de seneste trusler fra alle deltagere

over hele verden, og til gengæld kan vi forbedre onlinebeskyttelsen for alle.

Rapporteringen håndteres automatisk, og er ikke til gene for dig, og der medtages ikke personlige data i rapporterne. Rapportering af detekterede trusler er valgfrit, men vi beder dig dog slå denne funktion til for at hjælpe os med at forbedre beskyttelse for både dig og andre AVG brugere.



I dag er der langt flere trusler derude end almindelige vira. Forfattere af ondsindede koder og farlige websteder er meget opfindsomme, og der opstår ret ofte nye former for trusler, hvoraf det overvejende flertal er på internettet. Her er nogle af de mest almindelige:

- ***En virus er en ondsindet kode, der kopierer og spreder sig selv, ofte ubemærket indtil skaden er sket.*** Nogle vira er alvorlige trusler, der sletter eller med vilje ændrer filer, hvor de kommer frem, hvorimod nogle vira kan gøre noget tilsyneladende harmløst som f. eks. at afspille et stykke musik. Alle vira er imidlertid farlige på grund af den grundlæggende evne til at formere sig - selv en simpel virus kan optage hele computerens hukommelse på et øjeblik og medføre et nedbrud.

- ***En orm*** er en underkategori til virus, der i modsætning til virus ikke behøver et "bærerobjekt" at vedhæfte sig til. Den sender sig selv til andre computere, normalt via e-mail, og overbelaster derfor ofte mailservere og netværkssystemer.

- ***Spyware*** defineres almindeligvis som en kategori af malware (*malware = enhver form for ondsindet software, herunder vira*) der omfatter programmer - typisk trojanske heste - målrettet mod at stjæle personlige oplysninger, adgangskoder kreditkortnumre eller infiltrere en computer så angrigeren kan kontrollere den eksternt. Naturligvis uden computerejerens viden eller tilladelse.

- ***Potentielt uønskede programmer*** er en type spyware, der kan være, men ikke nødvendigvis er farlig for din computer. En specifik form for PUP er adware, software designet til at distribuere reklamer, normalt ved at vise popup-reklamer. Irriterende, men ikke decideret skadeligt.

- ***Sporings-cookies*** kan betragtes som en form for spyware, da disse små filer, der gemmes i webbrowseren og automatisk sendes til "forældre"-webstedet, når du besøger det igen, kan indeholde data som f.eks. din browserhistorik og lignende oplysninger.

- ***Exploit*** er en ondsindet kode, der udnytter en fejl eller sårbarhed i et operativsystem, internetbrowser eller et andet vigtigt program.

- ***Phishing*** er et forsøg på at få adgang til følsomme personlige data ved at udgive sig for en troværdig og velkendt organisation. Almindeligvis bliver de potentielle ofre kontaktet med en masseudsendt e-mail, der beder dem om f.eks. at opdatere deres bankoplysninger. For at kunne gøre det inviteres de til at følge det oplyste link, som fører til et falsk bankwebsted.

- ***Hoax*** er en masseudsendt e-mail, der indeholder farlige, alarmerende eller blot irriterende og ubrugelige oplysninger. Mange af de ovenstående trusler bruger hoax-e-mail til at spredes.

- ***Ondsindede websteder*** er websteder, som bevidst installerer ondsindet software på din computer, og hackede websteder, der gør det samme, disse er blot legitime websteder, der er kompromitterede til at inficere besøgende.

For at beskytte dig mod alle disse forskellige trusler inkluderer AVG disse specialiserede komponenter:

- ***Anti-virus*** for at beskytte din computer mod vira,

- ***Anti-spyware*** for at beskytte din computer mod spyware,

- ***Online Shield*** for at beskytte dig mod både vira og spyware, når du surfer på internettet,

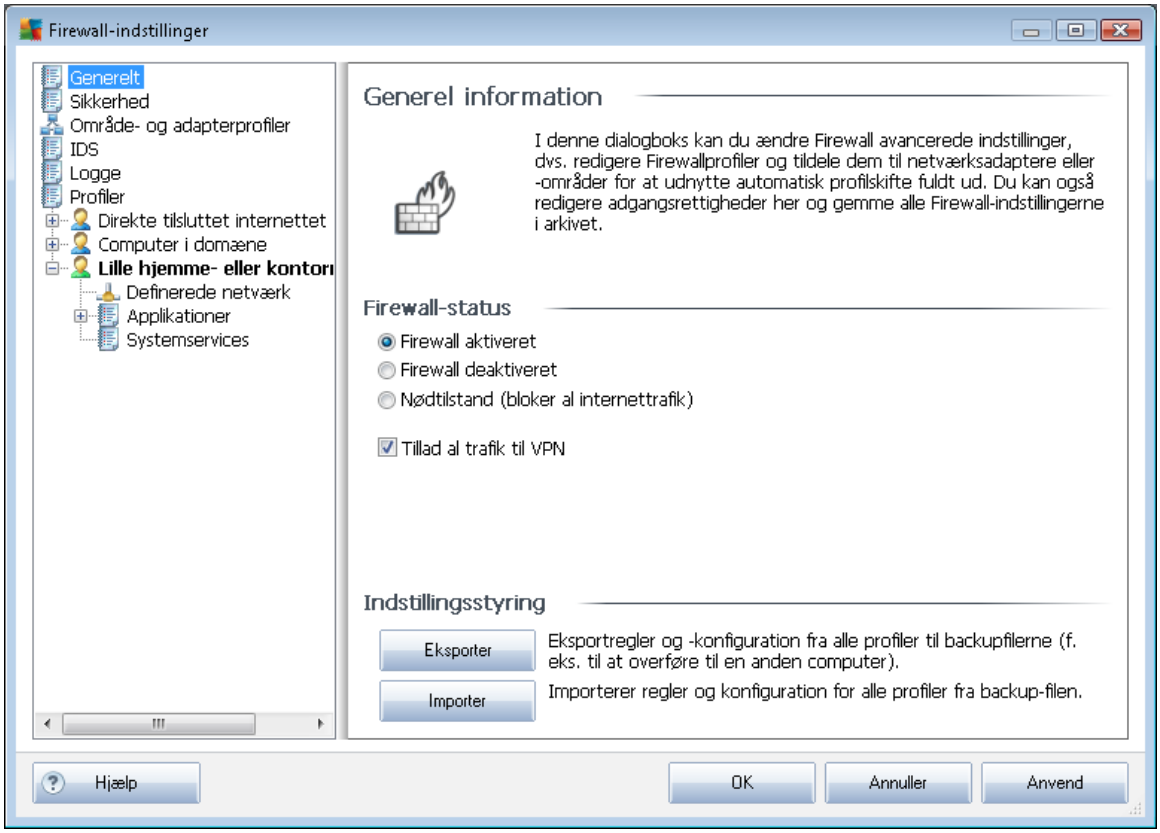
- ***LinkScanner*** for at beskytte dig mod andre online trusler, der er nævnt i dette kapitel.

10. 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 imidlertid kun beregnet til eksperter og erfarne brugere.***

10.1. Generelt

Dialogen ***Generelle oplysninger*** er opdelt i to sektioner:



Firewallstatus

I sektionen ***Firewall-status*** kan du skifte *Firewall*-status, når der er behov for det:

- ***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

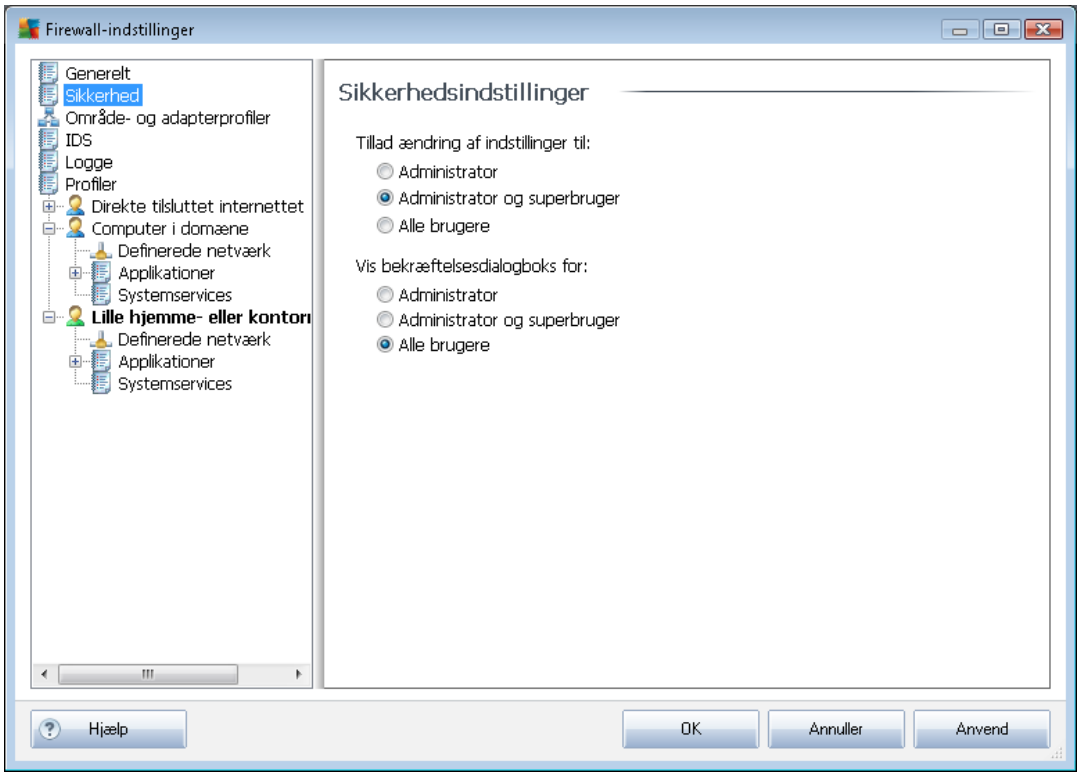
- ***Tillad al trafik til VPN*** – hvis du bruger en VPN-forbindelse *(Virtual Private Network)*, f.eks. til at oprette forbindelse til kontoret hjemmefra, anbefaler vi at markere dette felt. ***AVG Firewall*** vil automatisk søge gennem dine netværksadaptere, finde de der bruges til VPN-forbindelsen, og tillade alle programmer at oprette forbindelse til målnetværket *(gælder kun programmer, der ikke har fået tildelt en specifik Firewall-regel)*. På et standardsystem med fælles netværksadaptere, vil dette enkle trin spare dig for at skulle opsætte en detaljeret regel for hvert program, som skal bruges over VPN.

Bemærk: *For overhovedet at tillade VPN-forbindelse, er det nødvendigt at tillade kommunikation til følgende systemprotokoller: GRE, ESP, L2TP, PPTP. Dette kan gøres i dialogen Systemtjenester.*

Indstillingsstyring

I afsnittet ***Indstillingsadministration*** kan du ***Eksportere/Importere*** ***Firewall***-konfiguration, dvs. eksportere de definerede ***Firewall***-regler og -indstillinger til backup-filer eller importere hele backup-filen.

10.2. 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

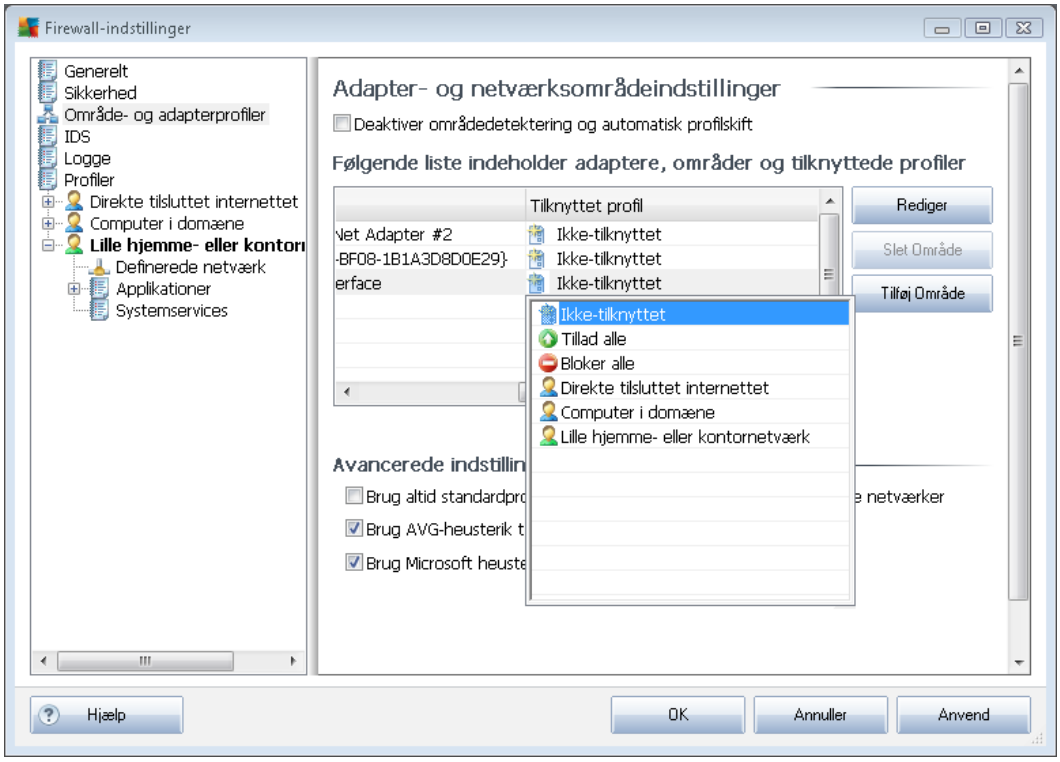
- ***Vis bekræftelsesdialog for*** - angiv hvem der skal have vist bekræftelsesdialoger (*dialoger der beder om en beslutning i situationer, der ikke er dækket af en defineret* ***Firewall****-regel*).

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

10.3. 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 fælles profil. 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 kan du tildele en specifik profil fra menuen med definerede profiler. Klik på det pågældende element i listen over adaptere, og vælg profilen for at åbne denne menu.

Avancerede indstillinger

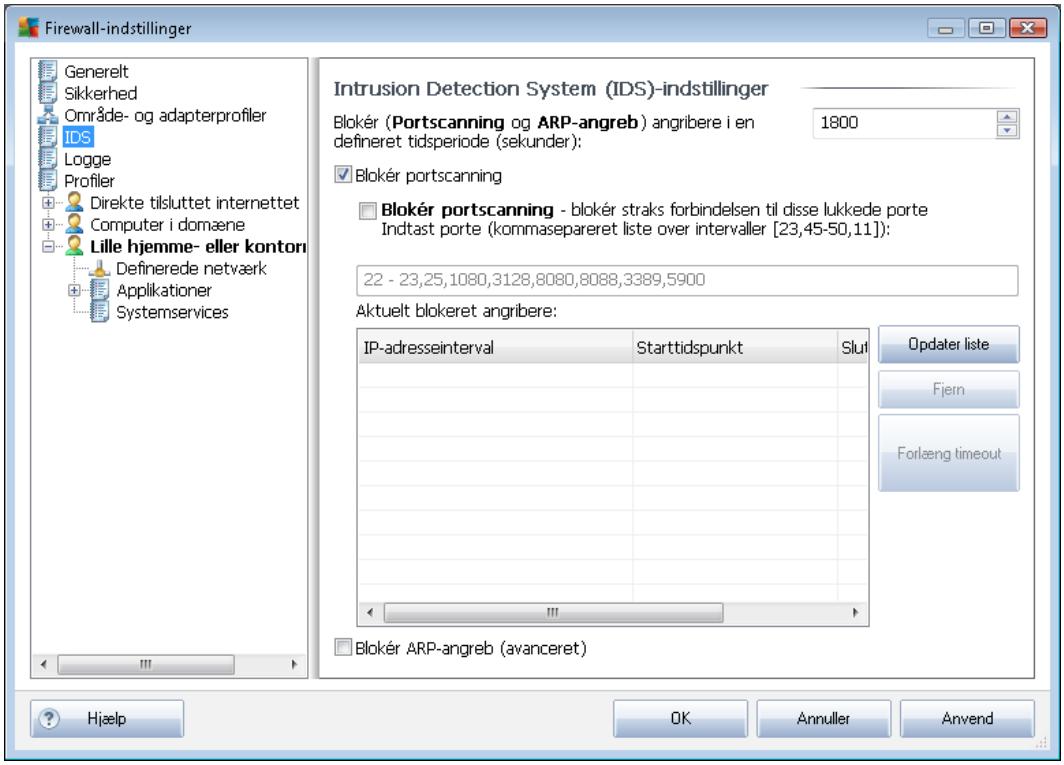
- ***Brug altid standardprofilen og vis ikke dialogen for ny netværksdetektering***- når din computer opretter forbindelse til et nyt netværk, vil ***Firewall*** advare dig og vise en dialog, der beder dig vælge en netværksforbindelsestype, og tildele den en ***Firewall-profil***. Hvis du ikke vil have denne dialog vist, skal du markere dette felt.

- ***Brug AVG heuristik til ny netværksdetektion*** - dig hente oplysninger om et nyligt detekteret netværk fra AVG's egen mekanisme (*denne valgmulighed er dog kun tilgængelig på VISTA OS, og højere*).

- ***Brug Microsoft heuristik til at detektere nye netværker*** - lader dig hente oplysninger om et nyligt detekteret netværk fra Windows-tjenesten (*denne valgmulighed er kun tilgængelig på Windows Vista og højere*).

10.4. IDS

Intrusion Detection System er en speciel adfærdsanalysefunktion, der er designet til at identificere og blokere mistænkelige kommunikationsforsøg over specifikke porte på computeren. Du kan konfigurere IDS-parametrene i følgende grænseflade:



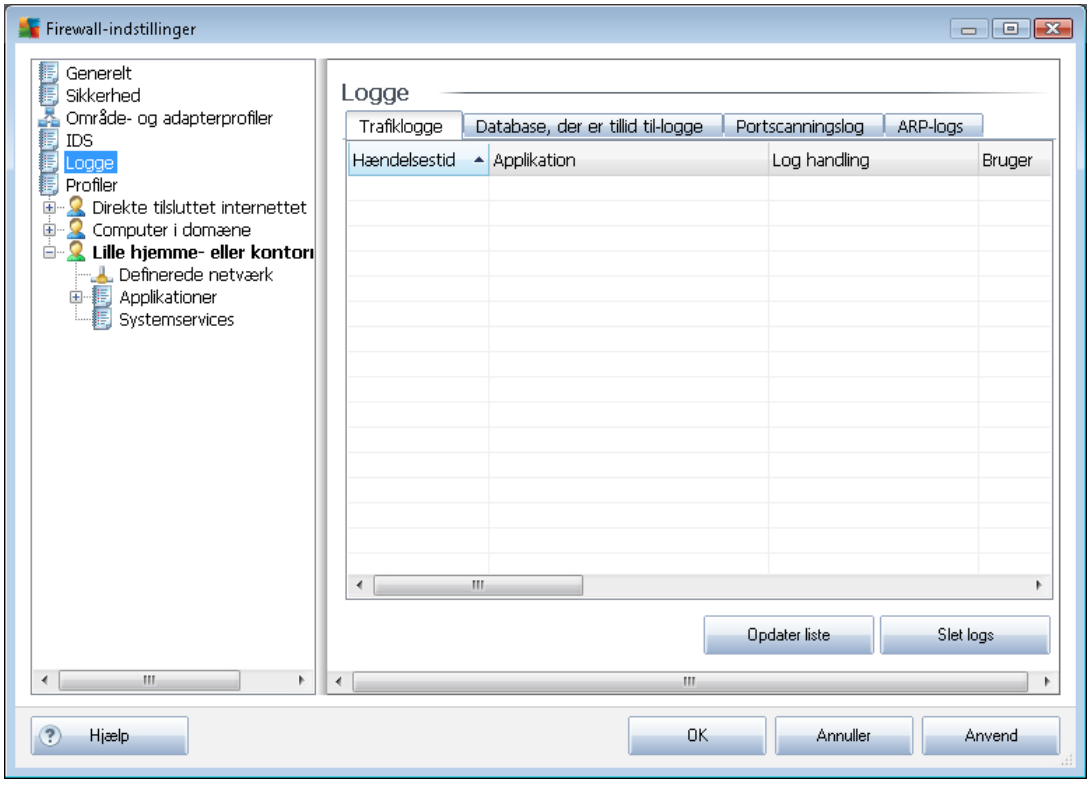
Dialogen ***Intrusion Detection System (IDS)-indstillinger*** indeholder disse konfigurationsindstillinger:

- ***Blokér angribere i en bestemt tidsperiode*** - kan du angive antallet af sekunder, en port skal være blokeret, når der detekteres et mistænkeligt kommunikationsforsøg på porten. Som standard er tidsintervallet indstillet til 1800 sekunder (*30 minutter*).
- ***Blokér portscanning*** – markér feltet for at blokere kommunikationsforsøg over alle TCP- og UDP-porte, der kommer til computeren udefra. For sådanne forbindelser tillades fem forsøg, og det sjette blokeres.
    - ***Sort portscanning*** – markér feltet for straks at blokere alle kommunikationsforsøg over porte, der er angivet i tekstfeltet herunder. Individuelle porte eller portintervaller skal adskilles med komma. Der findes en foruddefineret liste med anbefalede porte, hvis du ønsker at gøre brug af denne funktion.
    - ***Aktuelt blokerede angribere*** - dette afsnit viser eventuelle kommunikationsforsøg, der aktuelt blokeres af din ***Firewall***. En komplet historik over blokerede forsøg kan ses i dialogen ***Logge*** (*fanen Portscanningslog*).
- ***Blokér ARP-forsøg*** aktiverer blokering af specielle former for kommunikationsforsøg i et lokalt netværk, der detekteres af ***IDS*** som potentielt farlig. Den indstillede tid i ***Blokér angribere i en bestemt tidsperiode anvendes.*** Vi anbefaler, at det kun er erfarne brugere, der er fortrolige med typen og risikoniveauet for deres lokale netværk, der bruger denne funktion.

Betjeningsknapper

- ***Opdatér liste*** - tryk på knappen for at opdatere listen (*for at inkludere de nyeste blokerede forsøg*)
- ***Fjern*** - tryk for at annullere en valgt blokering
- ***Forlæng timeout*** - tryk for at forlænge tidsperioden for blokering af et valgt forsøg. En ny dialog med udvidede valgmuligheder vises, og du kan indstille et specifikt tidspunkt og dato, eller ubegrænset varighed.

10.5. Logge



I dialogen ***Logge*** kan du gennemse listen over alle loggede ***Firewall***-handlinger og hændelser med en detaljeret beskrivelse af relevante parametre (*hændelsestid, applikationsnavn, pågældende loghandling, brugernavn, PID, trafikretning, protokoltype, numre på eksterne og lokale porte osv.*) på fire faner:

- ***Trafiklogge*** - indeholder oplysninger om aktivitet i alle applikationer, der har forsøgt at oprette forbindelse til netværket.
- ***Pållidelig database-logge*** - *Pålidelig database* er AVG's interne database, som indsamler oplysninger om certificerede og pålidelige applikationer, som altid kan få tilladelse til at kommunikere online. Første gang en ny applikation forsøger at oprette forbindelse til

netværket (*dvs. hvis der endnu ikke er angivet en firewall-regel for applikationen*), er det nødvendigt at finde ud af, om netværksforbindelsen skal tillades på den pågældende applikation. Først søger AVG i *Pålidelig database*, og hvis applikationen er anført, bliver den automatisk tildelt adgang til netværket. Først derefter, hvis der ikke er tilgængelige oplysninger om applikationen i databasen, bliver du i en enkeltstående dialog spurgt, om du vil give applikationen adgang til netværket.

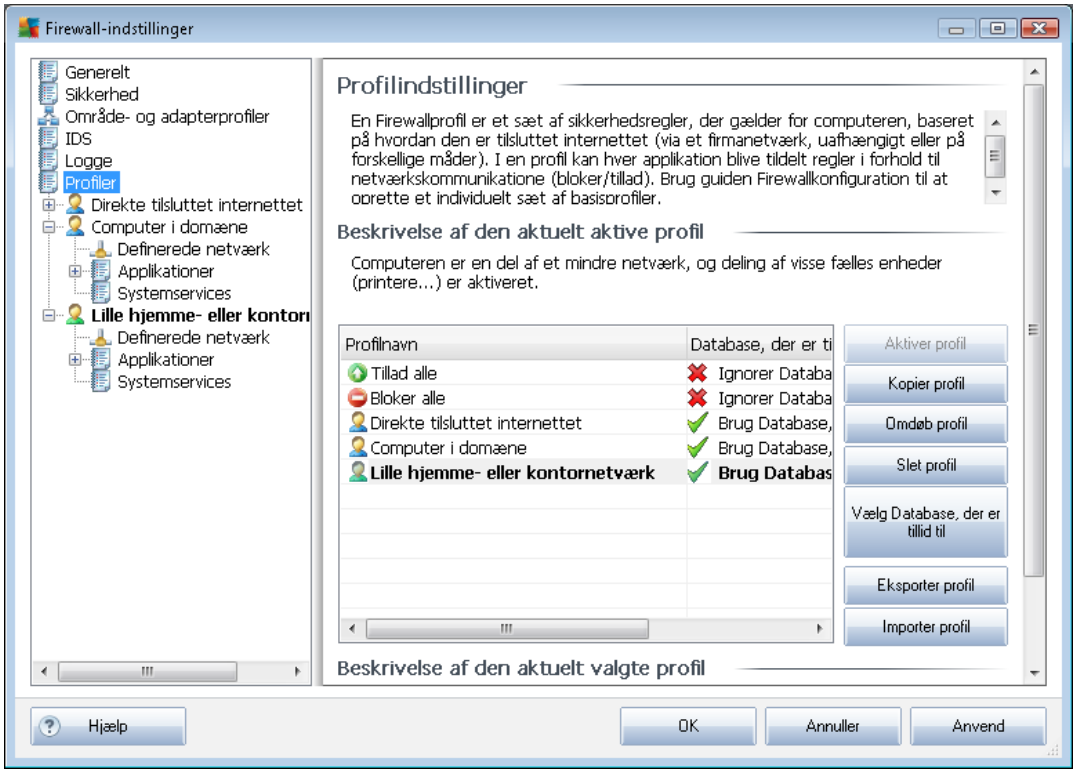
- ***Portscanningslog*** - tilbyder logging af al ***Intrusion Detection System***-aktivitet.
- ***ARP-logge*** - logger oplysninger om blokering af specielle former for kommunikationsforsøg i et lokalt netværk (valgmuligheden *Blokér ARP-forsøg*), der detekteres af ***Intrusion Detection System*** som potentielt farlig.

Betjeningsknapper

- ***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 liste*** - slet alle poster i tabellen.

10.6. 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
- ***Vælg Pålidelig database*** - for den valgte profil kan du beslutte at bruge oplysninger fra *Pålidelig database* (*(Pålidelig database er AVG's interne database, som indsamler data om certificerede og pålidelige applikationer, som altid kan få tilladelse til at kommunikere online.*)
- ***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

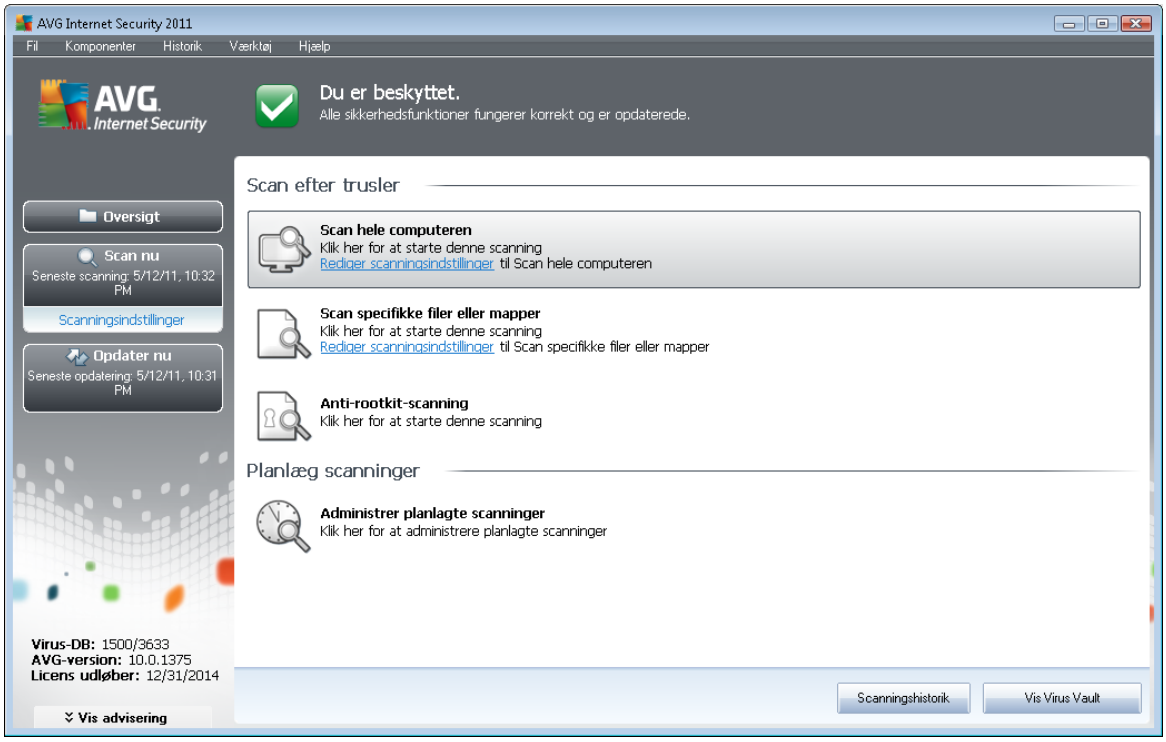
I dialogens nederste sektion findes beskrivelsen af den profil, der aktuelt er valgt i ovenstående liste.

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*):

11. AVG Scanning

Scanning er en vigtig del af funktionen **AVG Internet-sikkerhed 2011**. Du kan køre on-demand tests eller planlægge dem til periodisk kørsel, når det er bekvemt for dig.

11.1. Scanning-grænseflade



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

- oversigt over foruddefinerede scanninger - tre scanningstyper (defineret af softwareleverandøren) er klar til omgående brug efter behov eller planlagt.
    - ***Scanning af hele computeren***
    - ***Scan specifikke filer eller mapper***
    - ***Anti-rootkit-scanning***
- 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

11.2. Foruddefinerede scanninger

En af hovedfunktionerne i **AVG Internet-sikkerhed 2011** er scanning af udvalgte områder. 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.

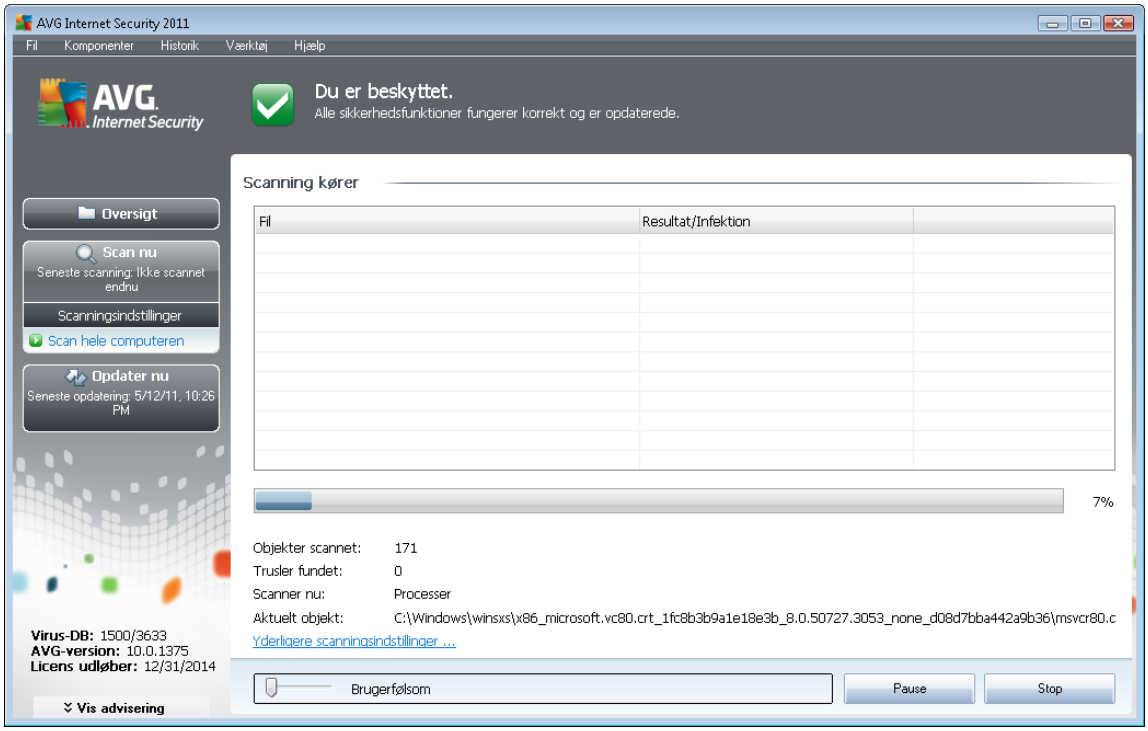
I **AVG Internet-sikkerhed 2011** vil du finde følgende typer scanning, der er foruddefineret af softwareleverandøren:

11.2.1. Scanning af hele computeren

Scanning af 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.

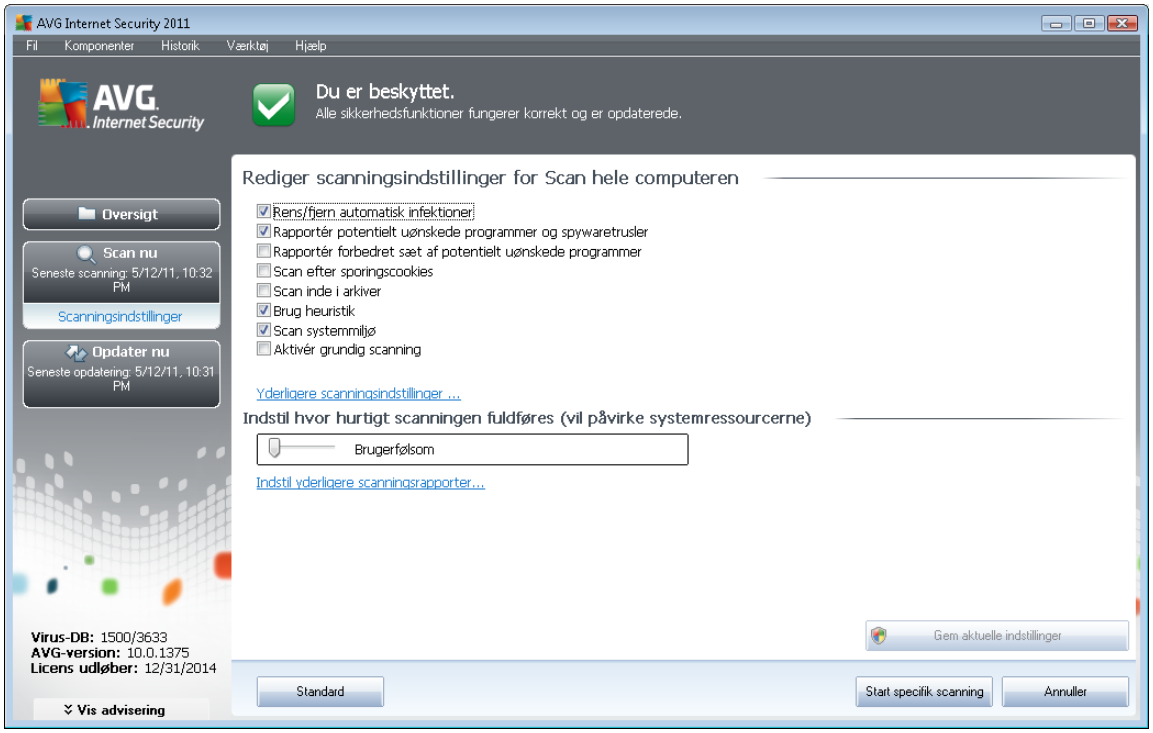
Scanningskørsel

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 (***Stop***) 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 tildialogen ***Rediger scanningsindstillinger for Scan hele computeren*** *(tilgængelig fra scanningsgrænsefladen via linket Rediger scanningsindstillinger for Scanning af hele computeren)*. ***Det anbefales at bevare standardindstillingerne, med mindre du har en god grund til at ændre dem!***



- ***Scanningsparametre*** - i listen over scanningsparametre kan du slå specifikke parametre til/fra efter behov:

  - ***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, vil det inficerede objekt flyttes til ***Virus Vault***.

  - ***Rapporter potentielt uønskede programmer og spywaretrusler*** (*aktiveret som standard*) - markér for at aktivere programmet ***Anti-spyware*** og scanne efter spyware og efter vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.

  - ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*) - markér for at detektere udvidede pakker af spyware: programmer, der er fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.

  - ***Scan efter sporingscookies*** (*slået fra 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*).

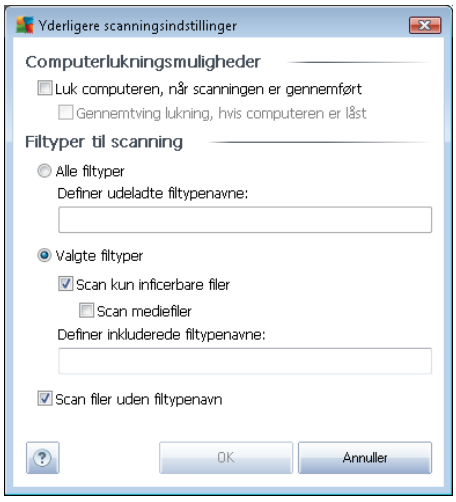
- **Scan inde i arkiver** (*slået fra som standard*) - disse parametre definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i arkiver, f.eks. ZIP, RAR, ...

- **Brug heuristik** (*slået til som standard*) - Heuristisk analyse (*dynamisk emulering af det scannede objektsinstruktioner 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.

- **Aktivér grundig scanning** (*slået fra som standard*) - i særlige situationer (*hvor der er mistanke om, at computeren er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som egentlig ikke kan blive inficeret, men bare for at være sikker. Husk at denne metode er ret tidskrævende.

- ***Yderligere scanningsindstillinger*** - linket åbner en ny ***Yderligere scanningsindstillinger*** -dialog, hvor du kan specificere følgende parametre:



  - **Computerlukningsmuligheder** - beslut, om computeren skal lukkes automatisk, når den igangværende scanningsproces er slut. 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***).

  - **Definer filtyper til scanning** - derudover skal du beslutte, om du vil have scannet:

    - ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en kommasepareret liste over filtypenavne, som ikke skal scannes;

    - ***Udvalgte filtyper*** - du kan angive, at du kun vil scanne filer, som er mulige at inficere (*filer som ikke kan blive inficeret, bliver ikke scannet, for eksempel visse almindelige tekstfiler, eller andre ikke eksekverbare filer*), herunder mediefiler (*video- og lydfiler - hvis du lader dette felt stå tomt, reducerer det*

scanningen yderligere, fordi disse filer ofte er ret store, og det ikke er særlig sandsynligt, at de er inficerede med virus). Igen kan du angive, hvilke filer, der altid skal scannes, ud fra filtypenavnene.

- Du kan også vælge at ***Scanne filer uden filtypenavn*** - denne indstilling er slået til som standard, og det anbefales, at du bevarer den sådan, medmindre du har en virkelig god grund til at ændre den. Filer uden filtypenavn er ret mistænkelige og bør altid scannes.

- ***Indstil hvor hurtigt scanningen fuldføres*** - du kan bruge skyderen til at ændre scanningsprioriteten. Som standard er denne indstillingsværdi sat til *brugerfølsomt niveau af automatisk ressourceforbrug.* Alternativt 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***-dialog, hvor du kan vælge, hvilke typer af mulige fund, der skal rapporteres:

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.*

11.2.2. Scan specifikke filer eller mapper

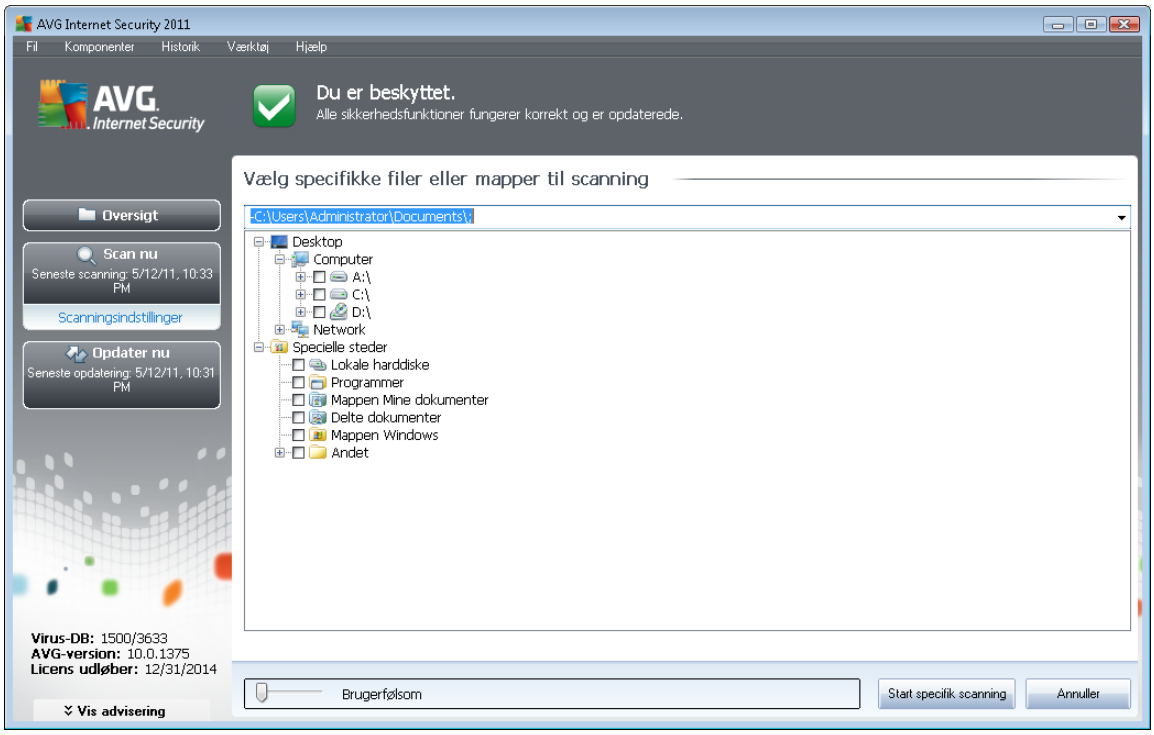
Scan specifikke filer eller mapper - scanner kun de områder af computeren, som du har valgt skal scannes (*valgte mapper, harddiske, disketter, cd'er osv.*). Scanningens forløb i tilfælde af detektering af virus og behandlingen af denne er den samme som ved scanning af hele computeren: fundne virus helbredes 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.

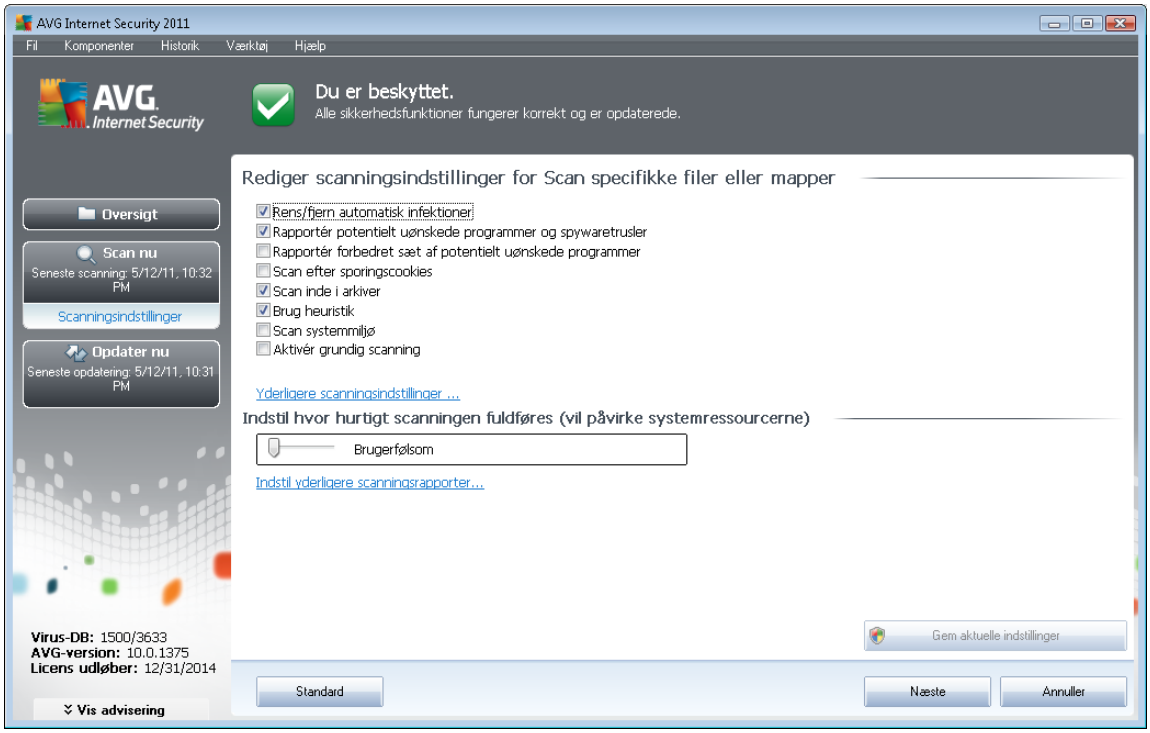
Det er også muligt at få scannet en specifik mappe, mens alle dens undermapper er undtaget fra denne scanning. Det gør du ved at skrive et minustegn "**-**" foran den automatisk genererede sti (*se skærmbillede*). Brug parameteren "!" for at undtage hele mappen fra scanning.

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, med mindre du har en god grund til at ændre dem!***



- ***Scanningsparametre*** - i listen over scanningsparametre kan du slå specifikke parametre til/fra efter behov:

  - ***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, vil det inficerede objekt flyttes til ***Virus Vault***.

  - ***Rapporter potentielt uønskede programmer og spywaretrusler*** (*aktiveret som standard*) - markér for at aktivere programmet ***Anti-spyware*** og scanne efter spyware og efter vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.

  - ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*) - markér for at detektere udvidede pakker af spyware: programmer, der er fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.

  - ***Scan efter sporingscookies*** (*slået fra 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*).

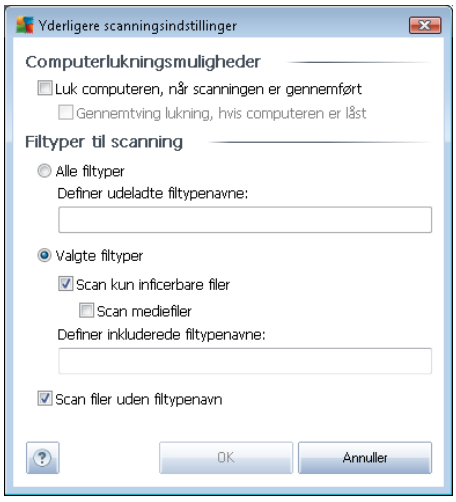
- **Scan inde i arkiver** (*slået til som standard*) - disse parametre definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i arkiver, f.eks. ZIP, RAR, ...

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

- **Scan systemmiljø** (*slået fra som standard*) - Scanningen kontrollerer også computerens systemområder.

- **Aktivér grundig scanning** (*slået fra som standard*) - i særlige situationer (*hvor der er mistanke om, at computeren er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som egentlig ikke kan blive inficeret, men bare for at være sikker. Husk at denne metode er ret tidskrævende.

- ***Yderligere scanningsindstillinger*** - linket åbner en ny ***Yderligere scanningsindstillinger*** -dialog, hvor du kan specificere følgende parametre:



  - ***Computerlukningsmuligheder*** - beslut, om computeren skal lukkes automatisk, når den igangværende scanningsproces er slut. 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***).

  - ***Definer filtyper til scanning*** - derudover skal du beslutte, om du vil have scannet:

    - ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en kommasepareret liste over filtypenavne, som ikke skal scannes;

    - ***Udvalgte filtyper*** - du kan angive, at du kun vil scanne filer, som er mulige at inficere (*filer som ikke kan blive inficeret, bliver ikke scannet, for eksempel visse almindelige tekstfiler, eller andre ikke eksekverbare filer*), herunder mediefiler (*video- og lydfiler - hvis du lader dette felt stå tomt, reducerer det*

scanningen yderligere, fordi disse filer ofte er ret store, og det ikke er særlig sandsynligt, at de er inficerede med virus). Igen kan du angive, hvilke filer, der altid skal scannes, ud fra filtypenavnene.

- Du kan også vælge at ***Scanne filer uden filtypenavn*** - denne indstilling er slået til som standard, og det anbefales, at du bevarer den sådan, medmindre du har en virkelig god grund til at ændre den. Filer uden filtypenavn er ret mistænkelige og bør altid scannes.

- ***Scanningsprioritet*** - du kan bruge skyderen til at ændre scanningsprioriteten. Som standard er denne indstillingsværdi sat til *brugerfølsomt niveau af automatisk ressourceforbrug.* Alternativt 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***-dialog, hvor du kan vælge, hvilke typer af mulige fund, der skal rapporteres:

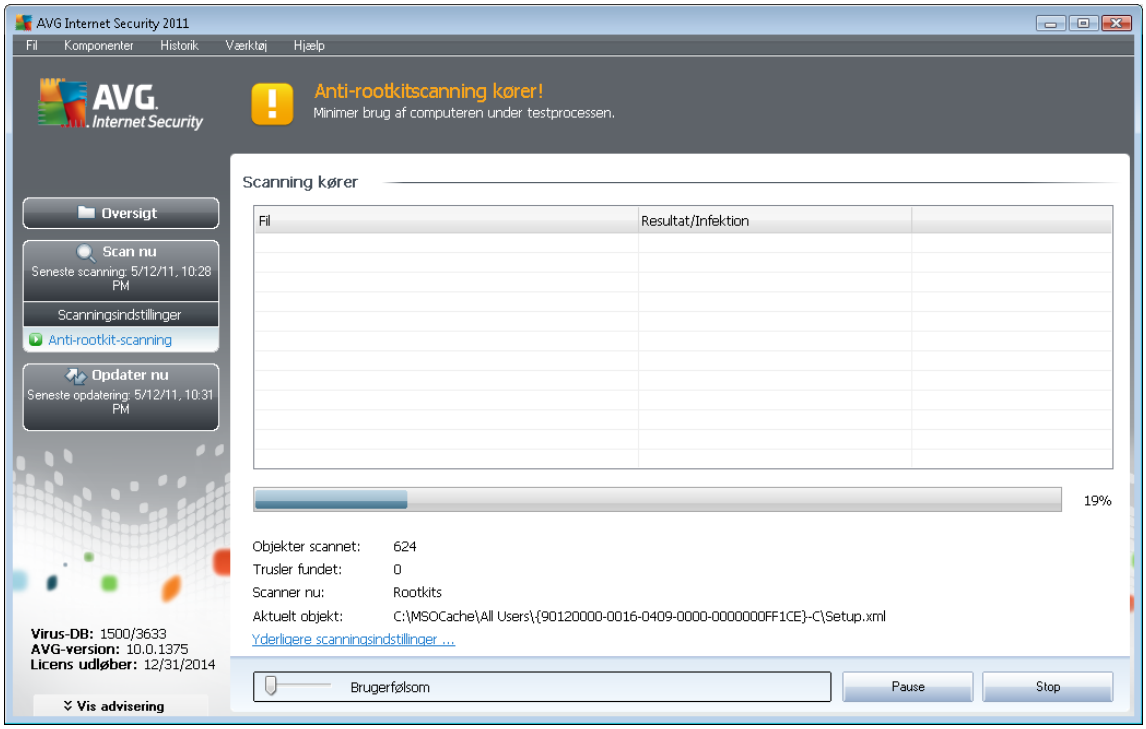
Advarsel: *Disse scanningsindstillinger er magen til parametrene for en ny defineret scanning - som beskrevet i kapitlet* ***AVG Scanning / Scanningsplanlægning / Hvordan der skal scannes****. Hvis du beslutter at ændre standardkonfigurationen for* ***Scan specifikke filer eller mapper****, kan du gemme 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).*

11.2.3. Anti-rootkit-scanning

Anti-rootkit-scanning søger efter mulige rootkits på din computer (*programmer og teknologier, som kan skjule malwareaktivitet på din computer*). Hvis et rootkit detekteres, betyder det ikke nødvendigvis, at din computer er inficeret. I visse tilfælde kan bestemte drivere eller dele af almindelige applikationer blive detekteret som rootkits ved en fejl.

Scanningskørsel

Anti-rootkit-scanning 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 (***Stop***) om nødvendigt.

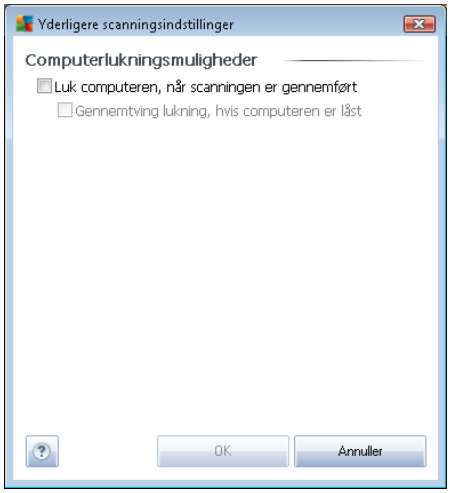


Redigering af scanningskonfiguration

Anti-rootkit-scanning køres altid i standardindstillingerne, og redigering af scanningsparametrene er kun tilgængeligt i dialogen ***AVG Avancerede indstillinger / Anti-rootkit***. I scanningsgrænsefladen er følgende konfiguration tilgængelig, men kun mens scanningen kører:

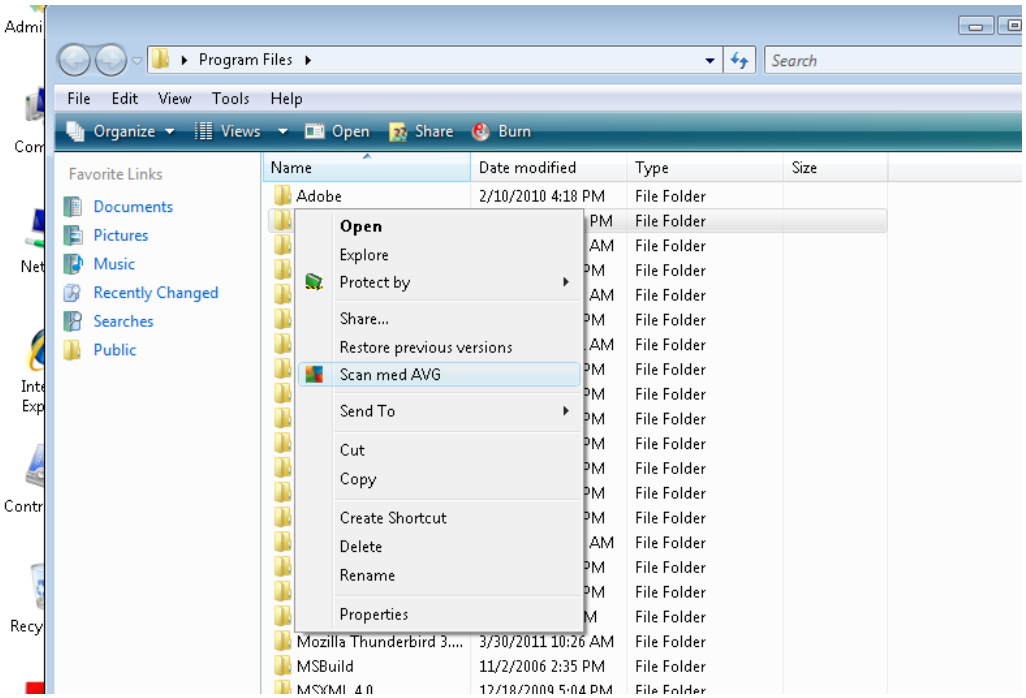
- ***Automatisk scanning*** - du kan bruge skyderen til at ændre scanningsprioriteten. Som standard er denne indstillingsværdi sat til *brugerfølsomt niveau af automatisk ressourceforbrug.* Alternativt kan du køre scanningen langsommere, hvilket betyder, at belastningen på systemressourcerne minimeres (*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*).

- ***Yderligere scanningsindstillinger*** - dette link åbner en ny ***Yderligere scanningsindstillinger***-dialog, hvor du kan definere mulige betingelser for lukning af computeren i forbindelse med ***Anti-rootkit-scanning*** (***Luk computeren, når scanningen er gennemført***, *muligvis* ***Gennemtving lukning, hvis computeren er låst***):



11.3. Scanning i Windows stifinder

Udover de foruddefinerede scanninger af hele computeren eller udvalgte områder af den, giver **AVG Internet-sikkerhed 2011** 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

11.4. Kommandolinjescanning

I **AVG Internet-sikkerhed 2011** 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 semikolon, 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.

11.4.1. 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 /filnavn/
- ***/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

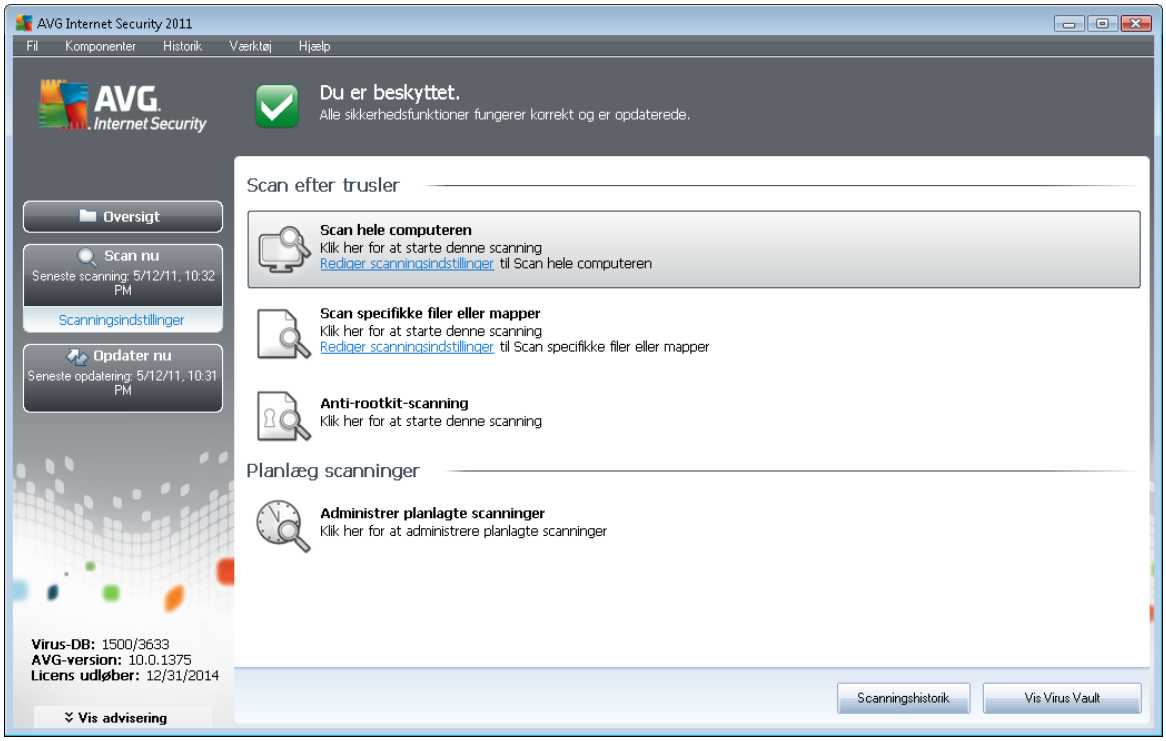
- ***/HELP*** Vis hjælp om dette emne
- ***/PRIORITET*** Indstil scanningsprioritet /Lav, Auto, Høj/ (se Avancerede indstillinger / Scanninger)
- ***/SHUTDOWN*** Luk computeren, når scanningen er fuldført
- ***/FORCESHUTDOWN*** Gennemtving computerlukning, når scanningen er fuldført
- ***/ADS*** Scan alternative datastrømme (kun NTFS)
- ***/ARCBOMBSW*** Rapportér genkomprimerede arkivfiler

11.5. Scanningsplanlægning

Med **AVG Internet-sikkerhed 2011** 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.

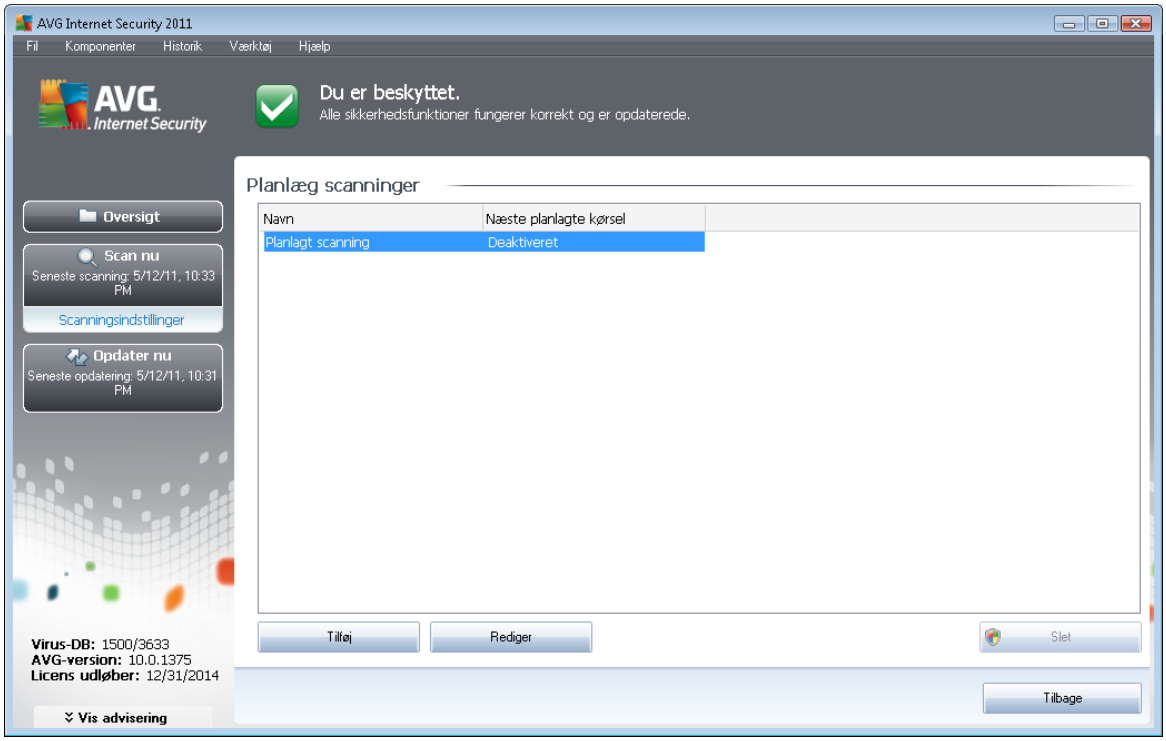
Du bør køre ***Scanning af hele computeren*** regelmæssigt, mindst en gang ugentligt. Hvis det er muligt, bør du køre en scanning af hele computeren dagligt - som indstillet i standardkonfigurationen for scanningsplanlægning. Hvis computeren er "altid tændt", kan du planlægge scanninger uden for arbejdstiden. 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:



Planlæg scanninger

Klik på det grafiske ikon i sektionen ***Planlæg scanninger*** for at åbne en ny ***Planlæg scanninger***-dialog, hvor du finder en liste over alle de aktuelt planlagte scanninger:



Du kan redigere/tilføje scanninger med 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.

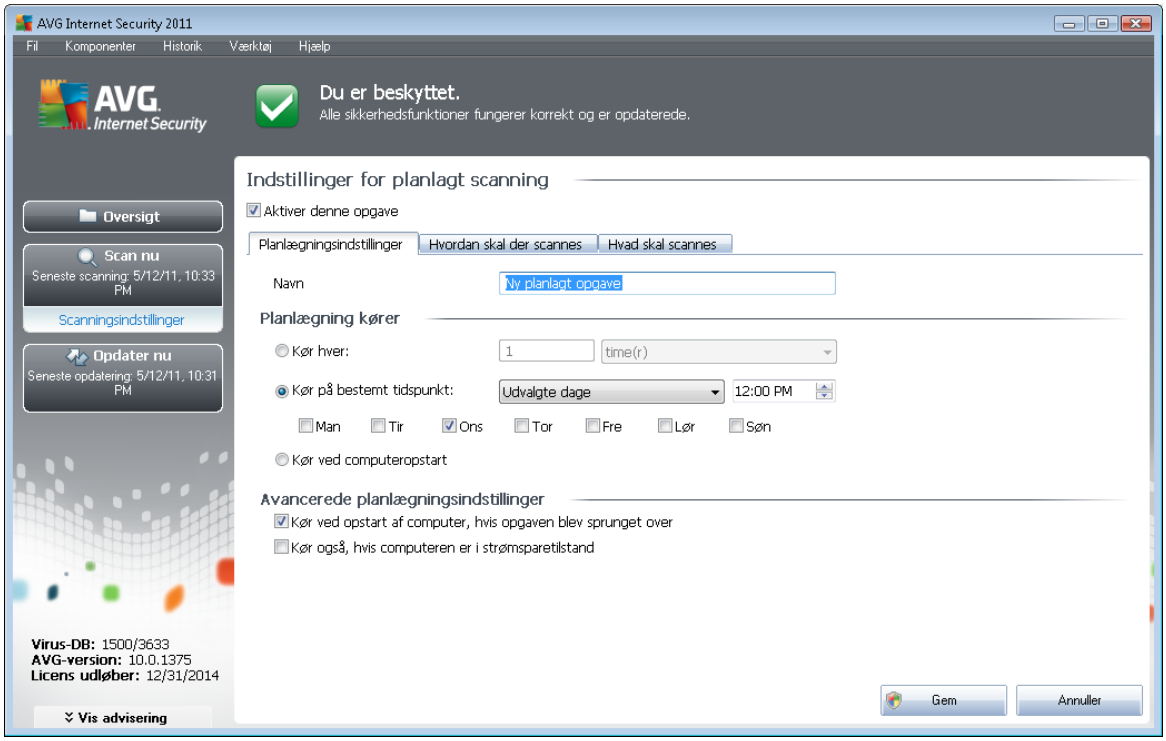
- ***Rediger scanningsplan*** - denne knap kan kun bruges, hvis du i forvejen har valgt en eksisterende test fra listen over planlagte test. I dette tilfælde vises knappen som aktiv, og du kan klikke på den for at skifte til dialogboksen ***Indstillinger for planlagt scanning*** fanen ***Planlægningsindstillinger***. 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.

- ***Tilbage*** - vend tilbage til AVG scanningsgrænseflade

11.5.1. Planlægningsindstillinger

Hvis du vil planlægge en ny test og regelmessig kørsel af denne, skal du åbne dialogen ***Indstillinger for planlagt test*** (*klik på knappen* ***Tilføj scanningsplan*** *i dialogen* ***Planlæg scanninger***). 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.

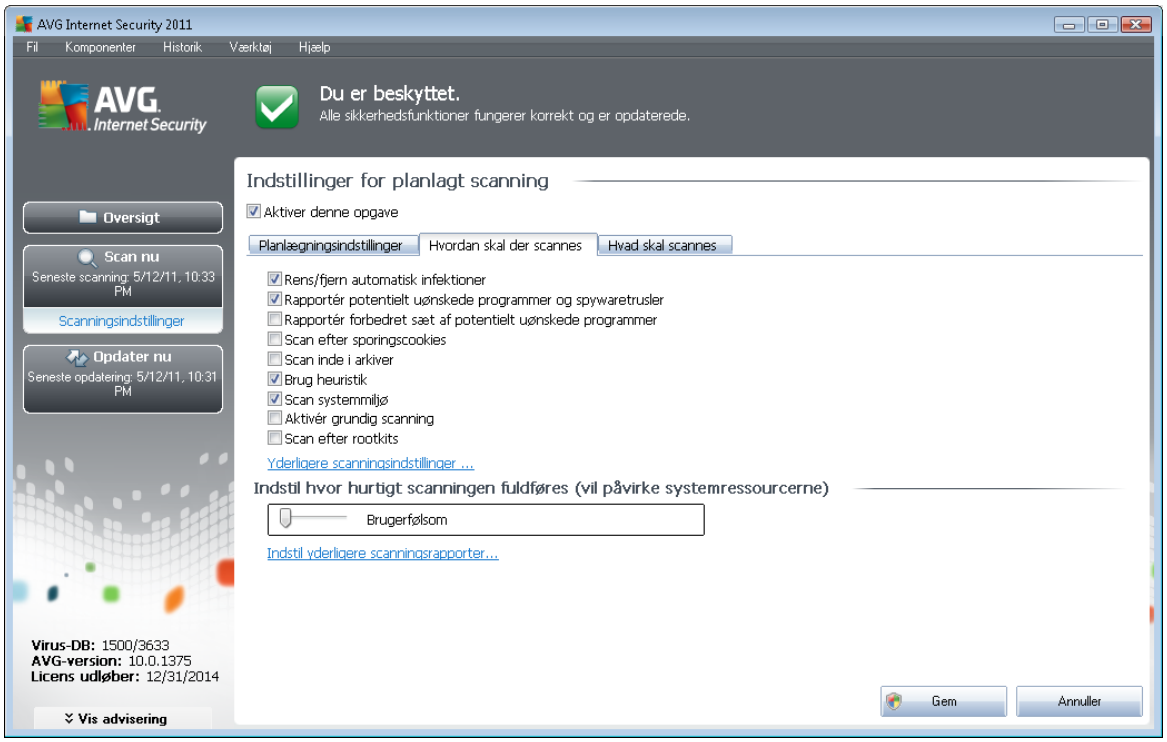
Betjeningsknapper i dialogen Indstillinger for planlagt scanning

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.

11.5.2. 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***.

- ***Rapporter potentielt uønskede programmer og spywaretrusler*** (*aktiveret som standard*): markér for at aktivere programmet ***Anti-spyware*** og scanne efter spyware og efter vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler at holde denne funktion aktiveret, da den øger computersikkerheden.

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*): markér for at detektere udvidede pakker af spyware: programmer, der er fuldstændig i orden og harmløse, når de fås direkte fra fabrikanten, men kan misbruges til skadelige formål senere. Dette er en ekstra funktion, som øger din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer, og er derfor som standard slået fra.

- ***Scan efter sporingscookies*** (*slået fra 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 fra 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, ...

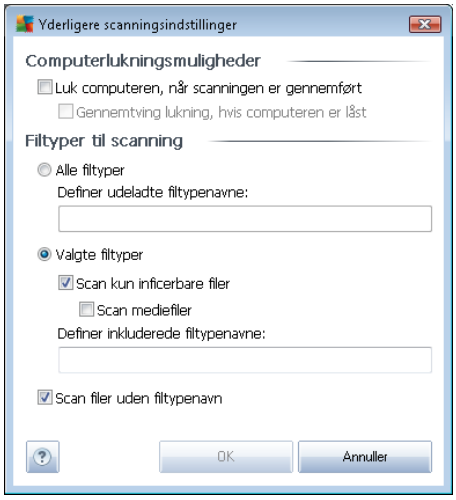
- ***Brug heuristik*** (*slået til som standard*): Heuristisk analyse (*dynamisk emulering af det scannede objektsinstruktioner i et virtuelt computermiljø*) er en af metoderne, der anvendes til detektering af virus under scanningen.

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

- ***Aktivér grundig scanning*** (*slået fra som standard*) - i særlige situationer (*hvor der er mistanke om, at computeren er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som egentlig ikke kan blive inficeret, men bare for at være sikker. Husk at denne metode er ret tidskrævende.

Derefter kan du ændre scanningskonfigurationen som følger:

- ***Yderligere scanningsindstillinger*** - linket åbner en ny ***Yderligere scanningsindstillinger*** -dialog, hvor du kan specificere følgende parametre:



- ***Computerlukningsmuligheder*** - beslut, om computeren skal lukkes automatisk, når den igangværende scanningsproces er slut. 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***).

- ***Definer filtyper til scanning*** - derudover skal du beslutte, om du vil have scannet:

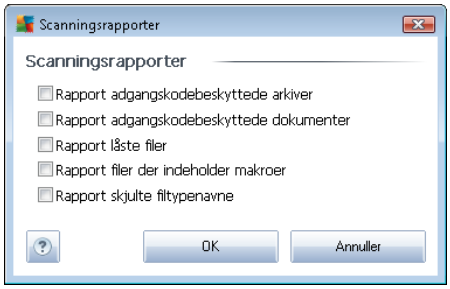
  - ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en kommasepareret liste over filtypenavne, som ikke skal scannes;

  - ***Udvalgte filtyper*** - du kan angive, at du kun vil scanne filer, som er mulige at inficere (*filer som ikke kan blive inficeret, bliver ikke scannet, for eksempel visse almindelige tekstfiler, eller andre ikke eksekverbare filer*), herunder mediefiler (*video- og lydfiler - hvis du lader dette felt stå tomt, reducerer det scanningen yderligere, fordi disse filer ofte er ret store, og det ikke er særlig sandsynligt, at de er inficerede med virus*). Igen kan du angive, hvilke filer, der altid skal scannes, ud fra filtypenavnene.

  - Du kan også vælge at ***Scanne filer uden filtypenavn*** - denne indstilling er slået til som standard, og det anbefales, at du bevarer den sådan, medmindre du har en virkelig god grund til at ændre den. Filer uden filtypenavn er ret mistænkelige og bør altid scannes.

- ***Indstil hvor hurtigt scanningen fuldføres*** - du kan bruge skyderen til at ændre scanningsprioriteten. Som standard er denne indstillingsværdi sat til *brugerfølsomt* niveau af automatisk ressourceforbrug. Alternativt 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***-dialog, hvor du kan vælge, hvilke typer af mulige fund, der skal rapporteres:



Bemærk: *Som standard er scanningskonfigurationen indstillet til optimal ydelse. Medmindre 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.*

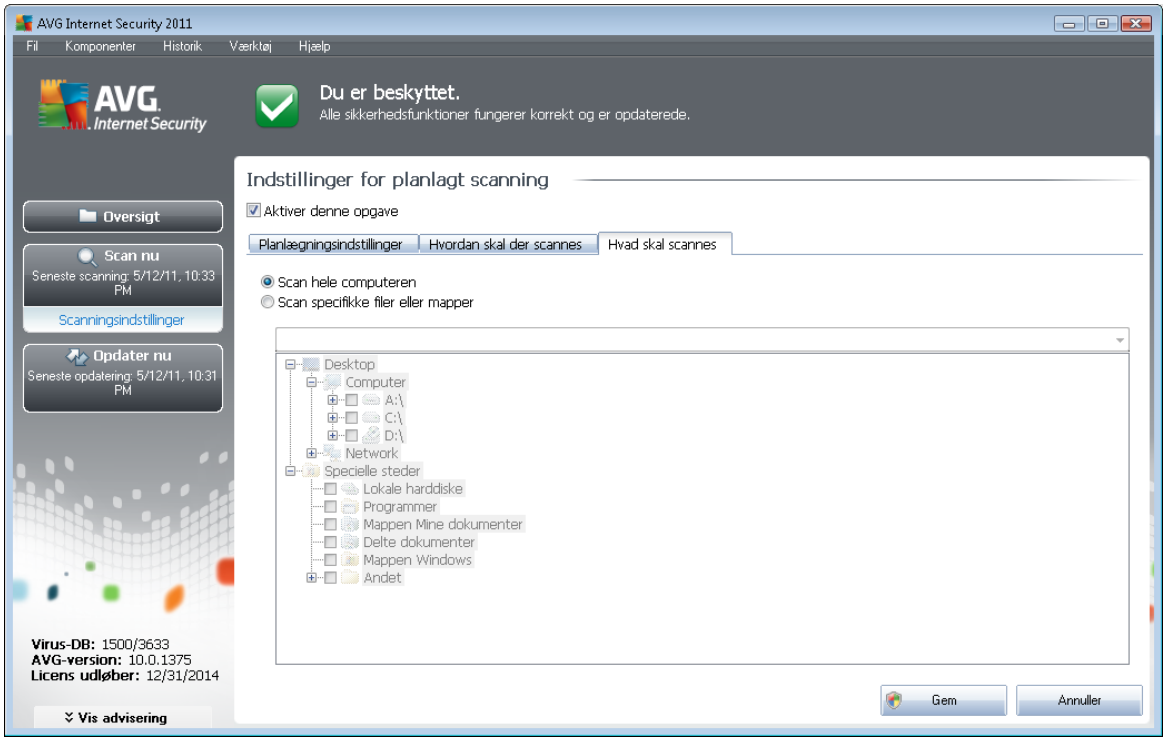
Betjeningsknapper

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.

11.5.3. 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 (*udvid elementer ved at klikke på plus-noden, indtil du finder den mappe, du vil scanne*). Du kan vælge flere mapper ved at markere de pågældende felter. De valgte mapper vises i tekstfeltet øverst i dialogen, og rullemenuen bevarer historikken over dine valgte scanninger til senere brug. Du kan også manuelt indtaste den fulde sti til den ønskede mappe (*hvis du indtaster flere stier, skal de adskilles med semikolon uden ekstra mellemrum*).

I træstrukturen kan du også se en gren kaldet ***Specielle placeringer***. Derefter findes en liste over placeringer, der vil blive scannet, når det pågældende afkrydsningsfelt er markeret:

- ***Lokale harddiske*** - alle harddiske på computeren
- ***Programmer***
    - C:\Programmer\
    - *i 64-bit version* C:\Programmer (x86)
- ***Mappen Mine dokumenter***
    - *for Win XP:* C:\Documents and Settings\Default User\Dokumenter\

- *for Windows Vista/7*: C:\Users\user\Documents\

- ***Delte dokumenter***
  - *for Win XP*: C:\Documents and Settings\All Users\Dokumenter\
  - *for Windows Vista/7*: C:\Users\Public\Documents\

- ***Windows-mappe*** - C:\Windows\

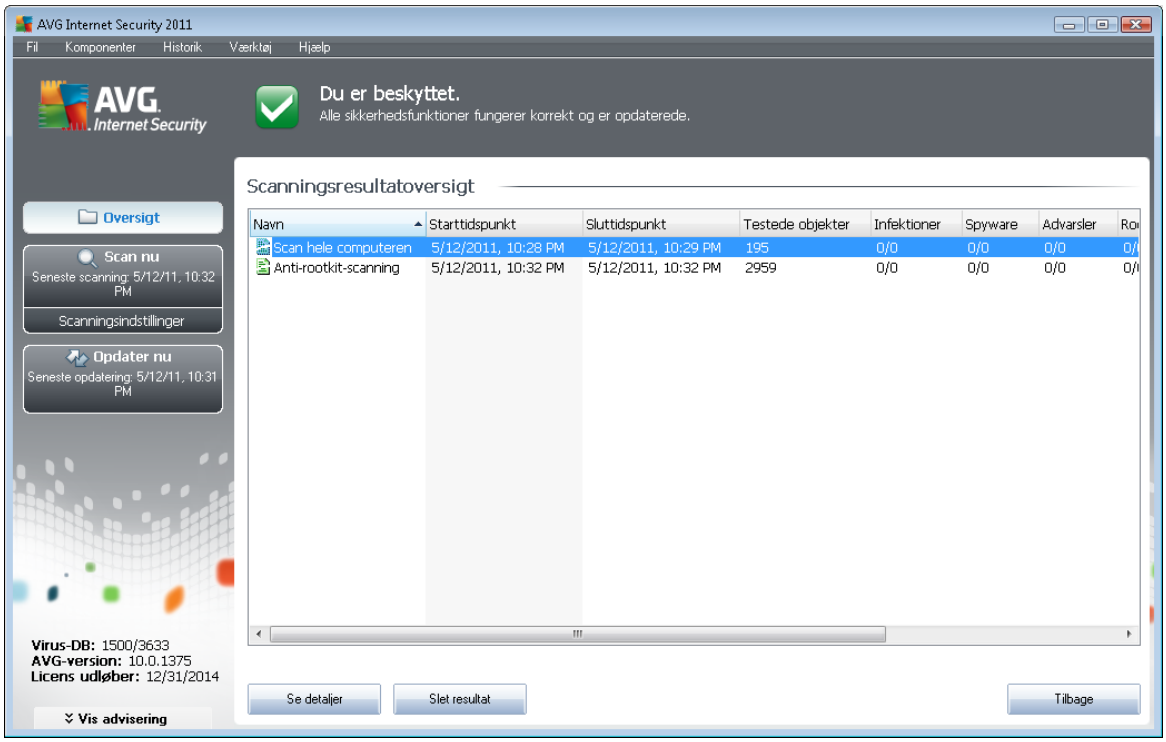
- ***Andet***
  - *Systemdrev* - harddisken, hvor operativsystemet er installeret (normalt C:)
  - *Systemmappe* - C:\Windows/System32\
  - *Mappen Midlertidige filer* - C:\Documents and Settings\User\Local\ (*Windows XP*); or C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
  - *Midlertidige internetfiler* - C:\Documents and Settings\User\Lokale indstillinger\Temporary Internet Files\ (*Windows XP*); or C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

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.

11.6. 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
- ***Advarsler*** - antallet af detekterede mistænkelige objekter
- ***Rootkits*** - antallet af detekterede rootkits
- ***Scanningslogoplysninger*** - oplysninger vedrørende scanningens forløb og resultat (typisk når den afsluttes eller afbrydes)

Betjeningsknapper

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

- ***Vis oplysninger*** - tryk på den for at skifte til dialogen ***Scanningsresultater*** for at se detaljerede data om den valgte scanning
- ***Slet resultat*** - tryk på den for at fjerne det valgte element fra scanningsresultatoversigten
- ***Tilbage*** - skifter tilbage til standarddialogboksen for AVG's scanningsgrænseflade

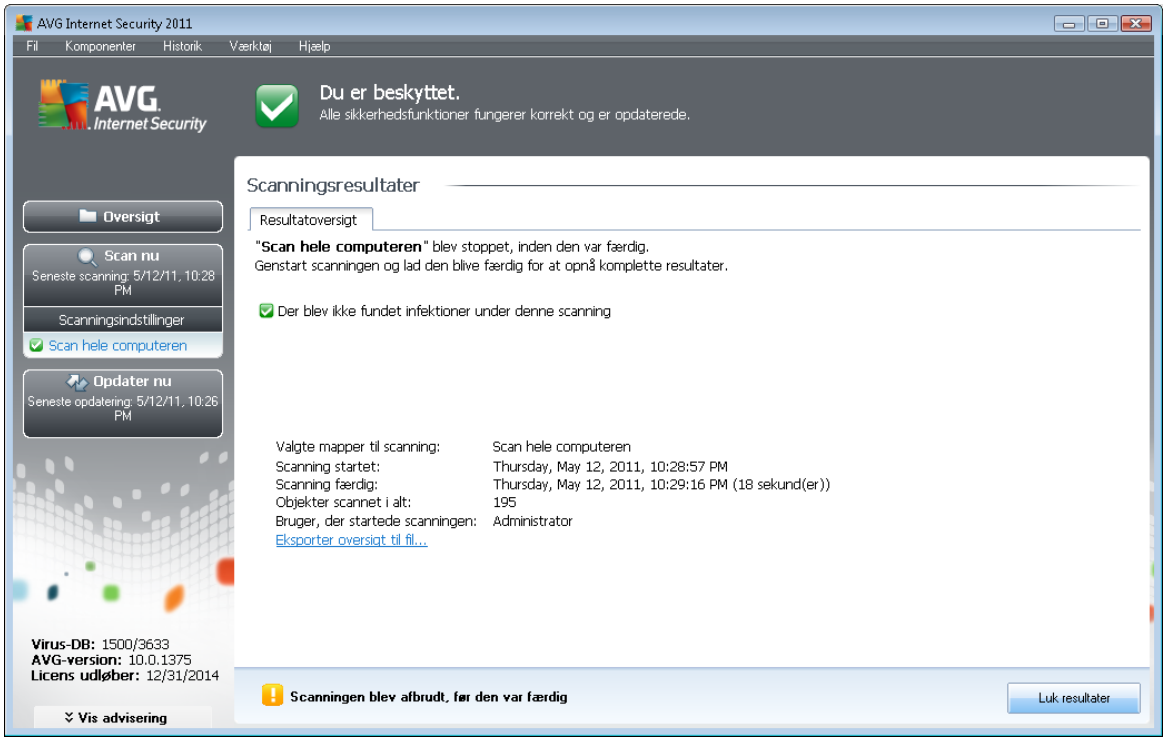
11.7. Scanningsresultatdetaljer

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 f.eks., hvis der blev detekteret cookies 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. Du vil her også finde oplysninger om objekter, der ikke kunne scannes (f.eks. adgangskodebeskyttede arkiver).

11.7.1. Fanen Resultatoversigt



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

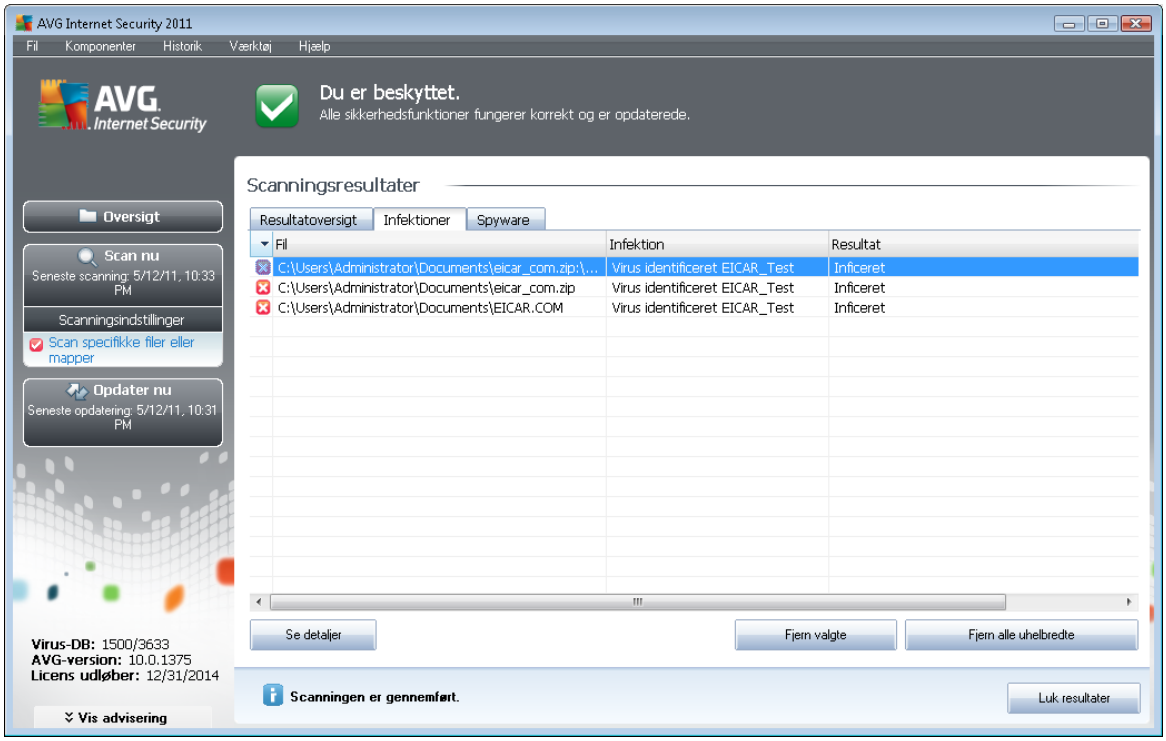
- detekterede virusinfektioner / spyware
- fjernede virusinfektioner / spyware
- antallet af virusinfektioner / spyware, der ikke kan fjernes eller helbredes

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***.

11.7.2. 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:

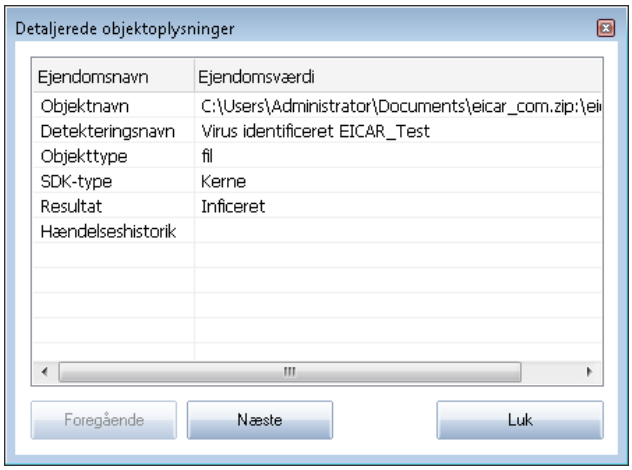
- ***Fil*** - fuld sti til det inficerede objekts oprindelige placering
- ***Infektioner*** - navn på den detekterede virus (*se Virus-opslagsværket online for yderligere oplysninger om specifikke vira*)
- ***Resultat*** - definerer den aktuelle status for det inficerede objekt, der blev detekteret under 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:

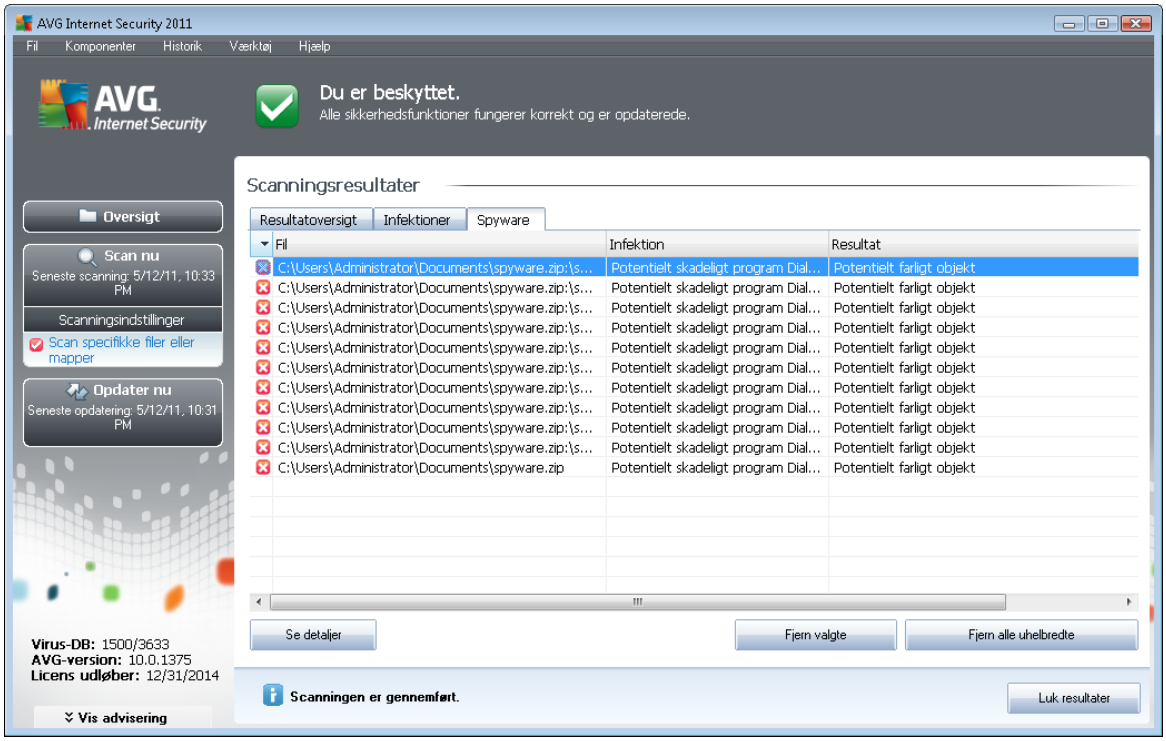
- ***Vis detaljer*** - knappen åbner et nyt dialogvindue med navnet ***Detaljerede objektoplysninger***:



  I denne dialog kan du finde detaljerede oplysninger om det detekterede inficerede objekt (*f.eks. inficeret objektnavn og placering, objekttype, SDK-type, detekteringsresultat og handlingshistorik, der er relateret til det detekterede objekt*). Med knapperne ***Forrige*** / ***Næste*** kan du se oplysninger om specifikke fund. Brug knappen ***Luk*** til at lukke dialogen.

- ***Fjern valgte*** - brug knappen til at flytte de valgte fund til ***Virus Vault***
- ***Fjern alle uhelbredte*** - 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***

11.7.3. 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:

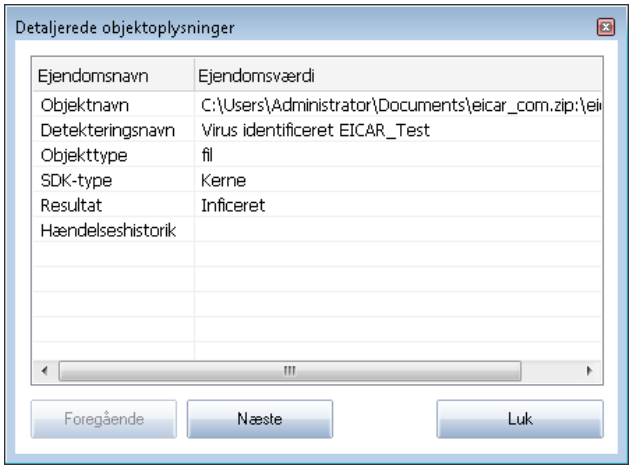
- ***Fil*** - fuld sti til det inficerede objekts oprindelige placering
- ***Infektioner*** - navn på detekteret spyware (*for oplysninger om specifikke vira henvises til* ***Virus-opslagsværket*** *online*)
- ***Resultat*** - definerer den aktuelle status for det objekt, der blev detekteret under scanningen:
    - ***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 fuldstændigt skal du genstarte computeren

Betjeningsknapper

Der findes tre betjeningsknapper i denne dialog:

- **_Vis detaljer_** - knappen åbner et nyt dialogvindue med navnet **_Detaljerede objektoplysninger_**:



I denne dialog kan du finde detaljerede oplysninger om det detekterede inficerede objekt (*f.eks. inficeret objektnavn og placering, objekttype, SDK-type, detekteringsresultat og handlingshistorik, der er relateret til det detekterede objekt*). Med knapperne **_Forrige_** / **_Næste_** kan du se oplysninger om specifikke fund. Brug knappen **_Luk_** til at forlade denne dialog.

- **_Fjern valgte_** - brug knappen til at flytte de valgte fund til ***Virus Vault***
- **_Fjern alle uhelbredte_** - 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***

11.7.4. 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. Den slags filer udgør ikke nogen direkte trussel for din computer eller sikkerhed. Oplysninger om disse filer er generelt brugbare, hvis der detekteres adware eller spyware på din computer. Hvis der kun detekteres advarsler af en AVG-test, er det ikke nødvendigt at foretage sig yderligere.

Dette er en kort beskrivelse af de almindeligste eksempler på den slags objekter:

- ***Skjulte filer*** - De skjulte filer er som standard ikke synlige i Windows, og visse vira eller andre trusler forsøger at undgå opdagelse ved at gemme deres filer med denne attribut. Hvis din AVG rapporterer en skjult fil, som du mistænker er ondsindet, kan du flytte den til din ***AVG Virus Vault***.
- ***Cookies*** - Cookies er almindelige tekstfiler, som anvendes af websteder til at gemme brugerspecifikke oplysninger, som senere bruges til at indlæse tilpassede webstedslayout, udfylde brugernavn automatisk osv.
- ***Mistænkelige registreringsdatabasenøgler*** - Visse former for malware gemmer sine oplysninger i Windows' registreringsdatabase for at sikre, at den indlæses ved opstart eller for at forlænge sin effekt på operativsystemet.

11.7.5. Fanen Rootkits

Fanen ***Rootkits*** viser oplysninger om rootkits, der blev detekteret under scanning, hvis du har kørt ***Anti-rootkit-scanningen***.

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.

Denne fanes opbygning er grundlæggende den samme som ***fanen Infektioner*** eller ***fanen Spyware***.

11.7.6. Fanen Information

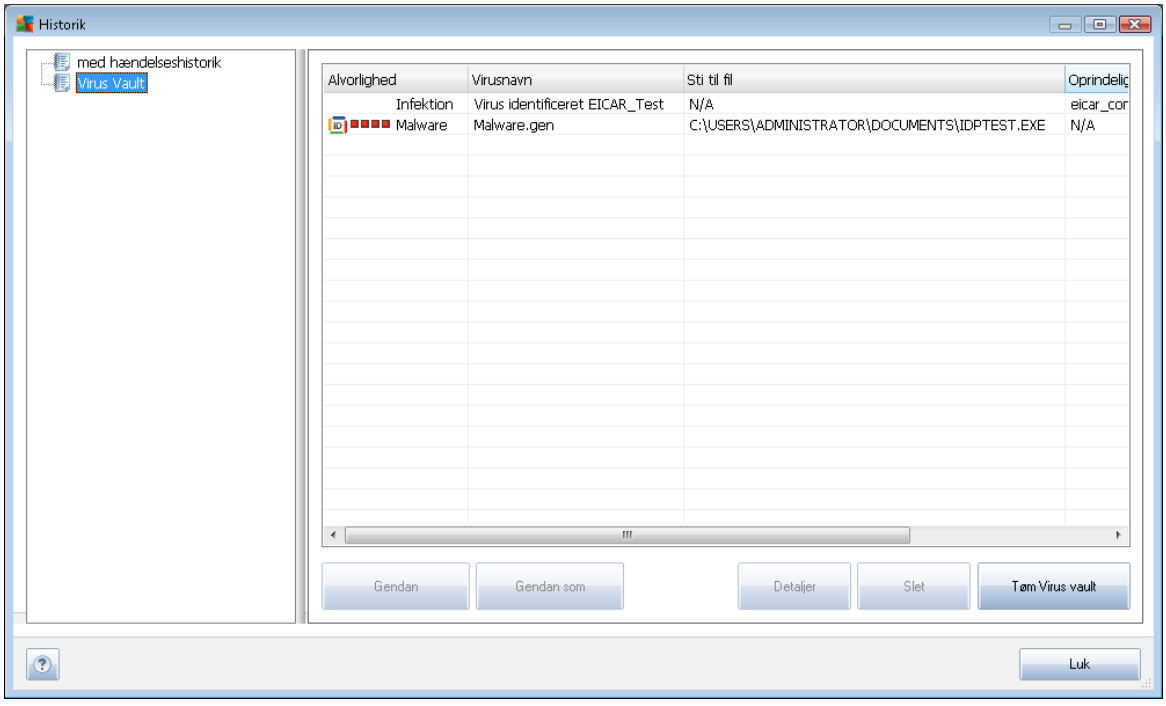
Fanen ***Information*** indeholder data om "fund", der ikke kan kategoriseres som infektioner, spyware osv. De kan heller ikke med vished kaldes farlige, men du bør være opmærksom på dem. AVG-scanning kan detektere filer, som muligvis ikke er inficerede men er mistænkelige. Disse filer rapporteres enten som ***Advarsel*** eller som ***Information***.

Alvorligheden ***Information*** kan rapporteres af følgende årsager:

- ***Runtime-pakket*** - Filen blev pakket med en mindre sædvanlig runtime-pakker, hvilket kan indikere et forsøg på at forhindre scanning af filen. Alle rapporter om en sådan fil indikerer dog ikke en virus.
- ***Runtime.pakket rekursivt*** - som ovenstående, dog mindre hyppigt i normal software. Sådanne filer er mistænkelige, og det bør overvejes at fjerne dem eller sende dem til analyse.

- ***Adgangskodebeskyttet arkiv eller dokument*** - Adgangskodebeskyttede filer kan ikke scannes af AVG (*eller andre antimalware-programmer*).
- ***Dokument med makroer*** - Det rapporterede dokument indeholder makroer, som kan være skadelige.
- ***Skjult filtypenavn*** - Filer med skjult filtypenavn kan se ud som f.eks. billeder men i virkeligheden være eksekverbare filer (*f.eks. billede.jpg.exe*). Det andet filtypenavn er ikke synligt i Windows som standard, og AVG rapporterer sådanne filer for at forhindre, at de åbnes ved et uheld.
- ***Ugyldig filsti*** - Hvis en vigtig systemfil kører fra en anden sti end standardstien (*f.eks. hvis winlogon.exe kører fra en anden mappe end Windows-mappen*), rapporterer AVG denne afvigelse. I visse tilfælde bruger vira navne på almindelige systemprocesser for at gøre deres tilstedeværelse mindre synlig i systemet.
- ***Låst fil*** - Den rapporterede fil er låst og kan dermed ikke scannes af AVG. Dette betyder sædvanligvis, at en fil konstant bruges af systemet (*f.eks. en swapfil*).

11.8. 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. Hovedformålet med ***Virus Vault*** er at opbevare en eventuelt slettet fil i et vist stykke tid, så du kan være sikker på, at du ikke længere behøver filen i dens oprindelige placering. Finder du ud af, at den manglende fil giver problemer, kan du sende den pågældende fil til analyse, eller gendanne den til dens oprindelige

placering.

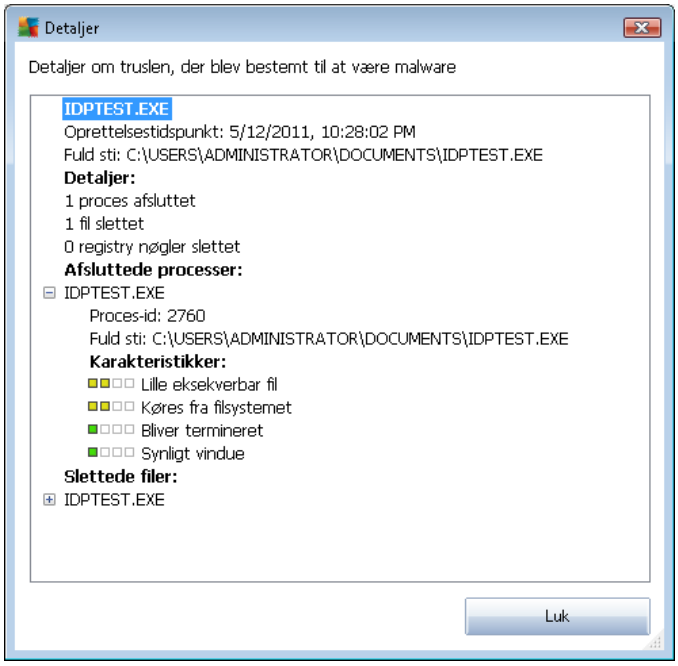
Virus Vault-grænsefladen åbnes i et separat vindue og indeholder en oversigt over oplysninger om inficerede objekter:

- ***Alvorlighed*** - hvis du bestemmer dig for at installere ***Identitetsbeskyttelse***-komponenten i din **AVG Internet-sikkerhed 2011**, viser denne sektion en grafisk identifikation af det pågældende funds alvorlighed på en firetrins skala fra uanstødelig ■□□□ op til meget farlig (■■■■). Og oplysninger om infektionstypen (*baseret på deres infektionsniveau - alle anførte objekter kan være definitivt eller potentielt inficerede*)
- ***Virusnavn*** - angiver navnet på den detekterede infektion i henhold til ***Virus-opslagsværket*** (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*** - flytter den inficerede fil til en valgt mappe
- ***Detaljer*** - denne knap gælder kun trusler, der er detekteret af ***Identitetsbeskyttelse***. Når du klikker på denne knap, vises en synoptisk oversigt over trusseldetaljer (*hvilke filer/ processer der er blevet påvirket, karakteristik for processen, osv.*). Vær opmærksom på, at for alle andre elementer end de, der er detekteret af IDP, er denne knap udtonet og inaktiv!



- ***Slet*** - fjerner den inficerede fil fuldstændig fra ***Virus Vault*** og denne handling kan ikke fortrydes

- ***Tøm Vault*** - fjerner alle ***Virus Vault*** indholdhelt. Når filer fjernes fra ***Virus Vault***, fjernes de permanent fra drevet (*de flyttes ikke til papirkurven*).

12. AVG Opdateringer

Det er afgørende at holde din AVG opdateret for at sikre, at alle nyopdagede vira bliver detekteret så hurtigt som muligt.

Eftersom AVG-opdateringer ikke frigives efter nogen fast plan, men i stedet som en reaktion på mængden og alvorligheden af nye trusler, anbefales det at søge efter nye opdateringer mindst en gang om dagen og gerne oftere. Kun på denne måde kan du sikre, at din **AVG Internet-sikkerhed 2011** også holdes opdateret i løbet af dagen.

12.1. Opdateringsniveauer

Du kan vælge mellem to opdateringsniveauer:

- ***Definitionsopdatering*** indeholder nødvendige ændringer for pålidelig beskyttelse mod virus. 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.

Bemærk: *Hvis der forekommer et tidsmæssigt sammenfald af en planlagt programopdatering og en planlagt scanning, tager opdateringsprocessen prioritet og scanningen vil blive afbrudt.*

12.2. 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.

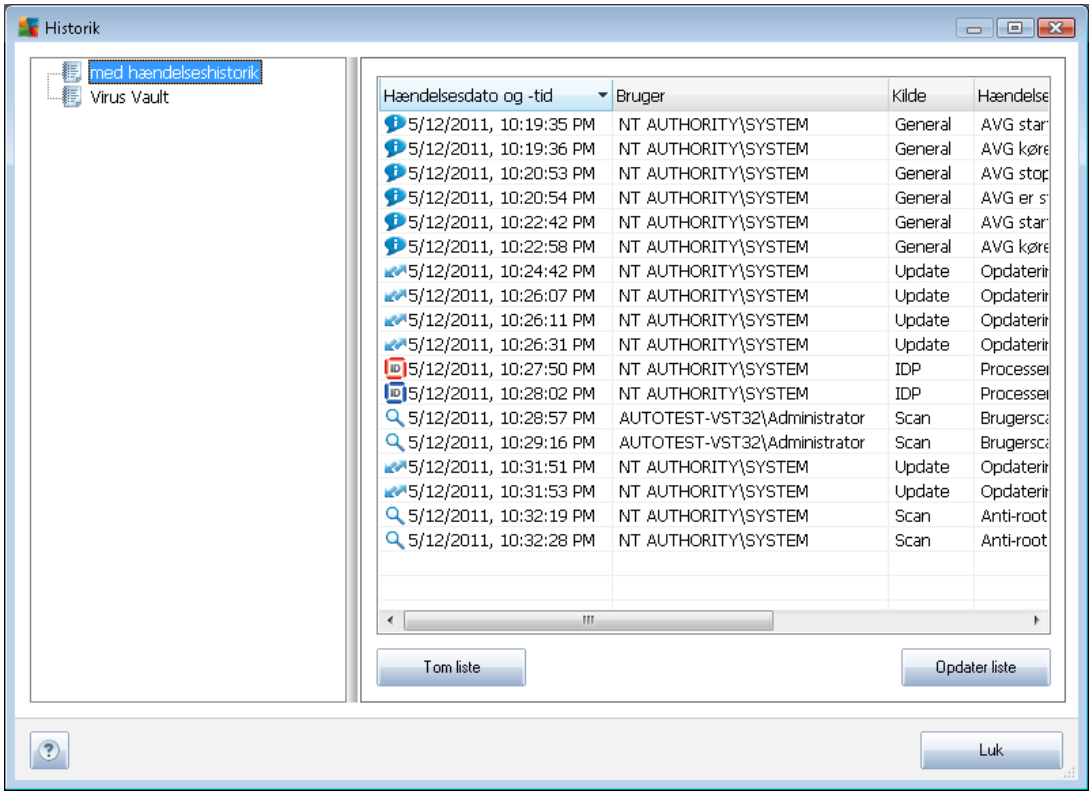
12.3. Opdateringsproces

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 mulighed er tilgængelig via Start / Alle programmer / Tilbehør / Systemværktøjer / Systemgendannelse. Dette anbefales dog kun for erfarne brugere!*

13. Hændelseshistorik



Der er adgang til dialogen ***Historik*** fra systemmenuen via punktet ***Historik/Log over hændelseshistorik***. I denne dialog findes en oversigt over vigtige hændelser, der er sket under brugen af **AVG Internet-sikkerhed 2011**. ***Historik*** 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

For hver hændelse vises følgende oplysninger:

- ***Hændelsesdato og -tid*** angiver nøjagtig dato og tid for, hvornår hændelsen fandt sted
- ***Bruger*** angiver hvem der initierede hændelsen
- ***Kilde*** angiver kildekomponenten eller en anden del af AVG-systemet, der udløste hændelsen

- ***Hændelsesbeskrivelse*** giver en kort sammenfatning af hvad der egentlig skete

Betjeningsknapper

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

14. FAQ og teknisk support

Skulle du støde på problemer med AVG, enten salgsmæssigt eller teknisk, kan du se ***FAQ***-sektionen på AVG's websted (http://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***.