AVG Internet-sikkerhed 2012

Brugervejledning

Dokumentrevision 2012.01 (1.9.2011)

Indhold

1. Introduktion

Denne brugervejledning indeholder omfattende dokumentation til **AVG Internet-sikkerhed 2012**.

AVG Internet-sikkerhed 2012 yder flere lag af beskyttelse i forbindelse med alt, hvad du foretager dig på internettet. Det betyder, at du ikke skal bekymre dig om identitetstiver, virus, eller om du besøger skadelige websteder. AVG Protective Cloud Technology og AVG Community Protection Network medfølger, hvilket betyder, at vi indsamler de seneste trusselsoplysninger og deler dem med vores gruppe, så vi er sikre på, at du får den bedste beskyttelse:

- Du kan helt trygt købe ind og bruge onlinebanken ved hjælp af AVG Firewall, Anti-Spam og Identitetsbeskyttelse
- Bevar trygheden på sociale netværk ved hjælp af AVG's beskyttelse af sociale netværk
- Surf og søg trygt ved hjælp af LinkScanners realttidsbeskyttelse

2. AVG Installationskrav

2.1. Understøttede operativsystemer

AVG Internet-sikkerhed 2012 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 2012, men kun uden IDP-komponenten.*

2.2. Minimum og anbefalede hardwarekrav

Minimum hardwarekrav for **AVG Internet-sikkerhed 2012**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM
- 1000 MB ledig harddiskplads (til installation)

Anbefalede hardwarekrav for **AVG Internet-sikkerhed 2012**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM
- 1550 MB ledig harddiskplads (til installation)

3. AVG Installationsproces

Hvor kan jeg finde installationsfilen?

For at installere **AVG Internet-sikkerhed 2012** på din computer skal du hente den nyeste installationsfil. Hvis du vil sikre dig, at du installerer en opdateret version af **AVG Internet-sikkerhed 2012**, anbefales det at hente installationsfilen fra AVG-webstedet (http://www.avg.com/). Afsnittet ***Supportcenter/Download*** indeholder en struktureret oversigt over installationsfilerne for hver AVG-udgave.

Hvis du ikke er sikker på, hvilke filer der skal hentes og installeres, kan det være en god ide at bruge tjenesten ***Vælg produkt*** nederst på websiden. Når du har besvaret tre enkle spørgsmål, definerer denne tjeneste lige præcis de filer, du skal bruge. Tryk på knappen ***Fortsæt*** for at blive omdirigeret til en komplet liste over filer, der kan hentes, og som er tilpasset til netop dine behov.

Hvordan ser installationsprocessen ud?

Når du har downloadet og gemt installationsfilen på din harddisk, kan du starte installationsprocessen. Installationen er en sekvens af dialoger, der er enkle og nemme at forstå. Alle dialoger beskriver kort, hvad du skal foretage dig ved hvert trin i installationsprocessen. Her giver vi en detaljeret beskrivelse af de forskellige dialoger:

3.1. Velkommen

Installationsprocessen starter med dialogen ***Velkommen til AVG-installationsprogrammet***:

Vælg installationssproget

Her i dialogen kan du vælge det sprog, der blev brugt under installationsprocessen. I det højre hjørne af dialogen klikker du på kombinationsfeltet for at vise sprogmenuen. Vælg det ønskede sprog, og installationsprocessen fortsætter på det valgte sprog.

NB! I øjeblikket har du kun valgt installationssproget. Applikationen AVG Internet-sikkerhed 2012 installeres på det valgte sprog og på engelsk, der altid installeres automatisk. Det er imidlertid muligt, der kan installeres med flere sprog, der kan arbejdes med, i AVG Internet-sikkerhed 2012. Du opfordres til at bekræfte dit fulde valg af alternative sprog i følgende konfigurationsdialoger, der kaldes Brugerdefinerede indstillinger.

Licensaftale

Derudover indeholder dialogen ***Velkommen til AVG-installationsprogrammet*** hele teksten til 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.

AVG-fortrolighedspolitik

Ud over licensaftalen giver denne konfigurationsdialog også mulighed for at få mere at vide om AVG-fortrolighedspolitikken. Du kan se linket ***AVG-fortrolighedspolitik*** i nederste venstre hjørne af dialogen. Klik på det for at blive omdirigeret til AVG-webstedet (http://www.avg.com/), hvor du kan finde hele indholdet om principperne bag AVG Technologies-fortrolighedspolitikken.

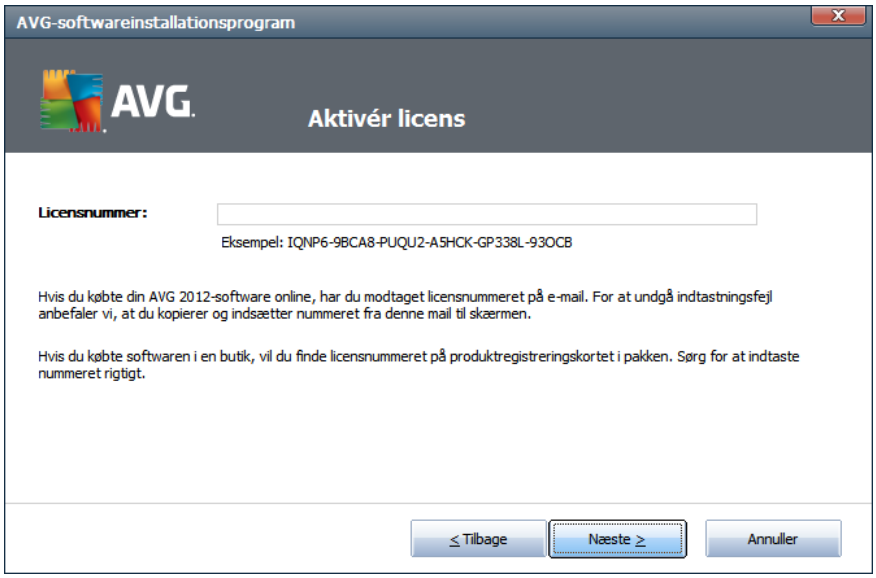
Betjeningsknapper

I den første konfigurationsdialog er der kun to tilgængelige kontrolknapper:

- ***Accepter*** – Klik for at bekræfte at du har læst, forstået og accepteret licensaftalen. Installation fortsætter, og du går et skridt videre til følgende konfigurationsdialog.
- ***Accepter ikke*** – Klik for at afvise denne licensaftale. Konfigurationsprocessen stopper med det samme. **AVG Internet-sikkerhed 2012** installeres ikke!

3.2. Aktivér din licens

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



Her finder du licensnummeret

Salgsnummeret kan findes på cd-emballagen i pakken til **AVG Internet-sikkerhed 2012**. Licensnummeret findes i den bekræftelses-e-mail, du modtog, efter du købte **AVG Internet-sikkerhed 2012** 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.

Sådan anvendes metoden med kopiering og indsættelse

Hvis du bruger metoden ***Kopiér og indsæt*** til at angive dit **AVG Internet-sikkerhed 2012**-licensnummer i programmet, sikrer du, at nummeret angives korrekt. Følg disse trin:

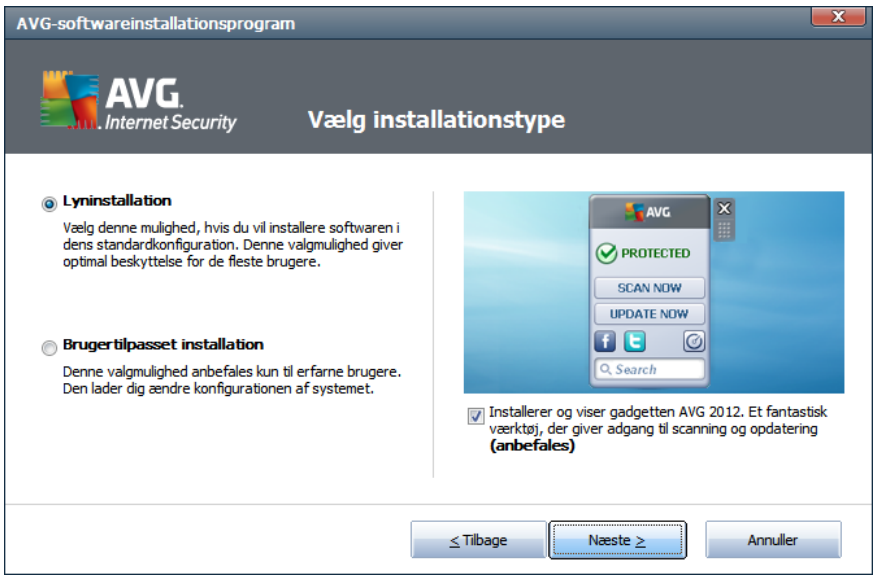
- Åbn den e-mail, der indeholder licensnummeret.
- Klik på den venstre museknap i begyndelsen af licensnummeret, og hold og træk musen til slutningen af nummeret, og slip så knappen. Nummeret skal nu være fremhævet.
- Tryk på og hold ***Ctrl*** nede, og tryk derefter på ***C***. Dette kopierer nummeret.
- Peg og klik på den position, hvor du ønsker at indsætte det kopierede nummer.
- Tryk på og hold ***Ctrl*** nede, og tryk derefter på ***V***. Dette indsætter nummeret for det sted, du har valgt.

Betjeningsknapper

Som i de fleste installationsdialoger er der tre tilgængelige kontrolknapper:

- ***Tilbage*** – Klik for at gå et trin tilbage til den forrige installationsdialog.
- ***Næste*** – Klik for at fortsætte installationen og gå et trin videre.
- ***Annuller*** – Klik for at afslutte installationen med det samme. **AVG Internet-sikkerhed 2012** installeres ikke!

3.3. Vælg installationstype



Installationstyper

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

For de fleste brugeres vedkommende anbefales det på det kraftigste at bevare den hurtige standardinstallation, som installerer **AVG Internet-sikkerhed 2012** i en fuldautomatisk tilstand med indstillinger, der er foruddefineret af programleverandøren. 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 Internet-sikkerhed 2012**-applikationen. Hvis du har valgt muligheden ***Lyninstallation***, skal du trykke på knappen ***Næste*** for at fortsætte til næste dialog, Installér AVG Sikkerhedsværktøjslinje.

Den brugerdefinerede installation bør kun bruges af erfarne brugere, der har en gyldig grund til at installere **AVG Internet-sikkerhed 2012** med indstillinger, der ikke er standard. Det kan f.eks. være for at tilpasse programmet til bestemte systemkrav. Når du har valgt denne mulighed, skal du trykke på knappen ***Næste*** for at fortsætte til dialogen Brugerdefinerede indstillinger.

Installation af AVG-gadgets

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 2012**, dvs. scanning og opdatering.

Betjeningsknapper

Som i de fleste installationsdialoger er der tre tilgængelige kontrolknapper:

- ***Tilbage*** – Klik for at gå et trin tilbage til den forrige installationsdialog.
- ***Næste*** – Klik for at fortsætte installationen og gå et trin videre.
- ***Annuller*** – Klik for at afslutte installationen med det samme. **AVG Internet-sikkerhed 2012** installeres ikke!

3.4. 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 2012** skal installeres. **AVG Internet-sikkerhed 2012** installeres som standard til programfilmapperne på C:-drevet. 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 2012**-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***.

Betjeningsknapper

Som i de fleste installationsdialoger er der tre tilgængelige kontrolknapper:

- ***Tilbage*** – Klik for at gå et trin tilbage til den forrige installationsdialog.
- ***Næste*** – Klik for at fortsætte installationen og gå et trin videre.
- ***Annuller*** – Klik for at afslutte installationen med det samme. **AVG Internet-sikkerhed 2012** installeres ikke!

3.5. Installér AVG Sikkerhedsværktøjslinje

I dialogen ***Installér AVG Sikkerhedsværktøjslinje*** skal du bestemme, om du vil installere AVG

Sikkerhedsværktøjslinje. Hvis du ikke ændrer standardindstillingerne, installeres denne komponent automatisk i din internetbrowser (*de understøttede browsere er Microsoft Internet Explorer v. 6.0 eller nyere og Mozilla Firefox v. 3.0 eller nyere*) og giver dig omfattende onlinebeskyttelse, når du surfer på nettet.

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.

3.6. Installationsforløb

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

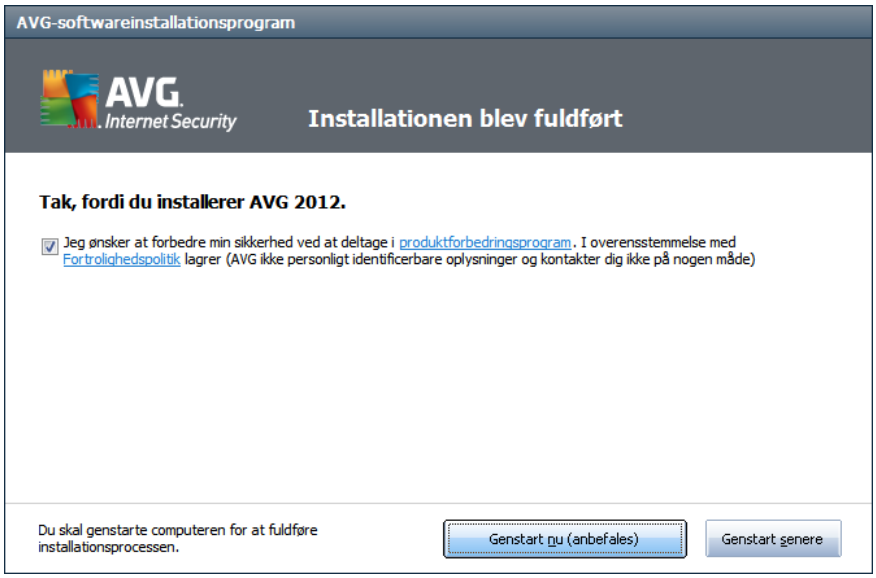
Når installationsprocessen er afsluttet, omdirigeres du automatisk til den næste dialog.

Betjeningsknapper

I denne dialog er der kun én kontrolknap tilgængelig – ***Annuller***. Denne knap bør kun bruges, hvis du vil stoppe installationsprocessen. Husk, at i sådant tilfælde er **AVG Internet-sikkerhed 2012** ikke installeret!

3.7. Installationen blev fuldført

Dialogen ***Installationen blev fuldført*** bekræfter, at din **AVG Internet-sikkerhed 2012** er blevet installeret og konfigureret:



Produktforbedringsprogram

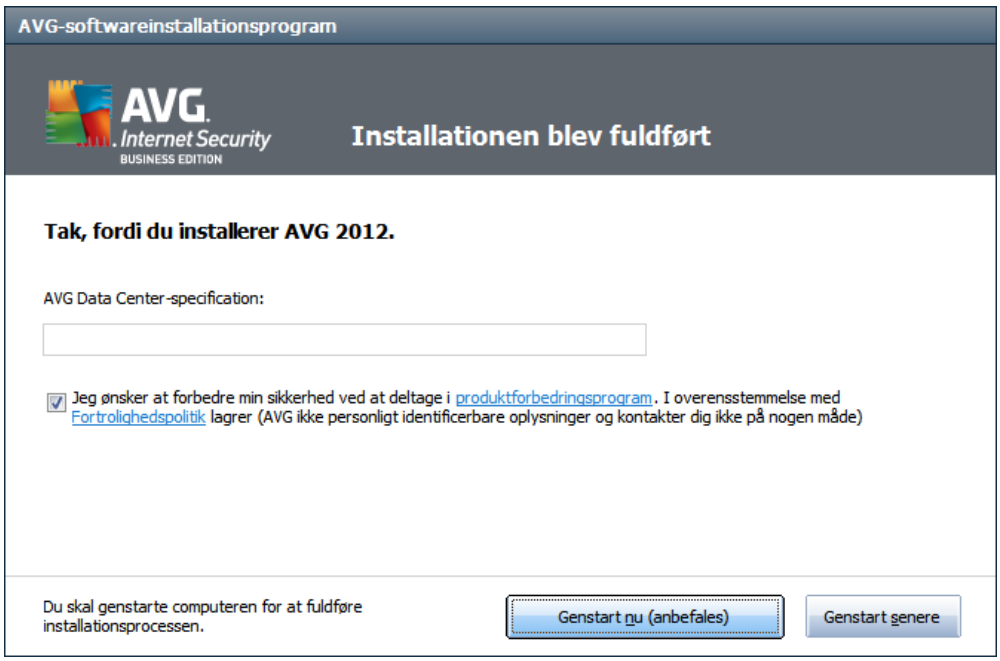
I denne dialog kan du bestemme, om du vil deltage i produktforbedringsprogrammet (*Du kan få flere oplysninger i kapitlet Avancerede AVG-indstillinger/Produktforbedringsprogram*), der indsamler anonyme oplysninger om de detekterede trusler, så den overordnede internetsikkerhed kan øges. Hvis du accepterer denne erklæring, skal du markere afkrydsningsfeltet ***Jeg accepterer at deltage i AVG 2012's internetsikkerhed og produktforbedringsprogram...*** *(indstillingen er som standard bekræftet)*.

Genstart af computer

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

Installation af erhvervslicens

Hvis du bruger en AVG-erhvervslicens, og hvis du tidligere har valgt at installere Ekstern administration *(se Brugerdefinerede indstillinger)*, vises en dialog for gennemførelsen af installationen 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 Du kan få detaljerede oplysninger om AVG-fjernadministration ved hjælp af brugervejledningen til AVG Business Edition, som kan hentes på AVG's websted (http://www.avg.com/).

Se kapitlet Komponentoversigt i denne dokumentation. For at gendanne standardkonfigurationen, der er forudindstillet af softwareleverabdøren, skal du bruge knappen ***Standard***.

Betjeningsknapper

Der er følgende kontrolknapper tilgængelige i dialogen:

- ***Genstart nu (anbefales)*** – Der kræves en genstart for at fuldføre installationsprocessen for **AVG Internet-sikkerhed 2012**. Det anbefales, at du genstarter computeren med det samme. **AVG Internet-sikkerhed 2012** er først fuldt installeret efter en genstart, så du er sikker og beskyttet.
- ***Genstart senere*** – Hvis du af en eller anden årsag ikke kan genstarte computeren nu, kan handlingen udskydes til et senere tidspunkt. Det anbefales imidlertid at genstarte med det samme. **AVG Internet-sikkerhed 2012** kan først beskytte computeren efter en genstart!

4. Efter installationen

4.1. Produktregistrering

Når du har afsluttet installationen af **AVG Internet-sikkerhed 2012**, kan du registrere produktet online på AVG-webstedet (http://www.avg.com/). Efter registreringen kan du få fuld adgang til din AVG-brugerkonto, nyhedsbrevet AVG Update og andre tjenester, der leveres eksklusivt til registrerede brugere.

Den nemmeste måde at registrere på er direkte i brugergrænsefladen i **AVG Internet-sikkerhed 2012**. Markér indstillingen Hjælp/Registrer nu i hovedmenuen. Du omdirigeres til siden ***Registrering*** på AVG-webstedet (http://www.avg.com/). Følg de instruktioner, der er angivet på siden.

4.2. Adgang til brugergrænseflade

Der er adgang til AVG-hoveddialogen 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 2012/AVG Brugergrænseflade***

4.3. 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 2012**. 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.

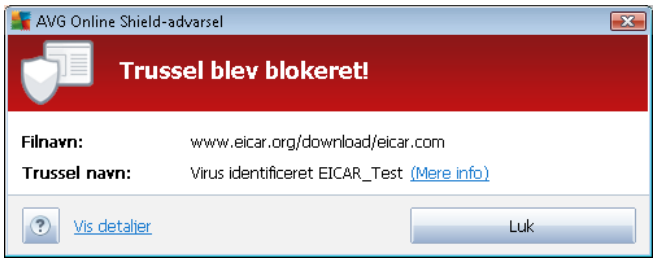
4.4. Eicar-test

For at bekræfte, at **AVG Internet-sikkerhed 2012** 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. Når du har bekræftet download af testfilen, vil Online Shield, (*som er en del af Linkscanner-komponenten*) reagere på den 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 giver dig mulighed for at downloade denne fil og gemme den på dit lokale drev, men Resident Shield (*i Anti-virus-komponenten*) detekterer "virussen", mens du forsøger at pakke den ud.

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

4.5. AVG standardkonfiguration

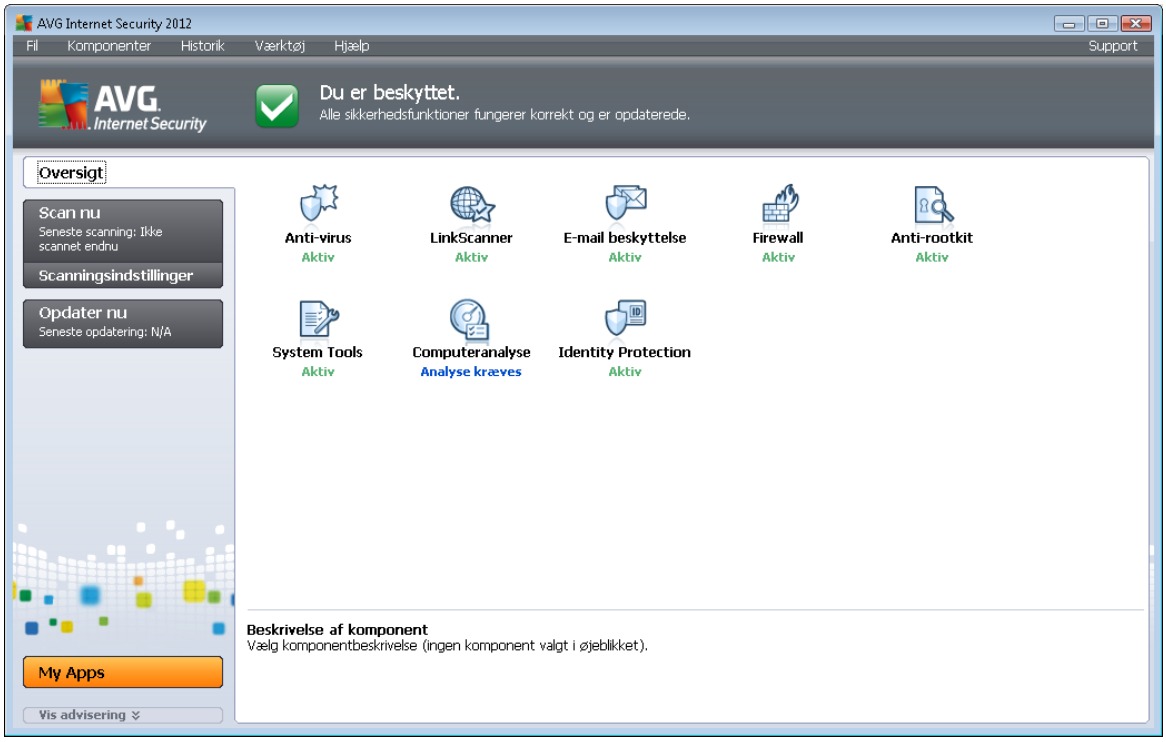
Standardkonfigurationen (*dvs. hvordan applikationen er sat op umiddelbart efter installationen*) af **AVG Internet-sikkerhed 2012** er konfigureret af softwareleverandøren, så alle komponenter og funktioner er indstillet til at opnå optimal ydelse.

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.

5. AVG-brugerflade

AVG Internet-sikkerhed 2012 åbner med hovedvinduet:



Hovedvinduet er opdelt i flere sektioner:

- ***Systemmenu*** *(øverste systemlinje i vinduet)* er standardnavigationen, som giver dig adgang til alle komponenter, tjenester og funktioner til **AVG Internet-sikkerhed 2012** – detaljer >>
- ***Info om sikkerhedsstatus*** *(øverste del af vinduet)* giver dig oplysninger om den aktuelle status for **AVG Internet-sikkerhed 2012** – detaljer >>
- ***Hurtige links*** *(venstre del af vinduet)* giver dig mulighed for at få adgang til de opgaver, som er de vigtigste og hyppigst anvendte af **AVG Internet-sikkerhed 2012** – detaljer >>
- ***My Apps*** *(nederste venstre del af vinduet)* åbner en oversigt over flere tilgængelige applikationer til **AVG Internet-sikkerhed 2012**: LiveKive, Familiesikkerhed og PC Tuneup
- ***Komponentoversigt*** *(midterste del af vinduet)* giver en oversigt over alle de komponenter, der er installeret i **AVG Internet-sikkerhed 2012** – detaljer >>
- ***Systembakkeikon*** *(nederste højre hjørne af skærmen i systembakken)* indikerer den aktuelle status for **AVG Internet-sikkerhed 2012** – detaljer >>
- ***AVG-gadget*** *(Windows-sidepanel, understøttet i Windows Vista/7)* giver hurtig adgang til scanning og opdatering i **AVG Internet-sikkerhed 2012** – detaljer >>

5.1. Systemmenuen

Systemmenuen er standardnavigationen, der anvendes i alle Windows-applikationer. Den er placeret vandret i øverste del af hovedvinduet **AVG Internet-sikkerhed 2012**. Brug systemmenuen til at få adgang til specifikke komponenter, funktioner og tjenester i AVG.

Systemmenuen er opdelt i fem hovedsektioner:

5.1.1. Fil

- ***Afslut*** - lukker **AVG Internet-sikkerhed 2012**'s brugergrænseflade. AVG-applikationen fortsætter med at køre i baggrunden, og din computer er stadigvæk beskyttet!

5.1.2. 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*** detekter virus, spyware, orme, trojanske heste, uønskede eksekverbare filer eller biblioteker i dit system og beskytter dig mod skadelig adware – detaljer >>
- ***Linkscanner*** beskytter dig mod webbaserede angreb, mens du søger og surfer på nettet – detaljer >>
- ***E-mail-beskyttelse*** kontrollerer dine indgående e-mail-meddelelser for SPAM og blokerer virus, phishing-angreb eller andre trusler – detaljer >>
- ***Firewall*** kontrollerer al kommunikation på netværksportene, beskytter dig mod skadelige angreb og blokerer alle forsøg på indtrængen – detaljer >>
- ***Anti-rootkit*** scanner for farlige rootkits, som er skjult inde i applikationer, drivere eller biblioteker – detaljer >>
- ***Systemværktøjer*** indeholder en detaljeret sammenfatning af AVG-miljøet og operativsystemoplysninger - detaljer >>
- ***Computeranalyse*** giver oplysninger om computerens status - detaljer >>
- ***Identitetsbeskyttelse*** beskytter hele tiden dine digitale aktiver mod nye og ukendte trusler – 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

5.1.3. 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
- Detektering af e-mailscanner – Åbner en dialog med en oversigt over vedhæftede filer i e-mail-meddelelser, som er detekteret som farlige af komponenten E-mail-beskyttelse
- Online Shield-fund – Åbner en dialog med en oversigt over de trusler, der er registeret af tjenesten Online Shield i komponenten LinkScanner
- 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 2012**-handlinger
- Firewall - åbner Firewall-indstillingsinterfacet på fanen Logge med en detaljeret oversigt over alle Firewall-handlinger

5.1.4. Værktøj

- Scan computer - skifter til AVG scanningsgrænseflade og starter en scanning af hele computeren.
- Scan valgt mappe... – Skifter til AVG-scanningsgrænsefladen og gør det muligt at definere inden for computerens træstruktur, hvilke filer og mapper der skal scannes.
- Scan fil... – Gør det muligt efter behov at køre en test på en fil, der er valgt via diskens træstruktur.
- Opdater - starter automatisk opdateringsprocessen for **AVG Internet-sikkerhed 2012**.
- ***Opdater fra mappe...*** – kører opdateringsprocessen fra de opdateringsfiler, der er placeret i en angiven mappe på den 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 Avancerede AVG-indstillinger, hvor du kan redigere AVG Internet-sikkerhed 2012 konfigurationen. Generelt anbefales det at bevare standardindstillingerne for applikationen, der er definerede af softwareleverandøren.
- Firewall-indstillinger... – Åbn en selvstændig dialog til avanceret konfiguration for Firewall-komponenten.

5.1.5. Hjælp

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

- ***Få hjælp online*** – Åbner AVG-webstedet (http://www.avg.com/) på midtersiden under kundesupport

- ***Dit AVG-internet*** – Åbner AVG-webstedet (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-webstedet (http://www.avg.com/). Angiv dine registreringsdata. Det er kun kunder, der registrerer deres AVG-produkt, som kan få gratis teknisk support.

Bemærk*: Hvis du bruger en prøveversion af* **AVG Internet-sikkerhed 2012***, 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 2012** *er installeret med et salgsnummer, vises elementerne som* ***Registrér*** *og* ***Aktivér****.*

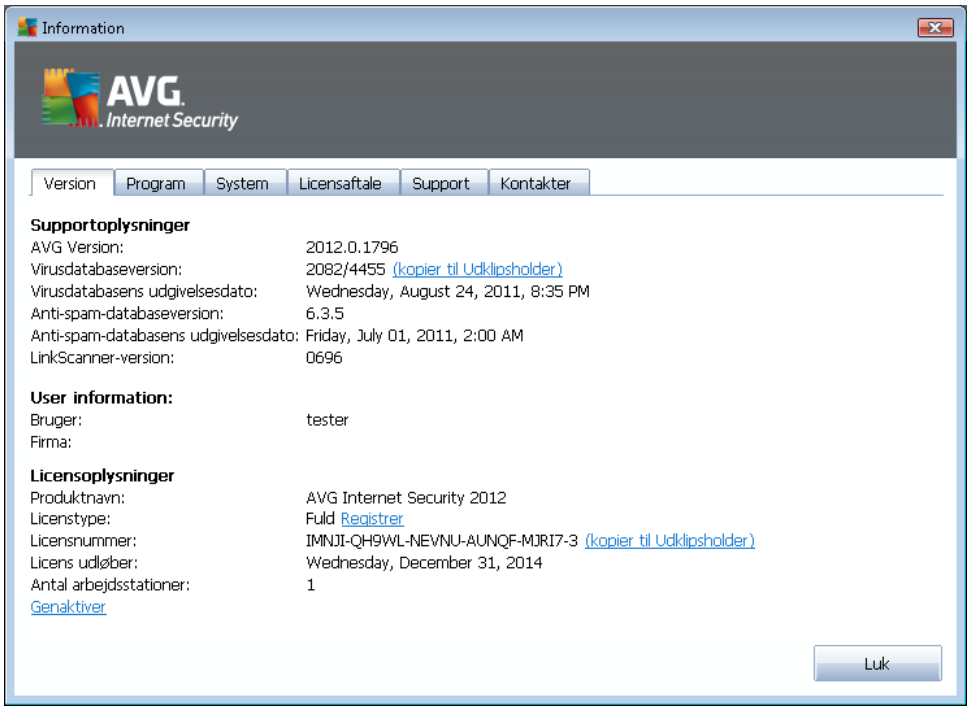
- ***Om AVG*** - åbner dialogen ***Information*** med fem faner, der indeholder data om programnavn, program- og virusdatabaseversion, systemoplysninger, licensaftale og kontaktoplysninger for ***AVG Technologies CZ***.

5.1.6. Support

Linket ***Support*** åbner en ny dialog ***Information***, som indeholder alle typer oplysninger, der kan være nødvendige, når du forsøger at få hjælp. Dialogen indeholder grundlæggende data om det installerede AVG-program (*program/databaseversion*), licensoplysninger og en liste over lynlink til support.

Dialogen ***Information*** er inddelt i seks faner:

Fanen ***Version*** er inddelt i tre sektioner:

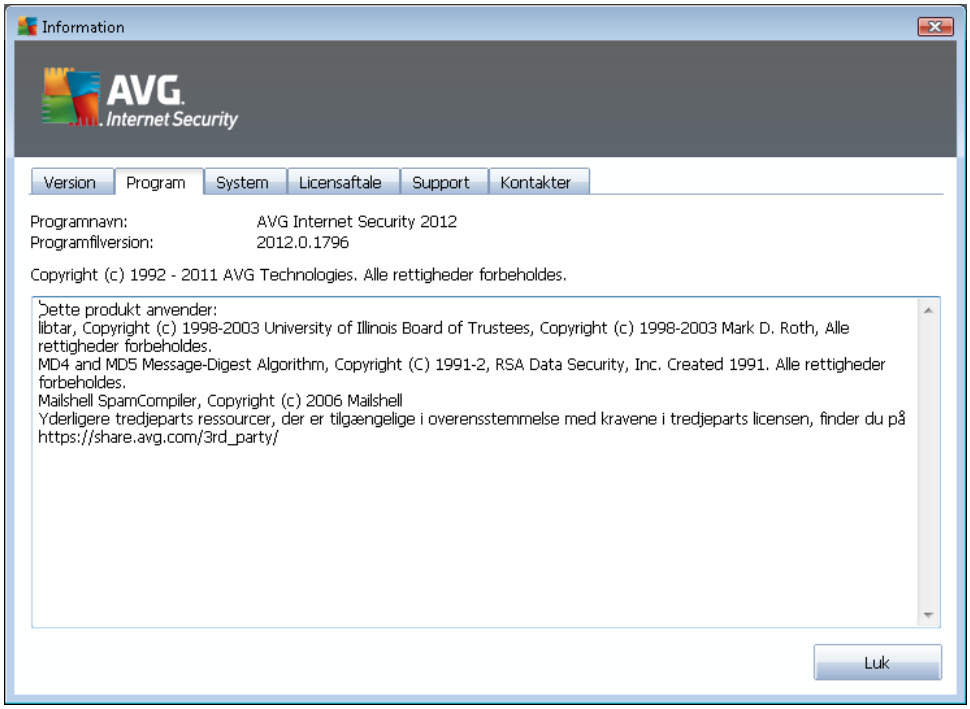


- ***Supportinformation*** – Angiver oplysninger, om **AVG Internet-sikkerhed 2012** versionen, virusdatabaseversionen, Anti-Spam-databaseversionen og LinkScanner-versionen.

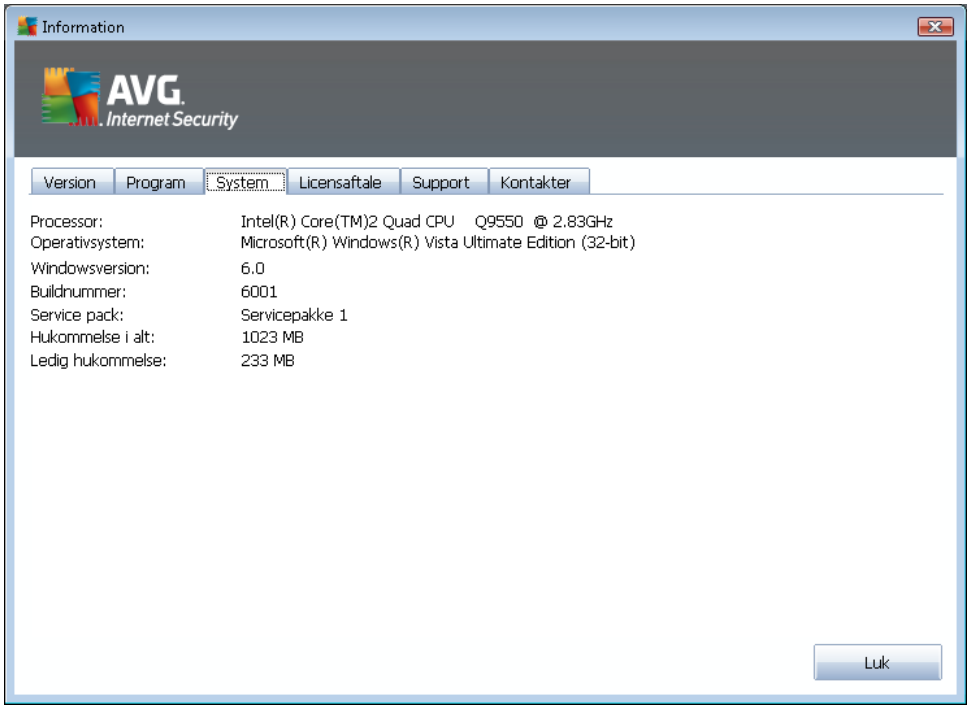
- ***Brugeroplysninger*** – Angiver oplysninger om den licenserede bruger og virksomhed.

- ***Licensoplysninger*** – Angiver oplysninger om licensen *(produktnavn, licenstype, licensnummer, udløbsdato og antal pladser*). I denne sektion kan du bruge bruge linket ***Registrer*** til at registrere dig **AVG Internet-sikkerhed 2012** online. Det vil give dig mulighed for at bruge AVG's tekniske support i fuldt omfang. Brug også linket ***Genaktiver*** for at åbne dialogen ***Aktivér AVG***: Angiv licensnummeret i det relevante felt for enten at udskifte salgsnummeret *(som du bruger under AVG Internet-sikkerhed 2012 installationen)*, eller hvis du vil ændre det aktuelle licensnummer for et andet*(f.eks. når du opgraderer til et senere AVG-produkt).*

Under fanen ***Program*** kan du finde oplysninger om filversionen af **AVG Internet-sikkerhed 2012**-programmet og om tredjepartskode, der anvendes i produktet:

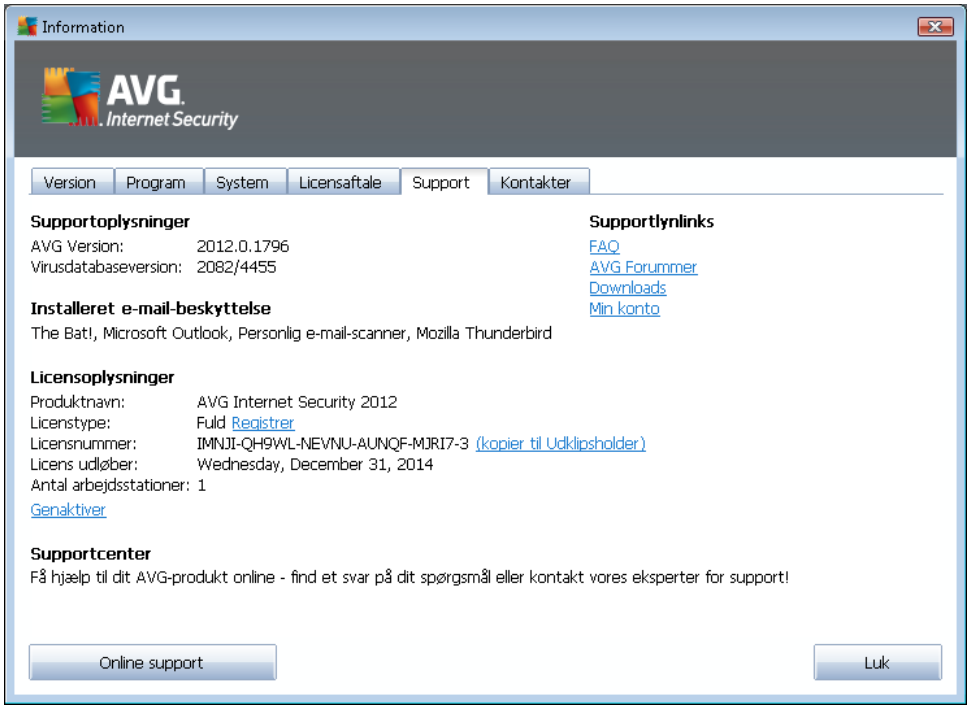


Fanen ***System*** indeholder en liste over parametre for dit operativsystem *(processortype, operativsystem og dets version, build-nummer, anvendte servicepakker, samlet størrelse på hukommelsen og størrelse på den ledige hukommelse)*:

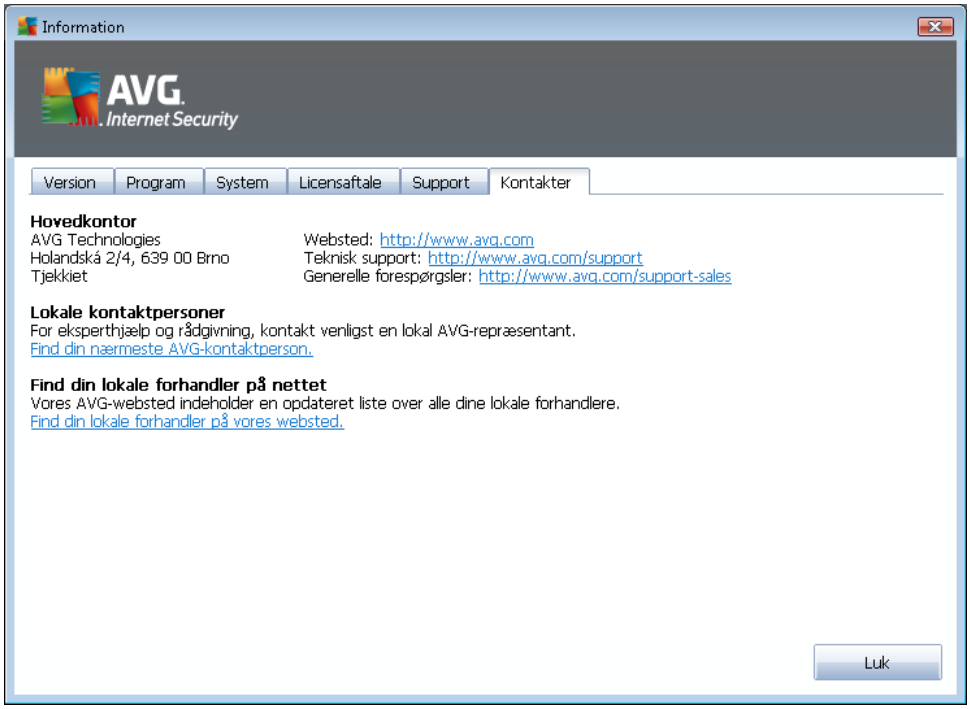


Under fanen ***Licensaftale*** kan du læse hele teksten i den licensaftale, der er indgået mellem dig og AVG Technologies:

Fanen ***Support*** indeholder en liste over alle mulighederne for at kontakte kundesupporten. Den indeholder også links til AVG-webstedet (http://www.avg.com/), AVG-grupper, FAQ... Derudover kan du finde oplysninger, som du måske kan få brug for, når du kontakter kundesupportteamet:



Fanen ***Kontakter*** indeholder en liste over alle kontakter i AVG Technologies samt kontakter til AVG-sælgere og -forhandlere:



5.2. Info om sikkerhedsstatus

Afsnittet ***Info om sikkerhedsstatus*** er placeret i den øverste del af hovedvinduet i **AVG Internet-sikkerhed 2012**. I denne sektion kan du altid finde oplysninger om den aktuelle sikkerhedsstatus for **AVG Internet-sikkerhed 2012**. Herunder er en oversigt over ikoner, der kan være afbilledet i denne sektion, og deres betydning:

 - Det grønne ikon angiver, at din ***AVG Internet-sikkerhed 2012 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 Internet-sikkerhed 2012**, og du har sandsynligvis besluttet at deaktivere en komponent af en eller anden årsag. Du er stadig beskyttet! Vær dog opmærksom på indstillingerne i den pågældende komponent! Dens navn er angivet i sektionen ***Info om sikkerhedsstatus***.

Det orange ikon vises, hvis du af en eller anden årsag har besluttet dig for at ignorere en komponents fejlstatus. Indstillingen ***Ignorer komponenttilstand*** er tilgængelig fra kontekstmenuen (*åbnes ved at højreklikke med musen*) over ikonet for den relevante

komponent i Komponentoversigt i hovedvinduet i **AVG Internet-sikkerhed 2012**. Vælg denne indstilling for at angive, at du er klar over komponentens fejltilstand, men at du af en eller anden årsag ønsker at beholde **AVG Internet-sikkerhed 2012** på denne måde, og at du ikke ønsker at få en advarsel via systembakkeikonet. Det kan være nødvendigt at bruge denne indstilling i en bestemt situation, men det anbefales på det kraftigste, at du hurtigst muligt slår indstillingen ***Ignorer komponenttilstand*** fra.

 - Det røde ikon angiver, at ***AVG Internet-sikkerhed 2012 er i kritisk status***! En eller flere komponenter fungerer ikke korrekt og **AVG Internet-sikkerhed 2012** 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 Internet-sikkerhed 2012 ikke er indstillet til optimal ydelse, vises den nye knap Reparer (og ellers Reparer alle, hvis problemet gælder mere end én komponent) ud for oplysningerne om sikkerhedsstatussen. Tryk på knappen for at starte en automatisk kørsel af programgennemsyn og konfiguration. Dette er en nem måde at indstille AVG Internet-sikkerhed 2012 på, så du opnår den bedst mulige ydelse og får 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 Internet-sikkerhed 2012's statusinformation kan til enhver tid også findes vha. systembakkeikonet.*

5.3. Lynlink

Lynklinks er placeret i venstre side af grænsefladen i **AVG Internet-sikkerhed 2012**. Disse links giver øjeblikkelig adgang til de vigtigste og oftest anvendte funktioner i applikationen, dvs. scanning og opdatering. Lynlinkene er tilgængelige i alle dialoger i brugergrænsefladen:

Lynlinks er rent grafisk inddelt i tre sektioner:

- ***Oversigt*** – Brug dette link til at skifte fra en åbnet AVG-dialog til standardvinduet, hvor der er en oversigt over alle installerede komponenter. *(Du kan få flere oplysninger i kapitlet Komponentoversigt)*
- ***Scan nu*** – Denne knap giver som standard oplysninger om den seneste scanningsstart *(dvs. scanningstype og dato for seneste scanning)*. Klik på kommandoen ***Scan nu*** for at

starte scanningen igen. Hvis du vil starte en anden scanning, kan du klikke på linket ***Scanningsindstillinger***. På den måde kan du åbne AVG's scanningsgrænseflade, hvor du kan køre scanninger, planlægge scanninger eller redigere deres parametre. *(Du kan få flere oplysninger i kapitlet AVG-scanning)*

- ***Opdater nu*** – Dette link indeholder dato og klokkeslæt for den seneste start af opdatering. Tryk på knappen for at køre opdateringsprocessen automatisk, og følg statussen på den. *(Du kan få flere oplysninger i kapitlet AVG-opdateringer)*

Lynlinks er altid tilgængelige i AVG-brugergrænsefladen. Når du bruger et lynklink til at køre en bestemt proces, det være sig en scanning eller en opdatering, skifter applikationen til en ny dialog, men alle lynlinkene er stadig tilgængelige. Derudover er kørselsprocessen yderligere illustreret grafisk i navigationen, så du har fuld kontrol over allerede startede processer, der kører i **AVG Internet-sikkerhed 2012** i øjeblikket.

5.4. Komponentoversigt

Sektionen Komponentoversigt

Sektionen ***Komponentoversigt*** er placeret midt på **AVG Internet-sikkerhed 2012** - brugergrænsefladen. Sektionen består af to dele:

- ***Oversigt over alle installerede komponenter*** – Består af grafiske paneler for alle installerede komponenter. Alle paneler er mærket med komponentens ikon samt oplysninger om, hvorvidt den respektive komponent er aktiv eller inaktiv for øjeblikket.

- ***Komponentbeskrivelse*** er placeret i nederste del af dialogen. Beskrivelsen angiver kort komponentens grundlæggende funktioner. Den angiver også oplysningerne om den aktuelle status for den valgte komponent.

Liste over installerede komponenter

I **AVG Internet-sikkerhed 2012** indeholder sektionen ***Komponentoversigt*** oplysninger om følgende komponenter:

- ***Anti-virus*** detekter virus, spyware, orme, trojanske heste, uønskede eksekverbare filer eller biblioteker i dit system og beskytter dig mod skadelig adware – detaljer >>

- ***Link Scanner*** beskytter dig mod webbaserede angreb, mens du søger og surfer på nettet – detaljer >>

- ***E-mail-beskyttelse*** kontrollerer dine indgående e-mail-meddelelser for SPAM og blokerer virus, phishing-angreb eller andre trusler – detaljer >>

- ***Firewall*** kontrollerer al kommunikation på netværksportene, beskytter dig mod skadelige angreb og blokerer alle forsøg på indtrængen– detaljer >>

- ***Anti-rootkit*** scanner for farlige rootkits, som er skjult inde i applikationer, drivere eller

biblioteker – detaljer >>

- ***Systemværktøjer*** indeholder en detaljeret sammenfatning af AVG-miljøet og operativsystemoplysninger - detaljer >>
- ***Computeranalyse*** giver oplysninger om computerens status - detaljer >>
- ***Identitetsbeskyttelse*** beskytter hele tiden dine digitale aktiver mod nye og ukendte trusler – detaljer >>
- ***Sikkerhedsværktøjslinje*** lader dig bruge valgte AVG-funktioner direkte fra din webbrowser - detaljer >>

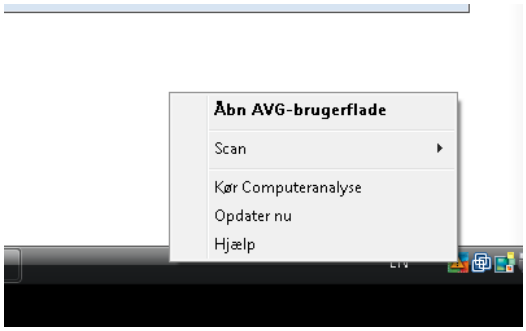
- ***Ekstern administration*** vises kun i AVG Business Editions, hvis du i løbet af installationsprocessen angav, at du ønskede denne komponent installeret

Tilgængelige handlinger

- ***Hold musen over et komponentikon*** for at fremhæve det i komponentoversigten. Samtidig vises komponentens grundlæggende funktioner i nederste del af brugergrænsefladen.
- ***Enkeltklik på et komponentikon*** for at åbne komponentens egen grænseflade med en liste over grundlæggende statistiske data.
- ***Højreklik med musen på et komponentikon*** for at udvide en kontekstmenu med flere valgmuligheder:
  - ***Åbn*** – Klik på denne valgmulighed for at åbne komponentens egen dialog *(med enkeltklik som på komponentikonet)*.
  - ***Ignorer komponentens tilstand*** – Vælg denne indstilling for at tilkendegive, at du er opmærksom på komponentens fejltilstand, men af en eller anden grund ønsker at beholde denne status, og at du ønsker ikke at blive advaret af systembakkeikonet.
  - ***Åbn i Avancerede indstillinger ...*** – Denne valgmulighed er kun tilgængelig for enkelte komponenter, f.eks. dem, der har muligheden for avancerede indstillinger.

5.5. Systembakkeikon

AVG-systembakkeikonet *(højreklik på systembakken i Windows i bunden af skærmen)* angiver den aktuelle status for **AVG Internet-sikkerhed 2012**. Det er altid synlig på systembakken, uanset om grænsefladen i **AVG Internet-sikkerhed 2012** er åbnet eller lukket:



Visning af AVG-systembakkeikon

- Hvis ikonet er i fuld farve og uden ekstra elementer, angiver det, at alle **AVG Internet-sikkerhed 2012**-komponenterne er aktive og fuldt funktionsdygtige. Dette ikon kan imidlertid også vises på denne måde i en situation, hvor en af komponenterne ikke virker helt, men brugeren har besluttet at ignorere komponenttilstanden. *(Hvis du bekræfter, at indstillingen for komponenttilstanden skal ignoreres, angiver du, at du er bevidst om komponentens fejltilstand, men at du af eller anden årsag ikke ønsker at blive advaret om situationen.)*

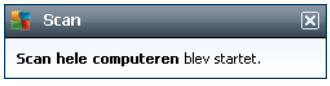
- Ikonet med et udråbstegn angiver, at en komponent *(eller endda flere komponenter)* er i en fejltilstand. Vær altid opmærksom på en sådan advarsel, og forsøg at fjerne konfigurationsproblemet for en komponent, som ikke er indstillet korrekt. Hvis du vil foretage ændringer i konfigurationen af komponenten, skal du dobbeltklikke på systembakkeikonet for åbne applikationens brugergrænseflade. Du kan få detaljerede oplysninger om, hvilke komponenter der er i fejltilstanden ved at se i afsnittet med oplysninger om sikkerhedsstatussen.

- systembakkeikonet kan derudover vises i fuld farve med blinkende og roterende lysstråle. Denne grafiske version signalerer en opdateringsproces, der startes i øjeblikket.

- Den alternative visning af et ikon i fuld farve med en pil betyder blot, at der køres **AVG Internet-sikkerhed 2012**-scanninger.

Oplysninger om AVG-systembakkeikonet

AVG-systembakkeikon oplyser derudover om aktuelle aktiviteter i dit **AVG Internet-sikkerhed 2012** og mulige statusændringer i programmet (*f.eks. automatisk start af en planlagt scanning eller opdatering, Firewall-profilskift, en komponents statusændring, hændelse med statusfejl ...*) via et pop op-vindue, der åbnes fra systembakkeikonet:



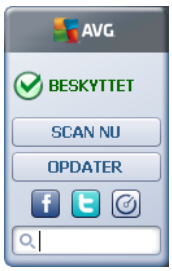
Handlinger, der er tilgængelige fra AVG-systembakkeikonet

AVG-systembakkeikon kan også bruges som et lynlink til at få adgang til brugergrænsefladen i **AVG Internet-sikkerhed 2012**. Du skal blot dobbeltklikke på ikonet. Hvis du højreklikker på ikonet, åbner du en kort kontekstafhængig menu med følgende indstillinger:

- ***Åbn AVG's brugergrænseflade*** – Klik for at åbne brugergrænsefladen i **AVG Internet-sikkerhed 2012**.
- ***Scanninger*** – Klik for at åbne kontekstmenuen for foruddefinerede scanninger (*Fuld computerscanning*, *Scanning af specifikke filer eller mapper*, *Anti-Rootkit-scanning*), og vælg den krævede scanning, som startes med det samme.
- ***Firewall*** – Klik her for at åbne kontekstmenuen for Firewall-indstillinger, hvor du kan redigere de vigtigste parametre: Firewallstatus (*Firewall aktiveret/Firewall deaktiveret/ Nødtilstand*), skift til gamertilstand og Firewall-profiler.
- ***Kør Computeranalyse*** – Klik for at starte komponenten Computeranalyse.
- ***Kører scanninger*** – Denne indstilling vises kun, hvis der i øjeblikket køres en scanning 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*** – Starter øjeblikket en opdatering.
- ***Hjælp*** – Åbner hjælpfilen på startsiden.

5.6. 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 2012**-funktioner, dvs. scanning og opdatering**:**



Hurtig adgang til scanning og opdatering

Hvis det er nødvendigt, giver ***AVG-gadget*** dig mulighed for at foretage en akut scanning eller opdatering

- ***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)*.

- ***Opdater nu*** – Klik på linket ***Opdater nu*** for at starte **AVG Internet-sikkerhed 2012** opdateringen direkte i gadgeten:

Adgang til sociale netværk

AVG-gadget har også et hurtig link, der giver dig forbindelse til de store sociale netværk. Brug de respektive knapper til at få forbindelse til AVG-grupper i Twitter, på Facebook eller LinkedIn:

- ***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

Andre tilgængelige funktioner via gadget

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

6. AVG Komponenter

6.1. Anti-virus

Anti-virus-komponenten er en grundsten i **AVG Internet-sikkerhed 2012** , og den kombinerer flere grundlæggende funktioner i et sikkerhedsprogram:

- Scanning-engine
- Indbygget beskyttelse
- Anti-spyware beskyttelse

6.1.1. Scanningsprogram

Scanningsprogrammet, som er grundlaget for ***Anti-Virus***-komponenten, scanner alle filer og al filaktivitet *(åbning/lukning af filer osv.)*for kendte vira. Alle detekterede virusser blokeres, så de ikke kan gøre noget, og renses derefter eller sættes i karantæne i Virus Vault.

Den vigtige funktion i AVG Internet-sikkerhed 2012-beskyttelsen er, at ingen kendte virus kan køre på computeren!

Detekteringsmetoder

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. ***Anti-Virus*** anvender følgende detekteringsmetoder:

- 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

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. **AVG Internet-sikkerhed 2012** kan også analysere og detektere eksekverbare applikationer eller DLL-biblioteker, der potentielt set kunne være uønsket i systemet. Vi kalder trusler for Potentielt uønskede programmer *(forskellige former for spyware, adware osv.)*. Derudover scanner **AVG Internet-sikkerhed 2012** systemets registreringsdatabase for mistænkelige poster, midlertidige internetfiler og sporingscookies og gør det muligt at behandle alle potentielt skadelige elementer på samme måde som alle andre infektioner.

AVG Internet-sikkerhed 2012 giver en uafbrudt beskyttelse af computeren!

6.1.2. Indbygget beskyttelse

AVG Internet-sikkerhed 2012 giver en løbende beskyttelse i form af en såkaldt indbygget beskyttelse. Komponenten ***Anti-Virus*** scanner alle filer *(med bestemte filtypenavne eller helt uden filtypenavne)*, der åbnes, gemmes eller kopieres. Det beskytter systemområderne i computeren samt flytbare medier (*flash-diske osv.*). Hvis der registreres en virus i en fil, der åbnes, stopper programmet handlingen, der udføres i øjeblikket, og forhindrer, at virussen kan aktivere sig selv. Normalt ville du ikke en gang bemærke processen, da den integrerede beskyttelse kører "i baggrunden". Du får kun besked, når der registreres trusler. Samtidigt blokerer ***Anti-Virus*** for aktivering af truslen og fjerner den.

Den indbyggede beskyttelse indlæses i hukommelsen i computeren under start, og det er vigtigt, at den er aktiveret hele tiden!

6.1.3. Anti-spyware beskyttelse

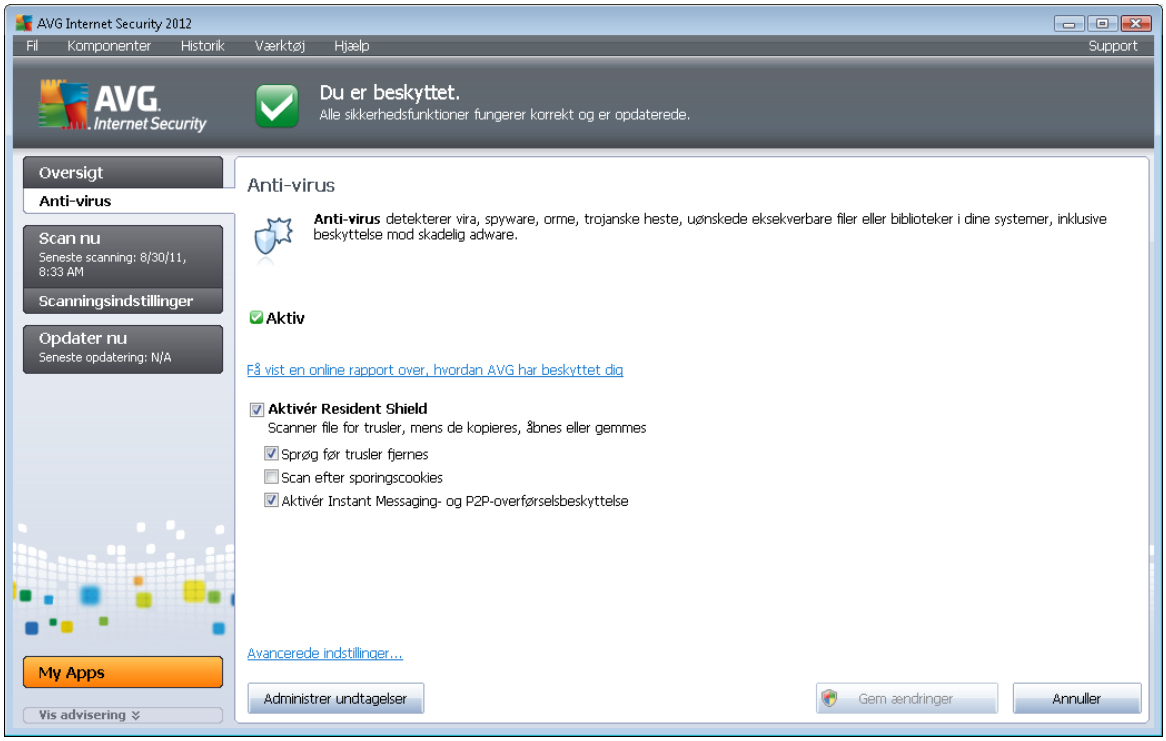
Anti-spyware består af en spywaredatabase, som bruges til at identificere kendte typer af spywaredefinitioner. AVG's spywareeksperter arbejder hårdt med at identificere og beskrive de nyeste spywaremønstre, så snart de dukker op, og derefter tilføje definitioner til databasen. Via opdateringsprocessen bliver de nye definitioner downloadet til din computer, så du altid er pålideligt beskyttet mod de nyeste spywaretyper. ***Anti-spyware*** giver dig mulighed for at scanne din computer for malware/spyware. Den detekterer også sovende og inaktiv malware, dvs. malware, der er downloadet men endnu ikke aktiveret.

Hvad er spyware?

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.

6.1.4. Anti-virus-grænseflade

Anti-virus-komponentens grænseflade giver kortfattede oplysninger om komponentens funktionalitet, oplysninger om komponentens aktuelle status *(aktiv)* og grundlæggende konfigurationsindstillinger for komponenten:



Konfigurationsindstillinger

Dialogen indeholder flere grundlæggende konfigurationsindstillinger for tilgængelige funktioner i komponenten ***Anti-virus***. Her kan du finde en kortfattet beskrivelse af disse:

- ***Se en onlinerapport om, hvordan AVG har beskyttet dig*** – Linket omdirigerer dig til en specifik side på AVG's websted (http://www.avg.com/). På siden kan du finde en detaljeret statistisk oversigt over alle de **AVG Internet-sikkerhed 2012** aktiviteter, der er udført på din computer inden for en specifik tidsperiode og samlet set.

- ***Aktivér Resident Shield*** – Denne indstilling giver dig mulighed for at slå indbygget beskyttelse til og fra. Resident Shield scanner filer, når de kopieres, åbnes eller gemmes. Når en virus eller enhver form for trussel detekteres, bliver du omgående advaret. Denne funktion er som standard slået til, og det anbefales, at du fortsætter med denne indstilling! Med indbygget beskyttelse slået til kan du yderligere beslutte, hvordan eventuelt detekterede infektioner skal behandles:

    - ***Fjern alle trusler automatisk*** / ***Spørg mig om lov til at fjerne trusler*** – Du kan også vælge en af disse indstillinger: Dette valg har ingen betydning for sikkerhedsniveauet og det afspejler kun, hvad du foretrækker.

    - ***Scan efter sporingscookies*** – Uafhængigt af de forrige indstillinger kan du beslutte, om du vil scanne efter sporingscookies. *(Cookies er 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.) I specifikke tilfælde kan du slå denne indstilling til for at opnå et maksimalt sikkerhedsniveau, men den er slået fra som standard.

- ***Aktivér Instant messaging-beskyttelse*** – Kontroller dette element, hvis du vil bekræfte, at kommunikationen i form af instant messaging(*f.eks. ICQ, MSN Messenger, ...*) er virusfri.

- ***Avancerede indstillinger***... – Klik på linket for at blive omdirigeret til den pågældende dialog i Avancerede indstillinger for **AVG Internet-sikkerhed 2012**. Her kan du redigere komponentens konfiguration indgående. Det er dog værd at bemærke, at standardkonfigurationen for alle komponenter er indstillet, så **AVG Internet-sikkerhed 2012** giver optimal ydelse og maksimal beskyttelse. Medmindre du har en god grund, anbefales det, at du beholder standardkonfigurationen!

Betjeningsknapper

I dialogen kan du bruge følgende kontrolknapper:

- ***Administrer undtagelser*** – Åbner en ny dialog ved navn Resident Shield – Undtagelser. Du kan også få adgang til dialogen fra hovedmenuen ved at gå til Avancerede indstillinger/Anti-virus/Resident Shield/Undtagelser *(se det pågældende kapitel for at få vist en detaljeret beskrivelse)*. I dialogen kan du angive filer og mapper, der skal udelades 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 *(eller mapper)*, der skal udelukkes fra scanningen, ved at vælge dem en ad gangen i navigationstræet for det lokale drev.

  - *Tilføj fil* – Angiv de filer, der skal udelukkes fra scanningen ved at vælge dem en ad gangen i navigationstræet for det lokale drev.

  - *Rediger element* – Giver dig mulighed for at redigere den angivne sti til en valgt fil eller mappe.

  - *Fjern element* – Giver dig mulighed for at fjerne stien til et valgt element på listen.

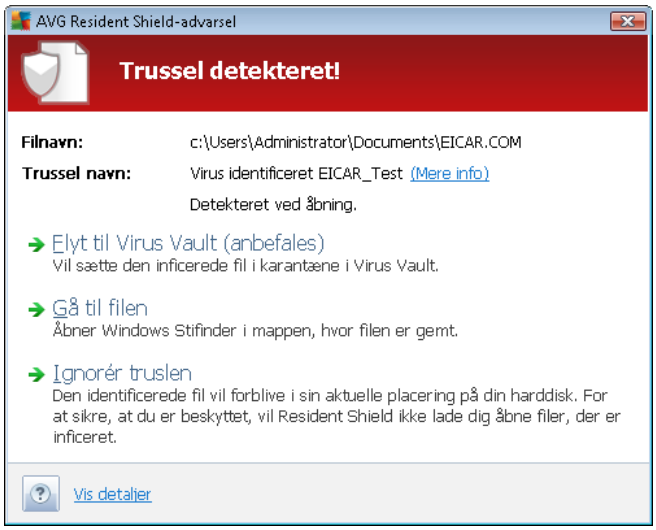
- ***Gem ændringer*** – Gem alle de ændringer af komponentens indstillinger, der er foretaget i denne dialog, og vend tilbage til brugergrænsefladen i **AVG Internet-sikkerhed 2012** (*Komponentoversigt*).

- ***Annuller*** – Afbryd alle ændringer af komponentens indstillinger i denne dialog. Der gemmes ingen ændringer. Du vender tilbage til brugergrænsefladen for **AVG Internet-sikkerhed 2012** (*Komponentoversigt*).

6.1.5. Resident Shield-opdagelser

Trussel detekteret!

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*).

Derudover skal du bestemme, hvilken handling der skal ske efterfølgende. Der er flere alternative indstillinger at vælge imellem. ***Bemærk, at ved særlige betingelser (hvilken type fil er inficeret, og hvor den er placeret), er ikke alle valgmulighederne altid tilgængelige!***

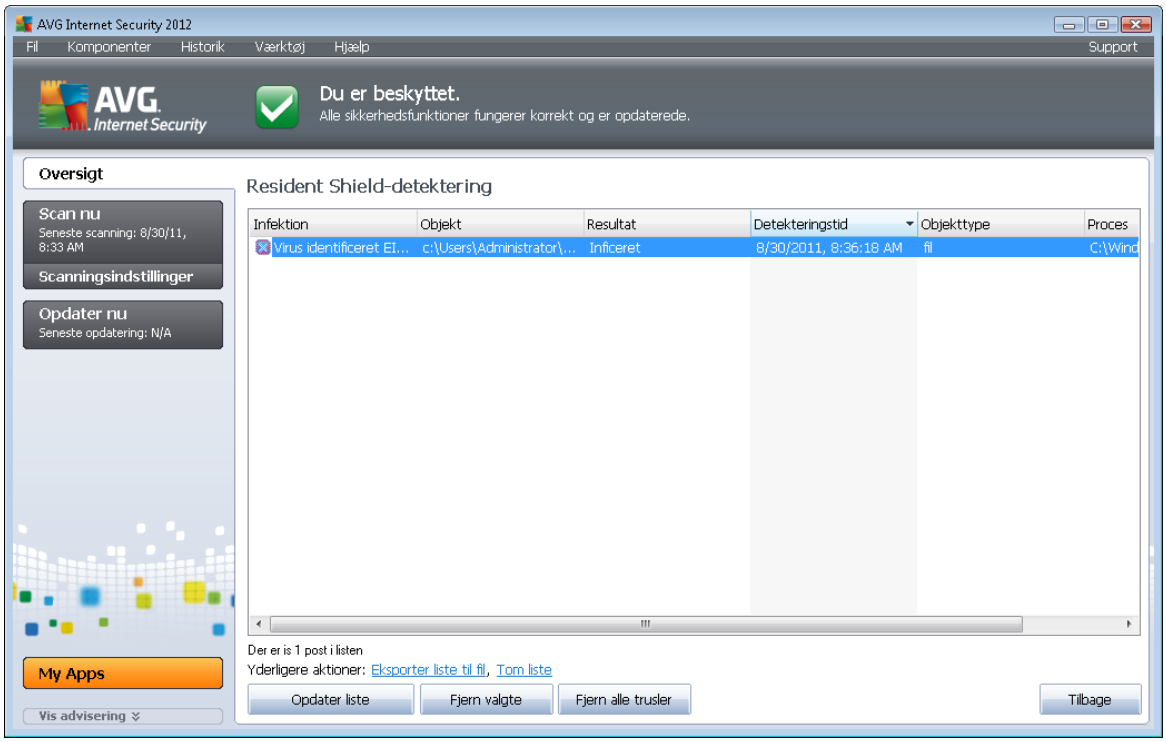
- ***Fjern trussel som superbruger*** - marker feltet, hvis du tror, at du muligvis ikke har tilstrækkelige rettigheder til at fjerne truslen som almindelig bruger. Superbrugere har udvidede adgangsrettigheder, og hvis truslen er placeret i en bestemt systemmappe, skal du muligvis bruge dette afkrydsningsfelt 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 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.

Oversigt over Resident Shield-registreringer

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***. Knappen ***Tilbage*** sender dig tilbage til den normaleAVG-hoveddialog (*Komponentoversigt*).

6.2. Linkscanner

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 er ikke beregnet til beskyttelse af serverplatforme!

Teknologien ***LinkScanner*** består af følgende hovedfunktioner:

- Søgeskjold indeholder en liste over websteder (URL-adresser), der er kendt som farlige. Når du søger med Google, Yahoo!, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask og Seznam, kontrolleres alle resultater ud fra denne liste, og der vises et vurderingsikon *(for Yahoo! søgeresultater viser kun resultatikonet "websted med exploit)*.

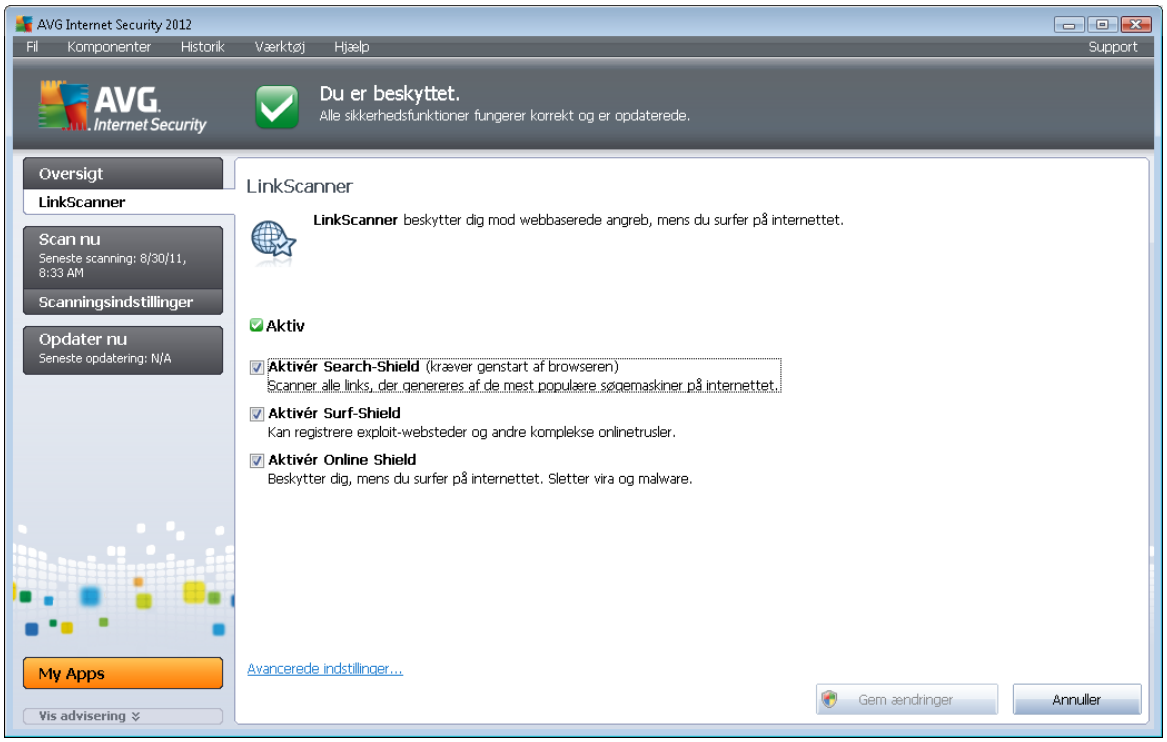
- Surfskjold scanner indholdet på de websteder, du besøger, uanset webstedets adresse. Selvom enkelte websteder ikke detekteres af Søgeskjold *(f.eks. når et nyt skadeligt websted oprettes, eller når et tidligere rent websted indeholder malware)*, bliver det detekteret og blokeret af Surfskjold, når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

- Online Shield fungerer som en realtidsbeskyttelse, når du surfer på internettet. Programmet scanner indholdet af besøgte websider samt de filer, der kan være på disse, og det sker endda før, de vises i webbrowseren eller overføres til computeren. Online Shield registrerer virus og spyware, der findes på den side, du er ved at besøge, og stopper overførslen med det samme, så der ikke kommer trusler over på computeren.

- ***AVG Accelerator***, som giver problemfri videoafspilning på nettet og gør det nemmere at foretage ekstra downloads. Når videoaccelerationen er i gang, får du besked via et pop op-vindue på systembakken.

6.2.1. Linkscanner-grænseflade

Komponenten LinkScanner s hoveddialog indeholder en kort beskrivelse af komponentens funktioner og oplysninger om dens aktuelle status *(aktiv)*:



I bunden af dialogen er der mulighed for en grundlæggende konfiguration af komponenten:

- ***Aktivér Søgeskjold*** – (*aktiveret som standard*): Fjern markeringen i afkrydsningsfeltet, hvis du har en god grund til at slå Søgeskjold-funktionen fra.
- ***Aktivér Surfskjold*** – (*aktiveret som standard*): Aktiver beskyttelse i (*realtid*) mod websteder med exploit-indhold, mens du forsøger at få adgang til dem. Kendte forbindelser til ondsindede websteder og deres exploitindhold blokeres, når de åbnes af brugeren via en webbrowser (*eller enhver anden applikation, der bruger HTTP*).
- ***Aktivér Online Shield*** – (*aktiveret som standard*): Realtidsscanning for virus eller spyware på websider, som du er ved at besøge. Hvis disse detekteres, stoppes overførslen med det samme, så der ikke kommer trusler over på computeren.

6.2.2. Detektering af 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 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*).

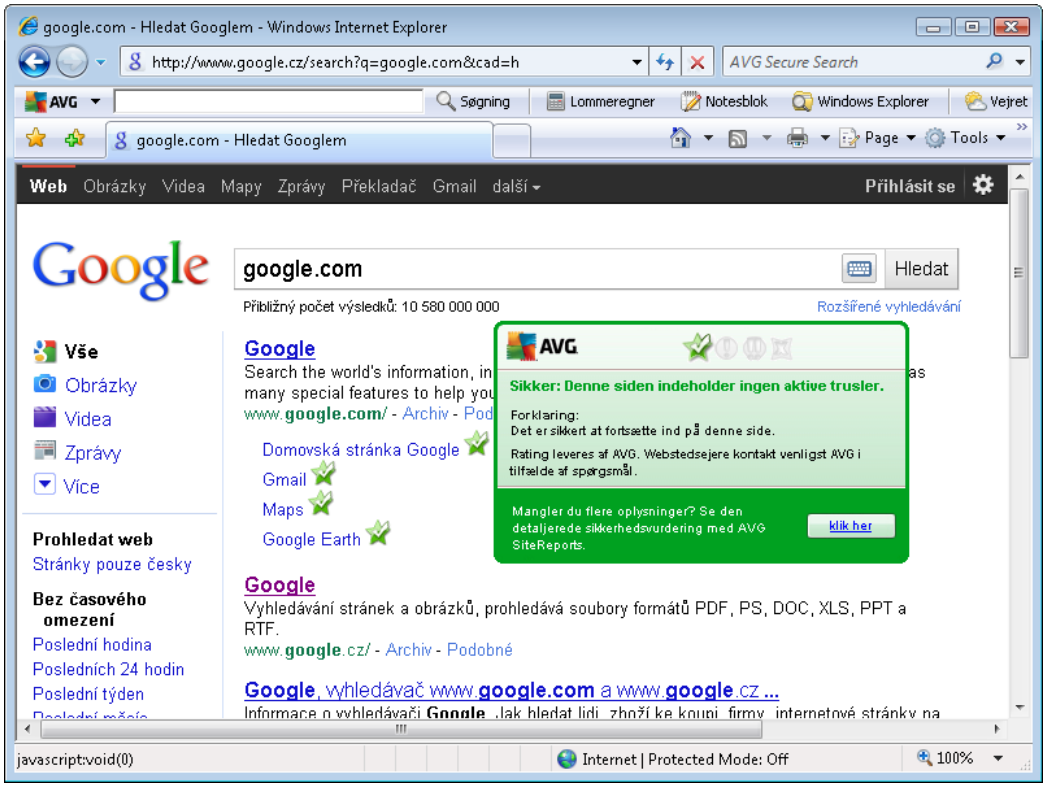
Siden, der linkes til, indeholder ingen trusler men er mistænkelig (*tvivlsom oprindelse eller motiv og anbefales derfor ikke til e-handel osv.*).

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.

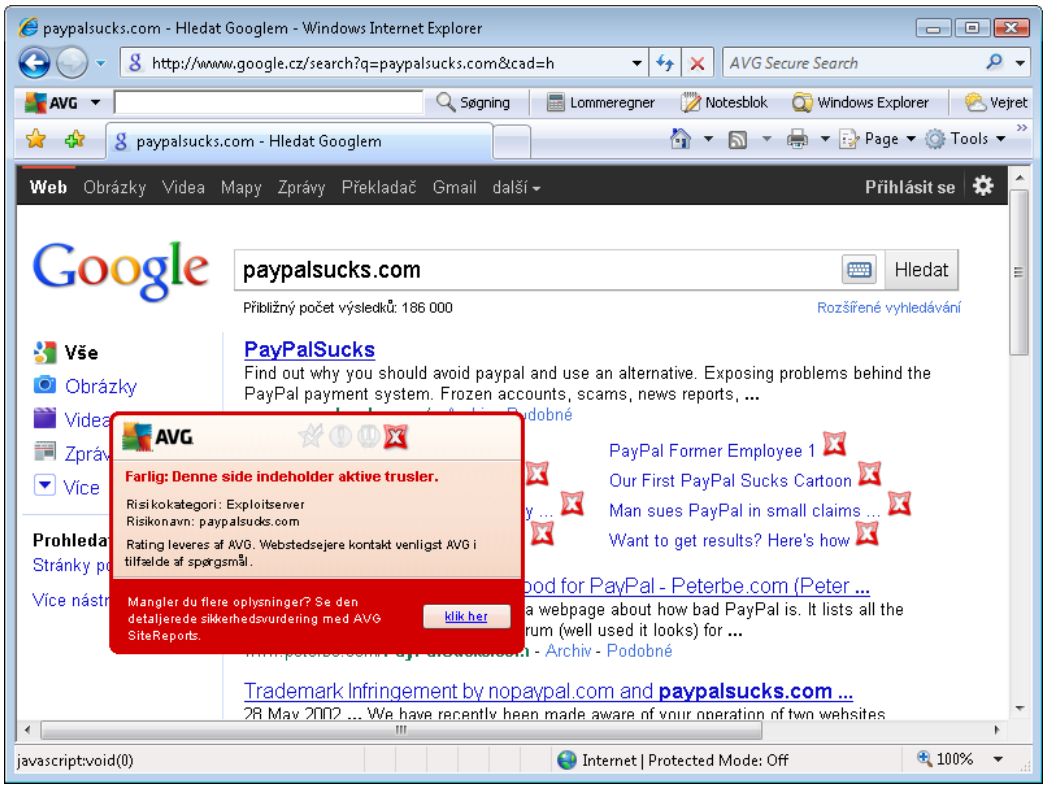
Hvis musen holdes over et individuelt ratingikon, vises detaljer om det pågældende link. Oplysninger omfatter yderligere oplysninger om truslen (*hvis der er nogen*):



6.2.3. Detektering af surfskjold

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

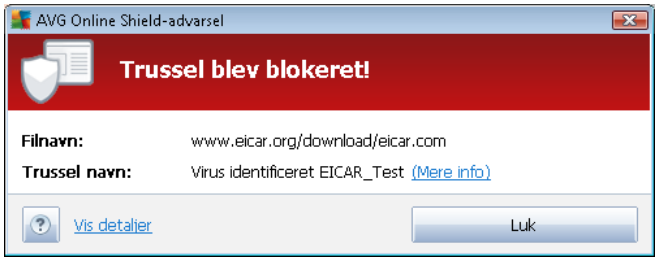
Hvis du støder på et ondsindet websted, vil Link Scanner advare dig i din webbrowser med et skærmbillede lignende dette:



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

6.2.4. Online Shield-detekteringer

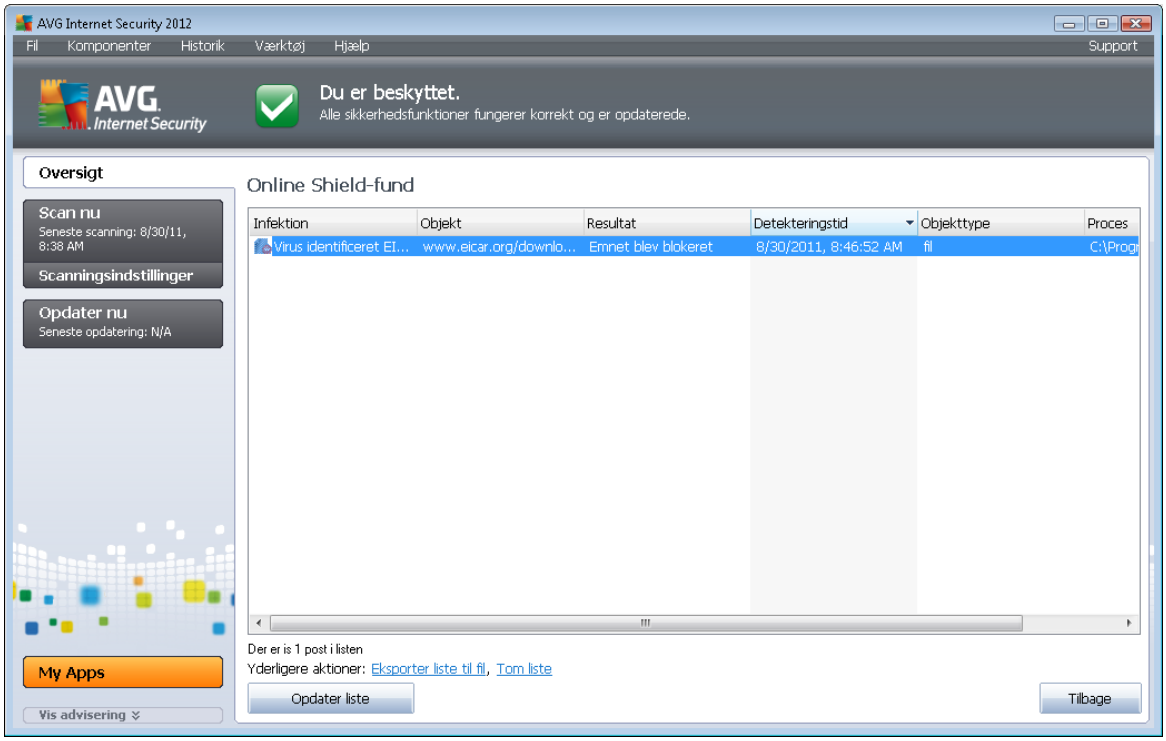
Online Shield scanner indholdet på besøgte websider og eventuelle filer på dem, før de vises i din webbrowser eller downloades til din computer. Hvis en trussel detekteres, bliver du omgående advaret med følgende dialog:



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***).

Betjeningsknapper

- ***Opdater liste*** – Opdaterer listen over resultater, der er registreret af ***Online Shield***
- ***Tilbage*** – Skifter tilbage til standard-AVG-hoveddialogen *(Komponentoversigt)*

6.3. E-mail beskyttelse

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.

Komponenten ***E-mail-beskyttelse*** tager sig af scanning af alle e-mail-meddelelser, der sendes eller modtages. Når en virus registreres i en e-mail, skal den med det samme flyttes til Virus Vault. Komponenten kan også frasortere visse typer vedhæftede filer i e-mails, og tilføje en certificeringstekst til infektionsfrie beskeder. ***E-mail-beskyttelse*** består af to hovedfunktioner:

- E-mail Scanner
- Anti-spam

6.3.1. E-mail-scanner

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 - 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 virus 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*).

E-mailscanneren er ikke beregnet til serverplatforme!

6.3.2. Anti-spam

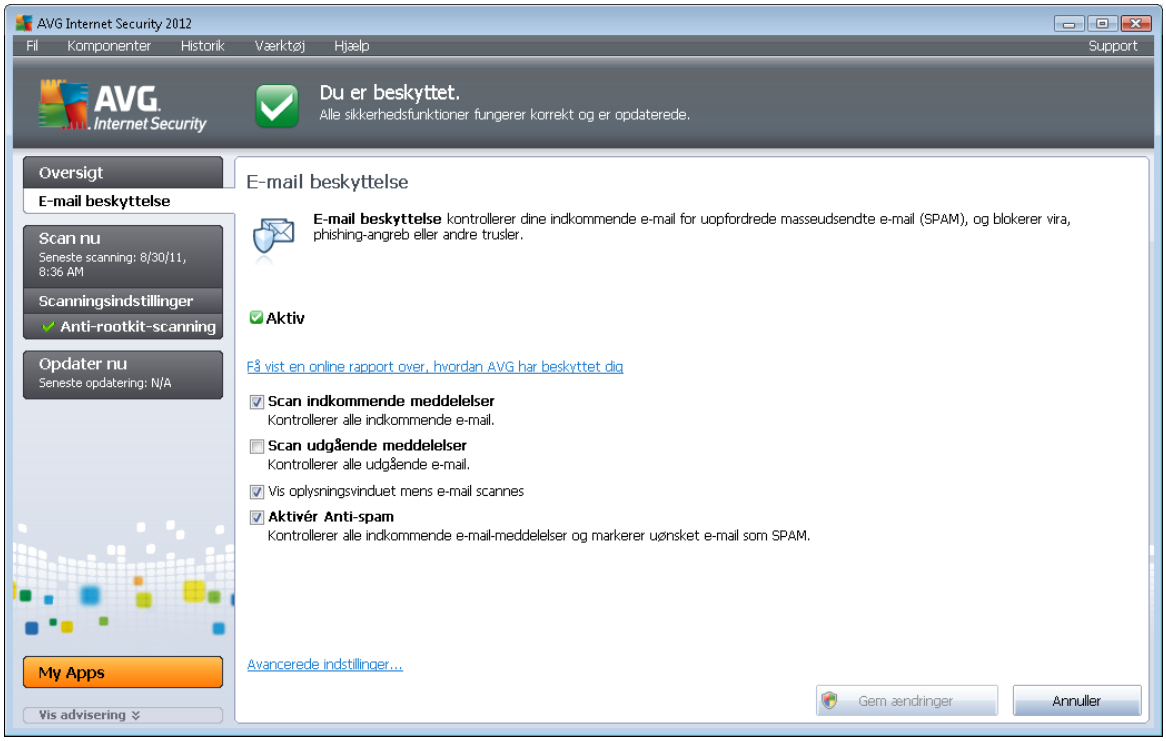
Hvordan fungerer Anti-spam?

Anti-spam kontrollerer alle indkommende e-mail-meddelelser og markerer uønsket e-mail som spam. ***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. ***Anti-spam***-komponenten anvender flere forskellige analysemetoder til behandling af hver e-mail-meddelelse, hvilket sikrer den maksimale beskyttelse imod uønskede e-mail-meddelelser. ***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*).

Hvad er 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.

6.3.3. Grænseflade til e-mail-beskyttelse



I dialogen ***E-mail-beskyttelse*** kan du findeen kort tekst, der beskriver komponentens funktion og indeholder oplysninger om dens aktuelle status*(aktiv).* Brug linket ***Få vist en onlinerapport over, hvordan AVG har beskyttet dig*** for at se statistik for **AVG Internet-sikkerhed 2012** -aktiviteter og -detekteringer på en dedikeret side på AVG's websted (http://www.avg.com/).

Grundlæggende indstillinger for e-mail-beskyttelse

I dialogen ***E-mail-beskyttelse***kan du også redigere nogle af komponentens elementære funktioner:

- ***Scan indgående meddelelser*** *(aktiveret som standard)* – Marker elementet for at angive, at alle e-mails, der sendes til din konto, skal scannes for virus.
- ***Scan udgående meddelelser*** *(deaktiveret som standard)* – Marker elementet for at bekræfte, at alle e-mails, der sendes fra din konto, skal scannes for virus.
- ***Vis meddelelsesvindue, mens e-mails bliver scannet*** *(aktiveret som standard)* – Markér indstillingen for at bekræfte, at du ønsker at få vist en beskeddialog over AVG-ikonet på systembakken under scanningen af dine e-mails.
- ***Aktivér Anti-spam*** *(aktiveret som standard)* – Marker elementet for at angive, om dine indgående e-mails skal filtreres for uopfordrede e-mails.

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.

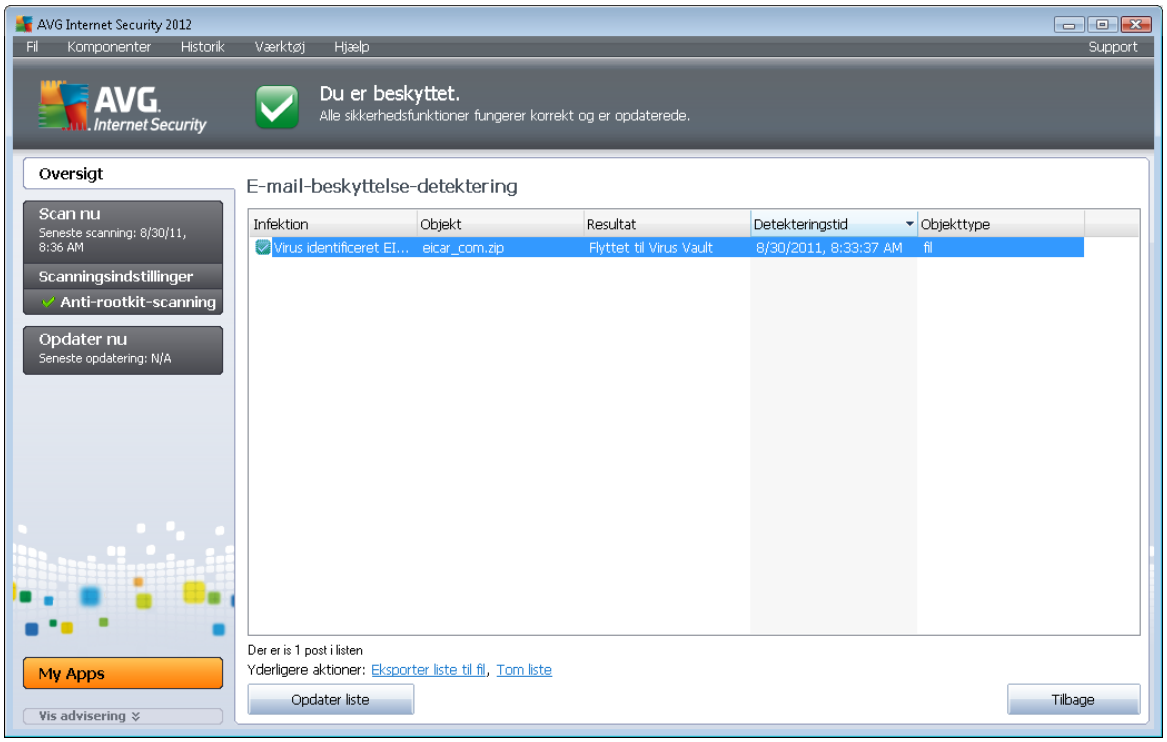
Ændringer i indstillingerne bør kun udføres af en erfaren bruger. Hvis det er nødvendigt at ændre AVG-konfigurationen, skal du vælge systemmenupunktet Værktøjer / Avancerede indstillinger og redigere AVG-konfigurationen i dialogen AVG Avancerede indstillinger, der åbnes.

Betjeningsknapper

Her er de tilgængelige kontrolknapper under fanen ***E-mail-beskyttelse*** :

- ***Gem ændringer*** - klik på denne knap for at gemme og anvende de ændringer, der er foretaget i denne dialog
- ***Annuller*** – Tryk på denne knap for at gå tilbage til standard-AVG-hoveddialogen (*Komponentoversigt*)

6.3.4. Detektering af e-mail-beskyttelse



I dialogen ***E-mail-scanner-detektering*** (*tilgængelig via systemindstillingen Historik/E-mail-scanner-detektering*) kan du se en liste med alle resultater, der er detekteret af komponenten E-mail-beskyttelse. 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 registrerede trusler.
- ***Tilbage*** – Skifter tilbage til den tidligere viste dialog.

6.4. Firewall

Firewall er et system, der gennemtvinger en adgangskontrol-politik mellem to eller flere netværk, ved at blokere/tillade trafik. Firewall indeholder et regelsæt, der beskytter det interne netværk mod angreb udefra *(typisk fra internettet)* og kontrollerer al kommunikation på hver eneste netværksport. Kommunikationen evalueres i henhold til de definerede regler, og er enten tilladt eller forbudt. Hvis ***Firewall*** registrerer forsøg på indtrængen, "blokerer" den forsøget og tillader ikke den indtrængende 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 de enkelte computere mod angreb, der startes af interne brugere på andre computere i netværket.

Computere, der ikke er beskyttet af Firewall, bliver et nemt mål for computerhackere og datatyve.

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.*

6.4.1. Firewall-principper

I **AVG Internet-sikkerhed 2012** styrer ***Firewall*** al trafik på alle computerens netværksporte. Ud fra disse definerede regler vurderer ***Firewall*** de applikationer, der enten køres på computeren *(og ønsker at oprette forbindelse til internettet eller det lokale netværk)*, eller som nærmer sig

computeren ude fra og forsøger at få forbindelse til computeren. For hver af disse applikationer kan ***Firewall*** derefter tillade eller forbyde kommunikation på netværksportene. Hvis applikationen er ukendt, spørger *(dvs. der ikke er defineret Firewall-regler)*, ***Firewall*** som standard, om du vil tillade eller blokere kommunikationsforsøget.

AVG-firewallen 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

6.4.2. 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, slettes, og det er ikke muligt at ændre dens indstillinger.
- ***Bloker alle*** - en Firewall-systemprofil, der er forudindstillet af producenten og altid forefindes. Når denne profil er aktiveret, blokeres al netværkskommunikation, og computeren er ikke tilgængelig via ydre netværk og kan ikke kommunikere udadtil. Denne systemprofil kan ikke kopieres eller slettes, og dens indstillinger kan ikke ændres.
- ***Brugerdefinerede profiler*** – Med en brugerdefineret profil kan du benytte muligheden for et automatisk skift af profil, der især kan være nyttigt, hvis du ofte opretter forbindelse til forskellige netværk *(f.eks. med en bærbar computer).* Brugerdefinerede profiler oprettes automatisk efter **AVG Internet-sikkerhed 2012** installationen og dækker eventuelle individuelle behov for regler til Firewall-politikken. Følgende brugerdefinerede profiler er tilgængelige:
    - ***Direkte tilsluttet internettet*** – Velegnet til almindelige stationære eller bærbare computere til hjemmebrug, der har en direkte forbindelse til internettet uden nogen ekstra beskyttelse. Denne indstilling anbefales også, når du kobler din bærbare

computer til ukendte og formentlig usikre netværk (*f.eks. på en internetcafe, et hotelværelse osv.*).De strengeste Firewall-politikker i denne profil sikrer, at sådanne computere er tilstrækkeligt beskyttet.

- ***Computer på et domæne*** – Egnet til computere på et lokalt netværk, typisk et skole- eller arbejdsnetværk. Det antages, at netværket er professionelt administreret og beskyttet af nogle ekstra foranstaltninger, så sikkerhedsniveauet kan være lavere end i ovennævnte tilfælde, da der er adgang til delte mapper, diskenheder osv.

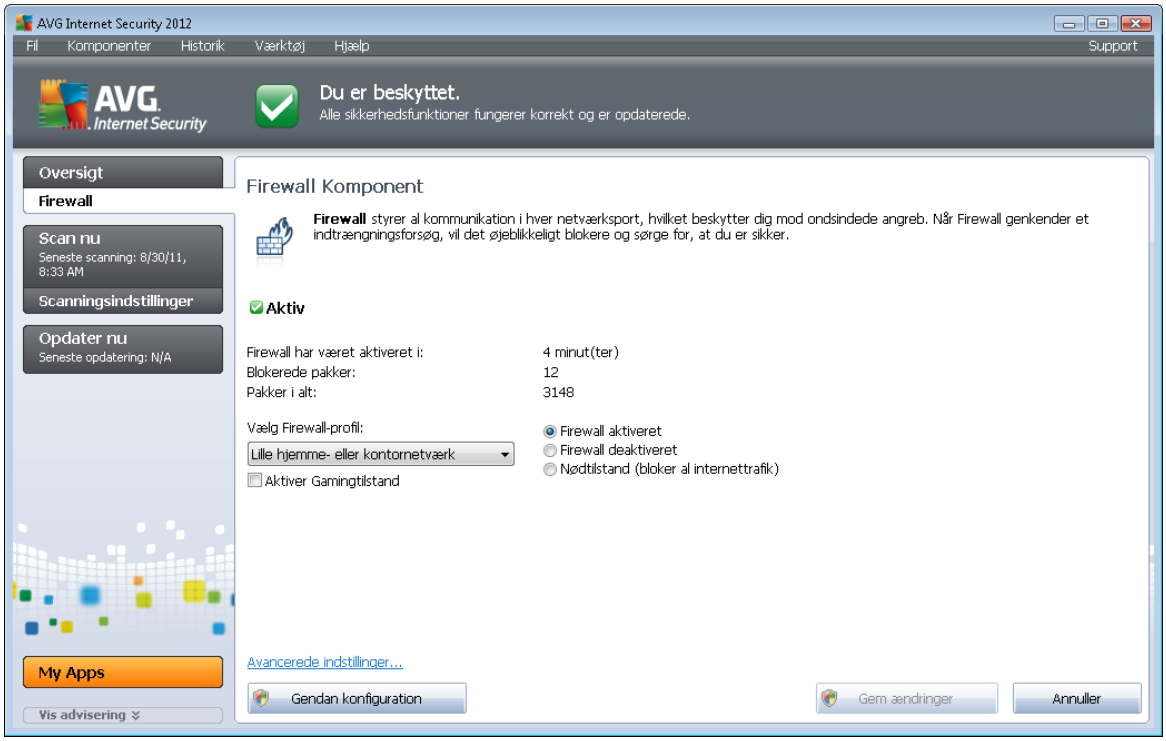
- ***Lille hjemme– eller kontornetværk*** – velegnet til computere på små netværk, typisk i hjemmet eller i små virksomheder. Denne type netværk har som regel ikke en "central" administrator og består kun af flere computere, der er indbyrdes forbundne, og som ofte deler en printer, scanner eller en lignende enhed, og det er noget, som firewallens regler skal afspejle.

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.

6.4.3. Firewall-grænseflade



Hoveddialogen ***Firewall-komponent*** indeholder nogle grundlæggende oplysninger om komponentens funktioner, dens status *(aktiv)* og en kort oversigt over statistikken for en komponent:

- ***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

Grundlæggende indstillinger for firewall

- ***Vælg Firewall-profil*** – vælg en af de definerede profiler i rullemenuen (*Du kan få en detaljeret beskrivelse af hver profil og dens anbefalede anvendelse i kapitlet Firewall-profiler*)
- ***Aktivér gamingtilstand*** – Marker denne indstilling for at sikre det under kørsel af fuldskærmsapplikationer (*spil, præsentationer, film osv.*), 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.
- I sektionen for grundlæggende indstillinger kan du derudover vælge mellem tre forskellige

indstillinger, der definerer den aktuelle status for komponenten Firewall:

- ***Firewall aktiveret*** *(som standard)* – Vælg denne indstilling for at give tilladelse til kommunikation til de applikationer, der er markeret som "tilladte" i det regelsæt, der er defineret 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: *Softwareudbyderen har installeret alle AVG Internet-sikkerhed 2012-komponenter for optimal 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 / 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*** – Tryk på denne knap for at gå tilbage til standard-AVG-hoveddialogen (*Komponentoversigt*).

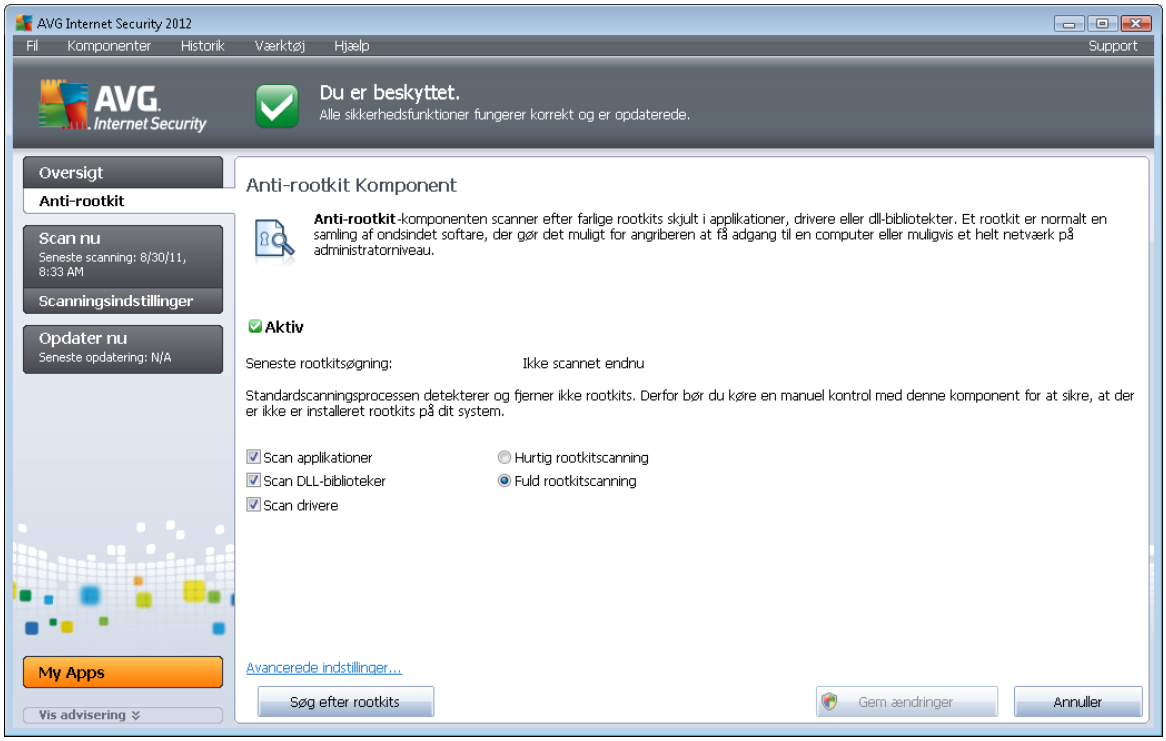
6.5. Anti-rootkit

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. ***Anti-rootkit*** kan detektere rootkits baseret på det foruddefineret sæt af regler. Bemærk, at alle rootkits detekteres *(ikke kun de inficerede)*. Hvis ***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.

Hvad er et 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.

6.5.1. Anti-rootkit-grænseflade



Dialogen ***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.

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.

Grundlæggende indstillinger for Anti-rootkit

I den nederste del af dialogen kan du 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

systemmappen (*typisk c:\Windows*).

- ***Fuld rootkitscanning*** – Scanner alle igangværende processer, indlæste drivere, systemmappen (*typisk c:\Windows*) samt alle lokale drev (*inklusive flashdrev, men ikke diskettedrev/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-hoveddialog (*Komponentoversigt*).
- ***Annuller*** – Tryk på denne knap for at vende tilbage til den almindelige AVG-hoveddialog (*komponentoversigt*) uden at gemme eventuelle ændringer.

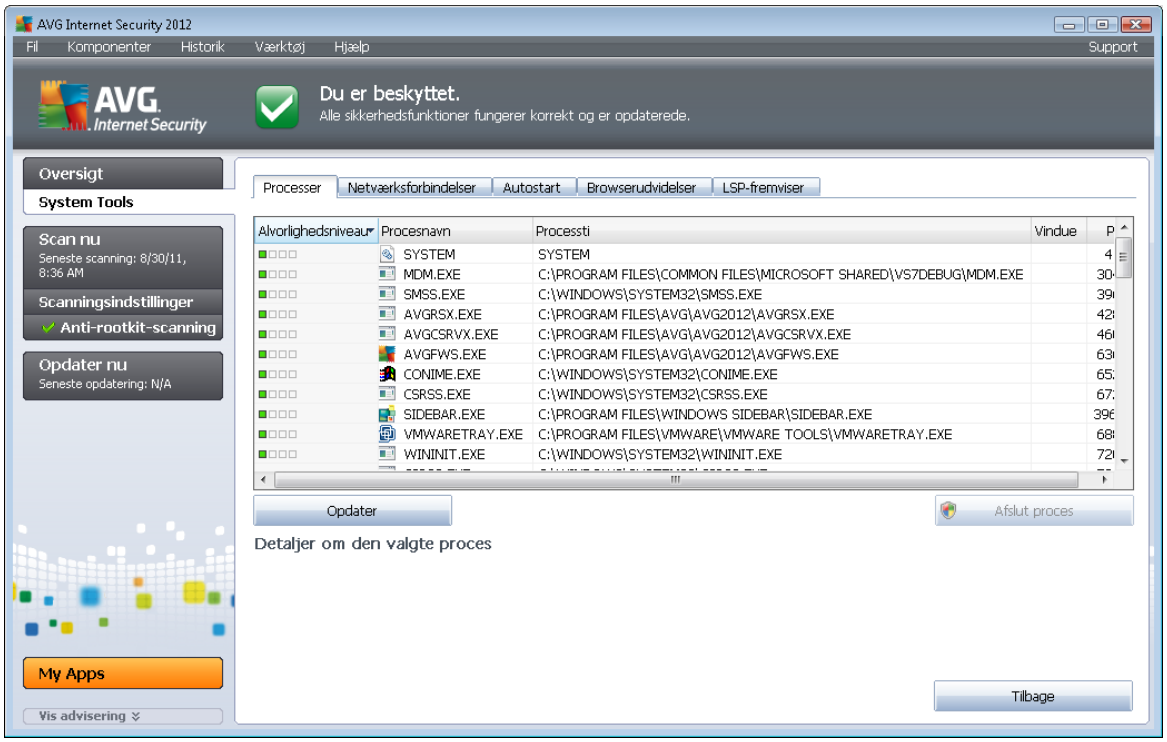
6.6. Systemværktøjer

Systemværktøjer henviser til værktøjer, der giver en detaljeret oversigt over **AVG Internet-sikkerhed 2012** 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!

6.6.1. 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

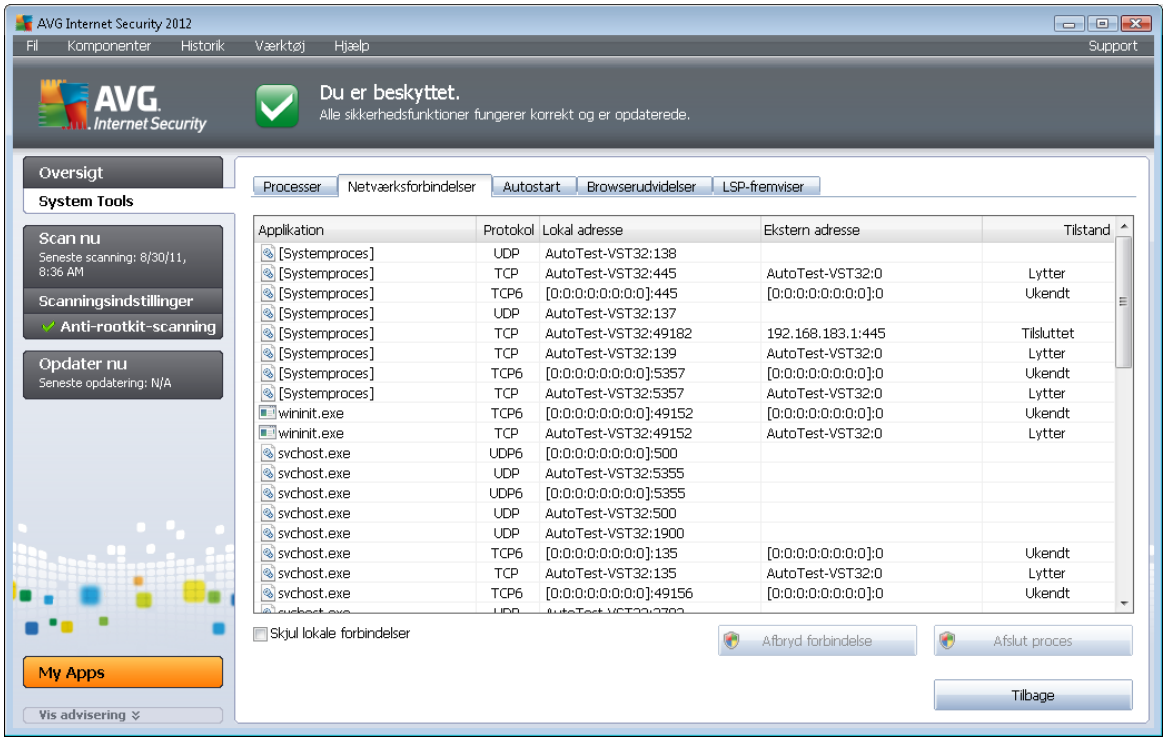
Betjeningsknapper

Her er de tilgængelige kontrolknapper under fanen ***Processer***:

- ***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 standard-AVG-hoveddialogen (*Komponentoversigt*)

6.6.2. 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.

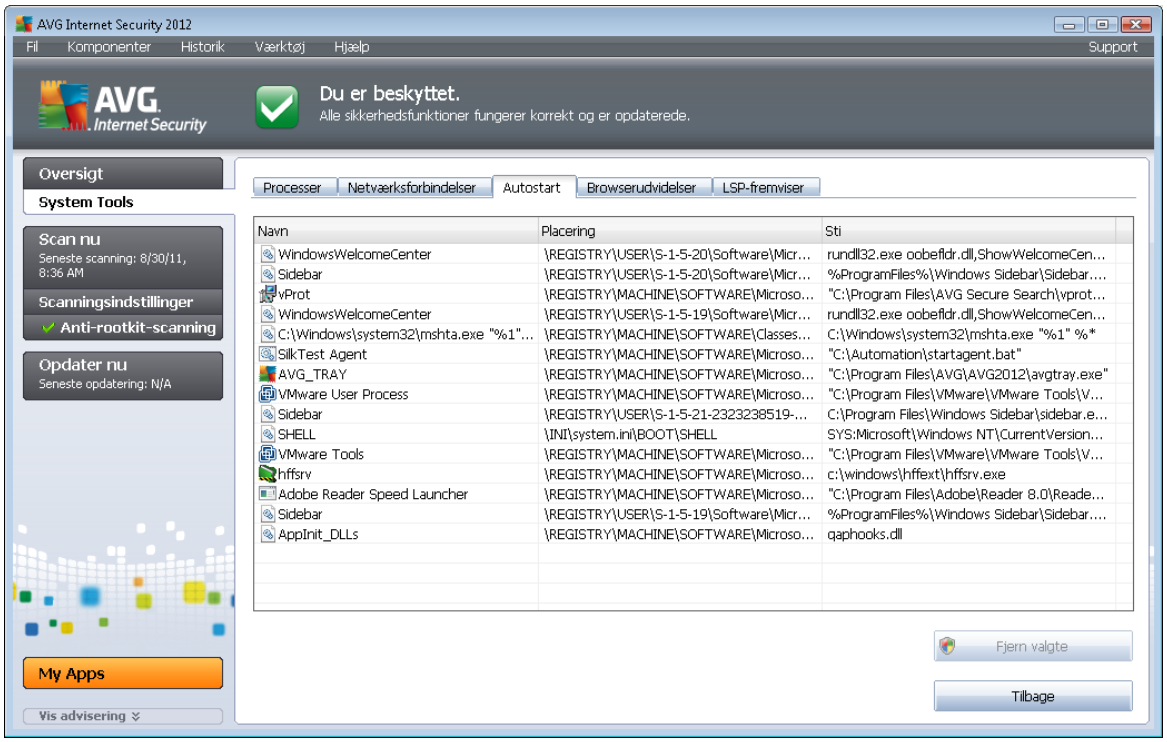
Betjeningsknapper

Her er de tilgængelige kontrolknapper under fanen ***Netværksforbindelser***:

- ***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*** – Skifter tilbage til standard-AVG-hoveddialogen (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!

6.6.3. 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.

Betjeningsknapper

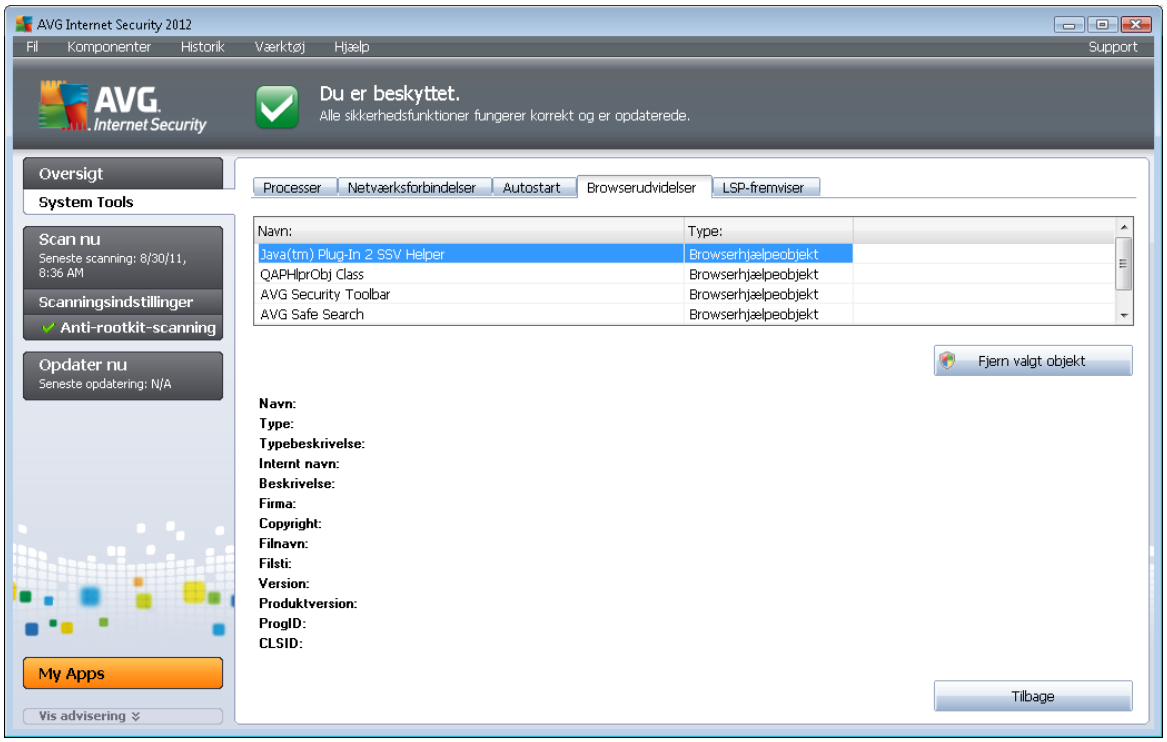
Her er de tilgængelige kontrolknapper under fanen ***Autostart***:

- ***Fjern valgte*** – Tryk på knappen for at slette en eller flere poster.

- ***Tilbage*** – Sender dig tilbage den normale AVG-hoveddialog *(oversigt over komponenter).*

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

6.6.4. 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.

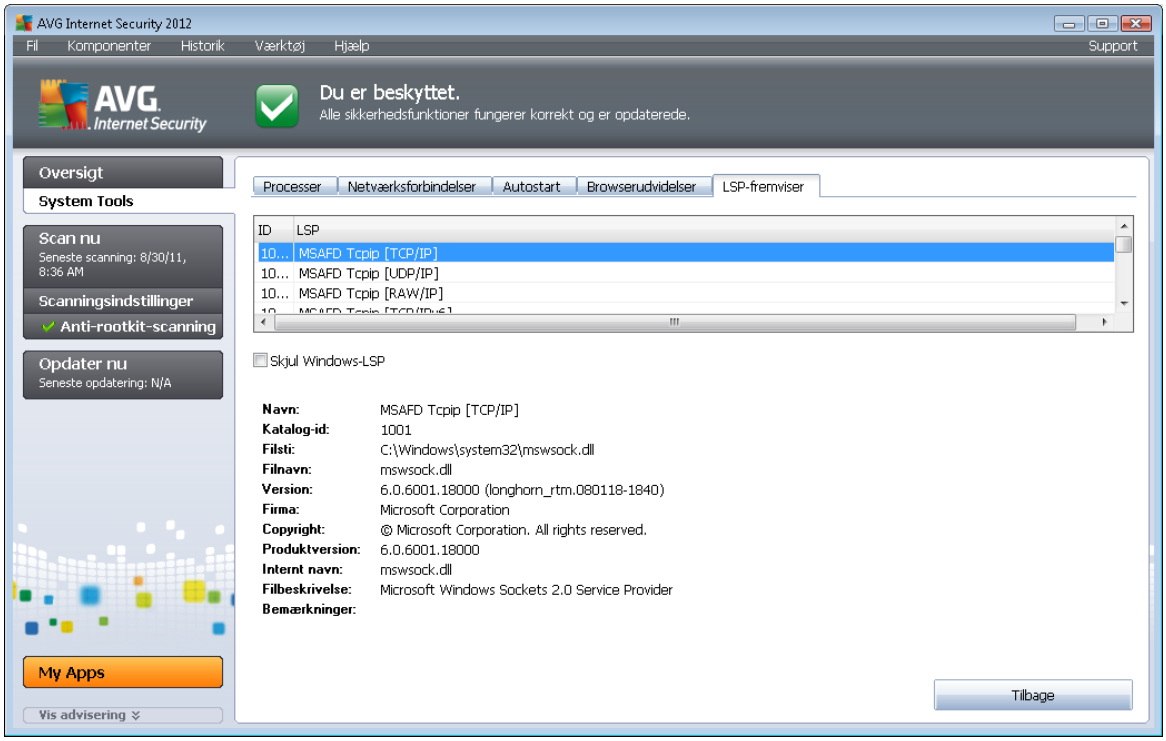
Betjeningsknapper

Her er de tilgængelige kontrolknapper under fanen***Browserudvidelser***:

- ***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*** – Sender dig tilbage til den normale AVG-hoveddialog *(Komponentoversigt).*

6.6.5. 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.

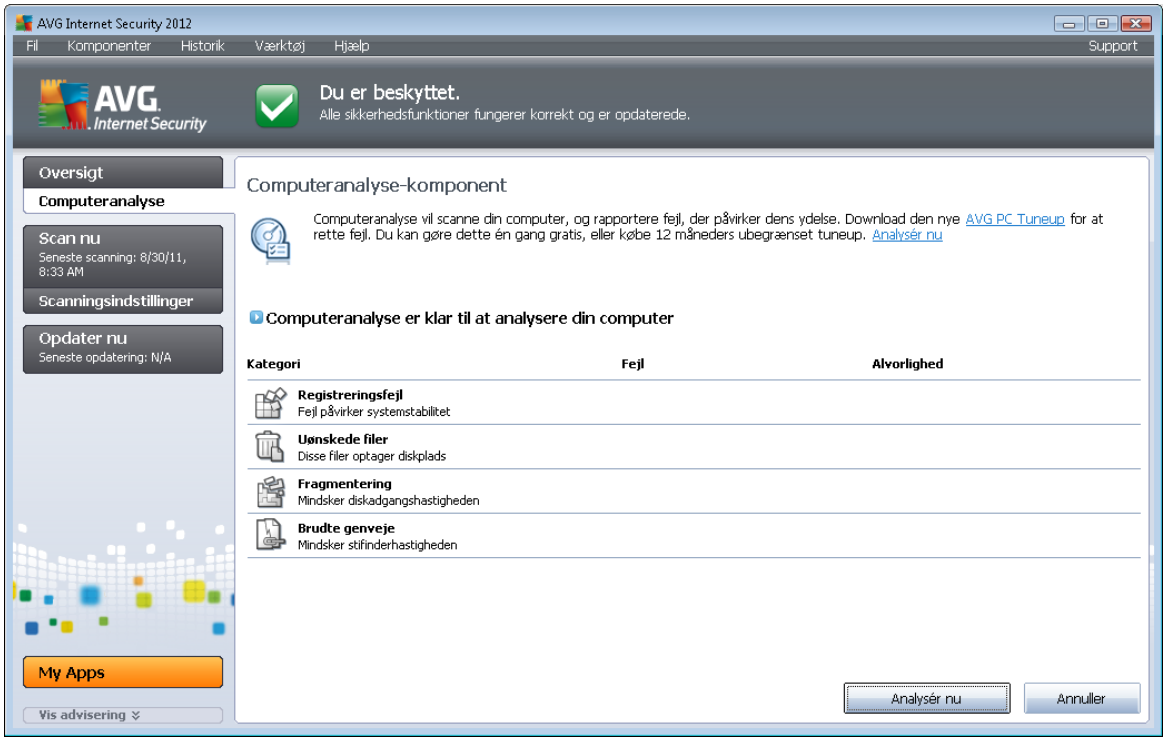
Betjeningsknapper

Her er de tilgængelige kontrolknapper under fanen ***LSP-fremviser***:

- ***Skjul Windows-LSP*** – Hvis du vil medtage Windows LSP på listen, skal du fjerne markeringen af dette element.
- ***Tilbage*** – Skifter tilbage til standard-AVG-hoveddialogen (*Komponentoversigt*).

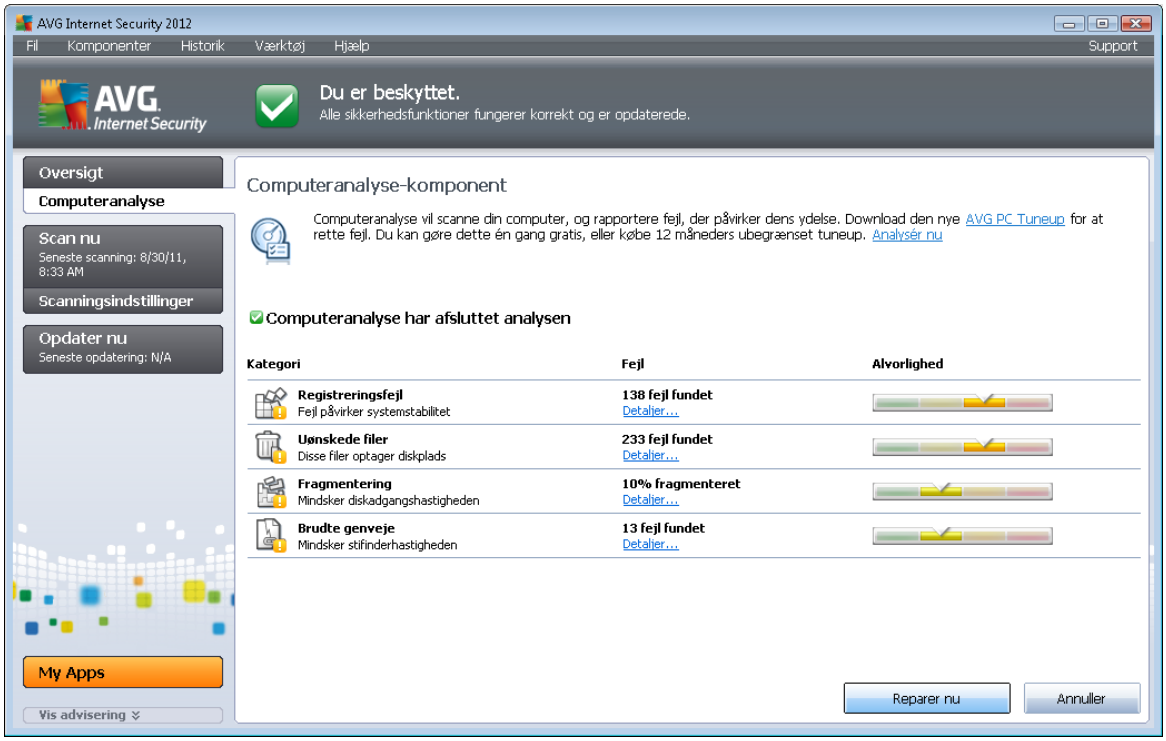
6.7. Computeranalyse

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*** – Beregner den procentdel af harddisken, der er fragmentet, dvs. brugt i for lang tid, så de fleste filer nu er spredt rundt 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 at starte den øjeblikkelige analyse af computeren
- ***Løs nu*** (*vises, når analysen afsluttes*) – Tryk på knappen for at gå til siden på AVG's websted (http://www.avg.com/), som indeholder detaljerede og opdaterede oplysninger vedrørende komponenten ***Computeranalyse***
- ***Annuller*** – Tryk på denne knap for at stoppe kørslen af analysen eller for at gå tilbage til standard-AVG-hoveddialogen (*Komponentoversigt*), når analysen er færdig

6.8. Identitetsbeskyttelse

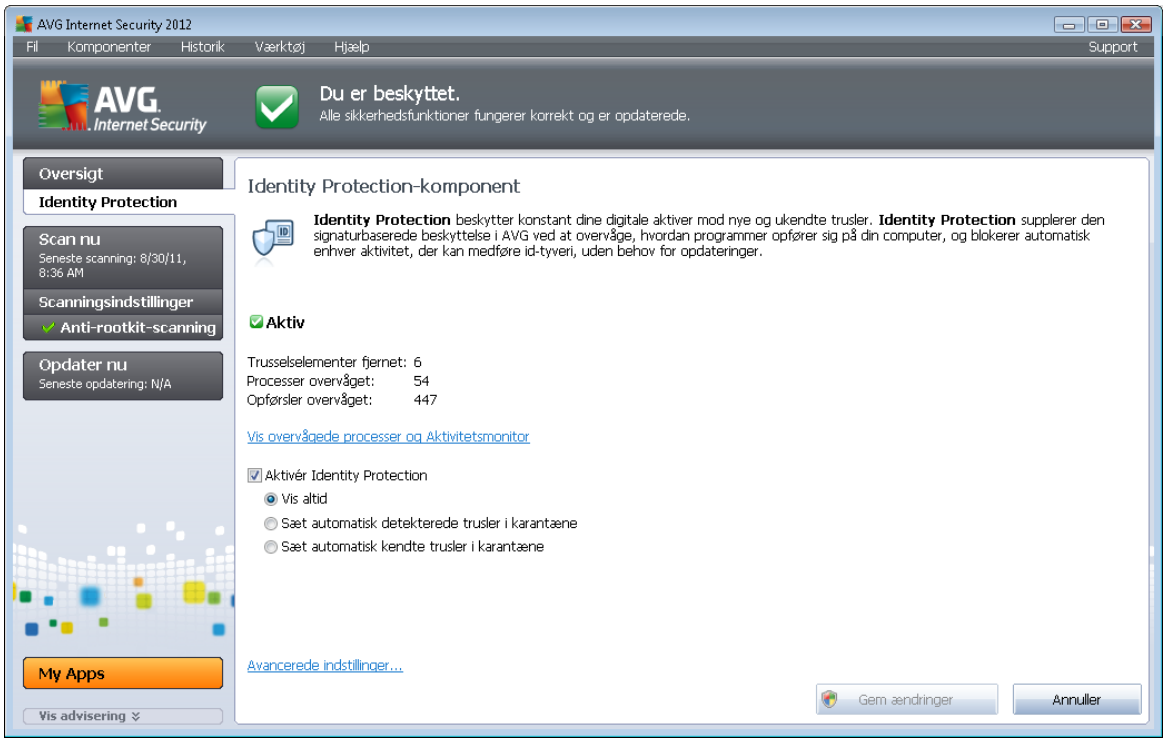
Identetsbeskyttelse er en antimalware-komponent, som beskytter dig mod alle former for malware (*spyware, botter, identitetstyveri, ...*) ved hjælp af adfærdsteknologi og yder dag nul-beskyttelse mod nye vira. ***Identitetsbeskyttelse*** er fokuseret på at forhindre identitetstyve i at stjæle dine adgangskoder, bankkontooplysninger, kreditkortnumre og andre personlige digitale værdier fra alle former for skadelig software (*malware*), som er rettet mod din pc. Det sørger for, at alle programmer, der kører på din pc, fungerer korrekt. ***Identitetsbeskyttelse*** opdager og blokerer kontinuerligt mistænkelig adfærd og beskytter din computer mod al ny malware.

Identitetsbeskyttelse beskytter computeren i realtid mod nye og ukendte trusler. Det overvåger alle

(også skjulte) processer og mere end 285 forskellige adfærdsmønstre, og det kan fastslå, om der sker noget skadeligt i systemet. Af denne grund kan den afsløre trusler, der endnu ikke er beskrevet i virusdatabasen. Når et ukendt stykke kode ankommer til din computer, bliver det omgående overvåget for ondsindet adfærd og sporet. Hvis det konstateres, at filen er skadelig, så flytter ***Identitetsbeskyttelse*** koden til Virus Vault og fortryder de ændringer, der måtte være foretaget i systemet *(kodeindsættelser, ændringer i registreringsdatabasen, portåbninger osv.)*. Du behøver ikke starte en scanning for at være beskyttet. Teknologien er meget proaktiv, kræver sjældent opdatering og er altid på vagt.

Identitetsbeskyttelse medfølger som en del af Anti-Virus. Vi anbefaler på det kraftigste, at begge komponenter er installeret, så du kan få en fuld beskyttelse af pc'en!

6.8.1. Identitets beskyttelses brugerflade



Identitetsbeskyttelse-dialogen giver en kort beskrivelse af komponentens grundlæggende funktioner, dens status *(aktiv)* og visse statistiske data:

- ***Trusselselementer fjernet*** – Angiver antallet af applikationer, der er registreret 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.

Grundlæggende indstillinger for identitetsbeskyttelse

I bunden af dialogen kan du redigere visse elementære egenskaber ved komponentens 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

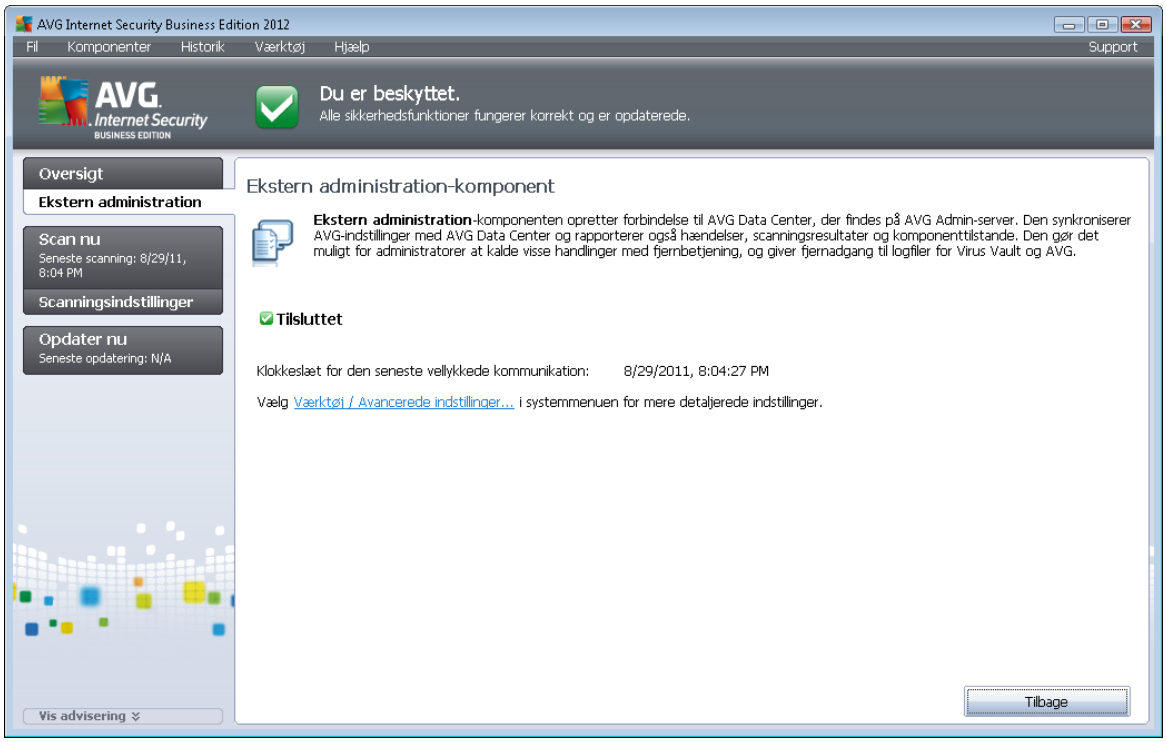
Betjeningsknapper

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*** – Tryk på denne knap for at gå tilbage til standard-AVG-hoveddialogen (*Komponentoversigt*)

6.9. Ekstern administration



Komponenten ***Ekstern administration*** vises kun i brugergrænsefladen i **AVG Internet-sikkerhed 2012**, hvis du har installeret erhvervsudgaven af produktet *(du kan få oplysninger om den licens, der er anvendt ved installationen, under fanen Version i dialogen Information, der kan åbnes ved hjælp af systemindstillingen Support)*. I dialogen ***Ekstern administration-komponent*** kan du finde oplysninger om, hvorvidt komponenten er aktiv og har forbindelse til serveren. Alle indstillinger for komponenten ***Ekstern administration*** skal foretages i ***Avancerede indstillinger / Ekstern administration***.

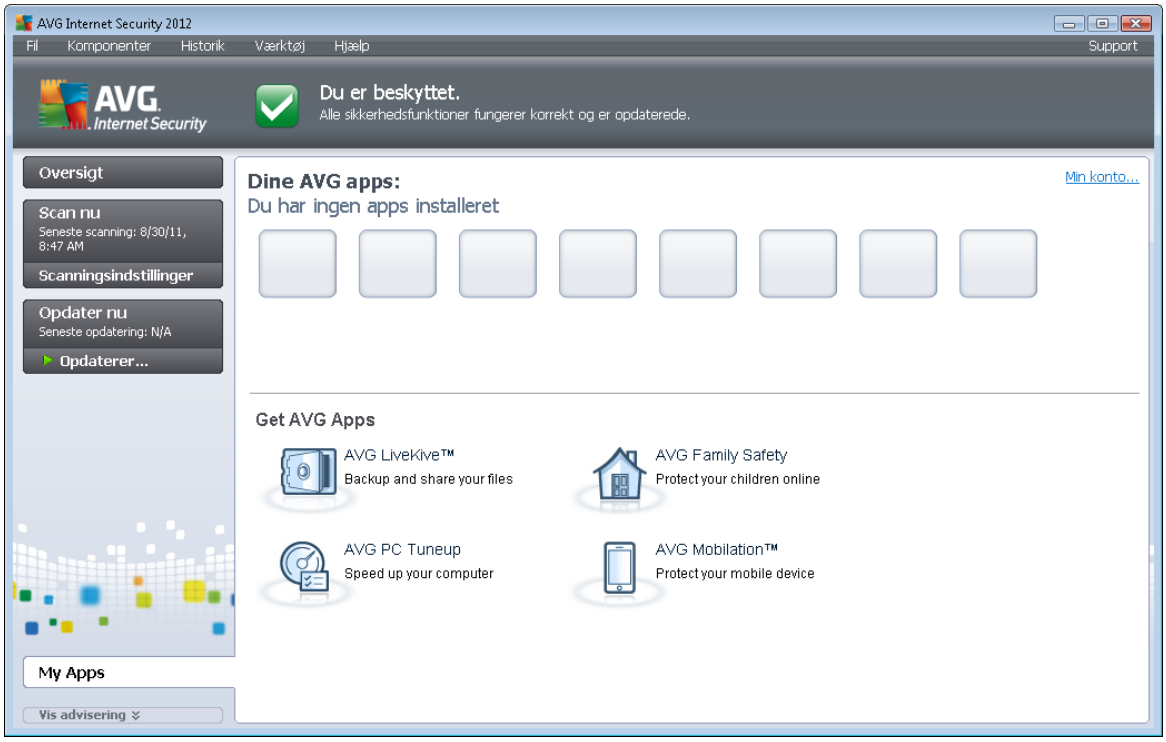
For en detaljeret beskrivelse af komponentens indstillinger og funktioner i systemet AVG Ekstern administration henvises til den specifikke dokumentation, der specifikt omhandler dette emne. Denne dokumentation er tilgængelig på AVG-webstedet(http://www.avg.com/) under afsnittet ***Supportcenter/Download/Dokumentation***.

Betjeningsknapper

- ***Tilbage*** – Tryk på denne knap for at gå tilbage til standard-AVG-hoveddialogen (*Komponentoversigt*).

7. My Apps

De tre følgende applikationer for LiveKive, Familiesikkerhed og PC Tuneup er tilgængelige som selvstændige AVG-produkter, og de er en valgfri del af din **AVG Internet-sikkerhed 2012**-installation. I dialogen ***Dine AVG-apps*** *(tilgængelige via knappen My Apps direkte i AVG-hoveddialogen)* kan du se en oversigt over de applikationer, der allerede er installeret og ellers er klar til at blive installeret:



7.1. LiveKive

LiveKive er dedikeret til onlinesikkerhedskopiering af data på sikre servere. ***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. ***LiveKive***-funktionerne omfatter:

- Sikkerhedsforanstaltning i tilfælde af, at din computer og/eller harddisk bliver korrupt
- Adgang til dine data fra enhver enhed, der er tilsluttet internettet
- Nem organisering
- Deling med alle, der har din tilladelse

Du kan få detaljerede oplysninger ved at gå til den dedikerede AVG-webside, hvor du også kan hente komponenten med det samme. Det kan du gøre ved at bruge PC LiveKive-linket i dialogen My Apps.

7.2. Familiesikkerhed

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.

Du kan få detaljerede oplysninger ved at gå til den dedikerede AVG-webside, hvor du også kan hente komponenten med det samme. Det kan du gøre ved at bruge Familiesikkerhed-linket i dialogen My Apps.

7.3. PC Tuneup

PC Tuneup-applikationen er et avanceret værktøj til detaljerede systemanalyser og -rettelser. Det kan være, hvordan hastigheden og den overordnede ydelse af computeren kan forbedres. ***PC Tuneup***-funktionerne omfatter:

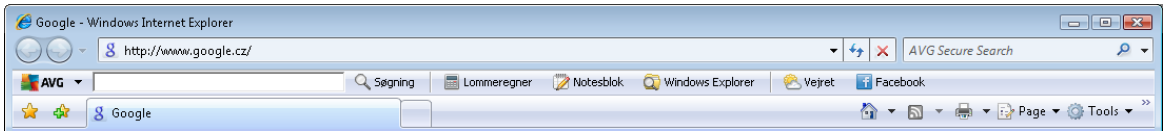
- Disk Cleaner – Fjerner uønskede filer, der gør en computer langsommere.
- Disk Defrag – Defragmenter diskdrev og optimerer placeringen af systemfiler.
- Rensning af registreringsdatabase – Reparerer fejl i registreringsdatabasen for at øge computerens stabilitet.
- Defragmentering af registreringsdatabase –Komprimerer registreringsdatabasen ved at fjerne hukommelseskrævende huller.
- Disk Doctor – Finder dårlige sektorer, mistede klynger og mappefejl og reparerer dem.
- Internetoptimering – Tilpasser indstillinger, så de passer til en bestemt internetforbindelse.
- Sporingsletning – Fjerner historikken over computer- og internetbrug.
- Disk Wiper – Rydder ledig plads på diske for at forhindre, at følsomme data gendannes.
- Filmakulator – Sletter de valgte filer, så de ikke kan gendannes på en disk eller et USB-drev.
- Filgendannelse – Gendanner filer, der slettes fra diske, usb-drev eller kameraer ved et uheld.
- Duplicate File Finder – Hjælper med at finde og fjerne duplikerede filer, som optager diskplads.
- Tjenestestyring – Deaktiverer unødvendige tjenester, der gør en computer langsommere.
- Startstyring – Gør det muligt at administrere programmer, der startes automatisk, når Windows startes.
- Afinstallationsstyring – Fjerner helt de softwareprogrammer, du ikke længere har brug for.
- Indstillingsstyring – Gør det muligt at indstille hundredvis af skjulte Windows-indstillinger.

- Joblisten – Viser alle kørende processer, tjenester og låste filer.
- Disk Explorer – Viser, hvilke filer der fylder mest på en computer.
- Systeminformation – Angiver detaljerede oplysninger om hardware og software, der er installeret.

Du kan få detaljerede oplysninger ved at gå til den dedikerede AVG-webside, hvor du også kan hente komponenten med det samme. Det kan du gøre ved at bruge PC Tuneup-linket i dialogen My Apps.

8. AVG Sikkerhedsværktøjslinje

AVG-sikkerhedsværktøjslinjen er et værktøj, som arbejder tæt sammen med komponenten LinkScanner og sørger for maksimal sikkerhed, når du søger på nettet. I **AVG Internet-sikkerhed 2012** er installationen af ***AVG-sikkerhedsværktøjslinje*** valgfri. Under installationsprocessen blev du bedt om at angive, om komponenten skal installeres. ***AVG-sikkerhedsværktøjslinjen*** er tilgængelig direkte i din internetbrowser. I øjeblikket er de understøttede internetbrowsere Internet Explorer (*version 6.0 eller nyere*) og/eller Mozilla Firefox (*version 3.0 eller nyere*). Ingen andre browsere understøttes *(hvis du anvender en alternativ internetbrowser, f.eks. Avant Browser, kan der opstå uforudsigelig adfærd)*.



AVG-sikkerhedsværktøjslinjen består af følgende elementer:

- ***AVG-logo*** med rullemenuen:
    - ***Brug AVG Secure Search*** – Giver dig mulighed for at søge direkte i ***AVG-sikkerhedsværktøjslinjen*** ved hjælp af søgemaskinen ***AVG Secure Search***. Alle søgeresultater kontrolleres løbende af tjenesten Søgeskjold, så du kan føle dig fuldstændig beskyttet på nettet.
    - ***Aktuelt trusselsniveau*** – Åbner websiden for viruslaboratoriet med en grafisk visning af det aktuelle trusselsniveau på nettet.
    - ***AVG-trusselslaboratorier*** – Åbner siden ***Webstedsrapporter*** på AVG's websted (http://www.avg.com/), hvor du kan søge efter specifikke trusler ved navn og få detaljerede oplysninger om dem.
    - ***Værktøjslinjen Hjælp*** – Åbner onlinehjælpen, som dækker alle funktioner i ***AVG-sikkerhedsværktøjslinjen***.
    - ***Indsend produkttilbagemeldinger*** – Åbner en webside med en formular, som du kan udfylde og give os din mening om ***AVG-sikkerhedsværktøjslinjen***.
    - ***Om...*** – Åbner et nyt vindue med oplysninger om din aktuelle version af ***AVG-sikkerhedsværktøjslinje***.
- ***Arkiveret søgning***– Søg på internettet ved hjælp af ***AVG-sikkerhedsværktøjslinjen*** for at føle dig fuldstændig sikker, eftersom alle viste søgeresultater er 100 % sikre. Indtast søgeordet eller en sætning i søgefeltet, og tryk på knappen ***Søg*** *(eller Enter)*. Alle søgeresultater kontrolleres løbende af tjenesten Søgeskjold *(i komponenten LinkScanner)*.
- Genvejstaster til hurtig adgang til disse applikationer: ***Lommeregner***, ***Notesblok***, ***Windows Stifinder***
- ***Vejret*** – Denne knap åbner en ny dialog, som giver dig oplysninger om vejret lige nu for din placering og vejrudsigten for de kommende to dage. Disse oplysninger opdateres med

jævne mellemrum, hvilket vil sige hver 3.-6. time. I dialogen kan du ændre den ønskede placering manuelt og bestemme, om temperaturoplysningerne skal vises i Celsius eller Fahrenheit.

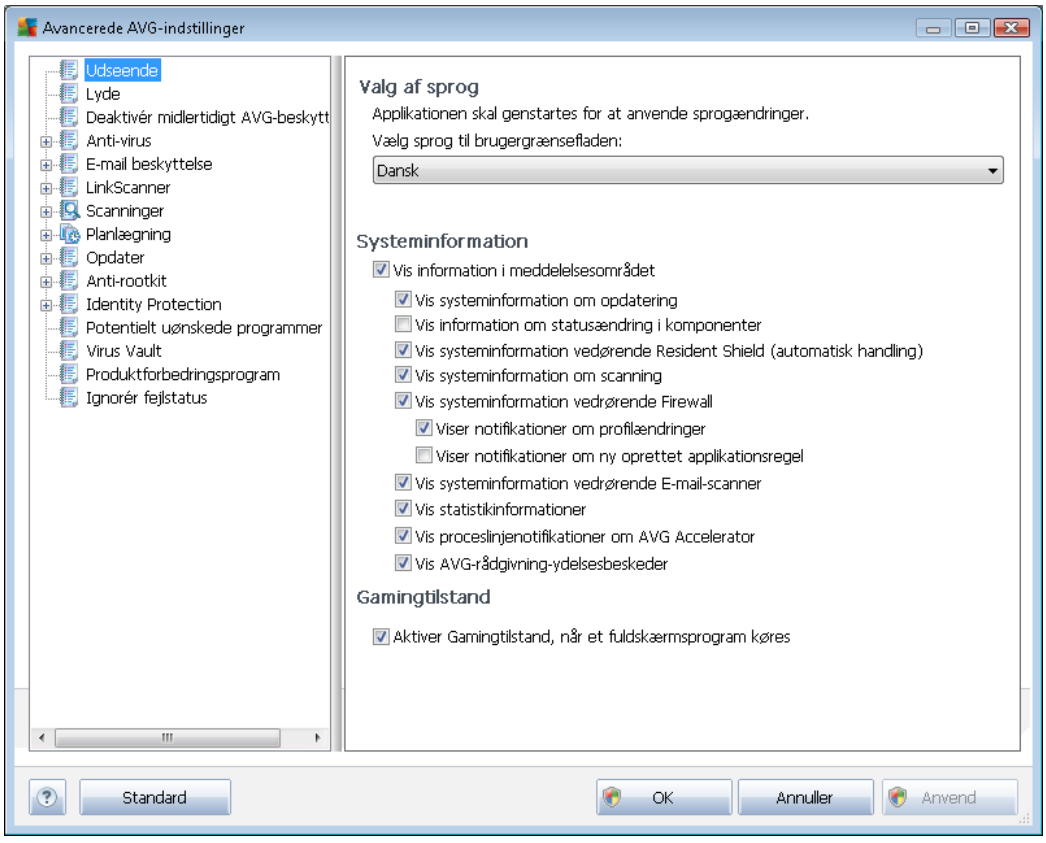
- ***Facebook*** – Denne knap giver dig mulighed for at få forbindelse til det sociale netværk Facebook direkte i ***AVG-sikkerhedsværktøjslinjen***. *adfærd.*

9. AVG Avancerede indstillinger

Den avancerede konfigurationsdialog for **AVG Internet-sikkerhed 2012** 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 Internet-sikkerhed 2012**-brugergrænsefladen og nogle få elementære indstillinger omkring applikationens adfærd:

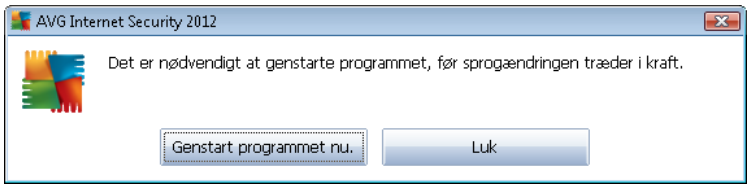


Valg af sprog

I sektionen ***Sprogvalg*** kan du vælge det ønskede sprog i rullemenuen. Det ønskede sprog vil herefter blive brugt i hele **AVG Internet-sikkerhed 2012**-brugergrænsefladen. Rullemenuen indeholder kun de sprog, du valgte at installere under installationsprocessen (*se kapitlet Brugerdefinerede indstillinger*), samt engelsk (*, som automatisk installeres som standard*). Hvis du er færdig med at ændre **AVG Internet-sikkerhed 2012** til et andet sprog, skal du genstarte applikationen. Følg disse trin:

- Vælg det ønskede sprog for applikationen i rullemenuen

- Bekræft dit valg ved at trykke på knappen ***Anvend****(nederst til højre i dialogen)*
- Tryk på ***OK***-knappen for at bekræfte
- Der vises en ny dialog, som oplyser dig om, at sprogændringerne først træder i kraft, når du har genstartet din **AVG Internet-sikkerhed 2012**
- Tryk på knappen ***Genstart applikationen nu*** for at acceptere programgenstart, og vent et øjeblik på, at sprogændringerne træder i kraft:



Systeminformation

I denne sektion kan du slå visning af beskeder fra systembakken om status for applikationen **AVG Internet-sikkerhed 2012** fra. Systembeskederne bliver som standard vist. Det anbefales kraftigt, at du beholder denne konfiguration! Systembeskeder informerer eksempelvis om scanninger eller opdateringer eller om statusændringer af **AVG Internet-sikkerhed 2012** -komponenten. Det er vigtigt at holde øje med disse meddelelser!

Hvis du af en eller anden grund beslutter dig for, at du ikke vil informeres på denne måde, eller hvis du kun vil se bestemte beskeder *(der er relateret til en specifik AVG Internet-sikkerhed 2012-komponent)*, kan du angive dine præferencer ved at markere eller fjerne markeringen fra følgende indstillinger:

- ***Vis beskeder i meddelelsesområdet*** *(er som standard slået til)* – Alle beskeder vises som standard. Fjern markeringen fra dette element for at slå visningen af alle beskeder fra systembakken fra. Når det er slået til, kan du yderligere vælge, hvilke specifikke tekstbobler, der skal vises:
  - ***Vis systembeskeder om opdateringer*** *(slå til som standard)* – Beslut om oplysninger om **AVG Internet-sikkerhed 2012** opdatering, forløb og afslutning skal vises.
  - ***Vis beskeder om ændringer af komponenternes status*** *(slå fra som standard)* – Beslut om oplysninger om komponentens aktivitet/inaktivitet eller eventuelle problemer med komponenten skal vises. Når du rapporterer om en komponentfejl, svarer denne indstilling til informationsfunktionen i systembakkeikonet, som rapporterer om problemer med en hvilken som helst **AVG Internet-sikkerhed 2012** komponent.
  - ***Vis systembeskeder vedrørende Resident Shield (automatisk handling)*** *(aktiveret som standard)* – Beslut, om oplysninger vedrørende lagring, kopiering og åbning af filer skal vises eller tilsidesættes (*denne konfiguration vises kun, hvis indstillingen Resident Shield Auto-heal er slået til*).

- ***Vis systembeskeder om scanning*** *(aktiveret som standard)* – Beslut, om oplysninger om automatisk kørsel af den planlagte scanning, forløbet og resultaterne skal vises.

- ***Vis beskeder vedrørende Firewall*** *(aktiveret som standard)* – Beslut, om oplysninger vedrørende Firewall-status og -kørsel, f.eks. aktiverings-/deaktiveringsadvarsler, eventuel blokering af trafik osv. skal vises. Dette element indeholder to specifikke valgmuligheder *(se afsnittet om Firewall i dette dokument for at få en detaljeret beskrivelse af dem)*:

  – ***Vis beskeder om profilændringer*** *(aktiveret som standard)* – Informerer dig om automatiske ændringer af Firewall-profiler.

  – ***Vis beskeder om nye applikationsregler*** *(deaktiveret som standard)* – Informerer dig om automatisk oprettelse af Firewall-regler for nye applikationer på baggrund af en sikker liste.

- ***Vis systembeskeder vedrørende E-mail scanner*** *(aktiveret som standard)* – Beslut, om oplysninger om scanning af alle indgående og udgående e-mail-meddelelser skal vises.

- ***Vis statistiske beskeder*** *(aktiveret som standard)* – Behold markeringen for at tillade regelmæssig visning af statistiske oplysninger i systembakken.

- ***Vis systembeskeder om AVG Accelerator*** *(aktiveret som standard)* – Beslut, om oplysninger om ***AVG Accelerator*** -aktiviteter skal vises. ***AVG Accelerator***-tjenesten, som giver problemfri videoafspilning på nettet og gør det nemmere at foretage ekstra downloads.

- ***Vis beskeder fra AVG Advice*** *(aktiveret som standard)* - ***AVG Advice*** overvåger de understøttede Internet-browsere *(Internet Explorer, Chrome, Firefox, Opera og Safari)* og giver dig besked, hvis din browser bruger mere end den anbefalede hukommelsesmængde. I dette tilfælde aftager din computers ydelse markant, og du anbefales at genstarte din internetbrowser for at fremskynde processen. Lad indstillingen ***Vis beskeder fra AVG Advice*** være slået til for at holde dig orienteret.

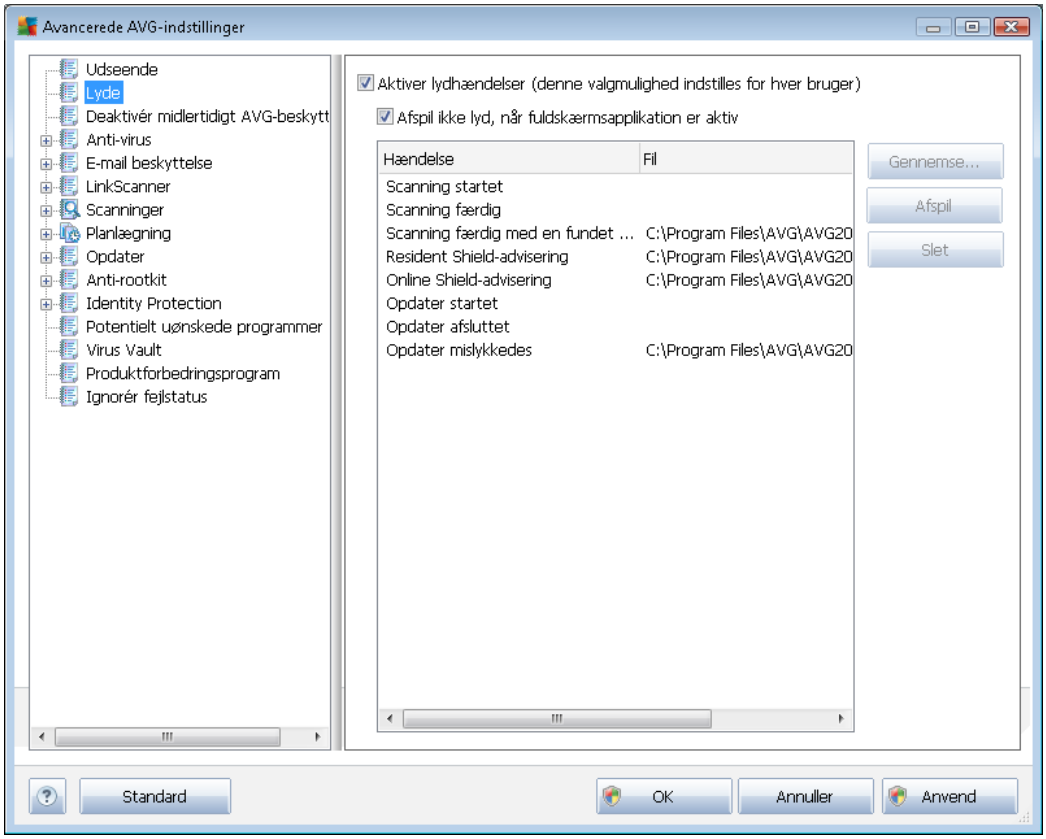
Gamingtilstand

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 ønsker at få oplysninger om bestemte **AVG Internet-sikkerhed 2012**-handlinger via et lydsignal:



Indstillingerne er kun gyldige for den aktuelle brugerkonto. Det betyder, at hver enkelt bruger på computeren kan have sine egne lydindstillinger. Hvis du ønsker et lydsignal, skal du sørge for, at ***Aktivér lydhændelser*** er markeret (*indstillingen er aktiveret som standard*) for at aktivere listen over alle relevante handlinger. Derudover kan det være en ide at markere indstillingen ***Afspil ikke lyd, når fuldskærmsapplikation er aktiv*** for at undertrykke lydsignalet i situationer, hvor det kan virke forstyrrende *(se også i afsnittet om spiltilstand i kapitlet Avancerede indstillinger/Udseende i dette dokument)*.

Betjeningsknapper

- ***Gennemse*** – Når du har valgt den relevante hændelse på listen, kan du bruge knappen ***Gennemse*** til at søge efter den ønskede fil, der skal tildeles til den, på disken. *(Bemærk, at det kun er *.wav-lyde, der understøttes i øjeblikket!)*

- ***Afspil*** – Hvis du vil lytte til den valgte lyd, skal du markere hændelsen på listen og trykke

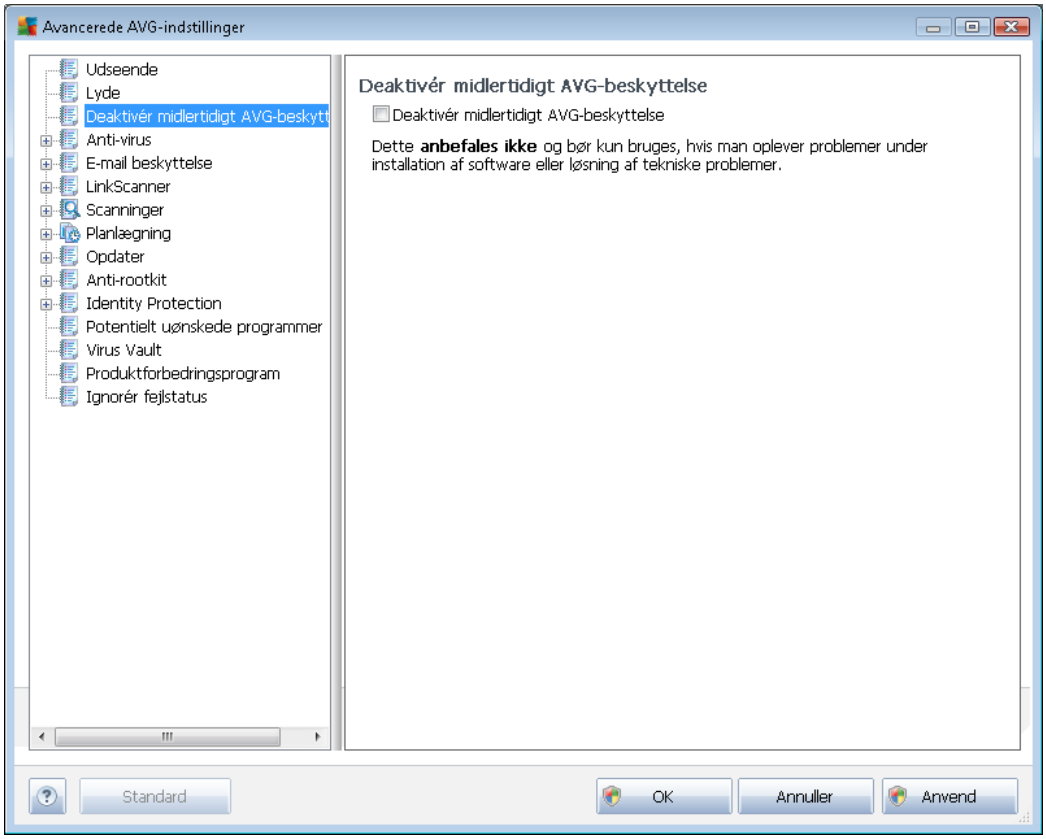
på knappen ***Afspil***.

- ***Slet*** – Brug knappen ***Slet*** til at fjerne den lyd, der er angivet for en bestemt hændelse.

9.3. Deaktivér midlertidigt AVG-beskyttelse

I dialogen ***Deaktivér midlertidigt AVG-beskyttelse*** har du mulighed for at deaktivere hele beskyttelsen fra din **AVG Internet-sikkerhed 2012** med det samme.

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



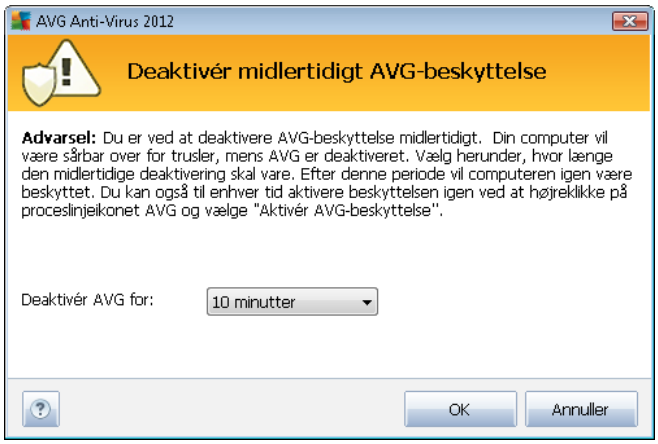
I de fleste tilfælde er det ***ikke nødvendigt*** at deaktivere **AVG Internet-sikkerhed 2012**, inden du installerer ny software eller drivere, selv ikke hvis installationsprogrammet eller softwareguiden anbefaler, at kørende programmet og applikationer slukkes først for at sikre, at der ikke forekommer unødvendige afbrydelser under installationsprocessen. Hvis du rent faktisk får problemer under installationen, skal du først prøve at deaktivere den indbyggede beskyttelse (*Aktivér Resident Shield*) . Hvis du midlertidigt skal deaktivere **AVG Internet-sikkerhed 2012**, 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.

Sådan deaktiveres AVG-beskyttelsen

- Markér afkrydsningsfeltet ***Deaktiver midlertidigt AVG-beskyttelse***, og bekræft valget ved

at trykke på knappen ***Anvend***

- I den nyligt åbnede dialog ***Deaktiver midlertidigt AVG-beskyttelse*** skal du angive, i hvor lang tid **AVG Internet-sikkerhed 2012** skal deaktiveres. Denne beskyttelse slås som standard fra i 10 minutter, hvilket skulle være nok til, at der kan foretages en almindelig opgave som f.eks. at installere ny software osv. Bemærk, at den første tidsgrænse, der kan indstilles, er 15 minutter, og af sikkerhedsmæssige årsager kan den ikke tilsidesættes af din egen værdi. Efter den angivne tidsperiode aktiveres alle deaktiverede komponenter automatisk igen.

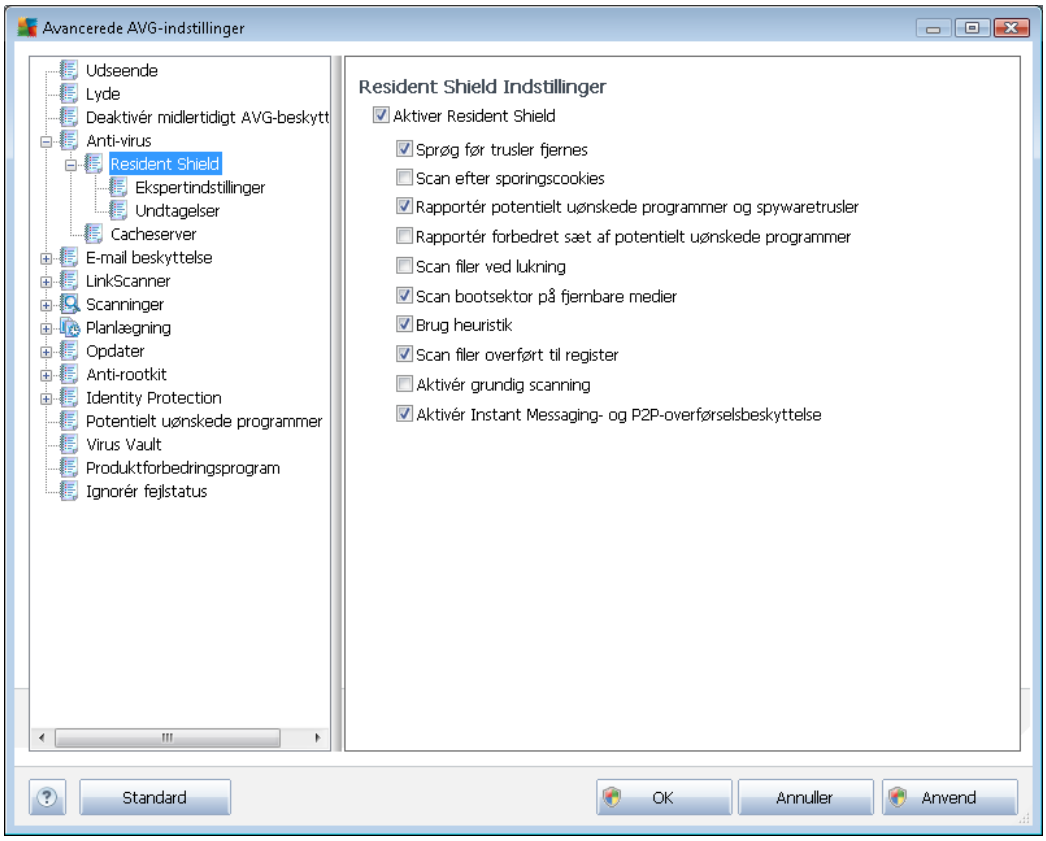


9.4. Anti-virus

Indtast emnetekst her.

9.4.1. Resident Shield

Resident Shield udfører en aktiv beskyttelse af filer og mapper mod virus, spyware og anden malware.



I dialogen ***Resident Shield-indstillinger*** kan du aktivere eller deaktivere den indbyggede beskyttelse helt ved at markere eller fjerne markeringen fra indstillingen ***Aktivér Resident Shield*** (*denne indstilling aktiveres som standard*). Herudover kan du vælge, hvilke funktioner i den indbyggede beskyttelse der skal aktiveres:

- ***Scan efter sporingscookies*** (*deaktiveret som standard*) – Denne parameter definerer, at cookies skal registreres under en scanning. (*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*) – Klik for at aktivere Anti-Spyware-programmet, og scan for spyware og virus. 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*** (*dekativeret som standard*) – Markér for at registrere den udvidede pakke med spyware: programmer, der er helt i orden og harmløse, når de købes direkte fra producenten, men som efterfølgende kan bruges til ondartede formål. 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 filer ved lukning***(*er deaktiveret som standard*) – Scanning ved lukning, sikrer, at AVG scanner aktive objekter (dvs. applikationer, dokumenter…), når de åbnes, og også når de lukkes. Det gør det muligt at beskytte computeren mod nogle avancerede virustyper.

- ***Scan bootsektor på flytbare medier*** (*slået til som standard*)

- ***Brug heuristik*** (*aktiveret som standard*) – Heuristisk analyse bruges til registrering af (*dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø*).

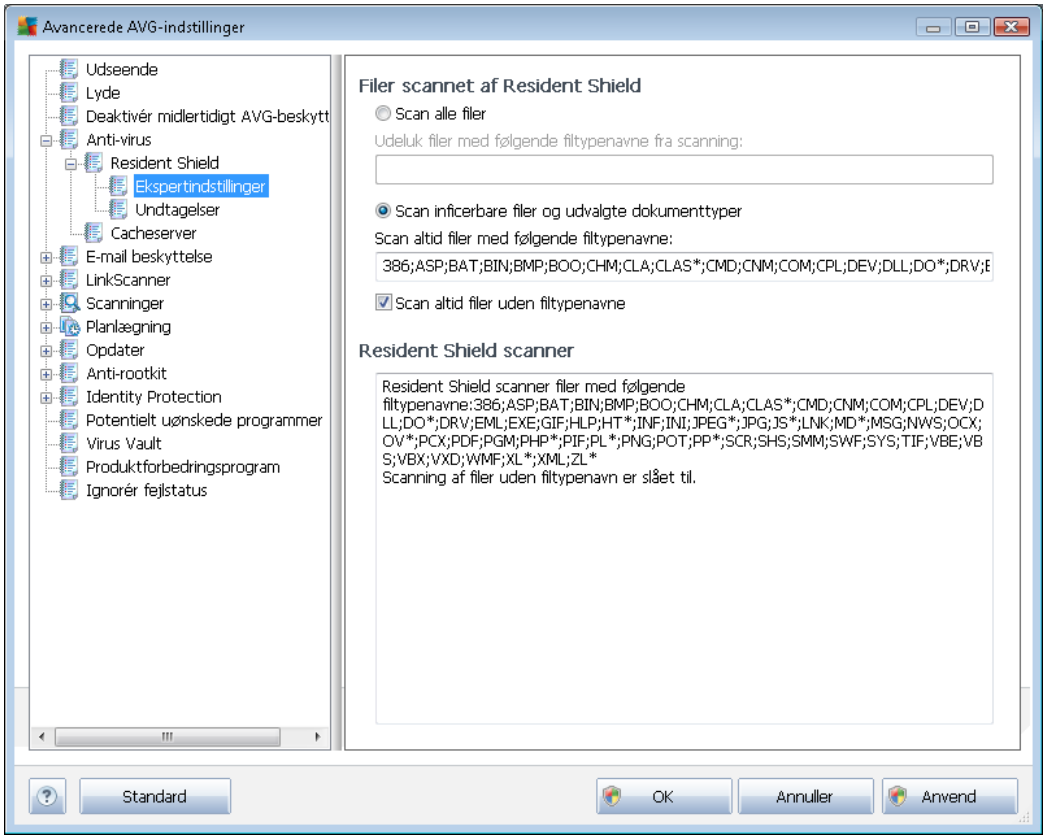
- ***Fjern alle trusler automatisk*** (*deaktiveret som standard*) – Alle registrerede infektioner heles automatisk, hvis der er en tilgængelig kur, og alle de infektioner, der ikke kan kureres, fjernes.

- ***Scan filer overført til register*** (*aktiveret som standard*) – Denne parameter definerer, at AVG scanner alle eksekverbare filer, der er føjet til startregistreringsdatabasen, for at undgå, at en kendt infektion afvikles, næste gang computeren startes.

- ***Aktivér grundig scanning*** (*deaktiveret som standard*) – Under særlige omstændigheder (*i ekstreme akutte situationer*) kan du markere denne indstilling for at aktivere de mest grundige algoritmer, som undersøger alle tænkelige trusler til bunds. Husk at denne metode er ret tidskrævende.

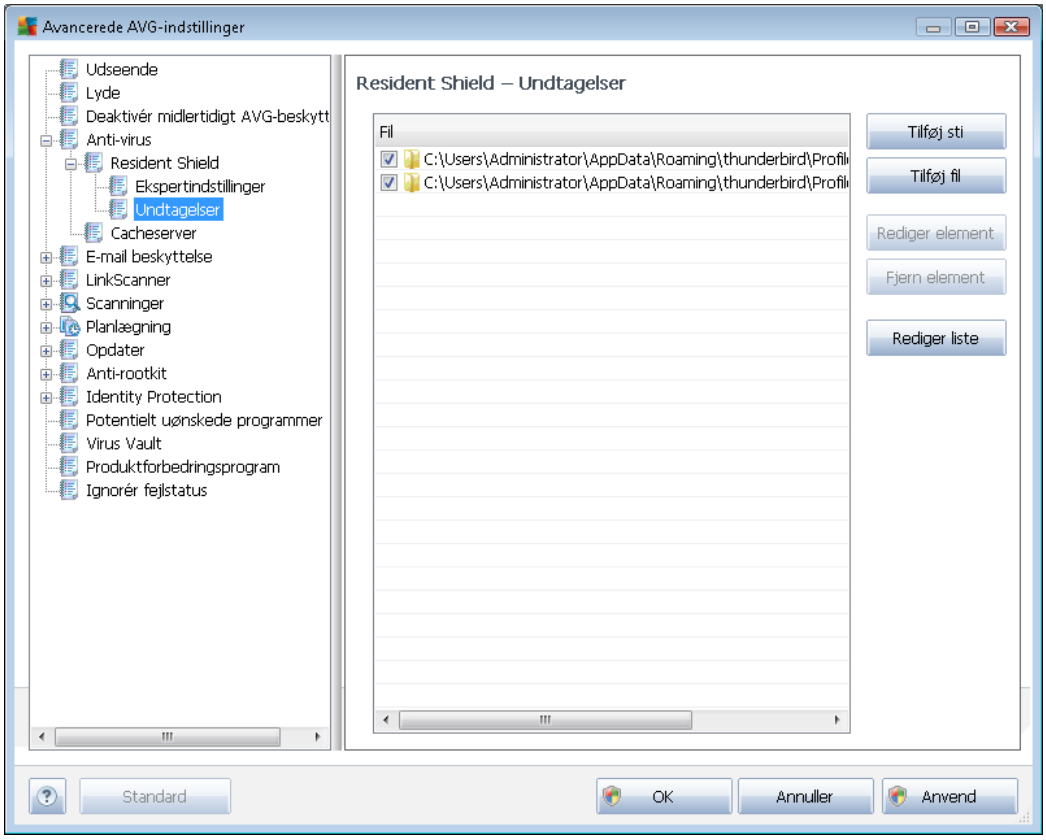
- ***Aktivér Instant Messaging-beskyttelse og P2P download-beskyttelse*** (*aktiveret som standard*) – Marker dette element, hvis du vil bekræfte, at instant messaging-kommunikation (*f.eks ICQ, MSN Messenger …*) og P2P-downloads er virusfri

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



Markér det pågældende afkrydsningsfelt for at angive, om du vil ***Scanne alle filer*** eller ***Kun scanne inficerbare filer og udvalgte dokumenttyper***. Hvis du har besluttet dig for sidstnævnte mulighed, kan du også angive en liste over udvidelser, der indeholder de filer, som skal udelades fra scanningen, samt en liste over filudvidelser, der indeholder de filer, som skal scannes i alle tilfælde.

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



Dialogen ***Resident Shield – Undtagelser*** gør det muligt at definere filer og/eller mapper, der skal udelukkes fra ***Resident Shield***-scanningen.

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

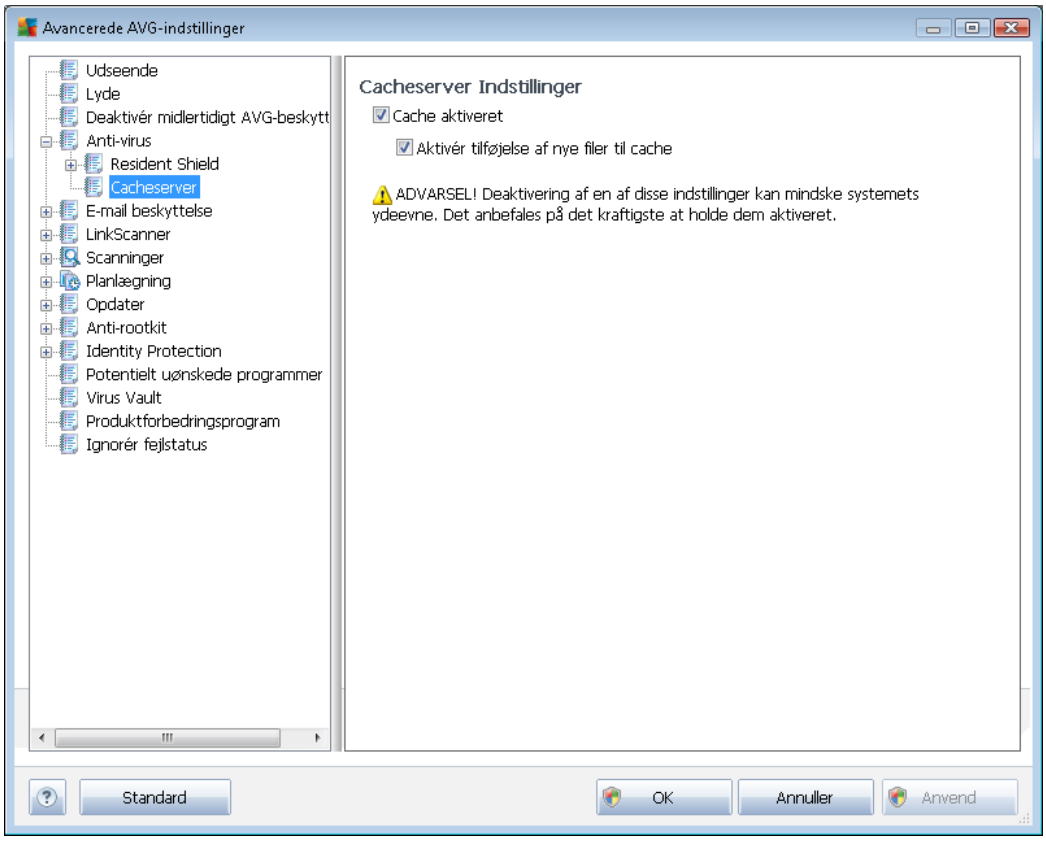
Betjeningsknapper

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
- ***Rediger liste*** – Giver dig mulighed for at redigere hele listen over definerede undtagelser i en ny dialog, som opfører sig som en normal teksteditor

9.4.2. Cacheserver

Dialogen ***Cacheserverindstillinger*** viser den cacheserverproces, der er beregnet til at fremskynde alle typer **AVG Internet-sikkerhed 2012**-scanninger:



Cacheserveren samler og bevarer oplysninger om troværdige filer (*en fil betragtes som troværdig, hvis den er underskrevet med en digital signatur fra en troværdig kilde*). Disse filer bliver derefter beskyttet, og de behøver ikke at blive scannet igen. Det er derfor, at disse filer springes over under scanningen.

Dialogen ***Cacheserverindstillinger*** indeholder følgende konfigurationsmuligheder:

- ***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.

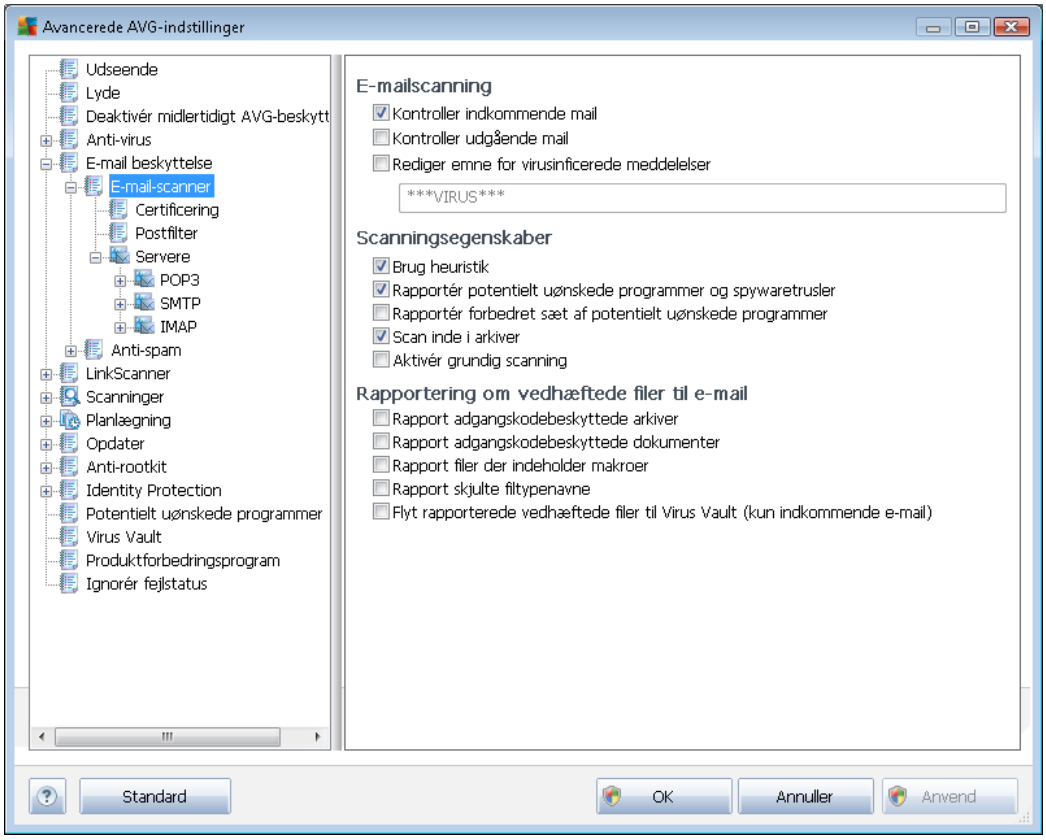
Medmindre du har en god begrundelse for at slå cacheserveren fra, anbefaler vi kraftigt, at du beholder standardindstillingerne og lader begge indstillinger være slået til! Ellers kan du opleve, at hastigheden og ydelsen for dit system aftager betydeligt.

9.5. E-mail-beskyttelse

I sektionen ***E-mail-beskyttelse*** kan du redigere en detaljeret konfiguration af E-mail-scanner og Anti-Spam:

9.5.1. 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.

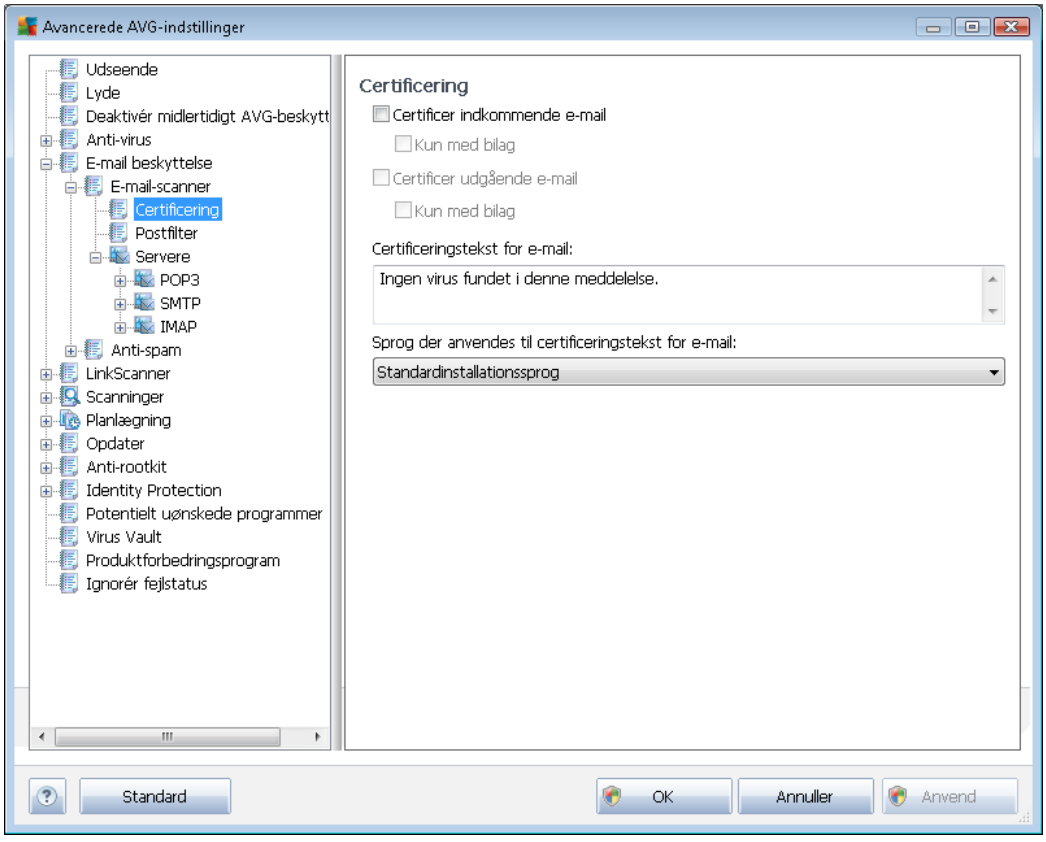
- ***Rapporter adgangskodebeskyttede dokumenter*** – dokumenter beskyttet med adgangskode er ikke mulige at scanne for vira. Marker feltet for at rapportere dem som potentielt farlige.

- ***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.

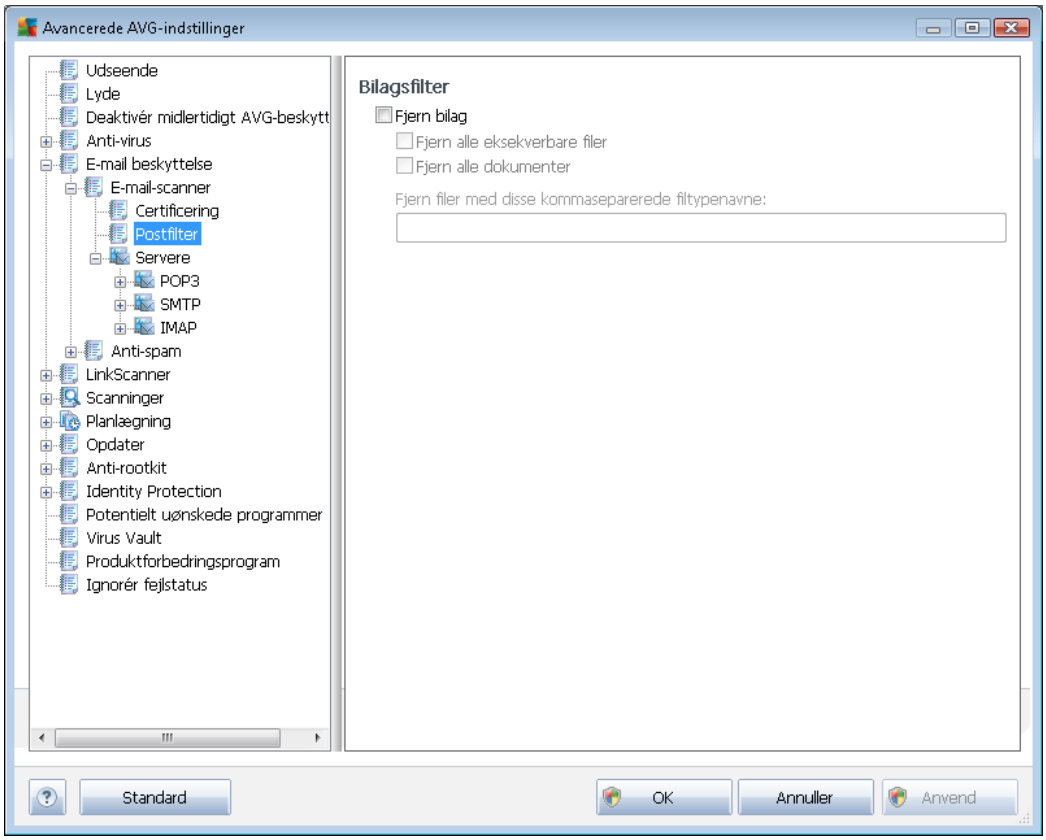
- ***Flyt rapporterede vedhæftede filer til Virus Vault*** - angiv om du vil have information via e-mail om adgangskodebeskyttede arkiver, adgangskodebeskyttede dokumenter, filer der indeholder makroer og/eller filer med skjulte filtypenavne, der detekteres som vedhæftet fil til den scannede e-mail-meddelelse. Hvis der identificeres en sådan meddelelse under scanningen, skal du definere, om det detekterede inficerbare objekt skal flyttes til Virus Vault.

I dialogen ***Certificering*** kan du markere de specifikke afkrydsningsfelter for at afgøre, om du vil certificere din indgående e-mail (***Certificer indgående e-mail***) og/eller udgående e-mail (***Certificer udgående e-mail***). Ud for hver af disse indstillinger kan du også angive parameteren ***Kun med vedhæftede filer*** , så certificeringen kun føjes til de e-mail-meddelelser, der indeholder vedhæftede filer.



Certificeringsteksten består som standard af grundlæggende oplysninger, der fastslår, at *Der blev ikke fundet nogen virus i denne meddelelse.* Disse oplysninger kan dog udvides eller ændres efter dine behov: Angiv den ønskede certificeringstekst i feltet ***Tekst til certificerings-e-mail*** . I sektionen ***Sprog i certificerings-e-mailen*** kan du definere, hvilket sprog den automatisk genererede del af certificeringen (*Ingen virus fundet i denne meddelelse*) skal vises på.

***Bemærk!** Det er kun standardteksten, der vises på det angivne sprog, og din brugerdefinerede tekst oversættes ikke automatisk!*



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:

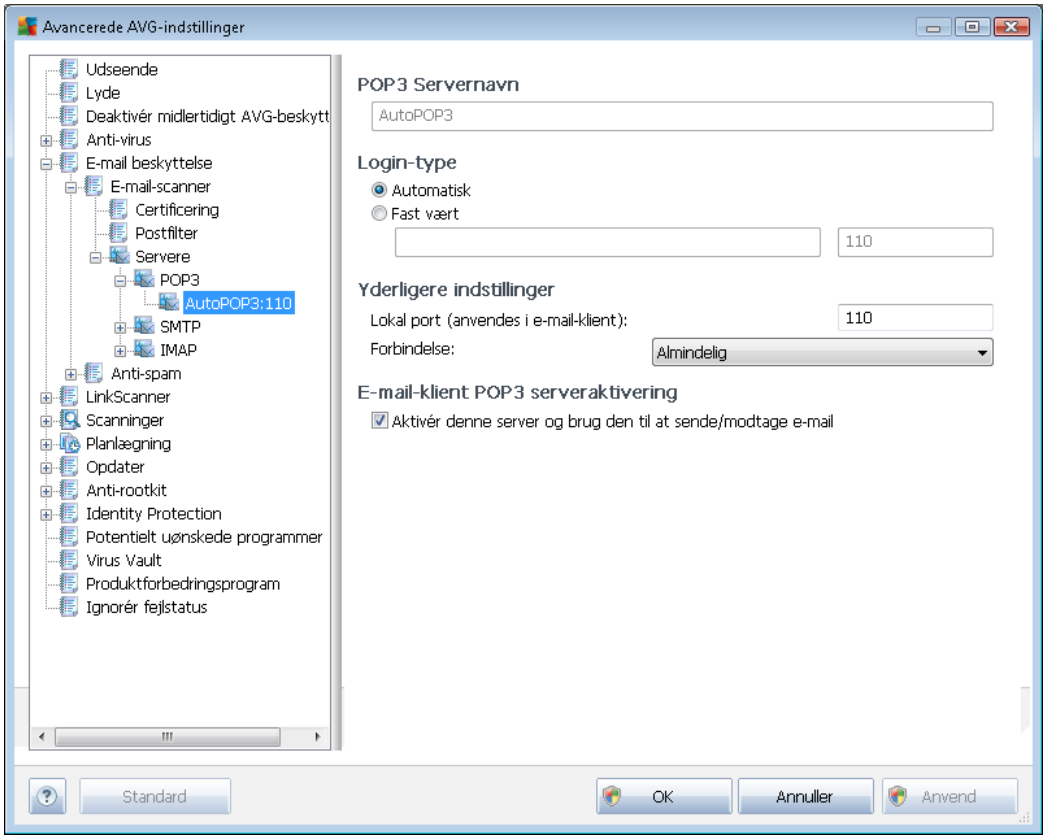
- ***Fjern alle eksekverbare filer*** - alle *.exe-filer bliver slettet
- ***Fjern alle dokumenter*** - alle *.doc, *.docx, *.xls, *.xlsx filer vil blive slettet
- ***Fjern filer med disse kommaseparerede filtypenavne*** - fjerner alle filer med de definerede filtypenavne

I sektionen ***Servere*** kan du redigere parametrene for E-mail-scanner-serverne:

- POP3-server
- SMTP-server

- IMAP-server

Du kan også definere en ny server til indgående og eller udgående post ved hjælp af knappen ***Tilføj ny server***.

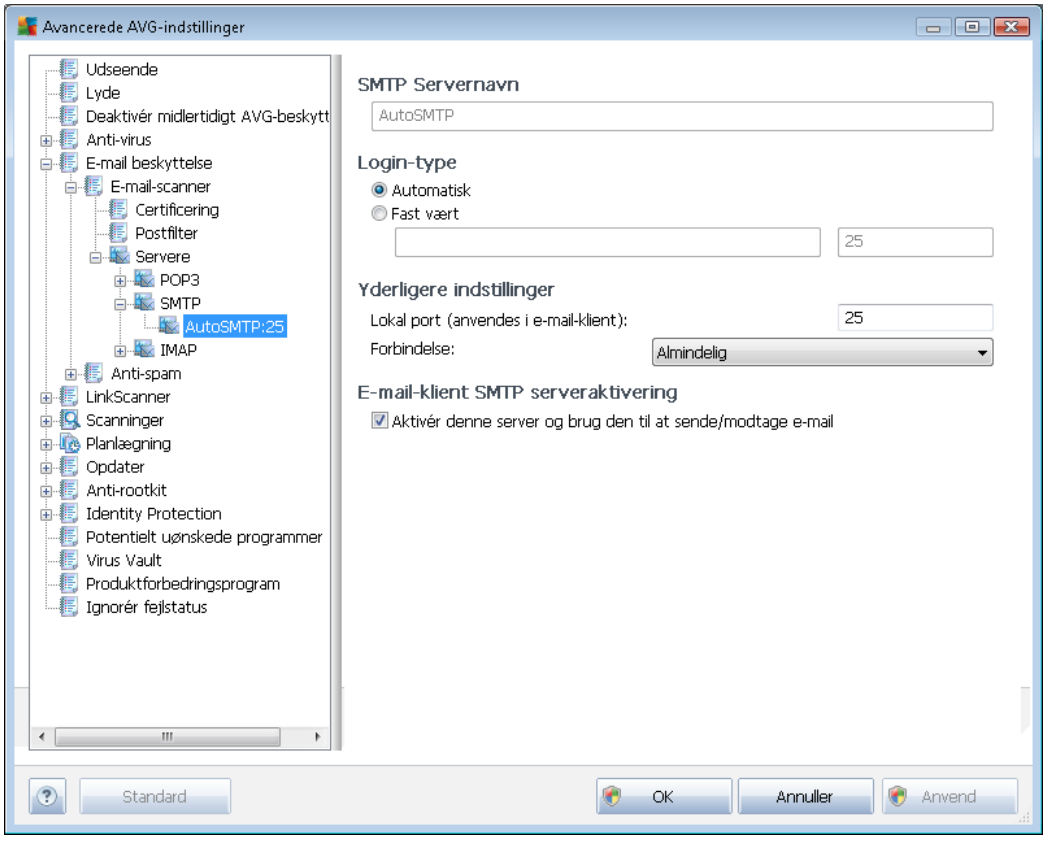


I denne dialogboks (*åbnes via **Servere / POP3***) kan du konfigurere en ny E-mail scanner-server vha. POP3-protokollen for indkommende e-mail:

- ***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.

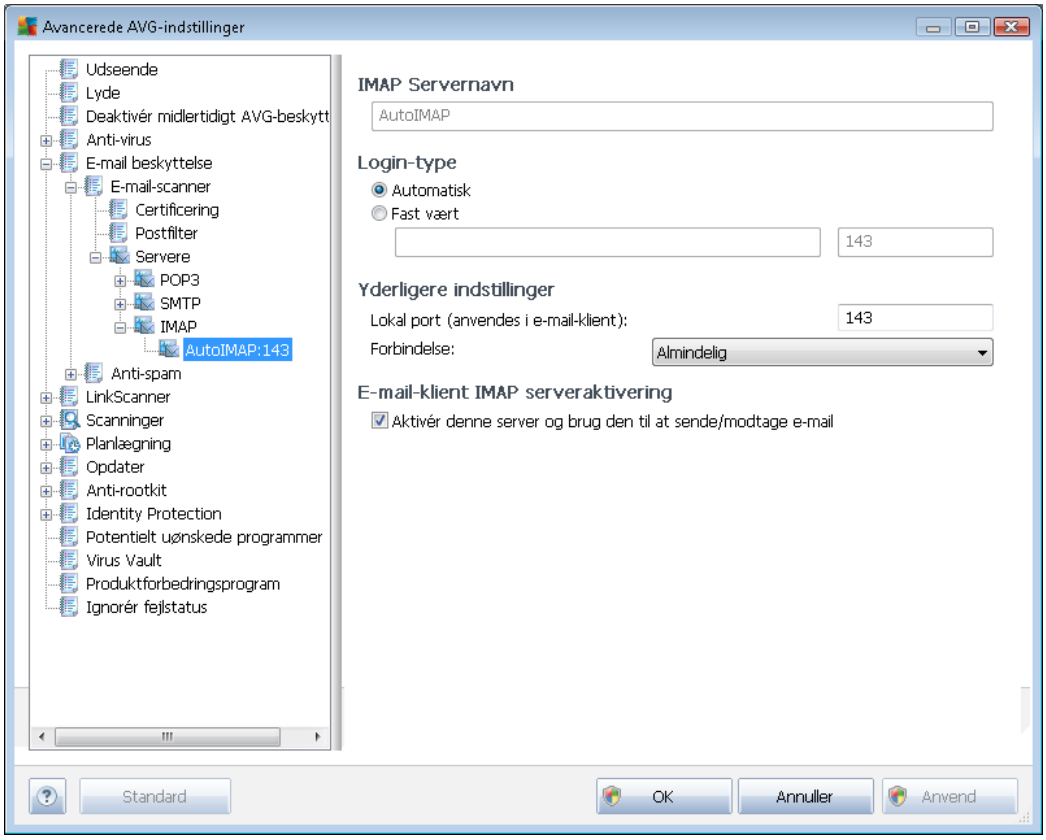
- ***Yderligere indstillinger*** - angiver mere detaljerede parametre:
  - ***Lokal port*** - angiver den port, hvor kommunikation fra din mailapplikation forventes. Du skal derefter angive denne port som port for POP3-kommunikation i dit e-mail-program.
  - ***Forbindelse*** - in i rullemenuen kan du 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-

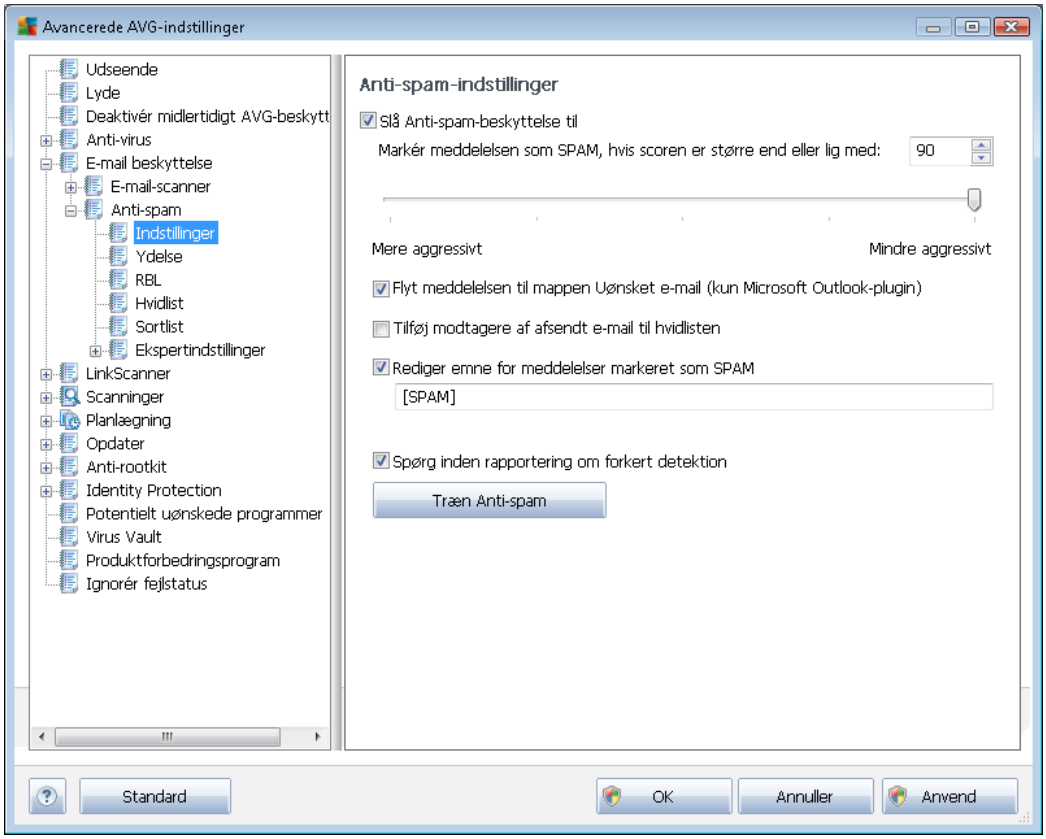
program.

- ***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

9.5.2. Anti-spam

Indtast emnetekst her.



I dialogen ***Anti-spam-indstillinger*** kan du markere eller fjerne markeringen fra afkrydsningsfeltet ***Slå Anti-spam-beskyttelse til*** for at tillade/forhindre 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.

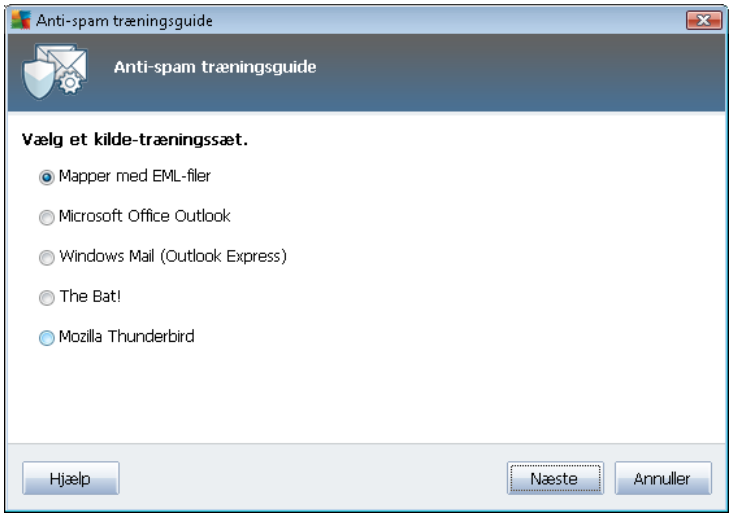
I dialogen ***Anti-spam-indstillinger*** kan du derudover definere, hvordan de detekterede spam-e-mails skal behandles:

- ***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*** – Det kræver, at du under installationsprocessen accepterer 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:

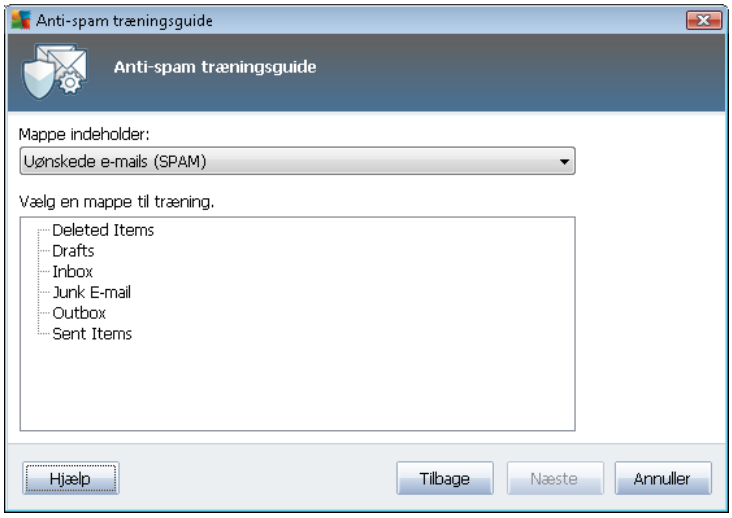
- ***En specifik e-mail-klient*** - hvis du bruger en af de anførte e-mail-klienter (*MS Outlook, Outlook Express, The Bat!,*), skal du helt enkelt vælge den pågældende indstilling.
- ***Mappe med EML-filer*** - hvis du bruger et andet e-mail-program, skal du først gemme meddelelserne i en specifik mappe (*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



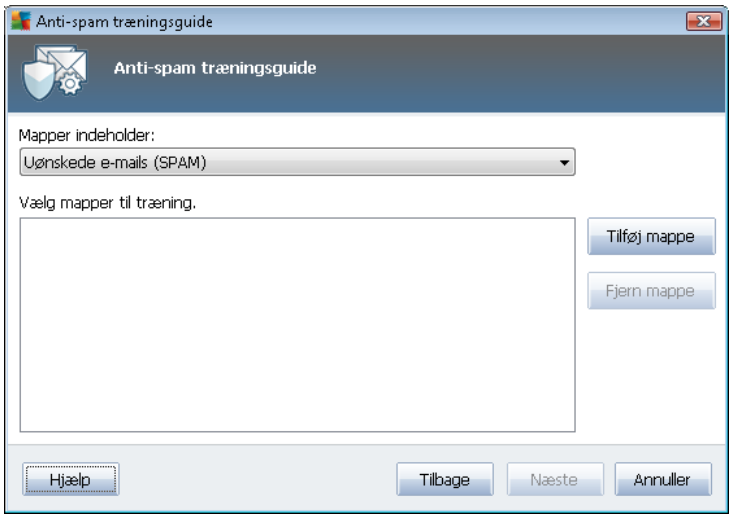
I denne dialog skal du vælge mappen med de meddelelser, du vil anvende til træning. Tryk på knappen ***Tilføj mappe*** for at finde mappen med .eml-filer (*gemte e-mail-meddelelser*). Den valgte mappe vises derefter i dialogen.

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

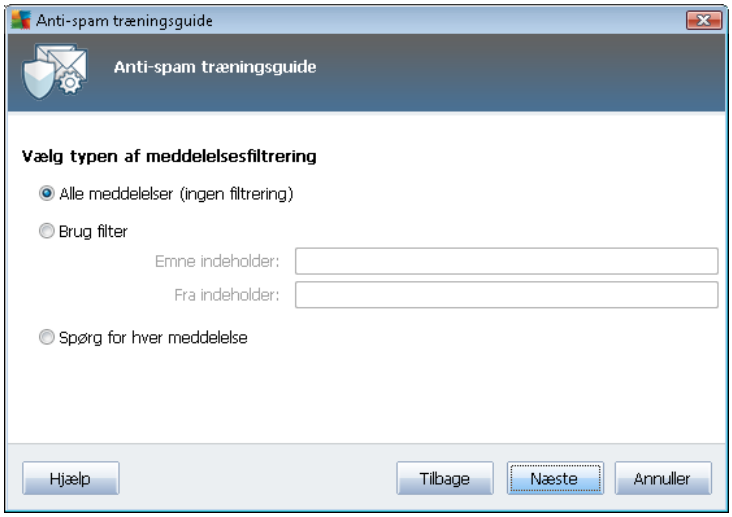
Når du bekræfter en af indstillingerne, vises en ny dialog.



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.

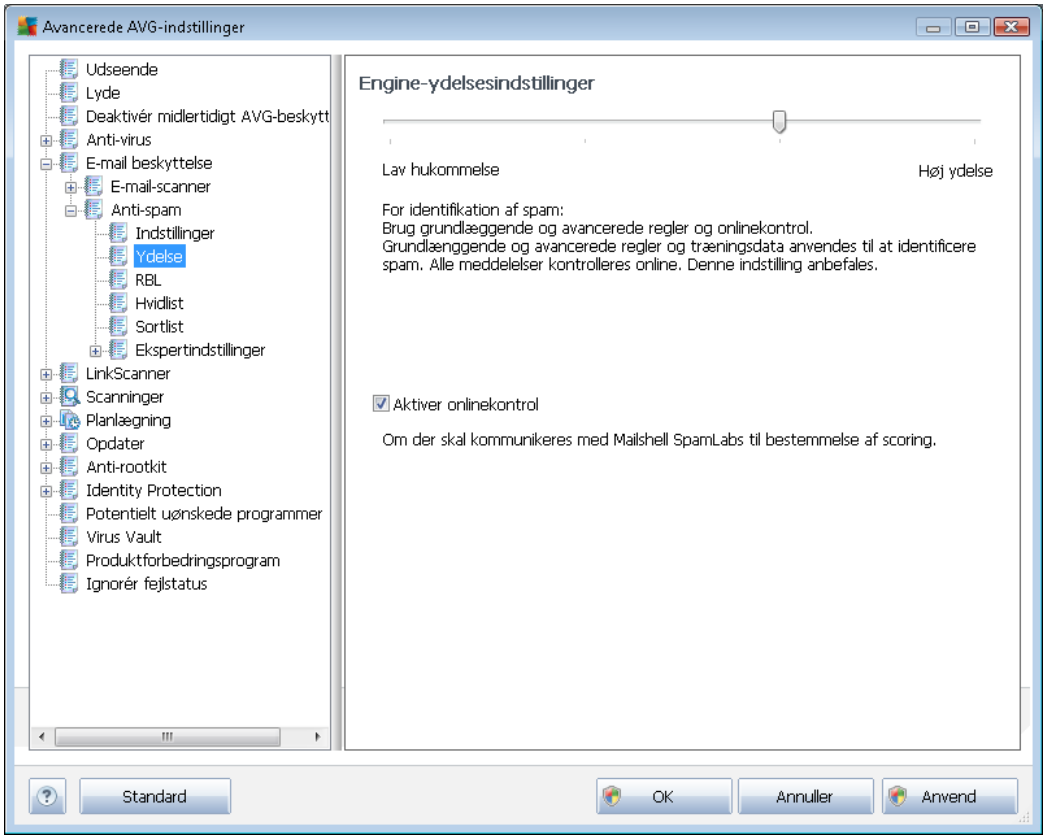
- ***Alle meddelelser (ingen filtrering)*** – Hvis du er sikker på, at den valgte mappe kun indeholder meddelelser, du vil bruge til træning, skal du markere indstillingen ***Alle meddelelser (ingen filtrering)***.

- ***Brug filter*** – Hvis du ønsker mere avanceret filtrering, kan du vælge indstillingen ***Brug filter*** . 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. Hvis du udfylder begge tekstfelter, anvendes også adresser, der kun svarer til en af de to betingelser!

- ***Spørg for hver meddelelse*** – Hvis du ikke er sikker på de meddelelser, der er indeholdt i mappen, og du ønsker, at guiden skal spørge dig om hver enkelt meddelelse *(så du kan fastslå, om den skal bruges til træning eller ej)*, skal du markere indstillingen ***Spørg for hver meddelelse***.

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.

Dialogen ***Engine-ydelsesindstillinger*** (*der er et link til den via indstillingen* ***Ydelse*** *i den venstre navigationsdel*) har indstillinger for ydelsen af komponenten ***Anti-Spam***:



Flyt skyderen til venstre ellller højre for at ændre scanningens ydelsesniveau mellem tilstandene ***Lav hukommelse*** / ***Høj ydelse***.

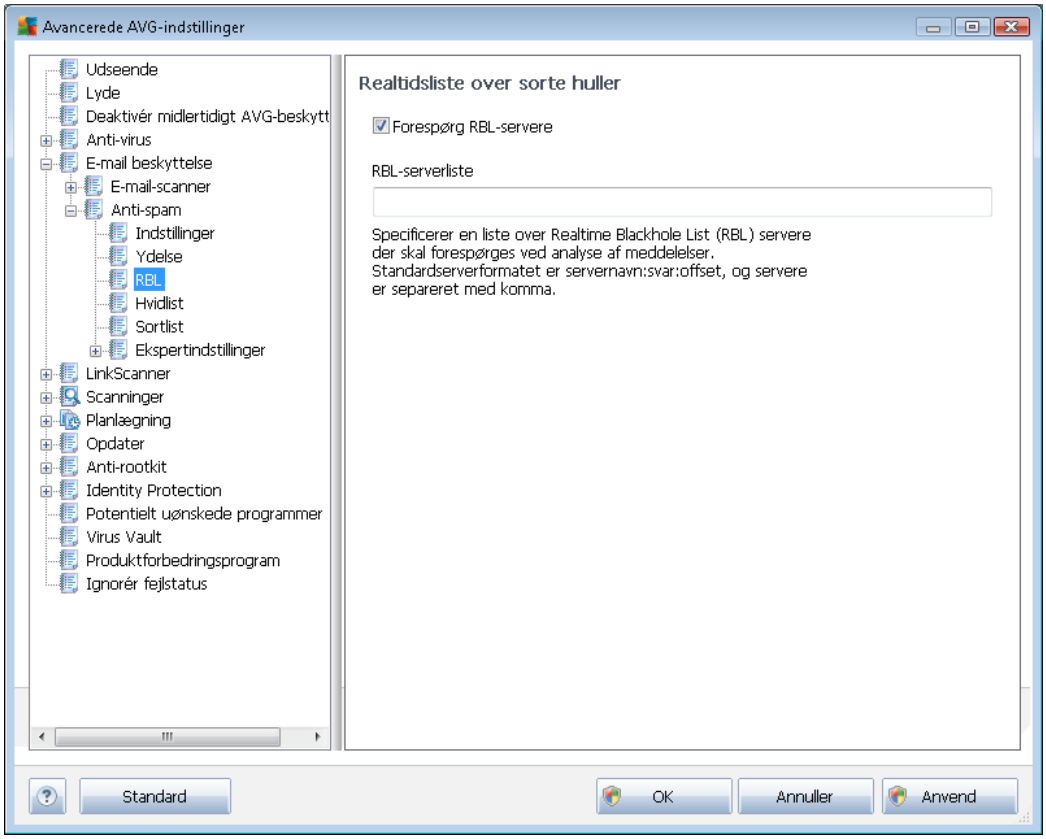
- ***Lav hukommelse*** – Der anvendes ingen regler under scanningsprocessen for at identificere spam. Kun træningsdata bruges til identifikation. Denne tilstand anbefales ikke til almindelig brug, medmindre computerhardwaren er virkelig dårlig.

- ***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 spam via 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!

Indstillingen ***RBL*** åbner en redigeringsdialog, der kaldes ***Realtidsliste over sorte huller***, hvor du kan slå funktionen ***Forespørg i RBL-servere*** til og fra:

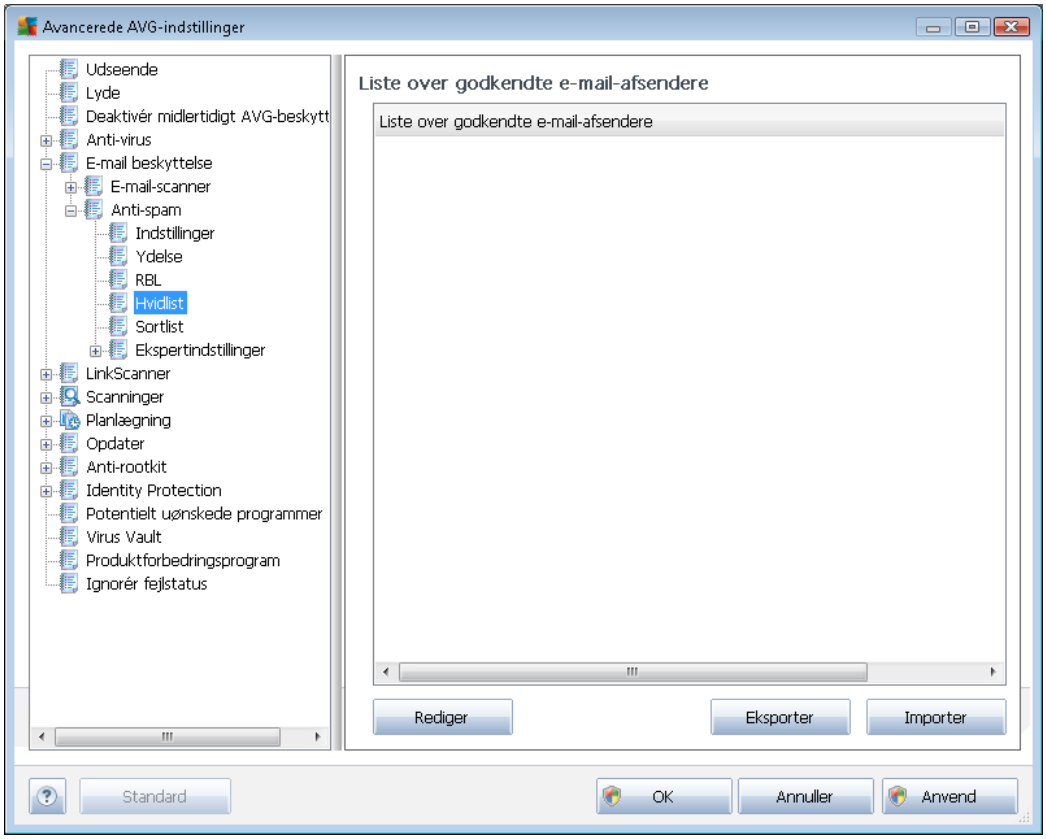


RBL-serveren (*Realtime Blackhole List*) er en DNS-server med en omfattende database over kendte spam-afsendere. Når denne funktion er aktiveret, vil alle e-mail meddelelser blive verificeret mod RBL-serverdatabasen og blive markeret som spam, hvis de er identiske med poster i databasen. RBL-serverdatabaserne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

RBL-serverliste gør det muligt at definere specifikke RBL-serverplaceringer (. *Undlad dette, da en aktivering af denne funktion på visse systemer og med visse konfigurationer kan gøre modtagelsen af e-mails langsommere, da hver enkelt meddelelse skal bekræftes i forhold til RBL-serverdatabasen).*

Der sendes ingen personlige data til serveren!

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.



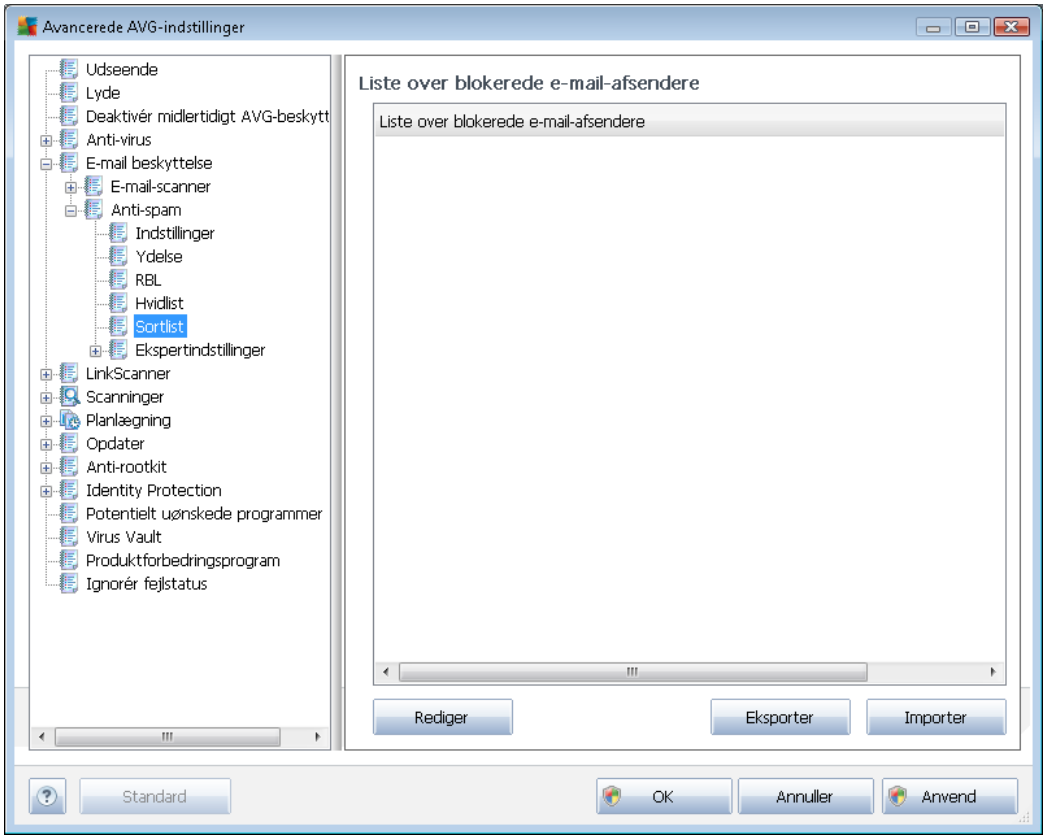
I redigeringsgrænsefladen kan du sammensætte en liste over afsendere, som du er sikker på aldrig vil sende dig uønskede meddelelser (spam). Du kan også sammensætte en liste med domænenavne (*f.eks. avg.com*), som du ved ikke genererer spammeddelelser. Når du først har klargjort en liste over afsendere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

Betjeningsknapper

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.

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.

Betjeningsknapper

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.

Grenen Avancerede indstillinger indeholder udvidede indstillingsmuligheder for Anti-spam-komponenten. Disse indstillinger er udelukkende 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.

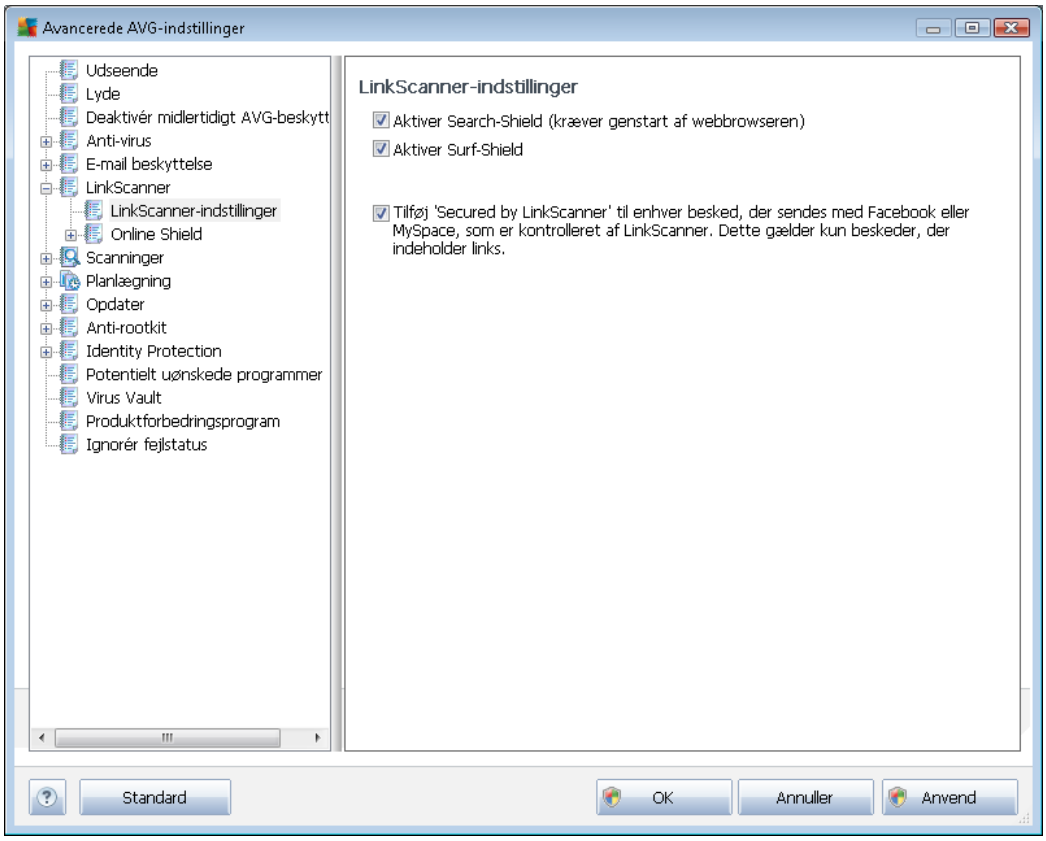
Hvis du stadig mener, det er nødvendigt at ændre Anti-spam-konfigurationen på det meget avancerede niveau, skal du følge vejledningen, der findes i selve brugergrænsefladen. Generelt findes der i hver dialog en enkelt specifik funktion, og du kan redigere den - beskrivelsen af den findes altid i selve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

9.6. Linkscanner

9.6.1. Linkscanner-instillinger

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

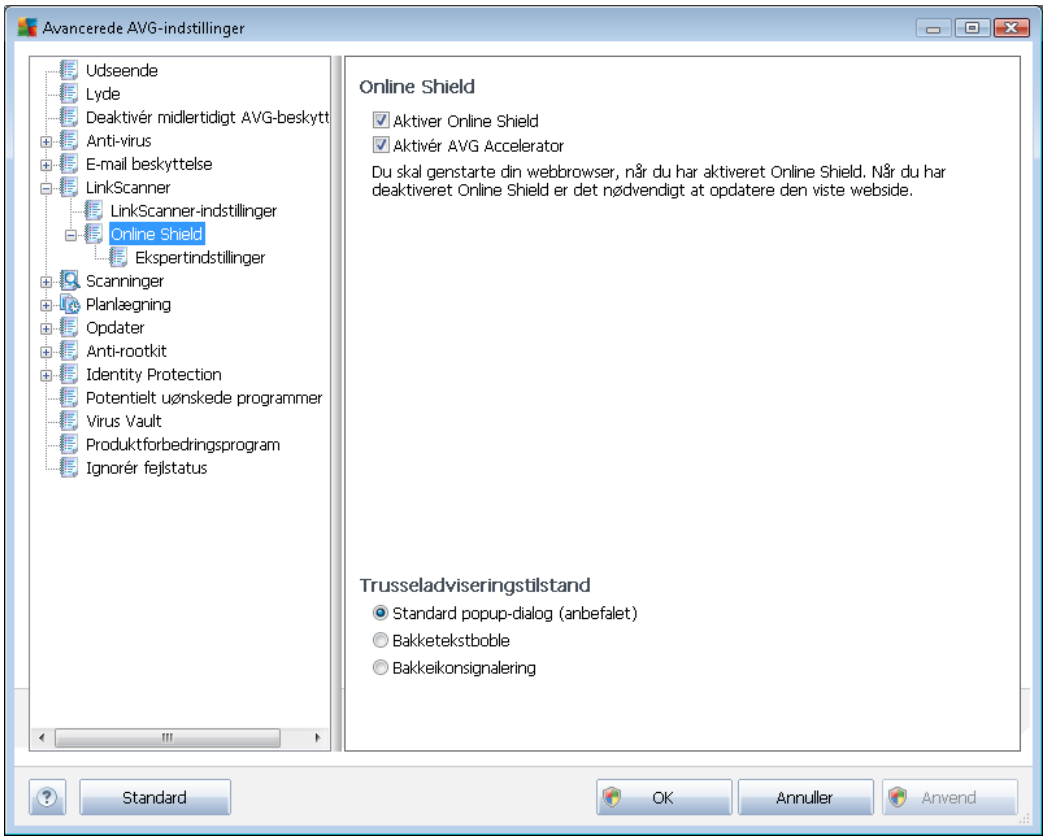


- ***Aktiver Søgeskjold*** - (*slået til som standard*): vejledende ikoner på søgninger udført i Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg, or SlashDot efter forudgående kontrol af indholdet på de websteder, der returneres af søgemaskinen.

- ***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' ...*** – (*aktiveret som standard*): Markér denne indstilling for at bekræfte, at du vil angive certificeringsmeddelelsen ved en Link Scanner-kontrol på alle meddelelser, der indeholder aktive hyperlinks, der blev sendt fra Facebook og MySpace.

9.6.2. Online Shield



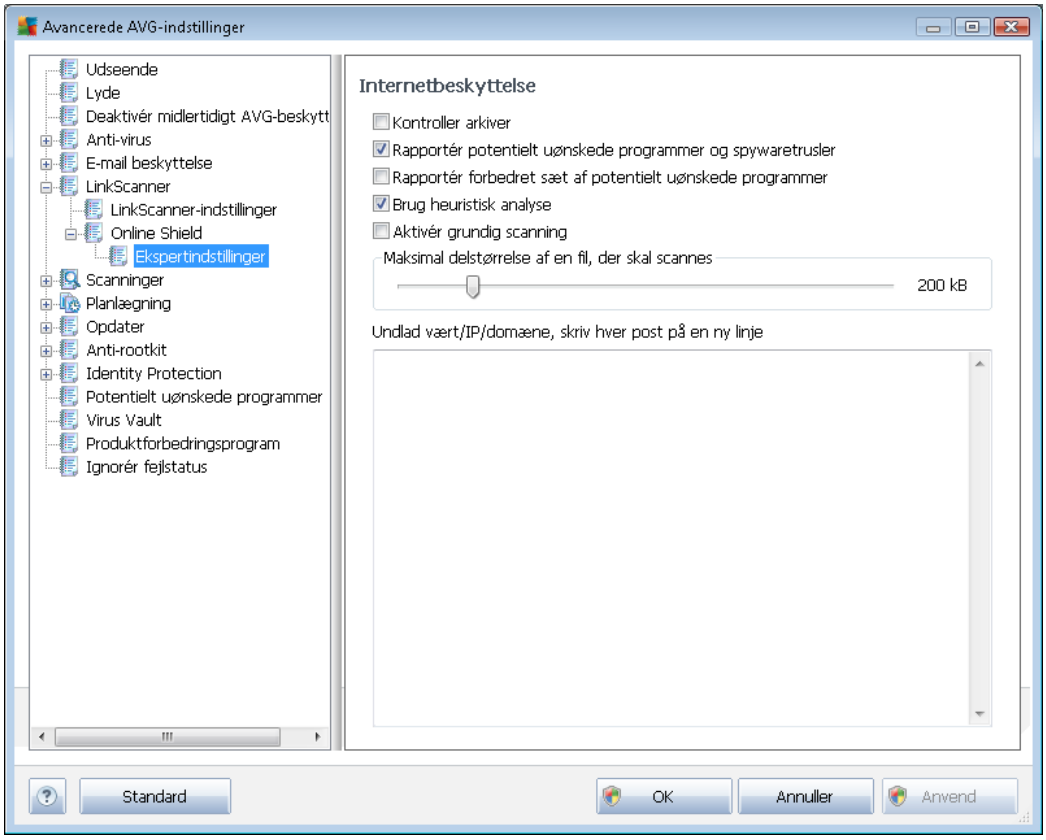
Dialogen ***Online Shield*** har følgende indstillingsmuligheder:

- ***Aktivér Online Shield*** *(aktiveret som standard)* – Aktiver/deaktiver hele ***Online Shield***-tjenesten. Hvis du ønsker flere avancerede indstillinger for ***Online Shield*** , skal du fortsætte til den efterfølgende dialog, der hedder Internetbeskyttelse.

- ***Aktivér AVG Accelerator*** *(aktiveret som standard)* - Aktiver/deaktiver tjenesten ***AVG Accelerator***, som medfører en problemfri videoafspilning på nettet og gør ekstra downloads nemmere..

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.



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*): Klik for at aktivere Anti-Spyware-programmet, og scan for spyware og virus. 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.

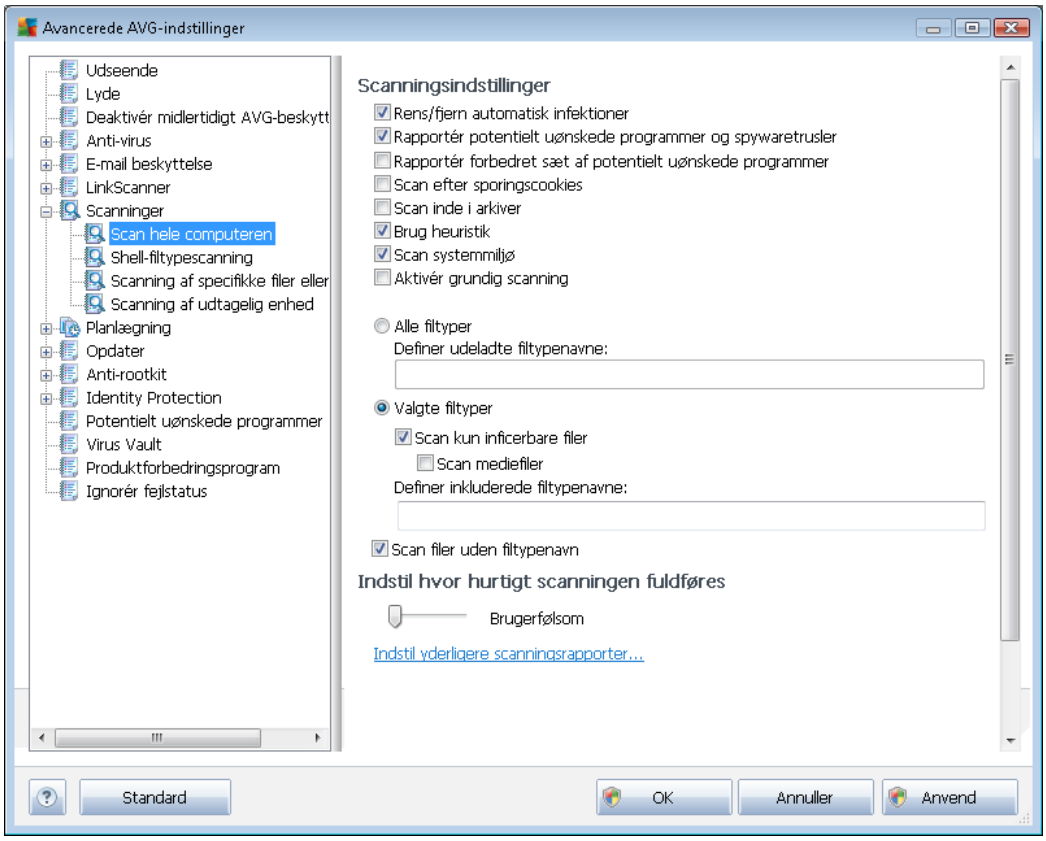
9.7. Scanninger

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
- ***Scanning af specifikke filer eller mapper*** – standardforuddefineret scanning af udvalgte områder på computeren
- ***Scanning af udtagelig enhed*** - specifik scanning af udtagelige enheder sluttet til computeren

9.7.1. Scanning af hele computeren

Indstillingen ***Fuld computerscanning*** gør det muligt at redigere parametrene for en af de scanninger, der er foruddefineret af scanningsleverandøren, Fuld computerscanning:



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 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.

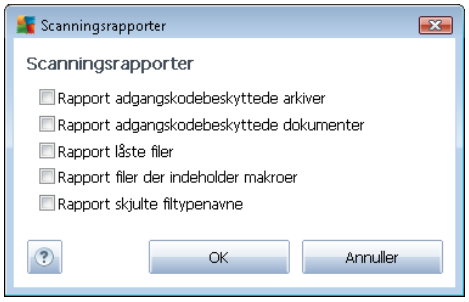
Indstil hvor hurtigt scanningen fuldføres

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.

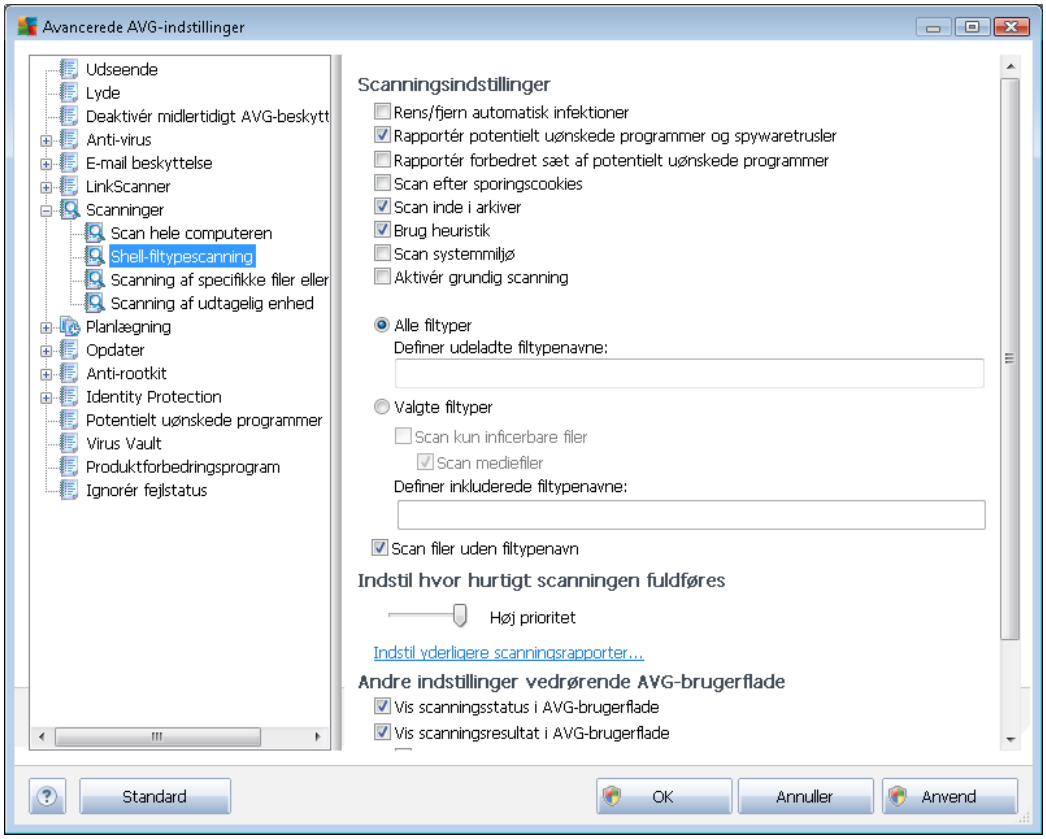
Indstil yderligere scanningsrapporter...

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:



9.7.2. 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:



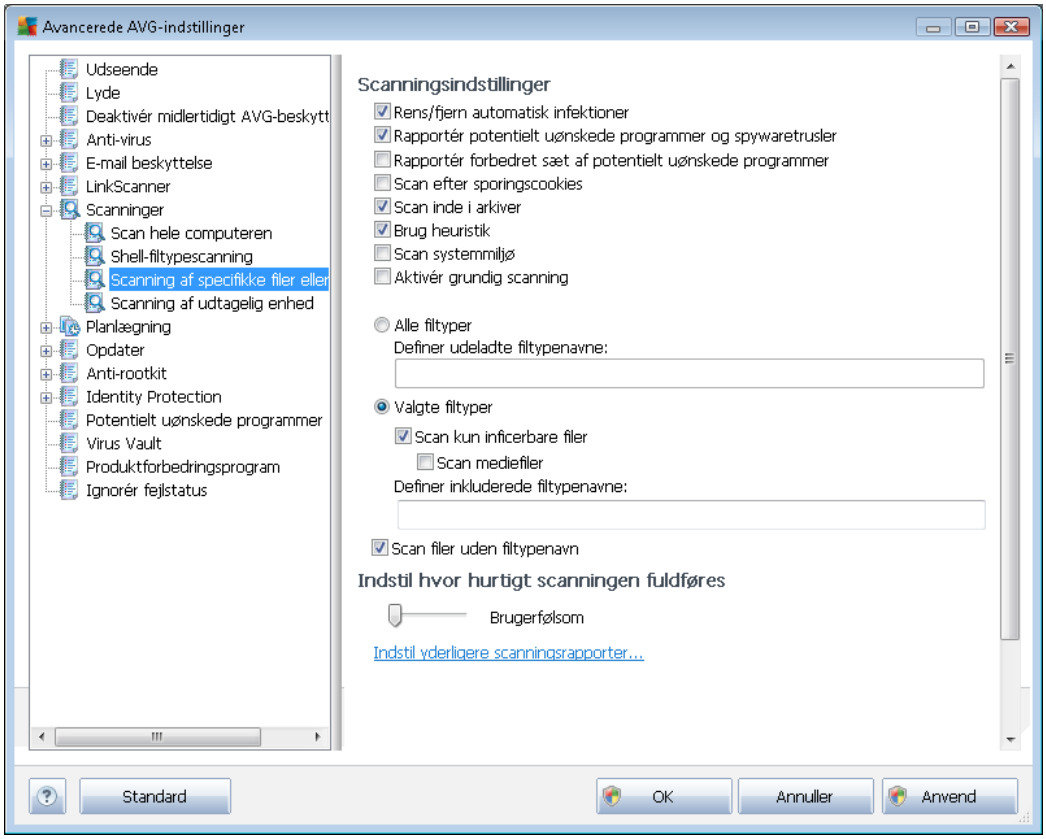
Parameterlisten er magen til listerne for Scanning af hele computeren. Standardindstillingerne varierer dog (*for eksempel kontrollerer Scanning af hele computeren ikke arkiver, men scanner systemmiljøet, mens det med Shell-udvidelsesscanning er omvendt*).

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

I forhold til dialogen Fuld computerscanning har dialogen ***Shell-udvidelsesscanning*** også sektionen ***Andre indstillinger, der er relateret til AVG-brugergrænsefladen***, hvor du kan angive, om scanningsprocessen og scanningsresultaterne skal være tilgængelige i AVG-brugergrænsefladen. Du kan også angive, at scanningsresuultatet kun vises, hvis der detekteres infektion under scanningen.

9.7.3. Scanning af 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:

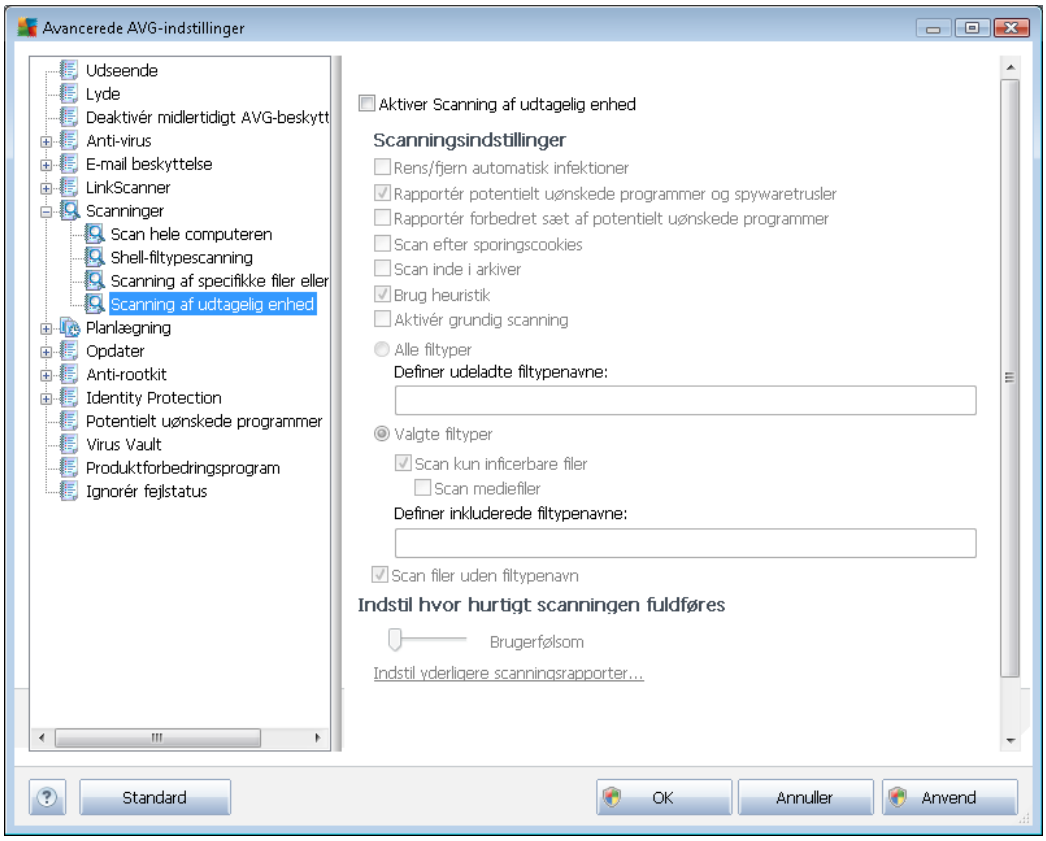


Alle parametre indstillet i denne konfigurationsdialog gælder kun for de områder, der er udvalgt til scanning med Scanning af specifikke filer eller mapper!

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

9.7.4. 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.*

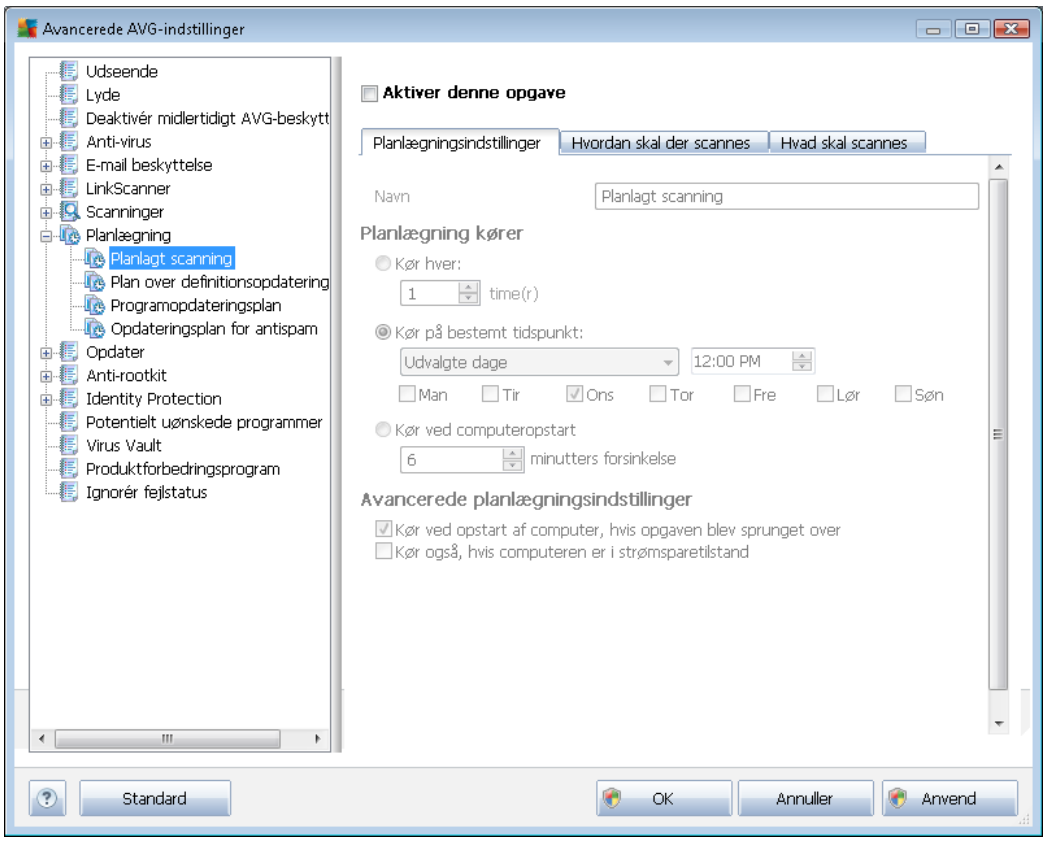
9.8. Planlægning

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

- Planlagt scanning
- Plan over definitionsopdatering
- Programopdateringsplan
- Anti-spam-opdateringsplan

9.8.1. 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:

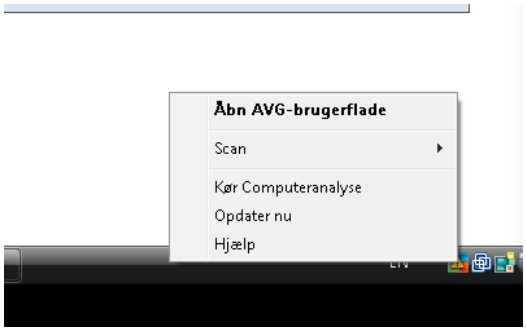
Planlægning kører

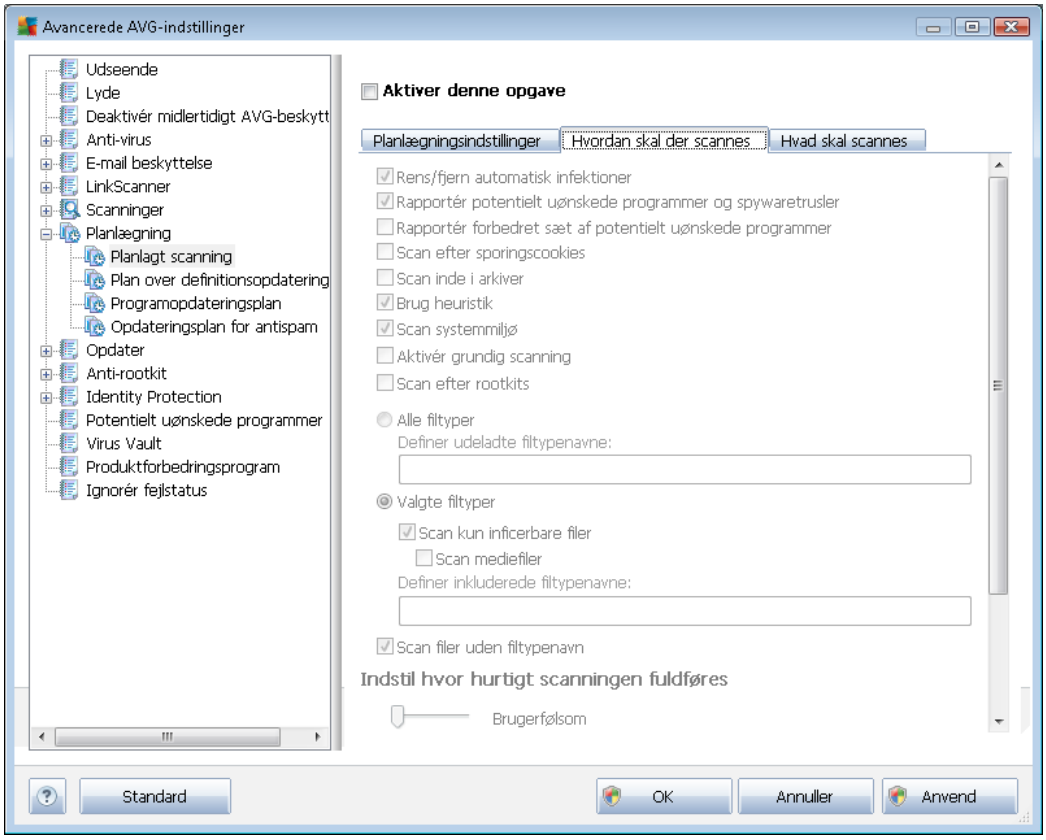
Her kan du angive tidsintervaller for kørsel af den nyplanlagte scanning. Tidsindstillingen kan enten defineres via den gentagne scanningsstart efter et bestemt tidsrum (***Kør hver ...***) eller ved at definere en præcis dato og et bestemt klokkeslæt (***Kør med bestemte mellemrum...***) eller muligvis ved at definere en hændelse, som scanningsstarten skal tilknyttes (***Kør ved computerstart***).

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.

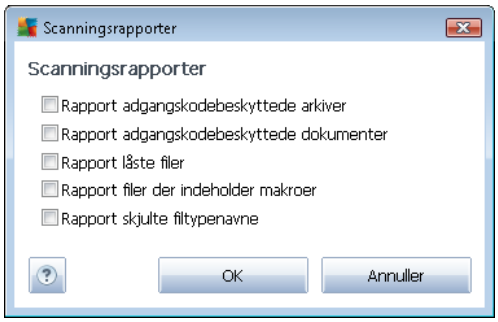
Indstil hvor hurtigt scanningen fuldføres

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.

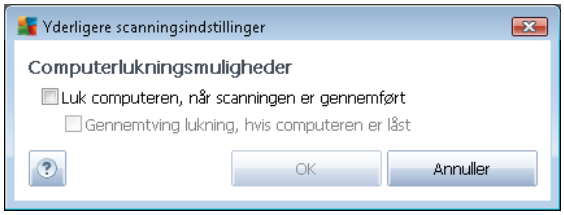
Indstil yderligere scanningsrapporter

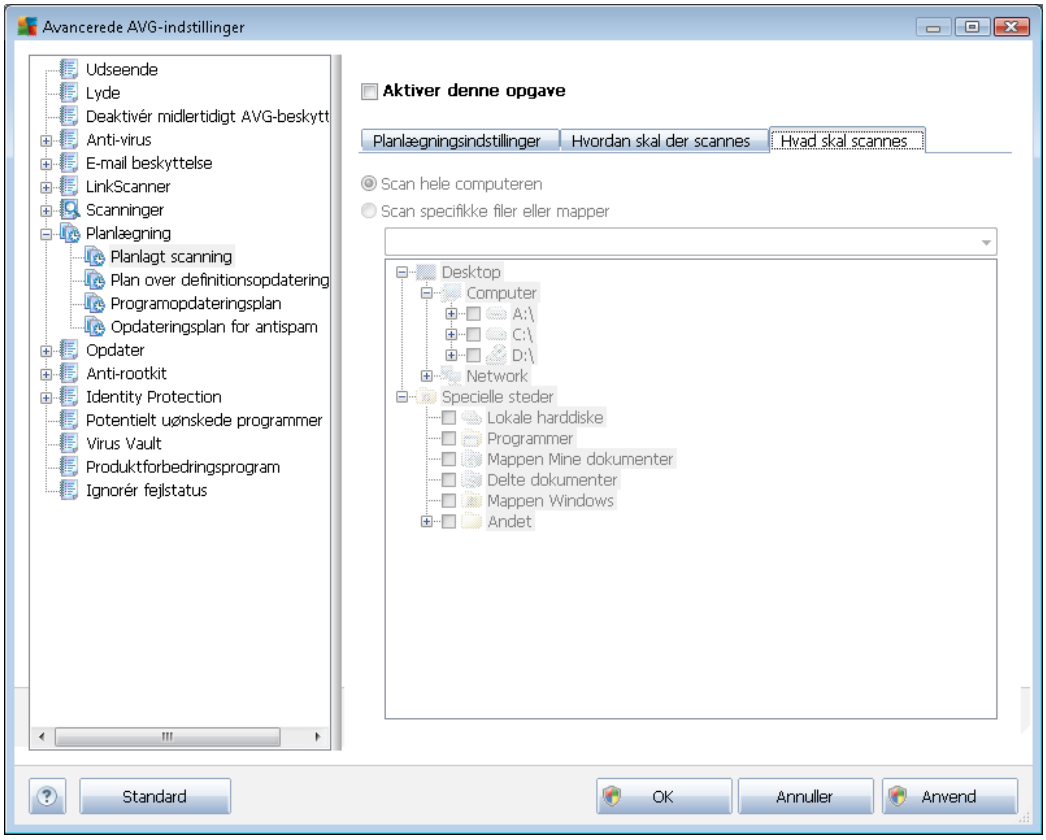
Klik på linket ***Indstil yderligere scanningsrapporter ...*** for at åbne det selvstændige dialogvindue ***Scanningsrapporter***, hvor du kan markere adskillige punkter for at definere, hvilke scanningsfund, der skal rapporteres:



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***).

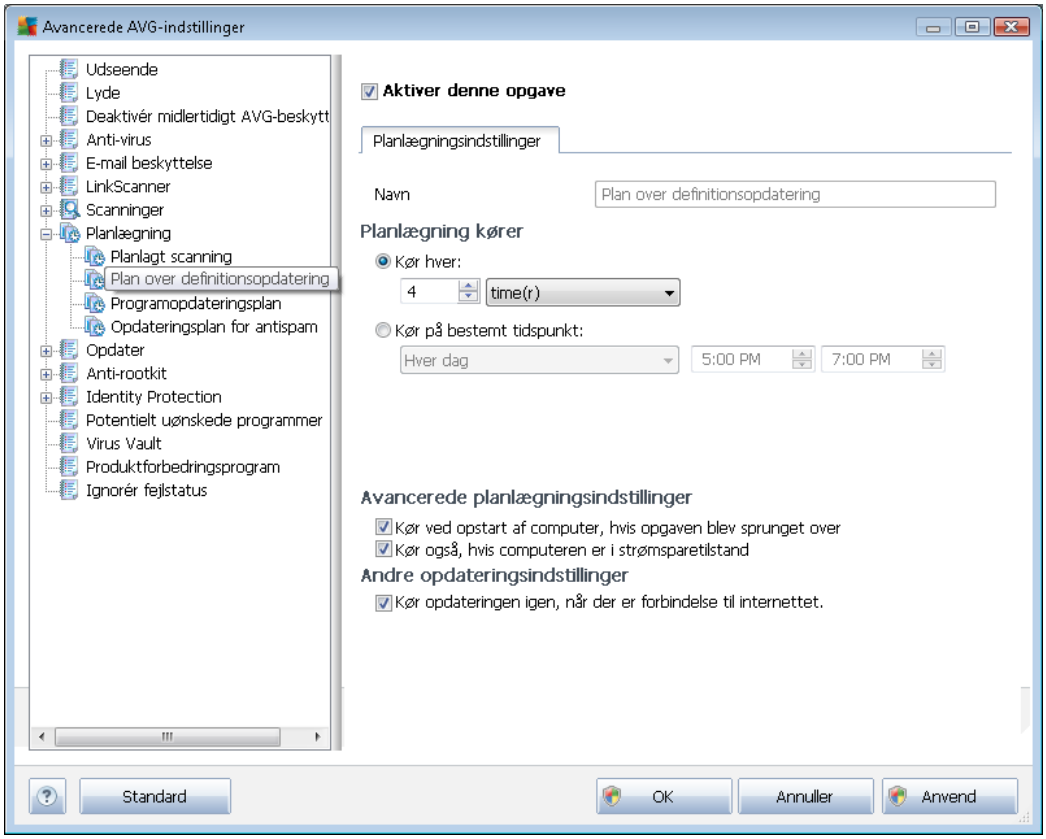




På fanen ***Hvad skal scannes*** kan du definere, om du vil planlægge scanning af hele computeren eller scanning af specifikke filer eller mapper. Hvis du vælger scanning af specifikke filer eller mapper, aktiveres træstrukturen nederst i denne dialogboks, og du kan angive mapper, der skal scannes.

9.8.2. Plan for opdatering af definitioner

Hvis det ***virkelig er nødvendigt***, kan du fjerne markeringen af indstillingen ***Aktivér denne opgave*** , så du blot deaktiverer den planlagte definitionsopdatering midlertidigt for så at kunne slå den til igen på et senere tidspunkt:



I denne dialog kan du konfigurere nogle detaljerede parametre for planen for definitionsopdatering. I tekstfeltet ***Navn*** (*deaktiveret for alle standardplaner*) står navnet, der af programleverandøren er tildelt netop denne plan.

Planlægning kører

I denne sektion skal du angive tidsintervallerne for start af definitionsopdateringer, der er planlagt for nylig. 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 dette afsnit får du mulighed for at definere, under hvilke betingelser definitionsopdateringerne skal startes eller ikke skal startes, hvis computeren kører i lav energitilstand eller er slukket helt.

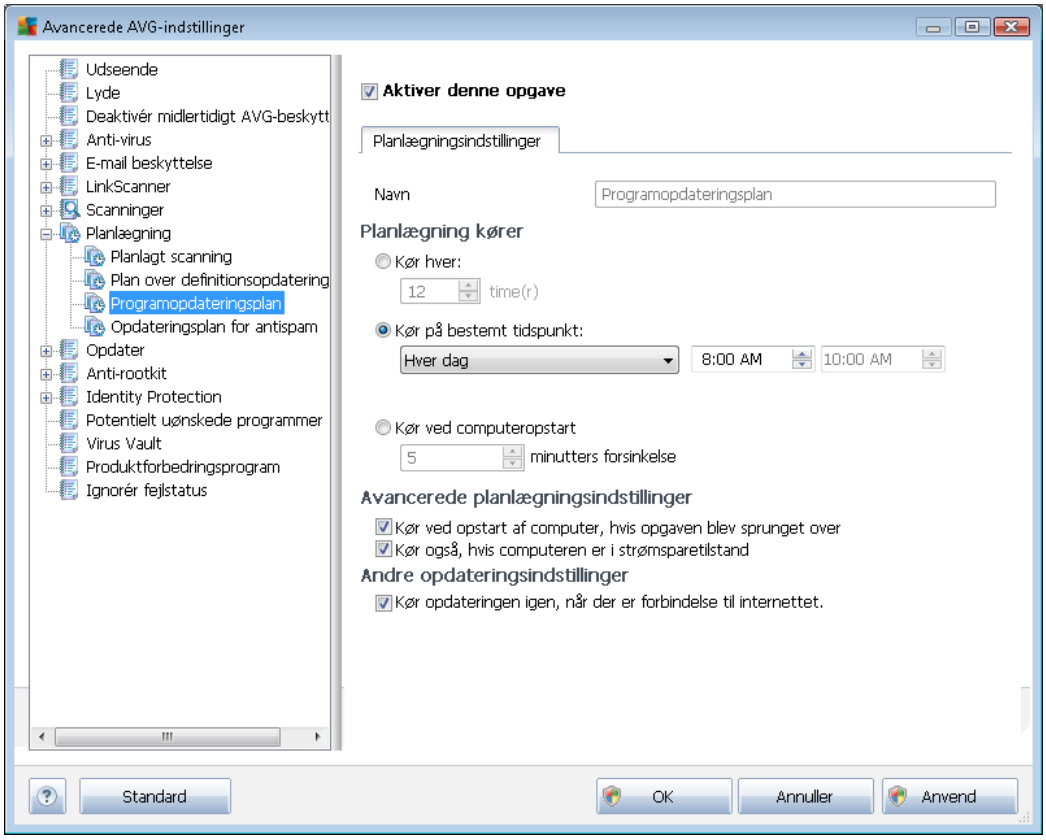
Andre opdateringsindstillinger

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*).

9.8.3. 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.

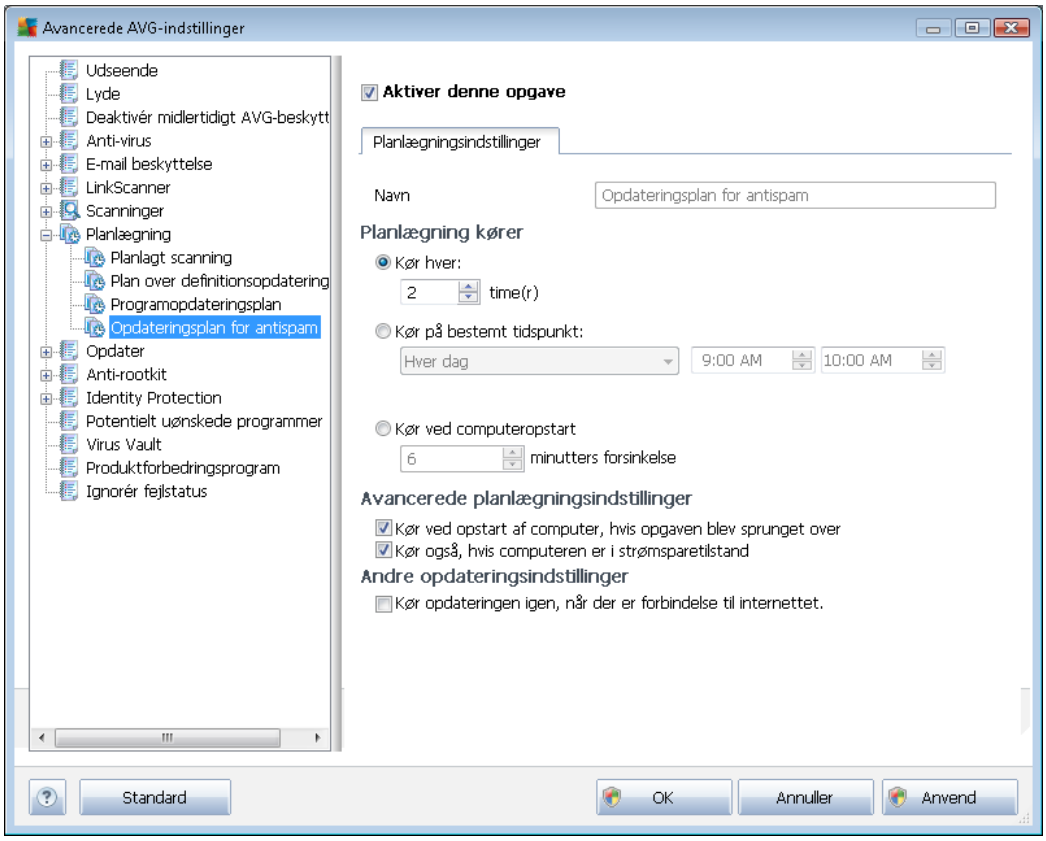
Andre opdateringsindstillinger

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 er startet på de angivne tidspunkt, får du besked om dette via et pop op-vindue, der åbnes over systembakkeikonet for AVG, (*hvis 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.*

9.8.4. Anti-spam opdateringsplan

Hvis det virkelig er nødvendigt, kan du fjerne markeringen i afkrydsningsfeltet ***Aktivér denne opgave*** for midlertidigt at deaktivere den planlagte opdatering af Anti-spam og slå den til igen senere:



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 i et specifikt tidsinterval...***) eller muligvis ved at definere en hændelse, der knyttes til kørsel af opdateringen (***Hændelse baseret på start 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.

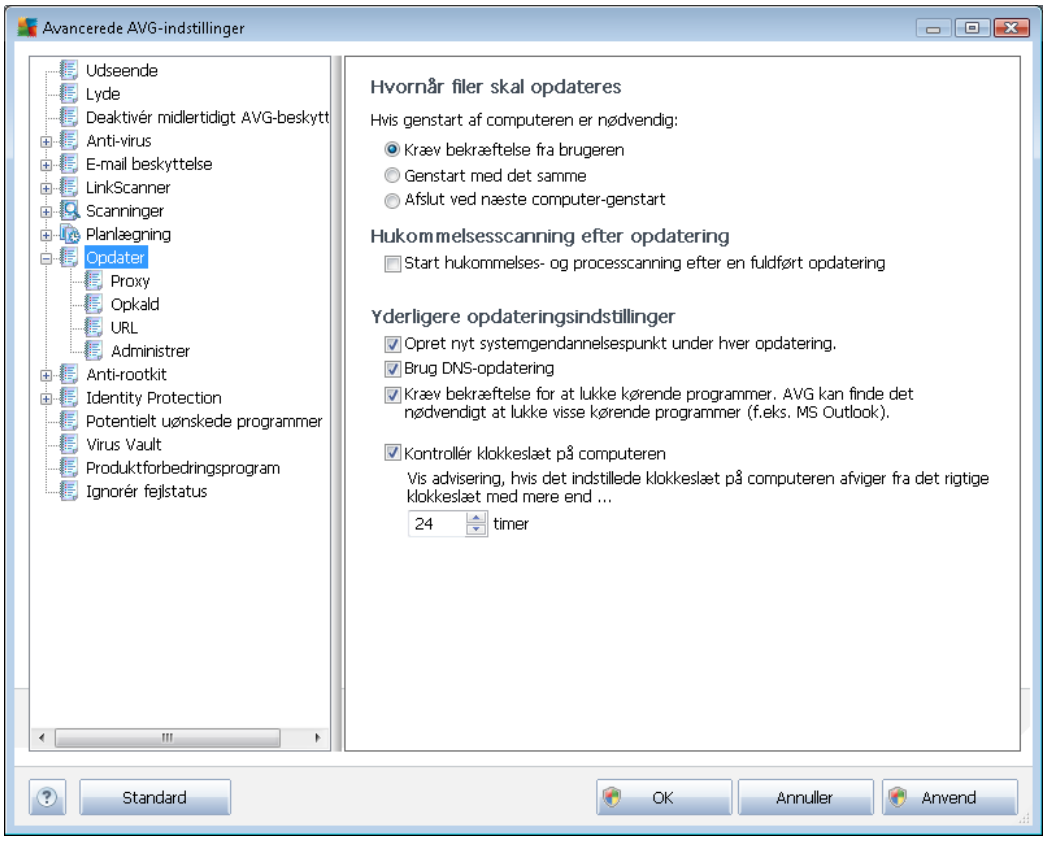
Andre opdateringsindstillinger

Markér 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 pop op-vindue, der åbnes over AVG-systembakkeikonet (*forudsat at du har bevaret standardkonfigurationen i dialogen Avancerede indstillinger/udseende).*

9.9. 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:

- ***Kræv bekræftelse fra brugeren*** *(som standard)* – Du bliver bedt om at godkende en pc-genstart for at færdiggøre opdateringsprocessen
- ***Genstart med det samme*** – Computeren genstartes umiddelbart efter, at opdateringsprocessen er afsluttet, og du behøver ikke godkende dette
- ***Udfør ved næste genstart af computeren*** – Færdiggørelsesprocessen for opdateringen udskydes, ind til den næste genstart af computeren. 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

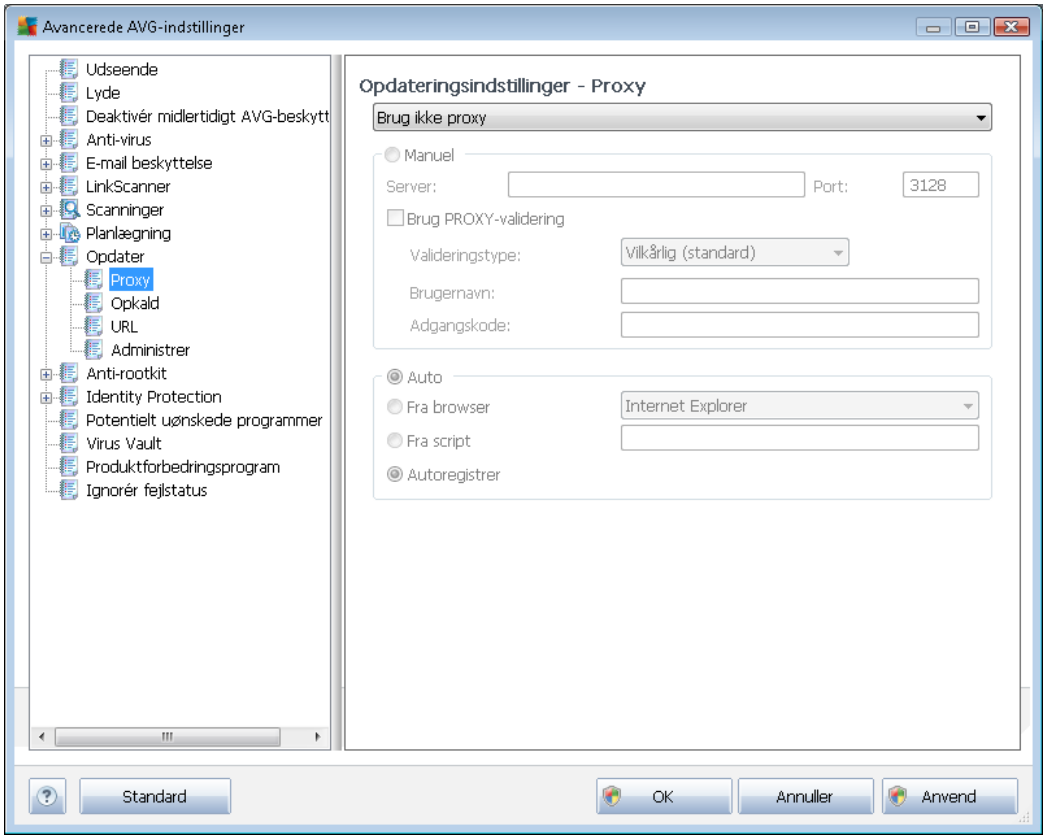
- ***Opret nyt systemgendannelsespunkt i løbet af hver programopdatering*** - før hver AVG programopdatering oprettes et systemgendannelsespunkt. I tilfælde af at opdateringsprocessen mislykkes, og dit operativsystem går ned, kan du altid gendanne dit operativsystem i dets oprindelige konfiguration fra 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 2012** 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.

- ***Kræv bekræftelse for at lukke kørende applikationer*** (*aktiveret som standard*) gør det muligt at sikre, at der ikke lukkes applikationer, der kører i øjeblikket, uden din tilladelse – hvis det er nødvendigt for at færdiggøre 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.

9.9.1. 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*** - 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.

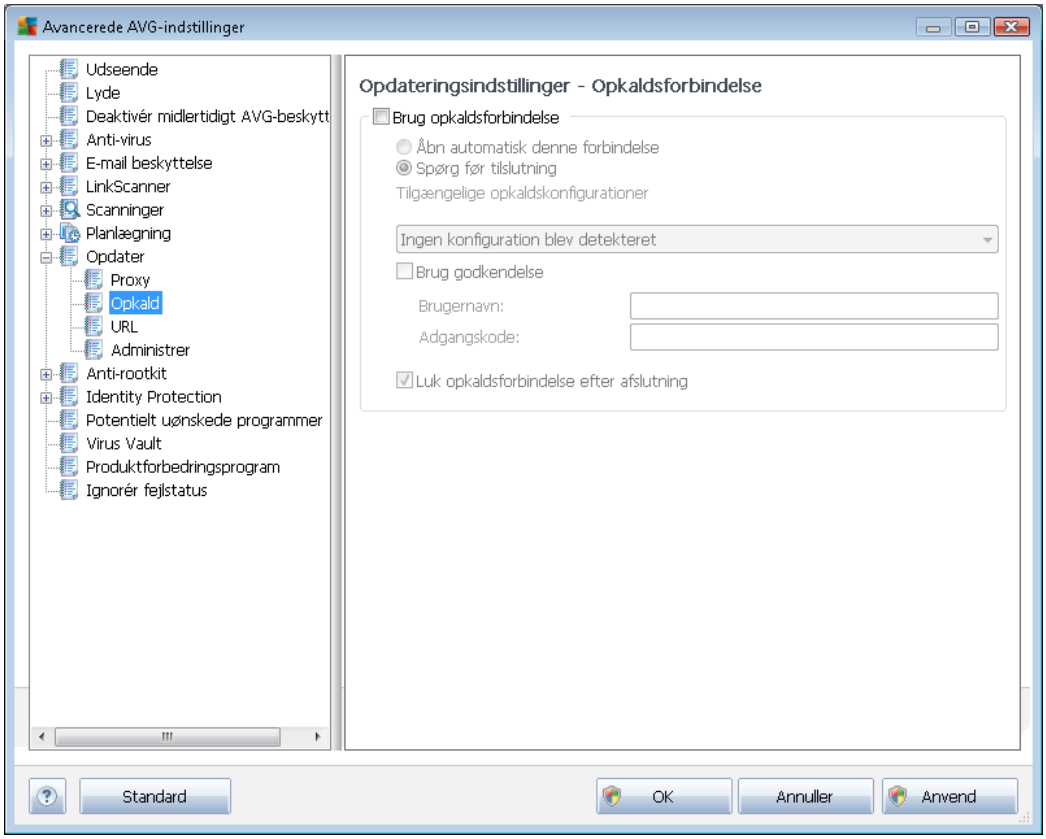
Automatisk konfiguration

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

9.9.2. Opkald

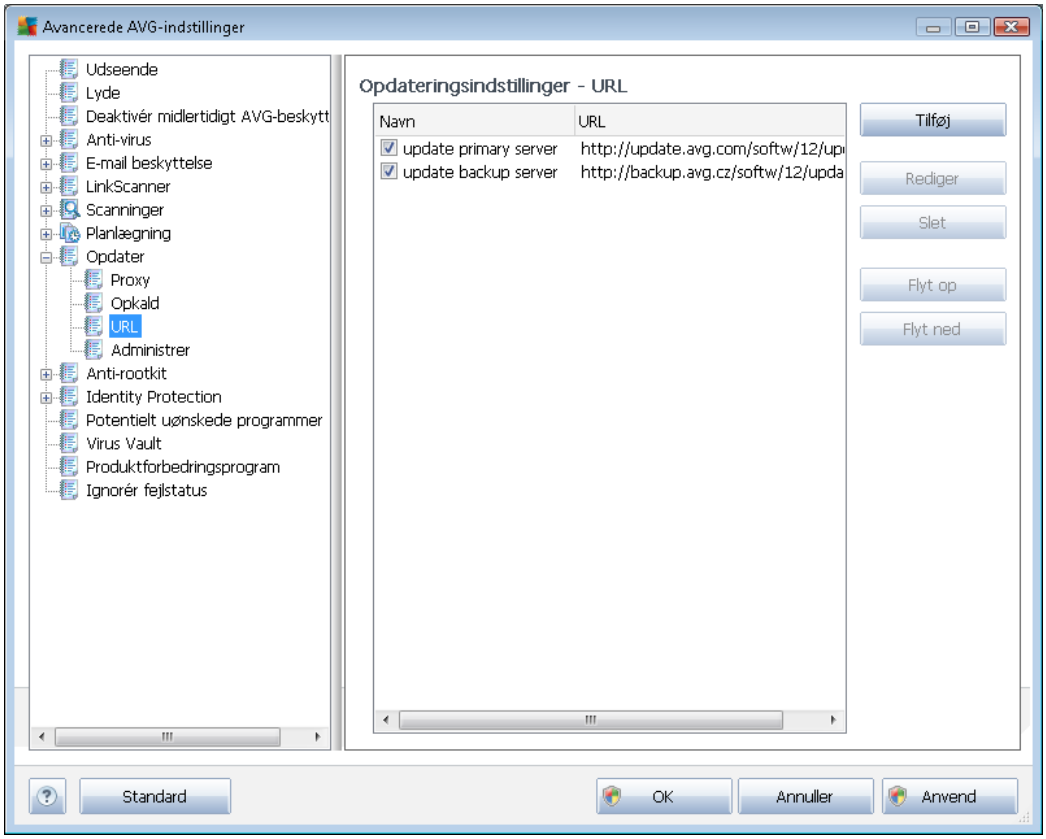
Alle parametre, der valgfrit defineres i dialogen ***Opdateringsindstillinger - Opkaldsforbindelse*** vedrører opkaldsforbindelsen til internettet. Dialogens felter er inaktive, indtil du sætter kryds ved ***Brug opkaldsforbindelser***, som aktiverer disse felter:



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***).

9.9.3. URL

I dialogen ***URL*** er der en liste over internetadresser, hvorfra opdateringsfilerne kan hentes:



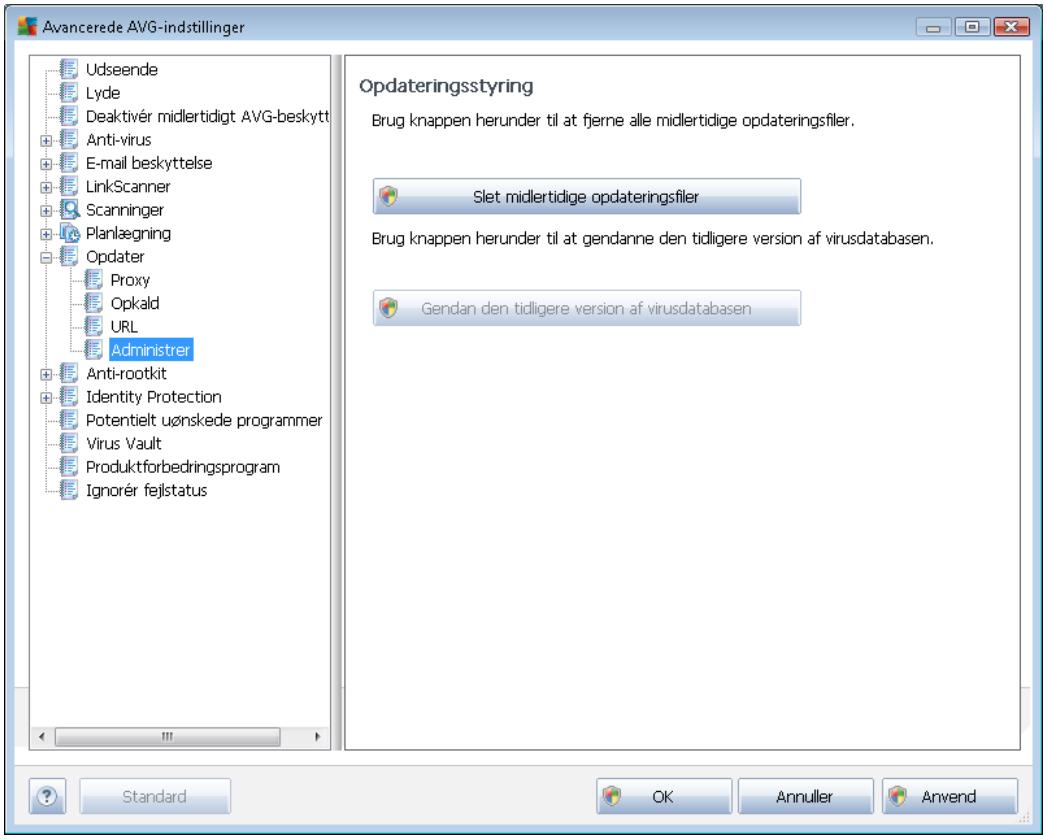
Betjeningsknapper

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

9.9.4. Administrer

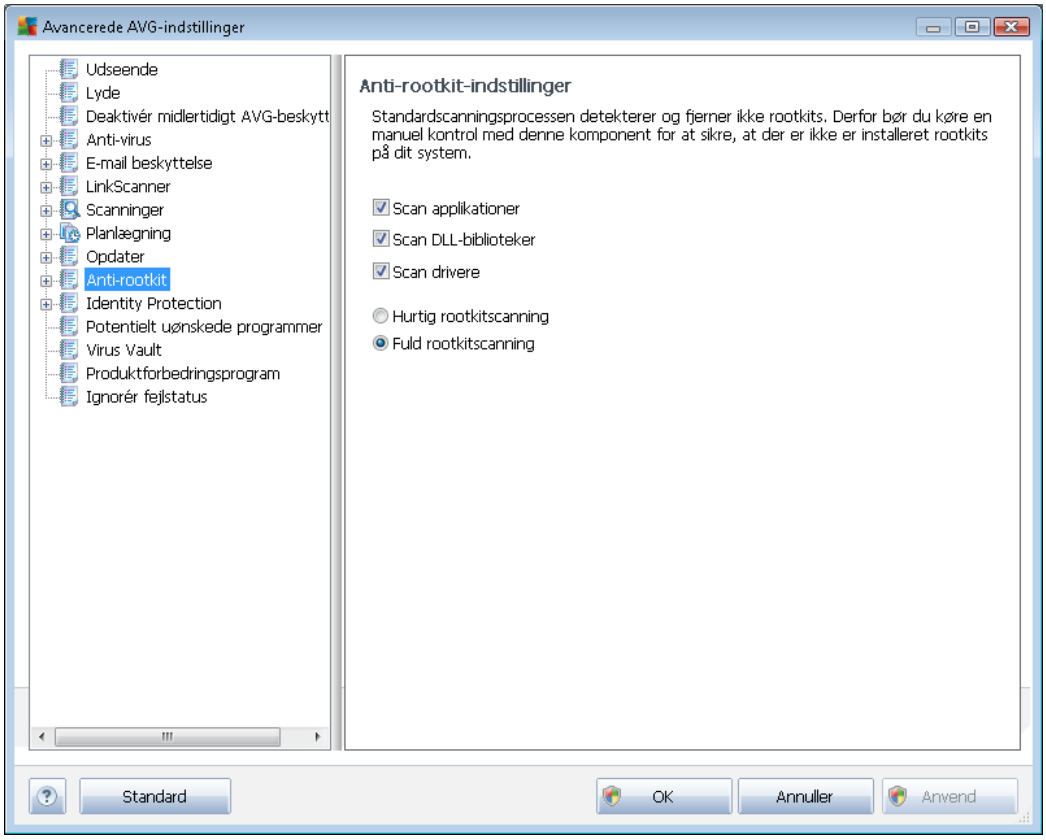
Dialogen ***Opdateringsstyring*** indeholder to indstillinger, der er tilgængelige via to knapper:



- ***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*)

9.10. Anti-rootkit

I dialogen ***Anti-rootkit-indstillinger*** kan du redigere konfigurationen af Anti-rootkit-komponenten:



Redigering af alle de funktioner i Anti-rootkit-komponenten, som findes i denne dialog, er også tilgængelig direkte fra Anti-rootkit-komponentens grænseflade.

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

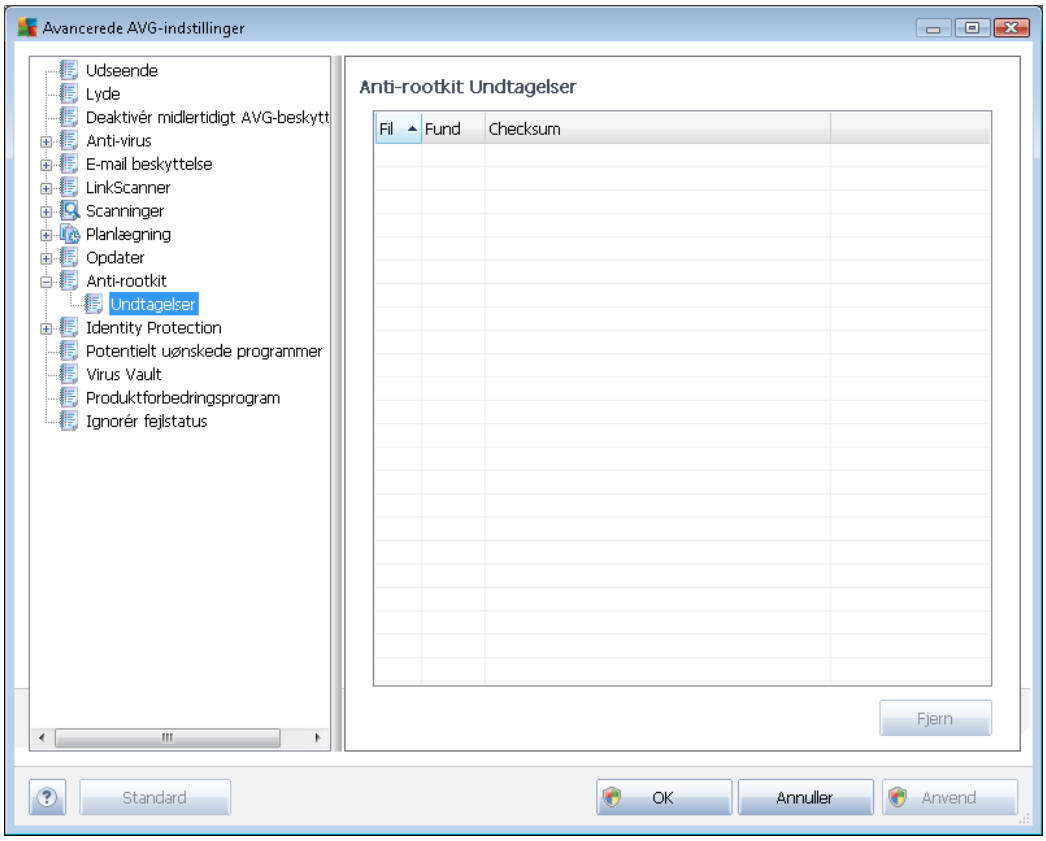
- ***Scan applikationer***
- ***Scan DLL-biblioteker***
- ***Scan drivere***

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*)

9.10.1. Undtagelser

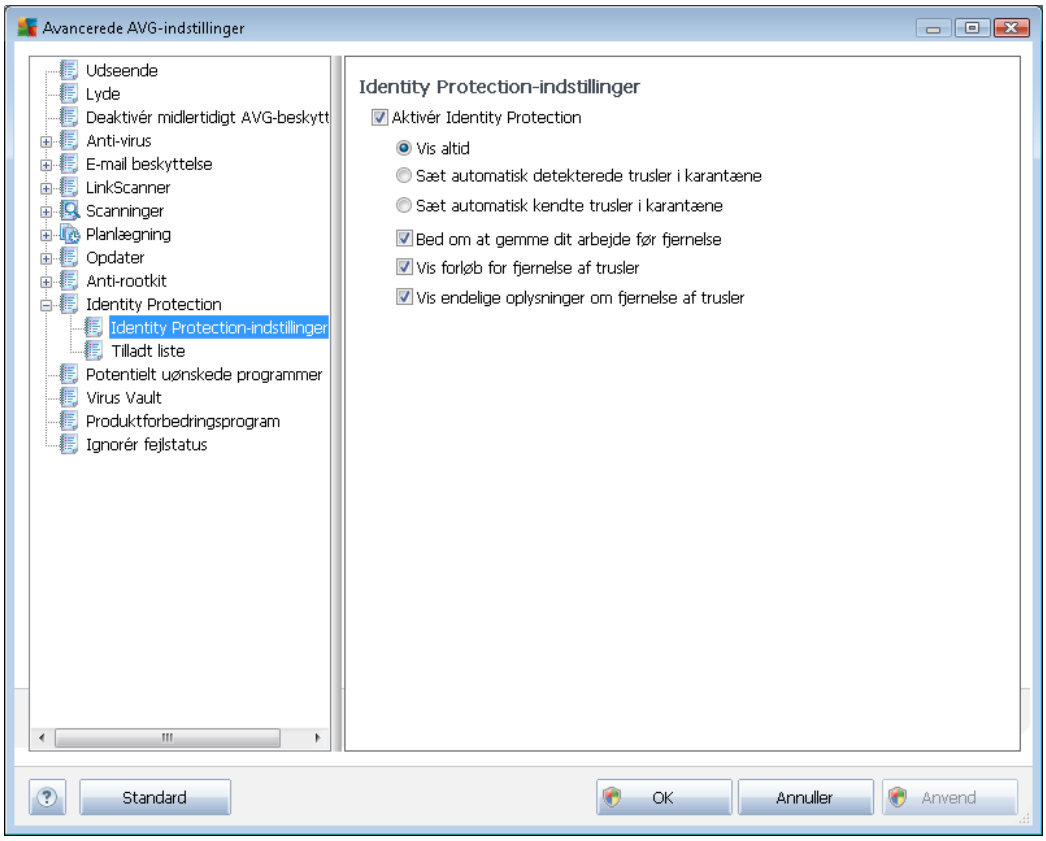
I dialogen ***Anti-Rootkit-undtagelser*** kan du definere bestemte filer *(f.eks. visse drivere, der kan blive registreret som rootkit, men er en falsk positiv)*, der skal udelukkes fra denne scanning:



9.11. Identitetsbeskyttelse

9.11.1. 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 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*** – Sørg for, at denne indstilling er markeret, hvis du ønsker, at alt der detekteres som malware automatisk og øjeblikkeligt flyttes til Virus Vault.

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

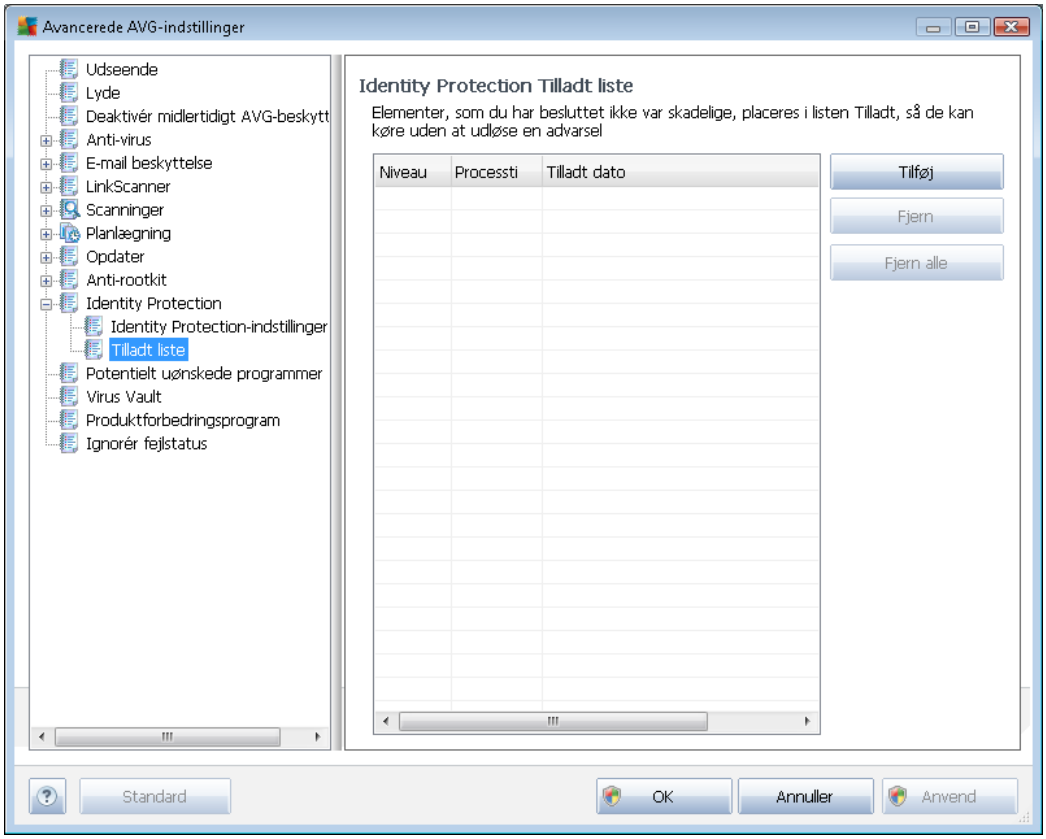
- ***Spørg om at gemme dit arbejde før fjernelse*** - (*slået til som standard*) - hold dette element markeret, hvis du ønsker at blive advaret, før programmet, der detekteres som potentiel malware, sættes i karantæne. Hvis du var i gang med at arbejde med programmet, kan dit projekt gå tabt og du skal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

9.11.2. 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:

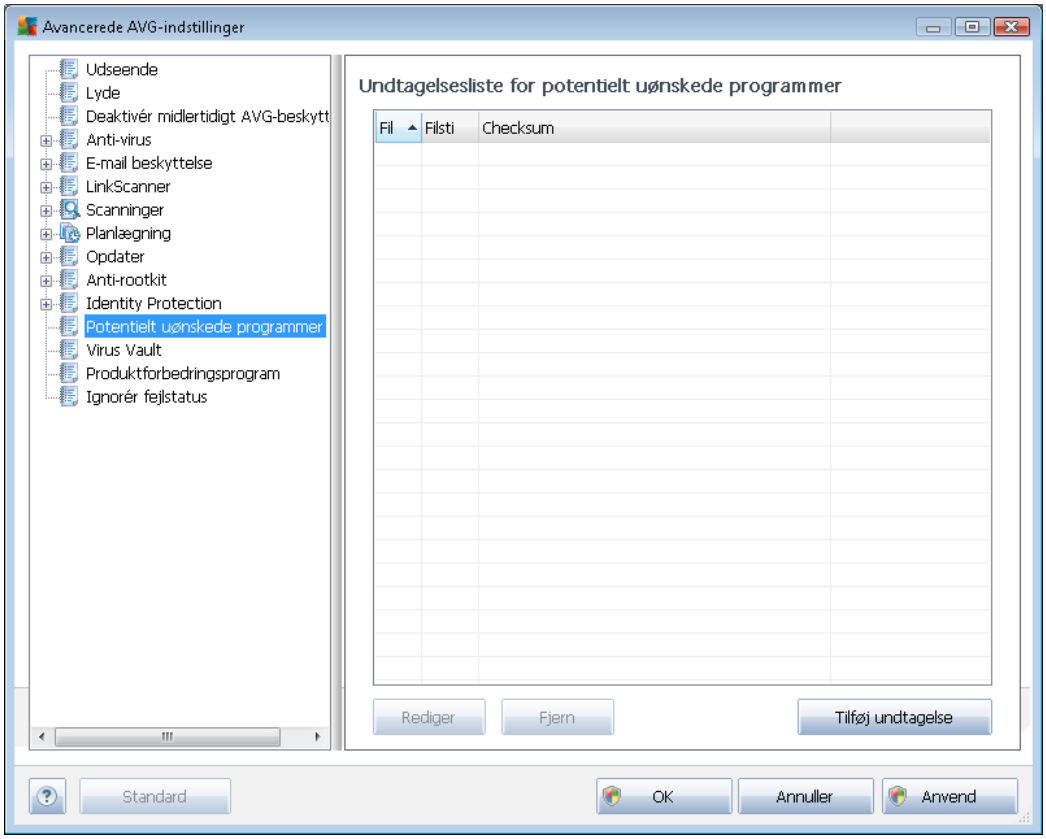
- ***Tilføj*** - tryk på denne knap for at føje en ny applikation til den tilladte liste. Følgende dialog vises:

  - ***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

9.12. Potentielt uønskede programmer

AVG Internet-sikkerhed 2012 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. En sådan adware registreres og rapporteres muligvis af **AVG Internet-sikkerhed 2012** som et *potentielt uønsket program*. Hvis du vil beholde et sådant program på computeren, kan du definere det som en potentielt uønsket program-undtagelse:



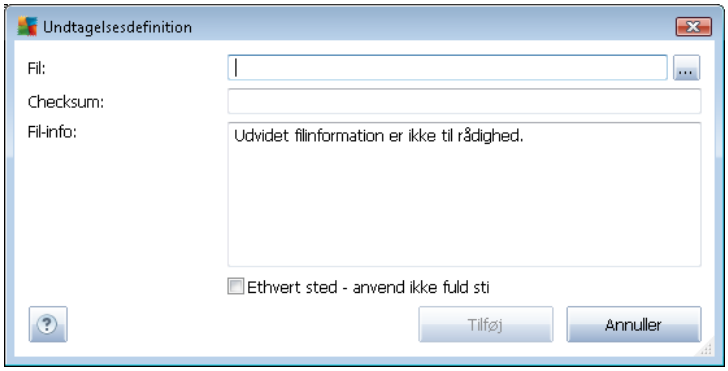
Dialogen ***Potentielt uønsket program-undtagelser*** viser en liste over allerede definerede og aktuelt gyldige undtagelser fra potentielt uønskede programmer. Du kan redigere listen, slette eksisterende elementer eller tilføje nye undtagelser. Følgende oplysninger kan findes i listen for hver enkelt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

- ***Fil*** – Angiver det eksakte navn for 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

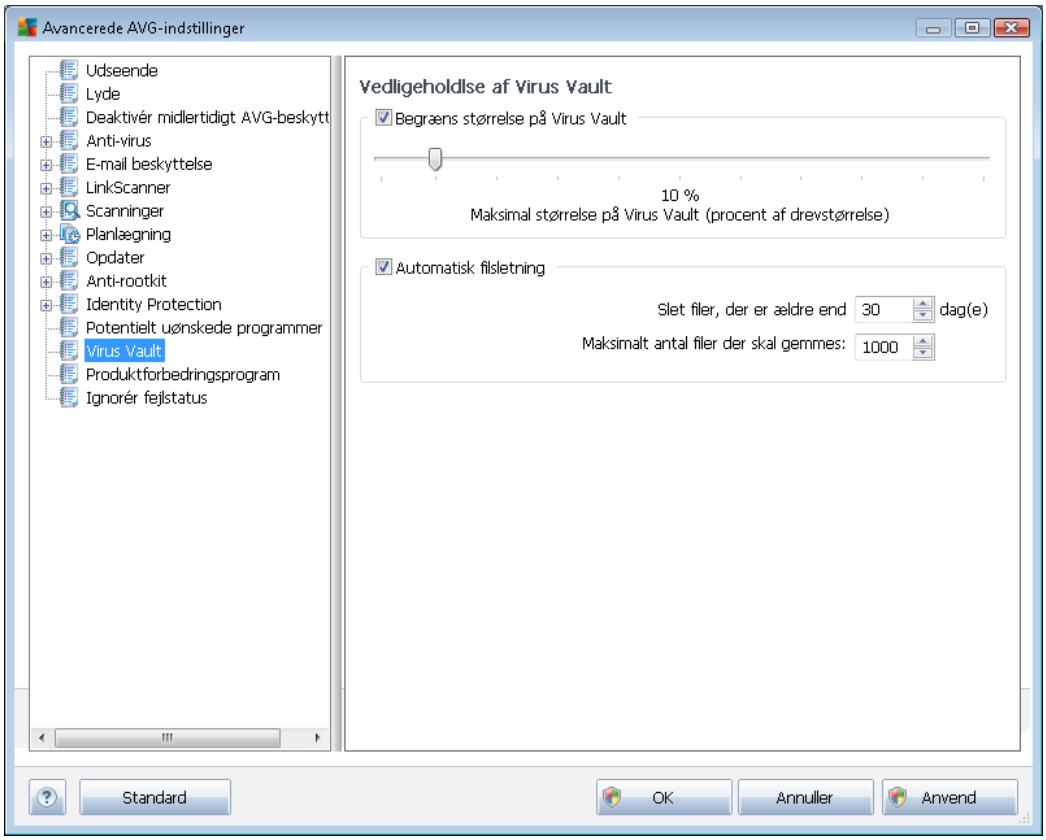
- ***Rediger*** - åbner en redigeringsdialog (*identisk med dialogen til definition af nye undtagelser, se nedenfor*) for en allerede defineret undtagelse, hvor du kan ændre undtagelsens parametre

- ***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.
  - ***Filoplysninger*** – Viser alle yderligere oplysninger om filen *(oplysninger om licens/ version m.m.)*
  - ***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, defineres den angivne fil som en undtagelse, uanset hvor den er placeret *(Du skal imidlertid under alle omstændigheder angive den fulde sti til den specifikke fil. Filen bruges derefter som et entydigt eksempel på muligheden for, at to filer kan vises med samme navn i systemet)*.

9.13. Virus Vault



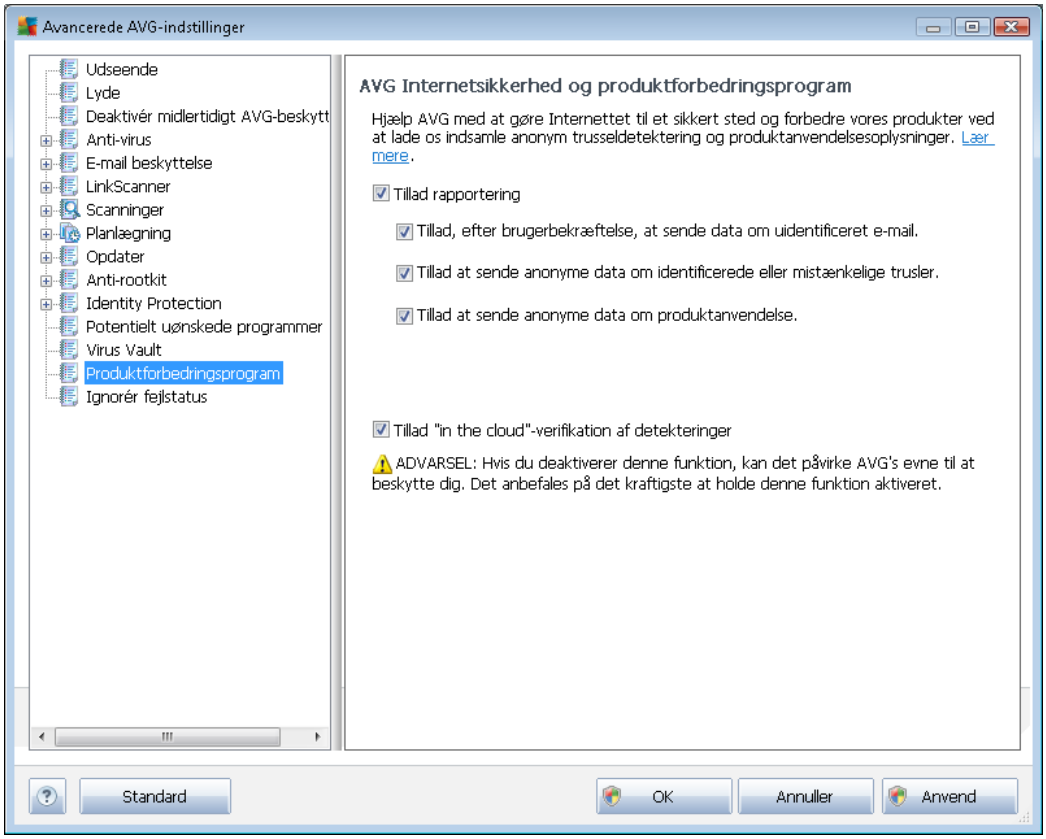
I dialogboksen ***Virus Vault-vedligeholdelse*** kan du definere adskillige parametre vedrørende administration af objekter, der opbevares i Virus Vault:

- ***Begræns størrelse af Virus Vault*** – Brug skyderen til at konfigurere maksimumstørrelsen på Virus Vault. Størrelsen angives proportionalt i forhold til størrelsen på den lokale disk.
- ***Automatisk filsletning*** – I denne sektion definerer du det maksimale tidsrum, som objekter skal opbevares i Virus Vault (***Slet filer, der er ældre end ... dage***), og det maksimale antal filer, der skal opbevares i Virus Vault (***Maksimalt antal filer der skal gemmes***).

9.14. Produktforbedringsprogram

Dialogen ***AVG's internetsikkerhed og produktforbedringsprogram*** opfordrer dig til at deltage i AVG's produktforbedring, så vi kan øge den generelle sikkerhed på internettet. Sørg for, at indstillingen ***Tillad rapportering*** er markeret for at give mulighed for at rapportere detekterede trusler til AVG-laboratorierne. 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 sker automatisk og er derfor ikke til ulejlighed for dig. Der medtages ikke personlige oplysninger i rapporterne. Det er valgfrit, om du vil rapportere registrerede trusler, men vi beder dig om, at denne indstilling er aktiveret. Det gør det muligt at forbedre beskyttelsen for 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:

- ***Virus*** er en skadelig kode, der kopierer og spreder sig selv, og bemærkes ofte ikke, før 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.

- ***Orme*** er en underkategori af virus, der modsat en almindelig virus ikke er "bærer" af noget objekt. Den er en selvstændig enhed og sender sig selv til andre computere, og det sker som regel via e-mails. Konsekvensen er ofte en overbelastning af e-mail-servere 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.

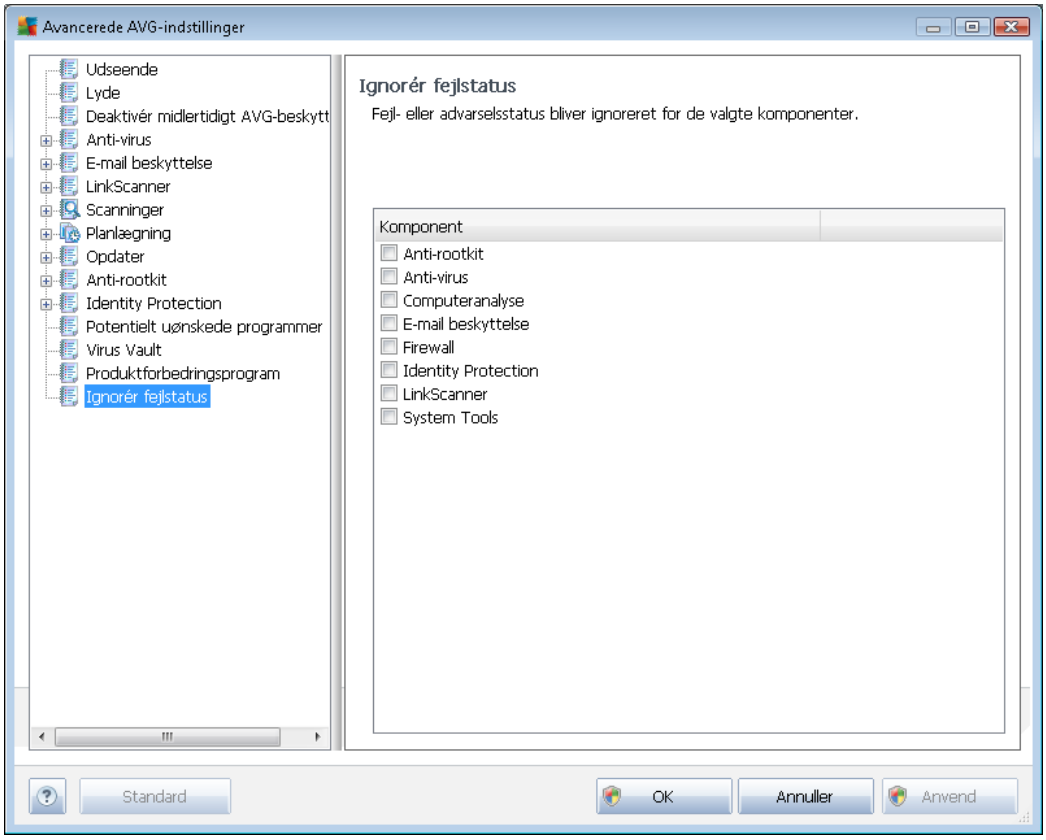
- ***Hoax*** er en masseudsendt e-mail, der indeholder farlige, alarmerende eller blot irriterende og ubrugelige oplysninger. Mange af de ovenstående trusler bruger hoax-e-mail til at spredes.

- ***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 former for trusler omfatter AVG Internet-sikkerhed 2012 specialiserede komponenter. Se afsnittet Komponentoversigt for at få en kort beskrivelse af dem.

9.15. Ignorér fejlstatus

I dialogen ***Ignorer fejlstatus***, kan du vælge de komponenter, du ikke ønsker besked 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:

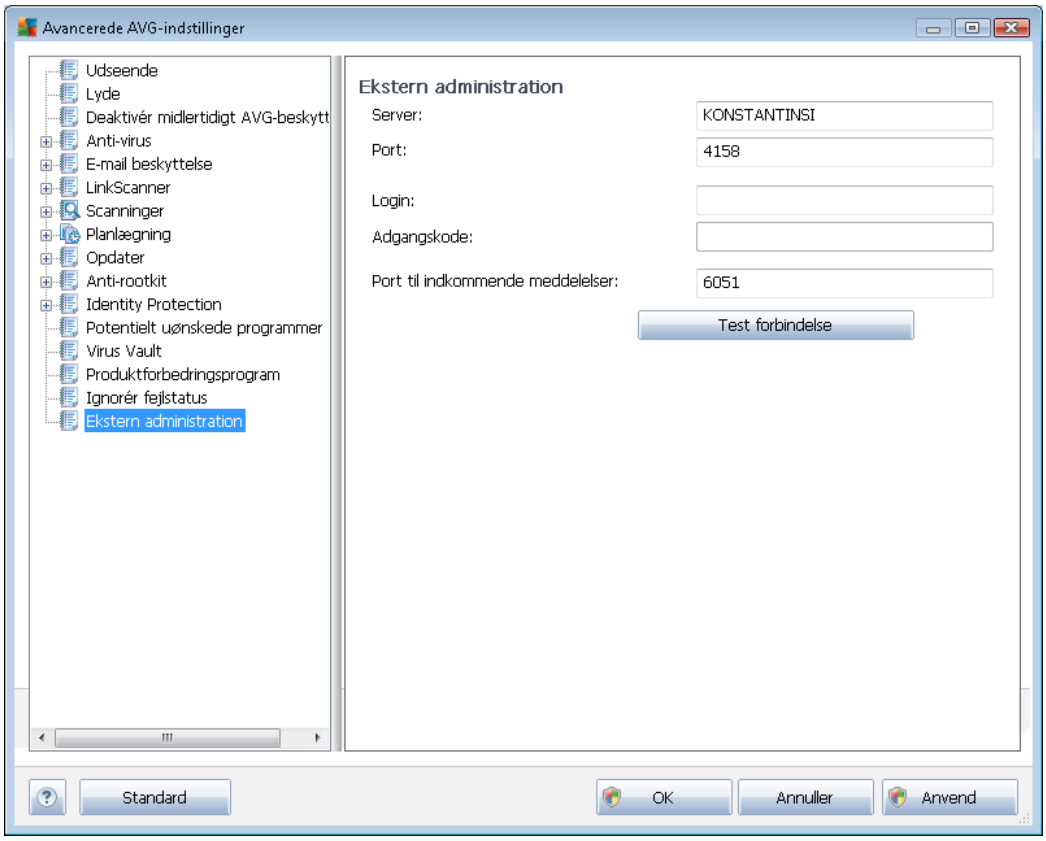
- systembakkeikonet - mens alle dele af AVG fungerer korrekt, vises ikonet i fire farver, men når der opstår en fejl, vises ikonet med et gult udråbstegn,
- tekstbeskrivelse af det eksisterende problem i sektionen Info om sikkerhedsstatus i AVG's hovedvindue

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 indstilling *(Ignorer komponenttilstand)* er også tilgængelig for bestemte komponenter direkte via komponentoversigten i hovedvinduet i AVG.

9.16. Ekstern administration

Indstillingen ***Ekstern administration*** og den tilhørende dialog vises kun i navigationstræet, hvis du har installeret **AVG Internet-sikkerhed 2012** ved hjælp af en AVG Business Edition-licens, og hvis du under installationsprocessen har bekræftet, at du vil installere komponenten ***Ekstern administration***. Du kan se en detaljeret beskrivelse af fjernadministration af installation og konfiguration ved at se den pågældende dokumentation for AVG Network Edition, som kan hentes på AVG's websted(http://www.avg.com/) under sektionen Supportcenter/Download.



Indstillingerne til ***Ekstern administration*** vedrører at oprette forbindelse fra AVG-klienten til det eksterne administrationssystem. Hvis du har planer om at oprette forbindelse fra den pågældende station til ekstern administration, skal du angive følgende parametre:

- ***Server*** - servernavn (eller serveren IP-adresse) hvor AVG Admin Server er installeret
- ***Port*** angiv nummeret på den port, hvor AVG-klienten kommunikerer med AVG Admin Server (*port nummer 4158 betragtes som standard - hvis du bruger dette portnummer, behøver du ikke at angive det direkte*)
- ***Login*** - hvis kommunikationen mellem AVG-klienten og AVG Admin Server er defineret som sikret, skal du oplyse dit brugernavn ...
- ***Adgangskode*** - ...og din adgangskode

- ***Port til indkommende meddelelser*** - nummer på den port, hvor AVG-klienten modtager indkommende meddelelser fra AVG Admin Server

Betjeningsknapper

Knappen ***Test forbindelse*** hjælper dig med at verificere, at alle de ovenstående data er korrekte og kan anvendes til at oprette forbindelse til DataCenter.

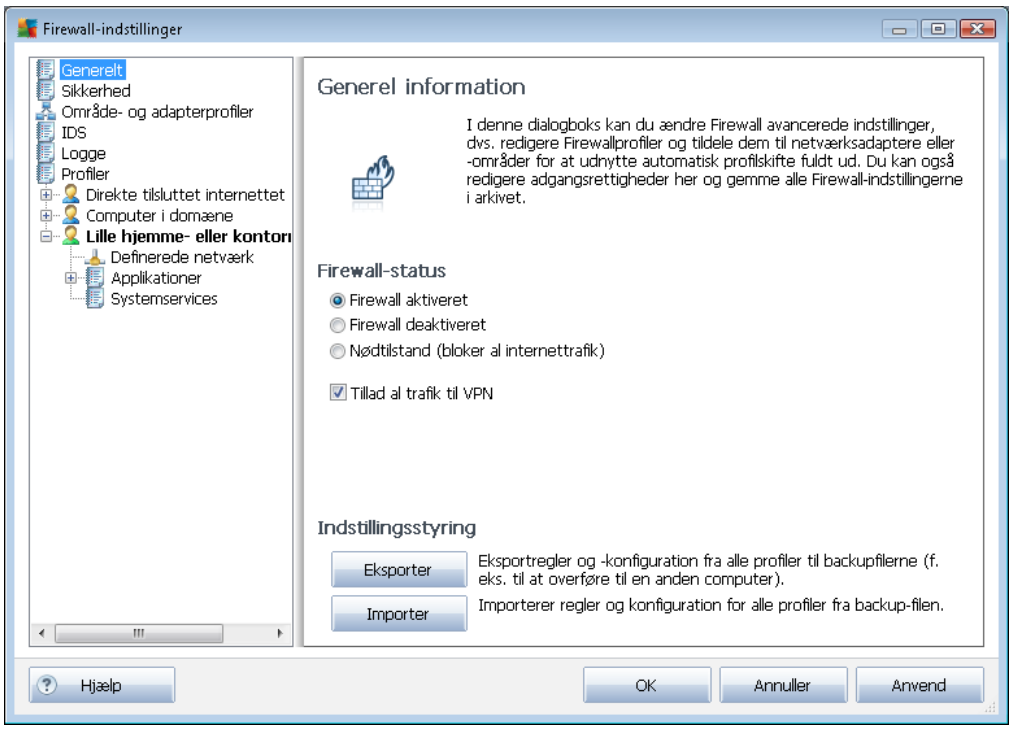
10. Firewall-indstillinger

Firewall-konfigurationen åbnes i et nyt vindue, hvor der i adskillige dialoger kan indstilles meget avancerede parametre for komponenten.

Softwareleverandører har imidlertid konfigureret alle AVG Internet-sikkerhed 2012-komponenter til at yde det optimale. Medmindre du har en reel grund til det, skal du ikke ændre standardkonfigurationen. Ændringer af indstillingerne bør kun foretages af en erfaren bruger!

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.

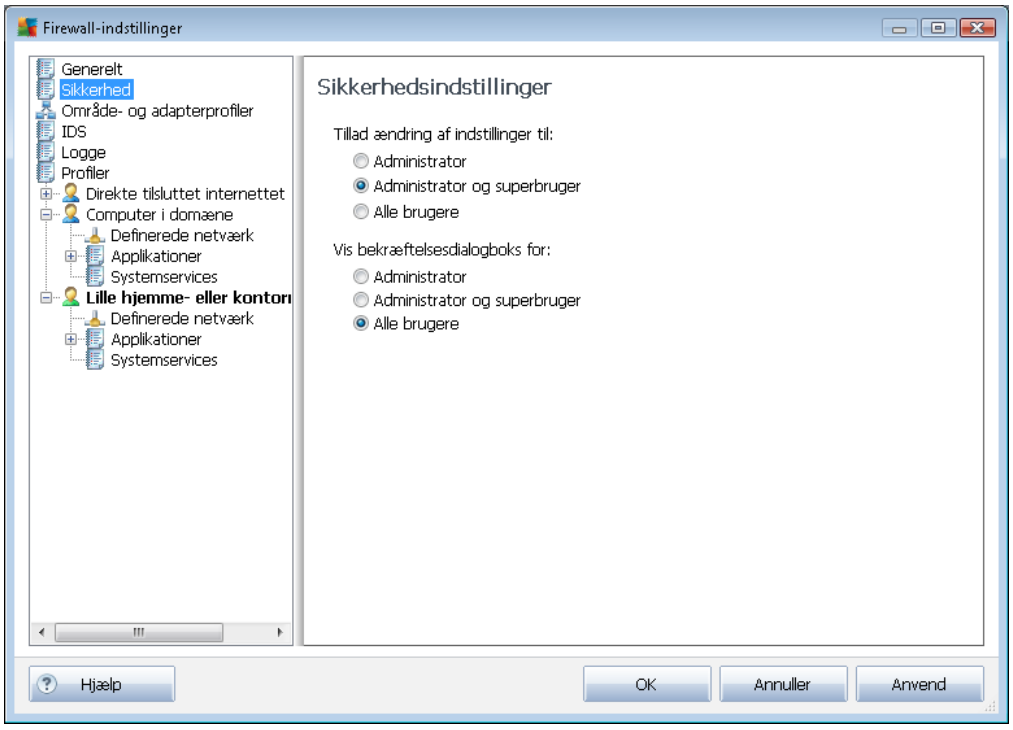
- ***Aktivér al trafik til VPN*** *(aktiveret som standard)* – hvis du bruger VPN *(Virtual Private Network)*-forbindelse, f.eks. for at få forbindelse til dit kontor hjemmefra, anbefaler vi, at du markerer afkrydsningsfeltet. ***AVG Firewall*** vil automatisk søge gennem dine netværksadaptere, finde 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 sektionen ***Indstillingsstyring*** kan du ***eksportere*** eller ***importere en*** Firewall-konfiguration, dvs. eksportere de definerede Firewall-regler og -indstillinger til en sikkerhedskopifil eller omvendt importere hele sikkerhedskopifilen.

10.2. Sikkerhed



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

- ***Tillad ændringer i indstillingerne for*** - angiv hvem der har lov til at ændre Firewall-konfigurationen.

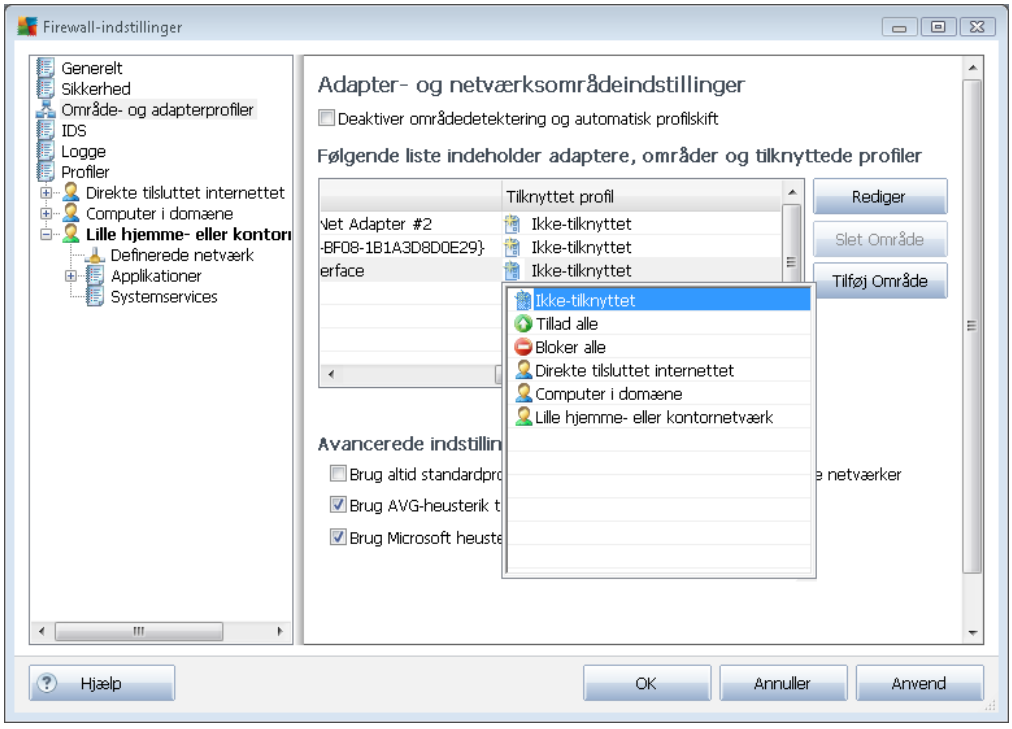
- ***Vis bekræftelsesdialog for*** – Angiv, for hvem bekræftelsesdialogen *(dialoger, der beder om en beslutning i en situation, der ikke er dækket af en defineret Firewall-regel)* skal vises.

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****(deaktiveret som standard)* – En af de definerede profiler kan tildeles til alle typer netværksgrænseflade på de tilsvarende områder. 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***.

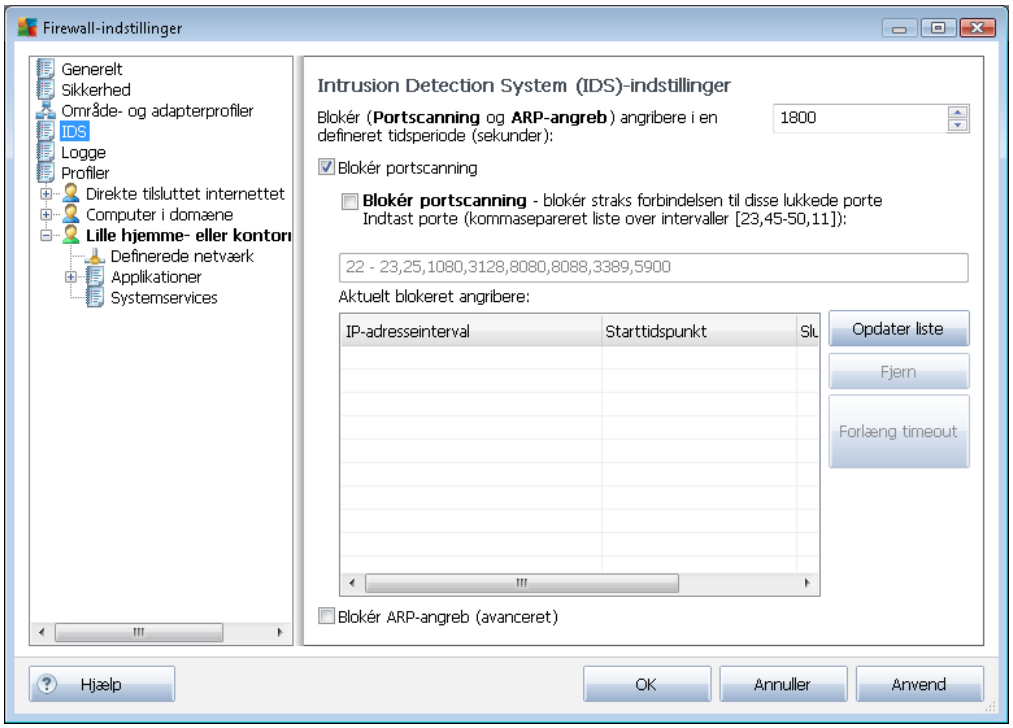
- ***Liste over adaptere, områder og tildelte profiler*** – På denne liste kan du finde en oversigt over detekterede adaptere og områder. Til hver kan du tildele en specifik profil fra menuen med definerede profiler. Venstreklik på det tilsvarende element på listen over adaptere *(i profilkolonnen Tildelt)*, og vælg profilen fra kontekstmenuen.

Avancerede indstillinger

- ***Brug altid standardprofilen, og vis ikke dialogen for ny netværksdetektering*** – Når din computer får forbindelse til et nyt netværk, vil Firewall advare dig og vise en dialog, hvor du bliver bedt om at vælge en netværksforbindelse, og tildele den til en Firewall-profil. Hvis du ikke vil have denne dialog vist, skal du markere dette felt.
- ***Brug AVG-heuristisk til detektering af nye netværk***– Aktiverer indsamling af oplysninger om et nyt detekteret netværk med AVG's egen mekanisme (*denne mulighed er dog kun tilgængelig på VISTA OS eller nyere*).
- ***Brug Microsoft-heuristik til detektering af nye netværk*** – Aktiverer hentning af oplysninger om et nyt detekteret netværk fra Windows-tjenesten (*denne mulighed er kun tilgængelig på Windows Vista eller nyere*).

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-parameterne i dialogen ***Intrusion Detection System-indstillinger (IDS)***:



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

- ***Bloker (Portscanning og ARP-angreb) angribere i en defineret tidsperiode (sekunder)*** – Her 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*).

- ***Bloker portscanning*** *(aktiveret som standard)* – Markér feltet for at blokere kommunikationsforsøg på alle TCP– og UDP-porte, der kommer til computeren udefra. For sådanne forbindelser tillades fem forsøg, og det sjette blokeres. Indstillingen er aktiveret som standard, og det anbefales at bevare denne indstilling. Hvis du bevarer indstillingen ***Bloker portscanning***, er der nogle yderligere muligheder for en detaljeret konfiguration *(ellers vil følgende element være deaktiveret)*:

  - ***Bloker portscanning*** – Markér afkrydsningsfeltet, så du øjeblikket kan blokere kommunikationsforsøg via de 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 blokeret angribere – I dette afsnit vises listen over kommunikationsforsøg, der aktuelt er blokeret af Firewall. Du kan se en komplet historik over blokerede forsøg i dialogen Log (*under fanen Portscanningslog*).

- ***Bloker ARP-angreb (avanceret)*** *(deaktiveret som standard)* – Markér denne indstilling for at aktivere blokering af særlige typer af kommunikationsforsøg i et lokalt netværk, der detekteres af ***IDS*** som potentielt farligt. 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.

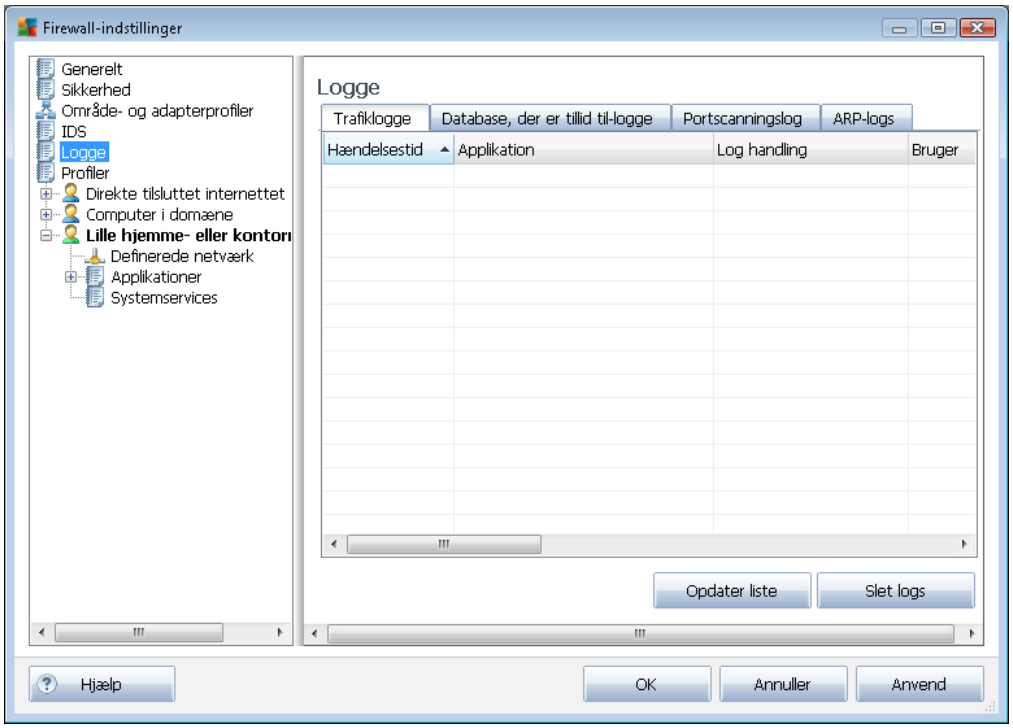
Betjeningsknapper

- ***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.

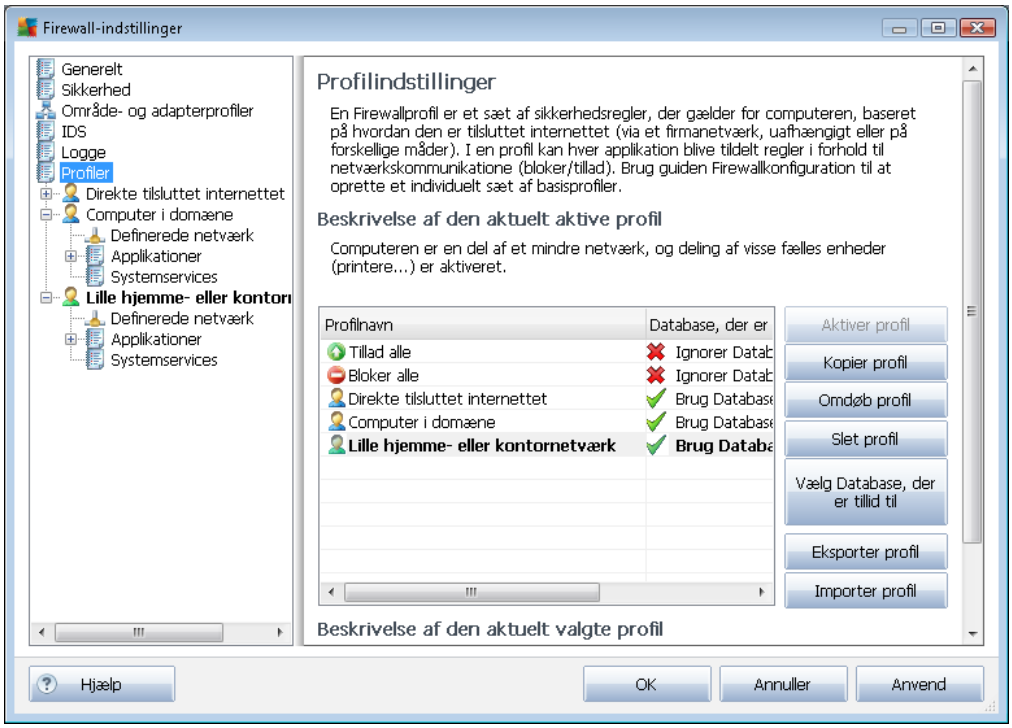
Betjeningsknapper

- ***Opdater liste*** – Alle logførte parametre arrangeres efter den valgte attribut: kronologisk (*datoer*) eller alfabetisk (*andre kolonner*) – Klik blot på den relevante kolonneoverskrift. Brug knappen ***Opdater liste*** til at opdatere de aktuelt viste oplysninger.

- ***Slet log*** – Sletter alle poster i diagrammet.

10.6. Profiler

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



Systemprofiler *(Tillad alle, Bloker alle)* kan ikke redigeres. Alle brugerdefinerede profiler *(med direkte forbindelse til internettet, computeren på domænet eller et lille hjemme- eller kontornetværk)* kan imidlertid efterfølgende redigeres i denne dialog ved hjælp af følgende kontrolknapper:

- ***Aktivér profil*** – Denne knap indstiller den valgte profil som aktiv, hvilket betyder, at den valgte profilkonfiguration anvendes af Firewall til at kontrollere netværkstrafikken.

- ***Dupliker profil*** – Opretter en identisk kopi af den valgte profil. Du kan redigere og omdøbe kopien til at oprette ny profil på et senere tidspunkt ud fra den duplikerede original.

- ***Omdøb profil*** – Gør det muligt at definere et nyt navn for en valgt profil.

- ***Slet profil*** – Sletter den valgte profil fra listen.

- ***Vælg pålidelig database*** – Du kan for den valgte profil vælge at bruge oplysningen *Pålidelig database* (*den pålidelige database er AVG's interne database, der indsamler data om pålidelige og certificerede applikationer, der altid må kommunikere via internettet.*).

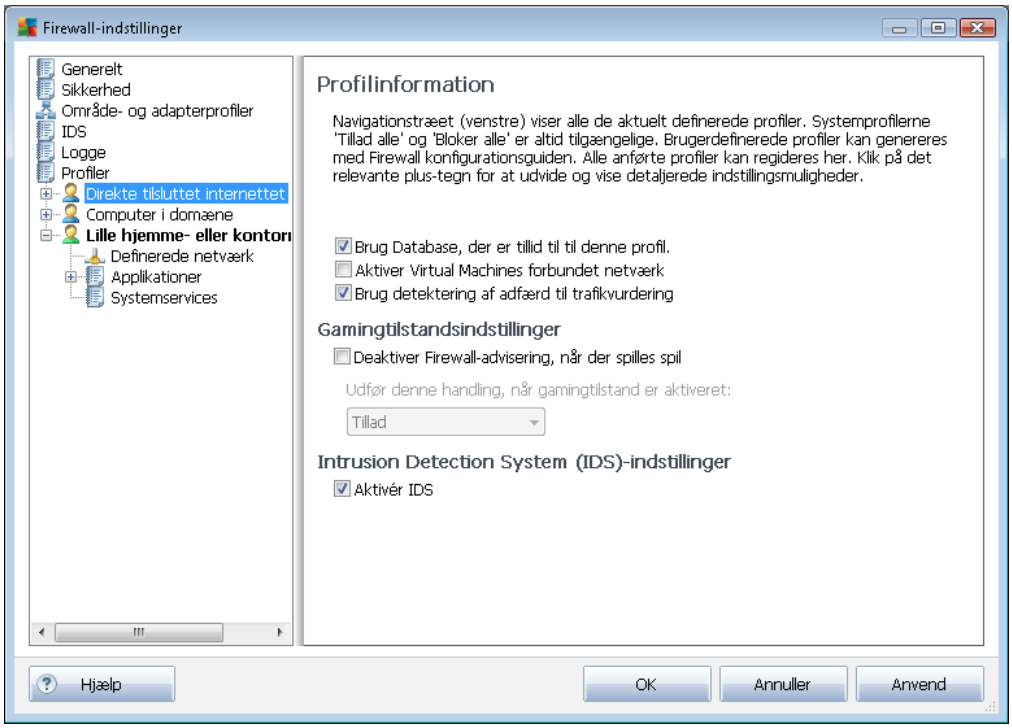
- ***Eksporter profil*** – Registrerer konfigurationen for den valgte profil i en fil, der gemmes til eventuelt fremtidig brug.

- ***Importer profil*** – Konfigurerer den valgte profils indstillinger ud fra de data, der er eksporteret fra den sikkerhedskopierede 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*):

10.6.1. Profilinformation



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

- ***Brug Pålidelig database til denne profil*** (*aktiveret som standard*) – Markér denne indstilling for at aktivere *Pålidelig database* (*, dvs. en intern AVG-database, der indsamler oplysninger om pålidelige og certificerede programmer, som kommunikerer via internettet. Hvis der endnu ikke er angivet en regel for den pågældende applikation, er det nødvendigt at finde ud af, om applikationen kan gives adgang til netværket. AVG søger først i Pålidelig database, og hvis applikationen er anført, bliver den betragtet som sikker og får tilladelse til at kommunikere via netværket. Ellers bliver du bedt om at beslutte, om*

applikationen skal have tilladelse til at kommunikere via netværket) for den pågældende profil

- ***Aktivér Virtual Machines forbundne netværk*** (*deaktiveret som standard*) – Marker dette element for at give tilladelse til virtuelle maskiner i VMware for at få direkte forbindelse til netværket.

- ***Brug detektering af adfærd til trafikvurdering*** (*aktiveret som standard*) – Markér denne indstilling for at give firewallen mulighed for at bruge funktionen Identitetsbeskyttelse, når et program evalueres – Identitetsbeskyttelse kan angive, om applikationen udviser mistænkelig adfærd, eller om det er pålideligt og må kommunikere via internettet.

Indstillinger for spiltilstand

I sektionen ***Gamingtilstandsindstillinger*** kan du fastslå og bekræfte ved at markere den indstilling, der angiver om Firewall-oplysningsmeddelelser skal vises, selvom der kører en fuldskærmsapplikation på computeren (*det er typisk spil, men gælder også andre fuldskærmsapplikationer, f.eks. PPT-præsenationer*), da oplysningsmeddelelser kan være noget forstyrrende.

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

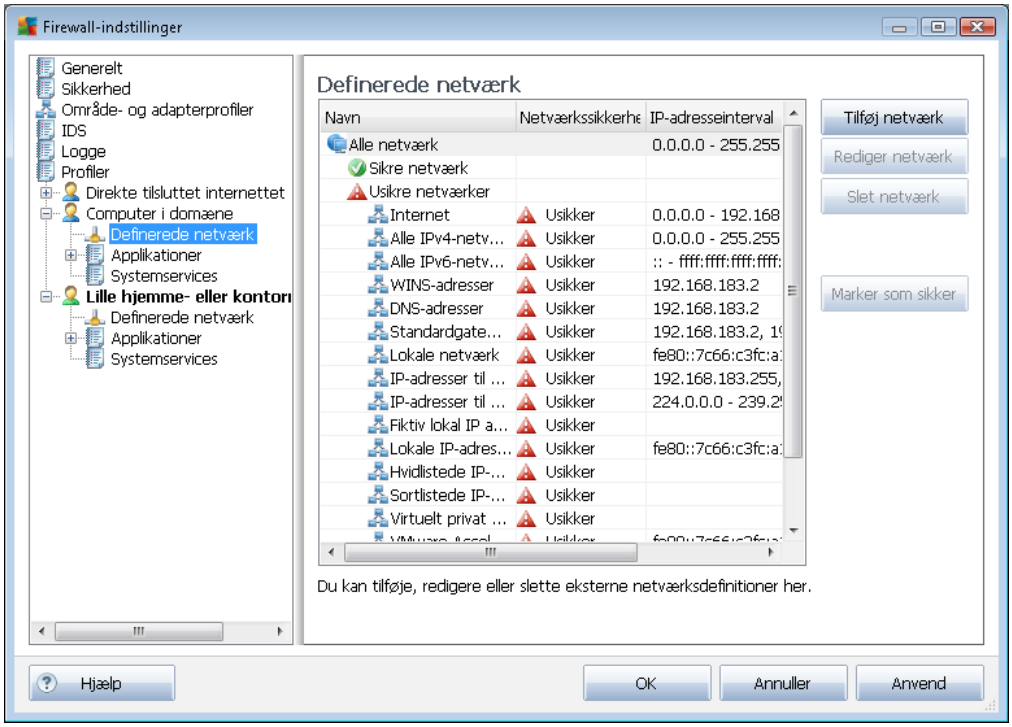
Når gamingtilstanden er slået til, bliver alle planlagte opgaver (*scanninger, opdateringer*) udsat, indtil programmet lukkes.

Intrusion Detection System (IDS)-indstillinger

Markér afkrydsningsfeltet ***Aktivér IDS*** for aktivere speciel adfærdsanalysefunktion, der er beregnet til at identificere og blokere mistænkelige kommunikationsforsøg over specifikke porte på computeren *(du kan få oplysninger om disse funktionsindstillinger i kapitlet IDS i denne dokumentation).*

10.6.2. Definerede netværk

Dialogen ***Definerede netværk*** indeholder en liste over alle netværk, som din computer er tilsluttet.

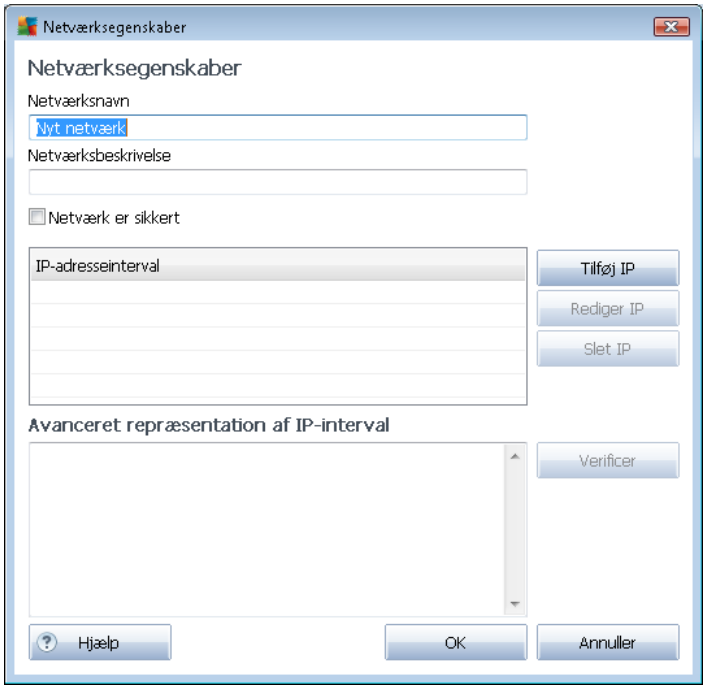


Listen indeholder følgende oplysninger om alle detekterede netværk:

- ***Netværk*** – Indeholder en navneliste over alle de netværk, som computeren er knyttet til.
- ***Netværkssikkerhed*** – Alle netværk betragtes som udgangspunkt som usikre, og kun hvis du er sikker på, at det pågældende netværk er sikkert, kan du markere det som sikkert (*klik på det element på listen, der henviser til det pågældende netværk, og vælg Sikker i kontekstmenuen*) – alle sikre netværk inkluderes herved i gruppen af netværk, som applikationen kan kommunikere med, hvor applikationsreglen indstillet til Tillad for sikker.
- ***IP-adresseområde***– Alle netværk detekteres automatisk og angives i form af et IP-adresseområde.

Betjeningsknapper

- ***Tilføj netværk*** – Åbner dialogen ***Netværksegenskaber*** , hvor du kan redigere parametrene for de nyeste netværk:



I denne dialog kan du angive ***Netværksnavn***, indtaste en ***Netværksbeskrivelse*** og muligvis tildele netværket sikke status. Det nye netværk kan enten defineres manuelt i en enkeltstående dialog, der åbnes med knappen ***Tilføj IP*** (alternativt ***Rediger IP*** / ***Slet IP***), i denne dialog kan du angive netværket ved at oplyse dets IP-område eller maske. For et stort antal netværk, der skal defineres som en del af den nyoprettede netværk, kan du bruge indstillingen ***Avanceret repræsentation af IP-område***: indtast listen over alle netværkene i det pågældende tekstfelt (*alle standardformater understøttes*) og tryk på knappen ***Verificer*** for at sørge for, at formatet kan genkendes. Tryk derefter på ***OK*** for at bekræfte og gemme dataene.

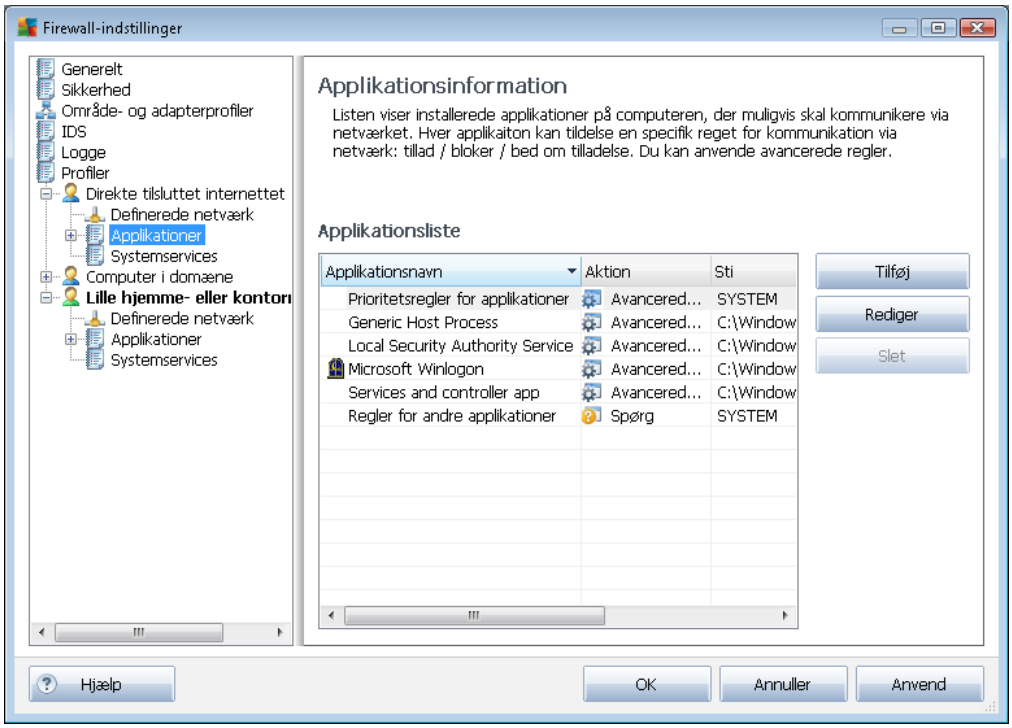
- ***Rediger netværk*** – Åbner dialogen ***Netværksegenskaber*** (*se ovenfor*), hvor du kan redigere parametrene for de netværk, som allerede er defineret (*dialogen er identisk med den dialog, hvor du tilføjer netværk, se beskrivelsen i forrige afsnit*).

- ***Slet netværk*** – Fjerner posten til et valgt netværk fra listen over netværk.

- ***Markér som sikker*** – Alle netværk betragtes som standard som usikre, og det kun, hvis du er sikker på, at det pågældende netværk er sikkert, at du kan bruge denne knap til at markere netværket som sikkert (*, og omvendt, når netværket er markeret som sikkert, ændres knappens tekst til "Markér som usikker"*).

10.6.3. Applikationer

Dialogen ***Applikationsoplysninger*** indeholder en liste over alle installerede applikationer, der kan have behov for at kommunikere over netværk, og ikoner til den tildelte handling:



Applikationerne på ***Listen over applikationer*** er dem, som detekteres på din computer (*og tildeles handlinger*). Følgende handlingstyper kan anvendes:

- - Tillad kommunikation for alle netværk
- - Tillad kun kommunikation for netværk defineret som Sikre
- - Bloker kommunikation
- - Vis spørgedialog (*brugeren vil kunne bestemme, om kommunikation skal tillades eller blokeres, når programmet forsøger at kommunikere over netværk*)
- - Avancerede indstillinger defineret

Bemærk, at kun allerede installerede applikationer kunne detekteres, så hvis du installerer en ny applikation senere, skal du definere Firewall-regler for den. Når den nye applikation forsøger at oprette forbindelse via netværket for første gang, vil Firewall som standard enten automatisk oprette en regel for den i henhold til Pålidelig database, eller spørge dig, om du vil tillade eller blokere kommunikationen. I sidstnævnte tilfælde kan du gemme dit svar som en pemanent regel (som så bliver anført i dialogen).

Du kan selvfølgelig også definere regler for den nye applikation med det samme - tryk på ***Tilføj*** i denne dialog og udfyld applikationsdetaljerne.

Ud over applikationerne indeholder listen også to specielle elementer:

- ***Prioritetsregler for applikationer*** (*øverst på listen*) har højere prioritet og anvendes altid før regler for et specifikt program.
- ***Andre applikationsregler*** (*nederst på listen*) bruges som "sidste udkald", hvis der ikke gælder specifikke regler, f.eks. for en ukendt og udefineret applikation.

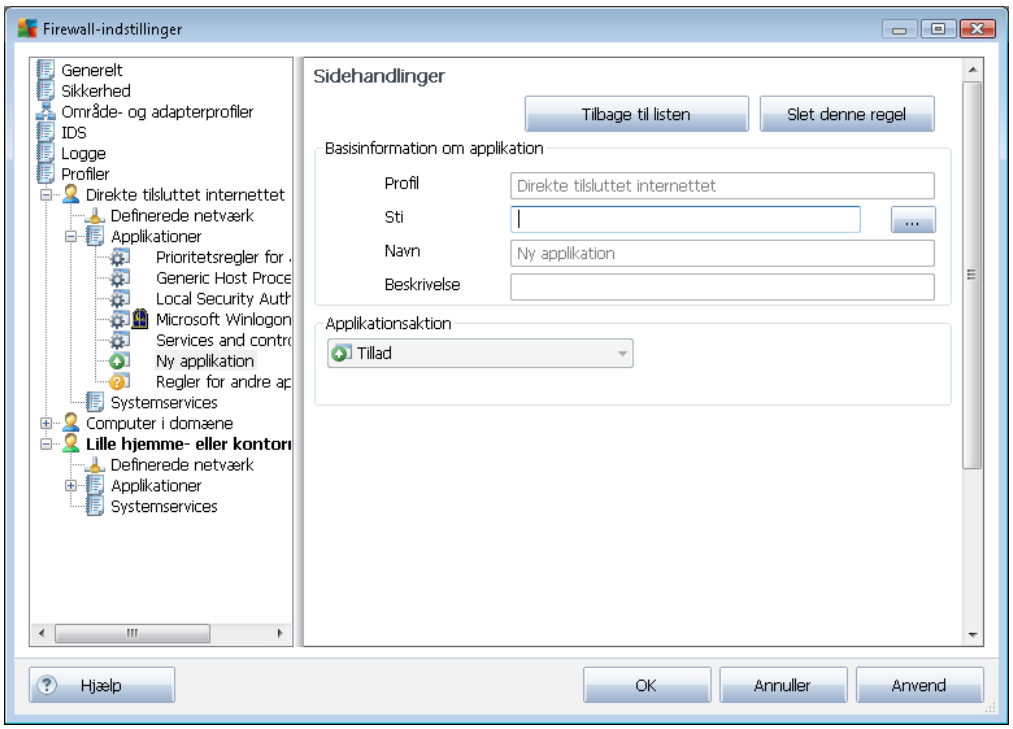
Disse elementer har andre indstillingsmuligheder end almindelige applikationer og er kun beregnede til erfarne brugere. Vi anbefaler på det kraftigste, at du ikke ændrer indstillingerne!

Betjeningsknapper

Denne liste kan redigeres ved hjælp af følgende betjeningsknapper:

- ***Tilføj*** – Åbner en tom Sidehandlinger-dialog til angivelse af nye applikationsregler
- ***Rediger*** – Åbner den samme Sidehandlinger-dialog med data til redigering af et eksisterende regelsæt for applikationen.
- ***Slet*** – Fjerner den valgte applikation fra listen.

Du kan definere indstillingerne for det relevante program mere detaljeret i dialogen ***Sidehandlinger***:



Betjeningsknapper

Der findes to betjeningsknapper øverst i dialogen:

- ***Tilbage til listen*** – Tryk på knappen for at få vist en oversigt over alle definerede applikationsregler.
- ***Slet denne regel*** – Tryk på knappen for at slette den applikationsregel, der vises i øjeblikket. ***Bemærk, at denne handling ikke kan fortrydes!***

Basisinformation om applikation

I denne sektion udfyldes applikationens ***Navn*** og eventuelt en ***Beskrivelse*** (*en kort kommentar til din egen information*). I feltet ***Sti*** indtastes den fulde sti til applikationen (*den eksekverbare fil*) på disken. Du kan også finde applikationen i træstrukturen ved at trykke på knappen "***...***".

Applikationsaktion

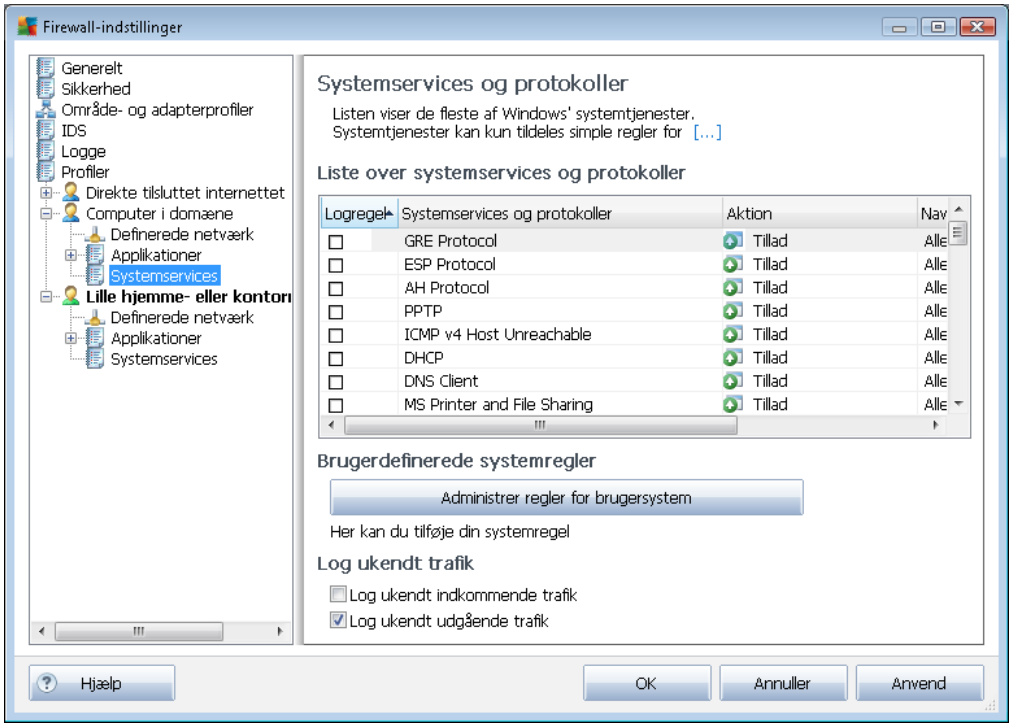
I rullemenuen kan du vælge Firewall-reglen for applikationen, dvs. hvad Firewall skal gøre, når applikationen forsøger at kommunikere via netværket:

- ***Tillad for alle*** – tillader applikationen at kommunikere via alle definerede netværk og adaptere uden begrænsninger.
- ***Tillad for sikre*** – tillader kun applikationen at kommunikere via netværker, der er defineret som sikre *(troværdige)*.
- ***Bloker*** – forbyder kommunikationen automatisk. Applikationen får ikke tilladelse til at oprette forbindelse til noget netværk.
- ***Spørg*** – Viser en dialog, hvor du kan beslutte, om du vil tillade eller blokere kommunikationsforsøget på dette tidspunkt.
- ***Avancerede indstillinger*** – Viser flere omfattende og detaljerede indstillingsmuligheder i nederste del af dialogen i sektionen ***Applikationsdetaljeregler***. Detaljerne anvendes i henhold til rækkefølgen i listen, så du kan bruge ***Flyt op*** og ***Flyt ned*** til at placere reglerne i listen efter den ønskede prioritet. Når du har klikket på en bestemt regel i listen, vises oversigten over regeloplysninger i nederste del af dialogen. Værdier, der er understreget med blåt, kan ændres ved at klikke i den pågældende indstillingsdialog. For at slette den markerede regel skal du bare trykke på ***Fjern***. Hvis du vil definere en ny regel, skal du bruge knappen ***Tilføj*** for at åbne dialogen ***Skift regeldetalje***, hvor du kan angive alle de nødvendige oplysninger.

10.6.4. Systemservices

Redigering i systemtjenesterne og protokoldialogerne er kun beregnet for ERFARNE BRUGERE!

Dialogen ***Systemtjenester og protokoller*** indeholder en liste over standardsystemtjenester og -protokoller i Windows, som muligvis er nødt til at kommunikere via netværket:



Liste over systemservices og protokoller

Diagrammet består af følgende kolonner:

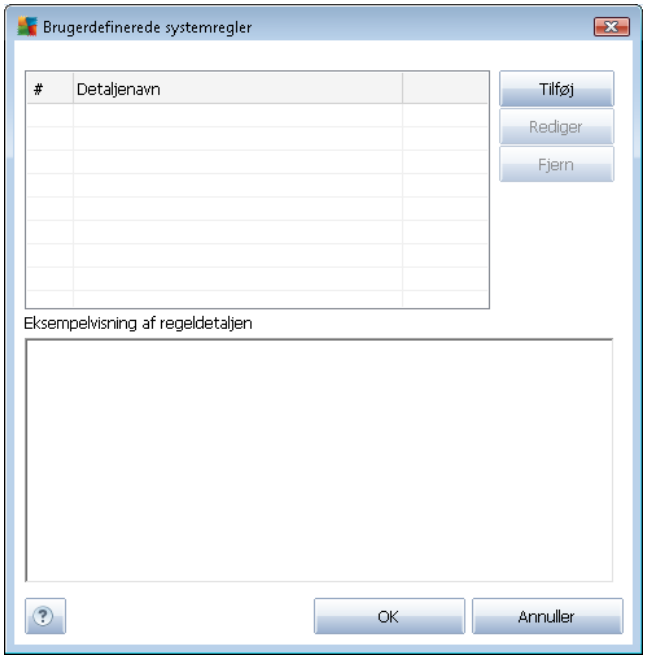
- ***Logregelshandling*** – Dette felt gør det muligt at aktivere anvendelsen af regler i log.
- ***Systemtjeneste og -protokoller*** – I denne kolonne vises navnet på den tilhørende systemtjeneste.
- ***Handling*** – I denne kolonne vises et ikon for den tildelte handling:
  - Tillad kommunikation for alle netværk
  - Tillad kun kommunikation for netværk defineret som Sikre
  - Bloker kommunikation
- ***Netværk*** – I denne kolonne angives det, hvilket specifikt netværk systemreglen anvendes

på.

Hvis du vil registere et element i listen (*inklusive de tildelte handlinger*), skal du højreklikke på elementet og vælge ***Redigér***. ***Redigering af systemregler bør dog kun foretages af erfarne brugere, og det frarådes på det kraftigste at redigere systemregler!***

Brugerdefinerede systemregler

Hvis du vil åbne en ny dialog, hvor du kan angive din egen systemtjenesteregel (*se billedet herunder*), skal du trykke på knappen ***Administrér regler for brugersystem***. Den øverste sektion af dialogen ***Brugerdefinerede systemregler*** viser en oversigt over alle oplysninger om den aktuelt redigerede systemregel, og den nederste sektion viser den valgte oplysninger. Brugerdefinerede regler kan redigeres, tilføjes eller slettes med den pågældende knap. Fabriksdefinerede regeloplysninger kan kun redigeres:



Husk, at detaljerede regelindstillinger er avancerede og beregnet til netværksadministratorer, der har brug for fuld kontrol over konfigurationen af Firewall. Hvis du ikke er bekendt med kommunikationsprotokoltyper, netværksportnumre, IP-adressedefinitioner osv, bedes du ikke modificere disse indstillinger! Hvis du skal ændre konfigurationen, henvises til den pågældende dialoghjælpefil for specifikke oplysninger.

Log ukendt trafik

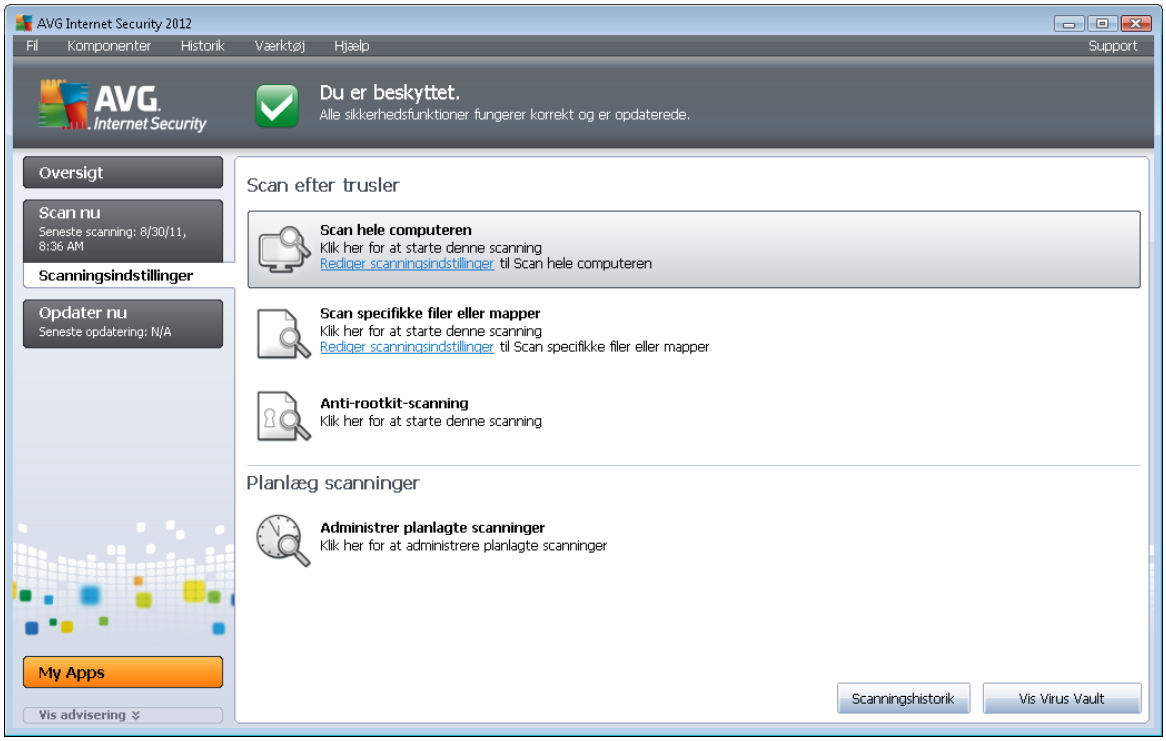
- ***Log ukendt indkommende trafik*** *(deaktiveret som standard)* – Markér afkrydsningsfeltet for at registrere alle ukendte eksterne forsøg på at oprette forbindelse til computeren i Log.
- ***Log ukendt udgående trafik*** *(aktiveret som standard)* – Markér afkrydsningsfeltet for at

registrere alle ukendte forsøg fra computeren på at oprette forbindelse til et eksternt sted i Log.

11. AVG Scanning

AVG Internet-sikkerhed 2012 kører som standard ikke nogen scanninger, så ligesom efter den første scanning er du her fuldstændig beskyttet af de indbyggede komponenter i **AVG Internet-sikkerhed 2012**, som altid er på vagt og beskytter mod mistænkelige koder. Du kan selvfølgelig planlægge en scanning til at køre med jævne mellemrum eller starte en scanning manuelt, som passer til dine aktuelle behov.

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 2012** 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.

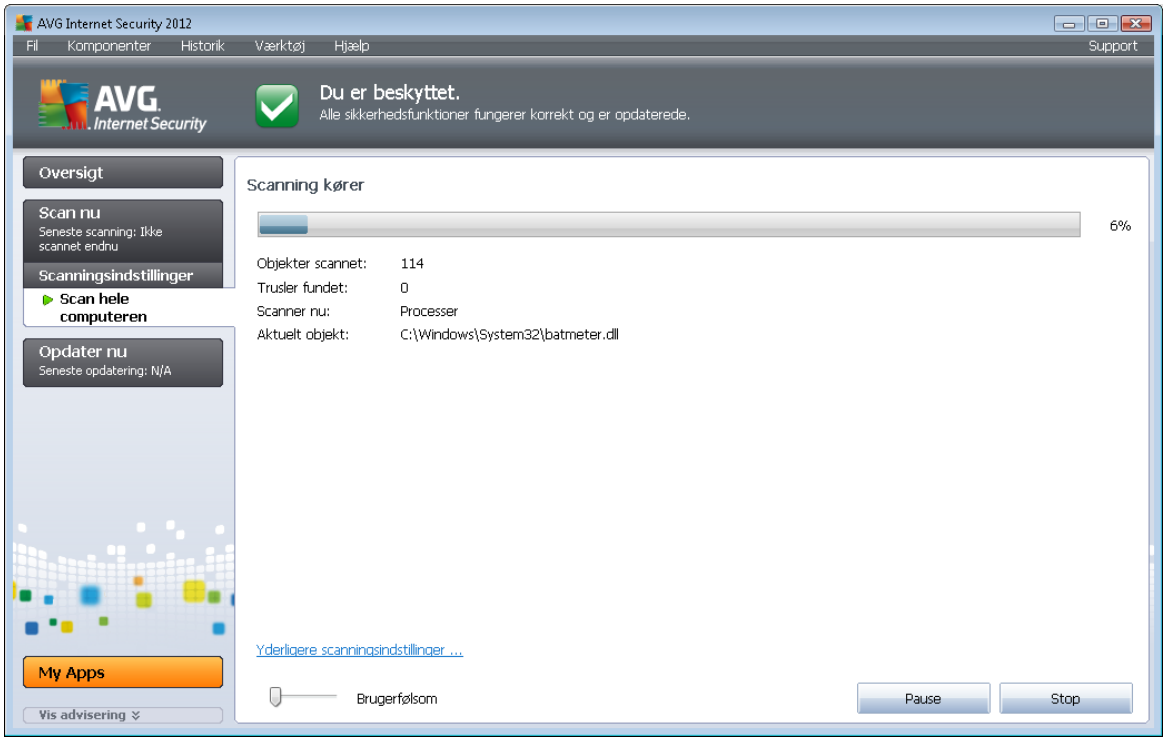
I **AVG Internet-sikkerhed 2012** vil du finde følgende typer scanning, der er foruddefineret af softwareleverandøren:

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.

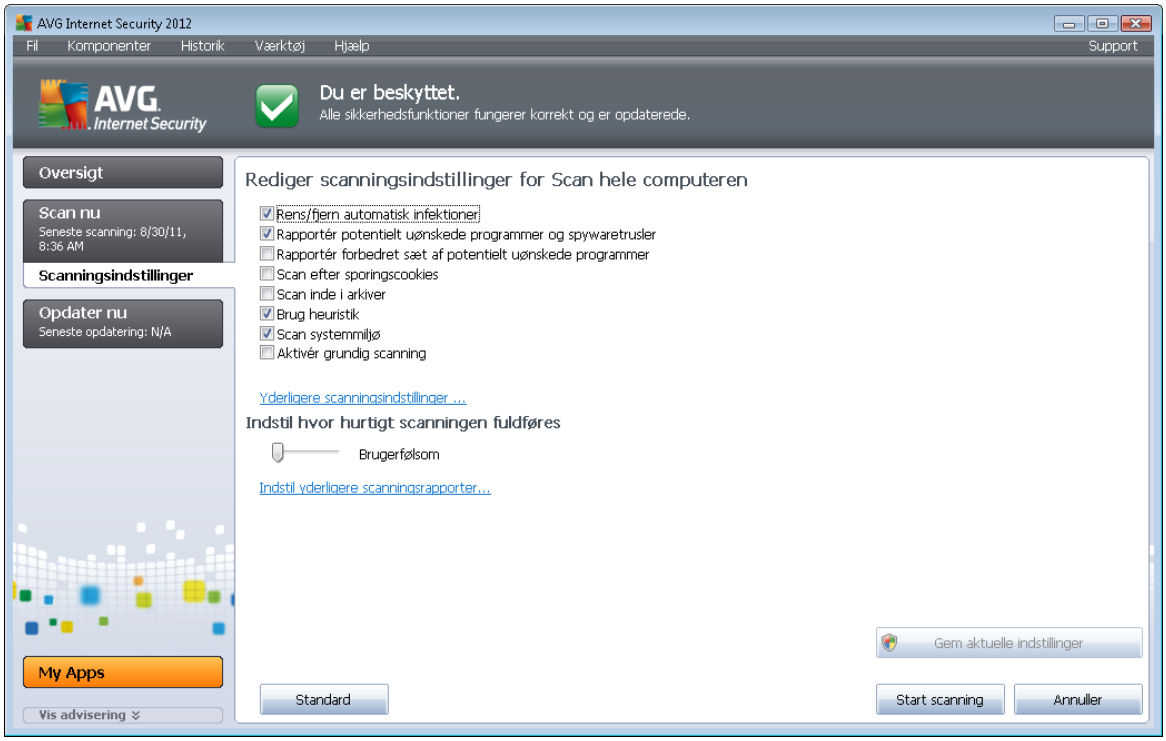
Scanningskørsel

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*).

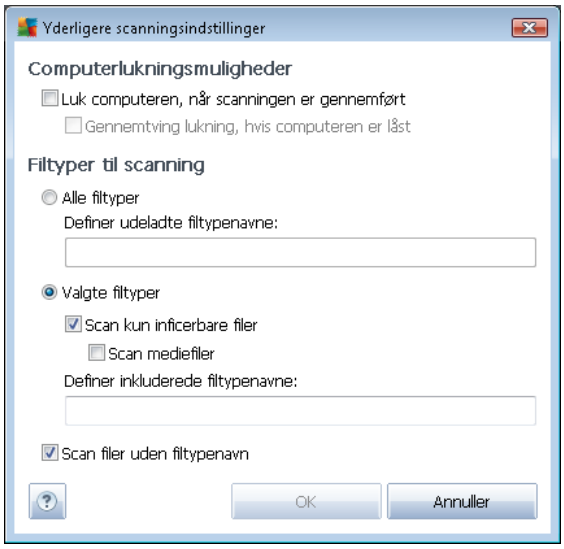
- ***Scan inde i arkiver*** (*slået fra som standard*) - disse parametre definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i arkiver, f.eks. ZIP, RAR, ...

- ***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***).

  - ***Filtyper til scanning*** – Du bør også angive, om du vil scanne:

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

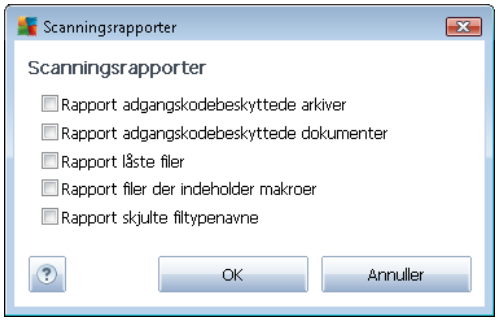
    - ***Udvalgte filtyper*** - du kan angive, at du kun vil scanne filer, som er mulige at inficere (*filer som ikke kan blive inficeret, bliver ikke scannet, for eksempel*

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.

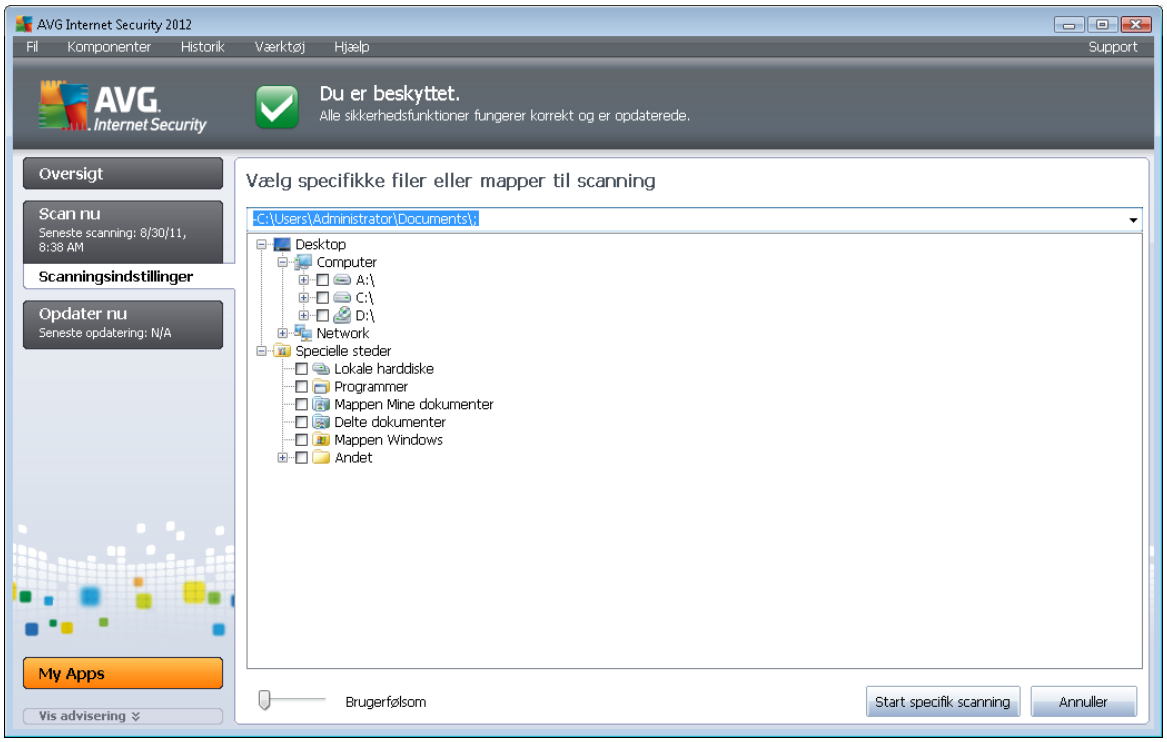
Scanningskørsel

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.

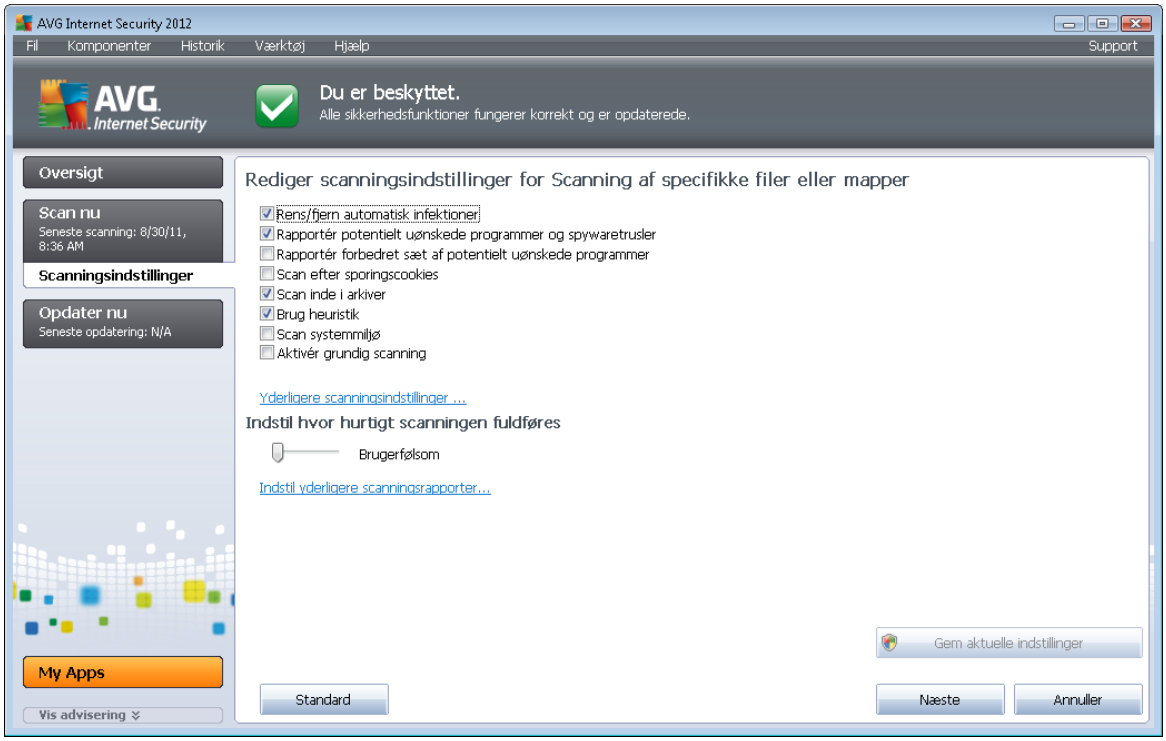
Det er også muligt at få scannet en specifik mappe, mens alle dens undermapper er undtaget fra denne scanning. Det gør du ved at skrive et minustegn "**-**" foran den automatisk genererede sti (*se skærmbillede*). Brug parameteren "**!**" for at undtage hele mappen fra scanning.

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*).

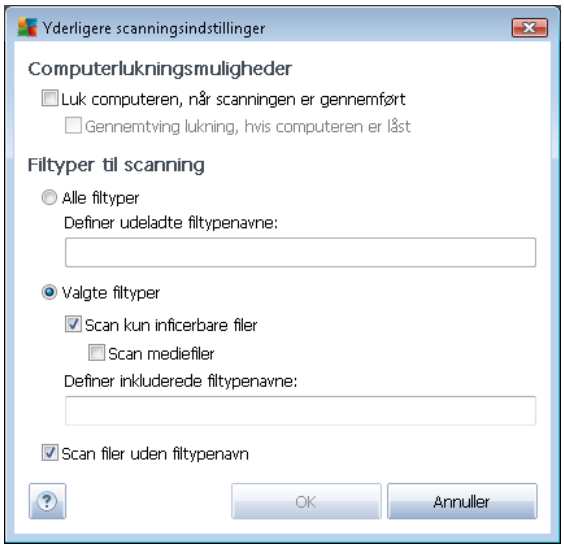
- ***Scan inde i arkiver*** (*slået til som standard*) - disse parametre definerer, at scanningen skal kontrollere alle filer, også hvis de er lagret i arkiver, f.eks. ZIP, RAR, ...

- ***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***).

  - ***Filtyper til scanning*** – Du bør også angive, om du vil scanne:

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

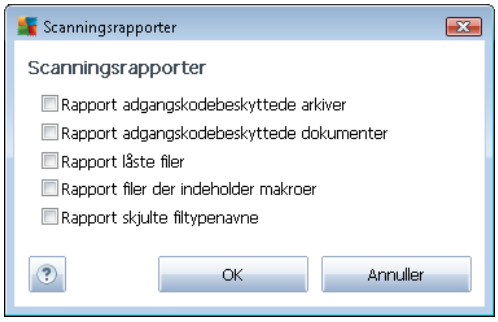
    - ***Udvalgte filtyper*** - du kan angive, at du kun vil scanne filer, som er mulige at inficere (*filer som ikke kan blive inficeret, bliver ikke scannet, for eksempel*

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).*

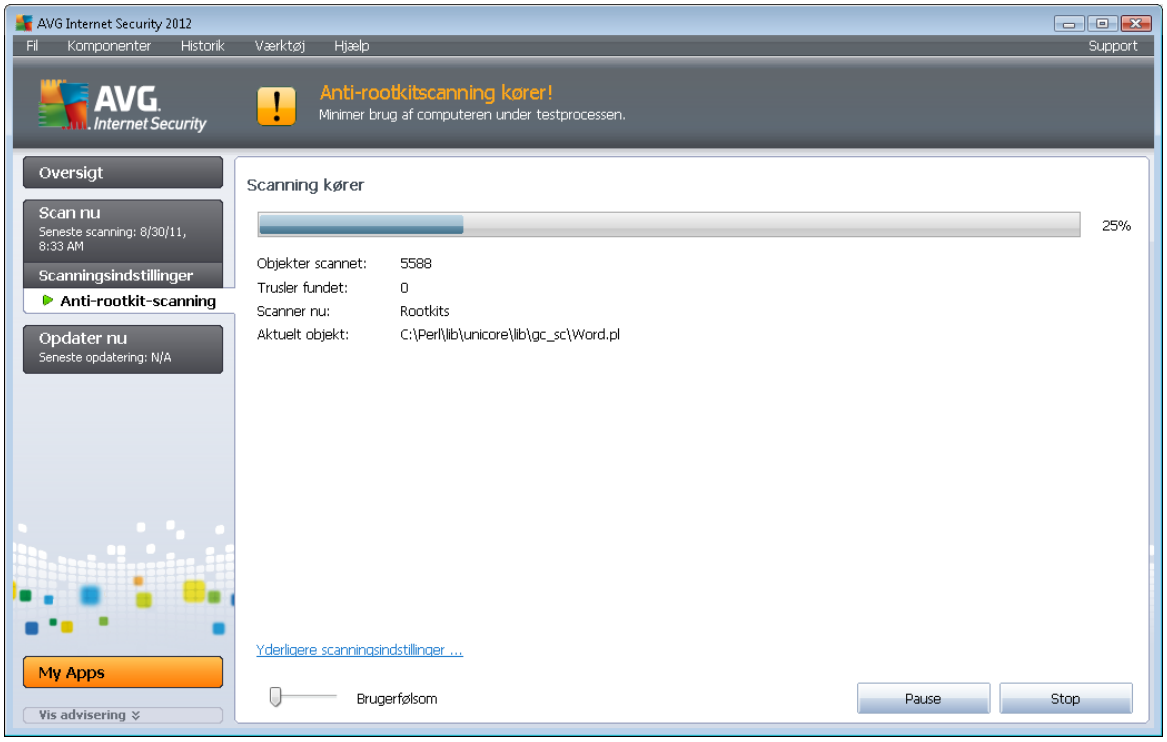
11.2.3. Anti-rootkit-scanning

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.

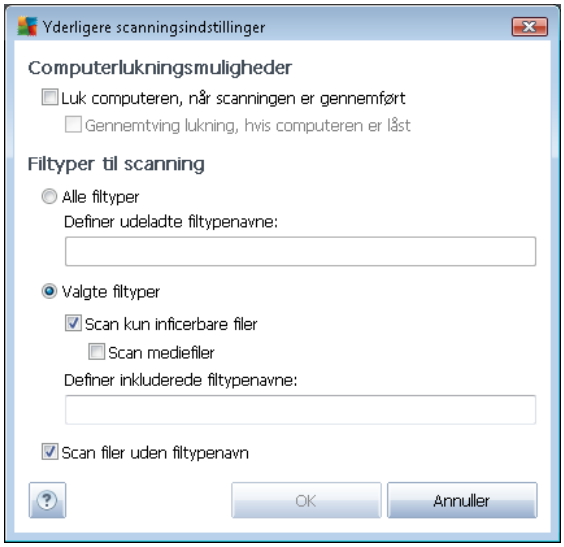


Redigering af scanningskonfiguration

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:

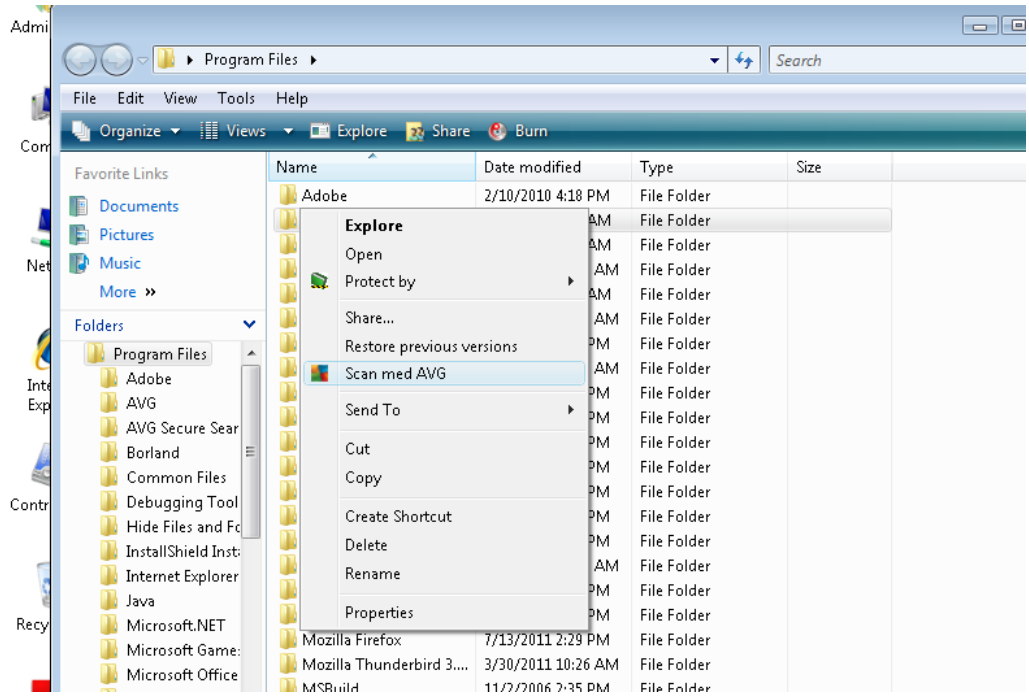
- ***Automatisk scanning*** - du kan bruge skyderen til at ændre scanningsprioriteten. Som standard er denne indstillingsværdi sat til *brugerfølsomt niveau af automatisk ressourceforbrug.* Alternativt kan du køre scanningen langsommere, hvilket betyder, at belastningen på systemressourcerne minimeres (*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 2012** 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:



- Markér den fil *(eller mappe)*, du vil kontrollere
- Højreklik med musen på objektet for at åbne kontekstmenuen

- Vælg ***Scan med*** for at få AVG til at scanne filen**AVG Internet-sikkerhed 2012**

11.4. Kommandolinjescanning

I **AVG Internet-sikkerhed 2012** 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

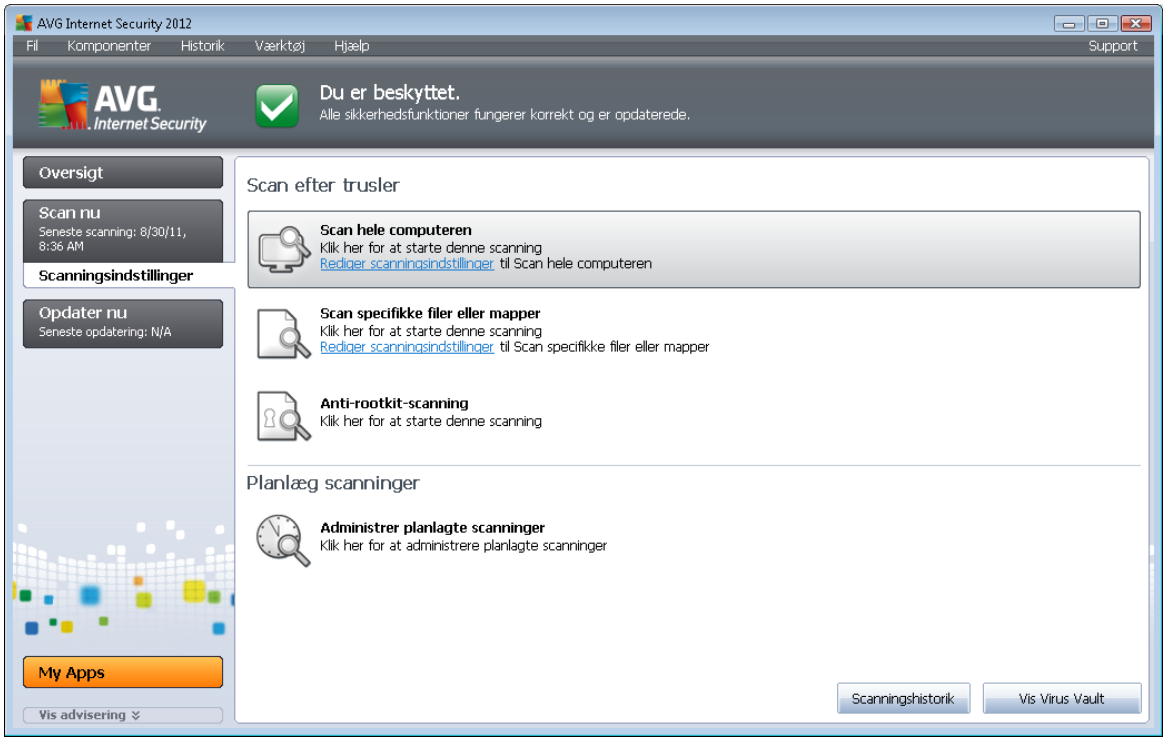
- ***/COO*** Scan cookies
- ***/?*** Vis hjælp om dette emne
- ***/HELP*** Vis hjælp om dette emne
- ***/PRIORITET*** Angiv scanningsprioritet/Lav, Auto, Høj/ *(se Avancerede indstillinger/Scanninger)*
- ***/SHUTDOWN*** Luk computeren, når scanningen er fuldført
- ***/FORCESHUTDOWN*** Gennemtving computerlukning,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

11.5. Scanningsplanlægning

Med **AVG Internet-sikkerhed 2012** 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.

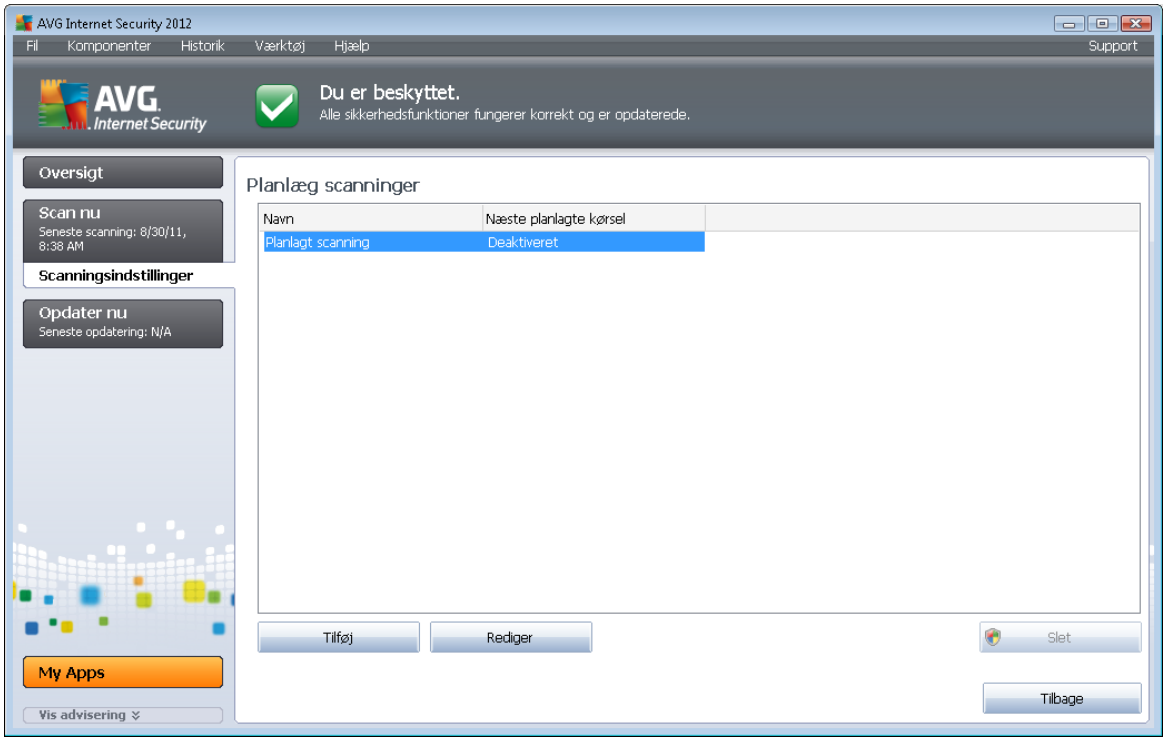
Du bør køre Scanning af hele computeren regelmæssigt, mindst en gang ugentligt. Hvis det er muligt, bør du køre en scanning af hele computeren dagligt - som indstillet i standardkonfigurationen for scanningsplanlægning. Hvis computeren er "altid tændt", kan du planlægge scanninger uden for arbejdstiden. 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 dialog ***Planlæg scanninger***, hvor du kan finde en liste over alle de scanninger, der er planlagt i øjeblikket:

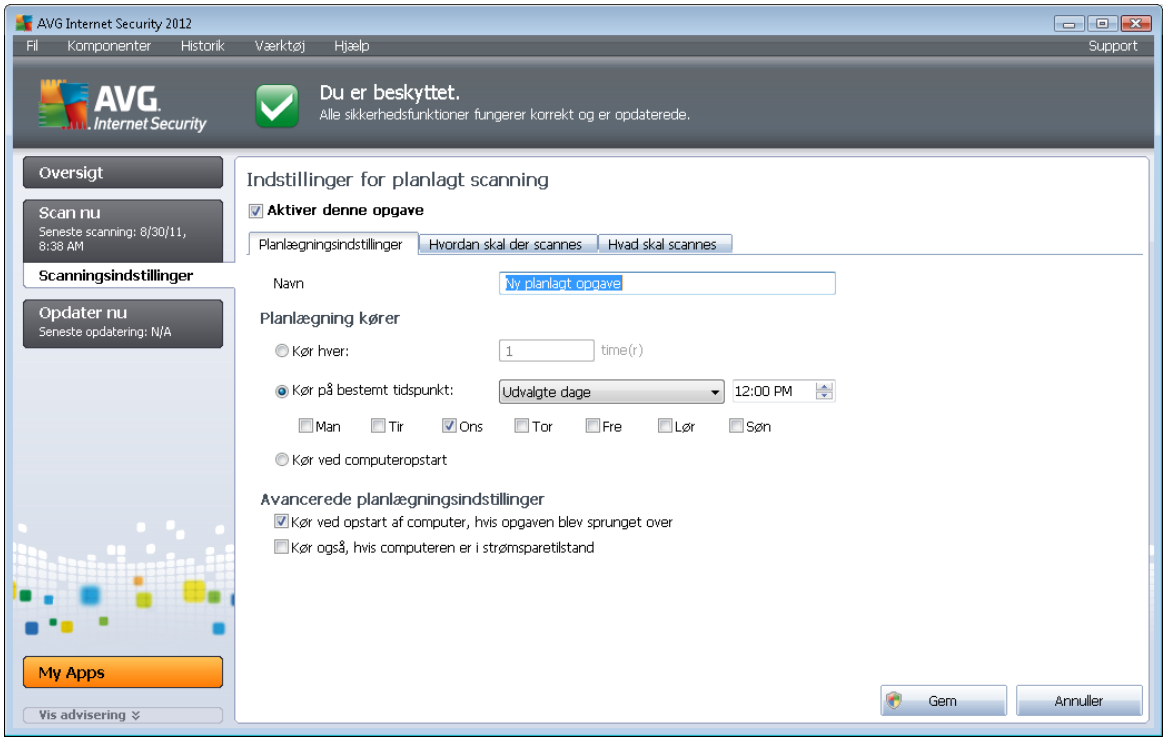


Du kan redigere/tilføje scanninger med følgende betjeningsknapper:

- ***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***). Dialogen er inddelt i tre faner: ***Planlægningsindstillinger****(se billede herunder, standardfanen, du automatisk omdirigeres til*), Hvordan skal der 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.

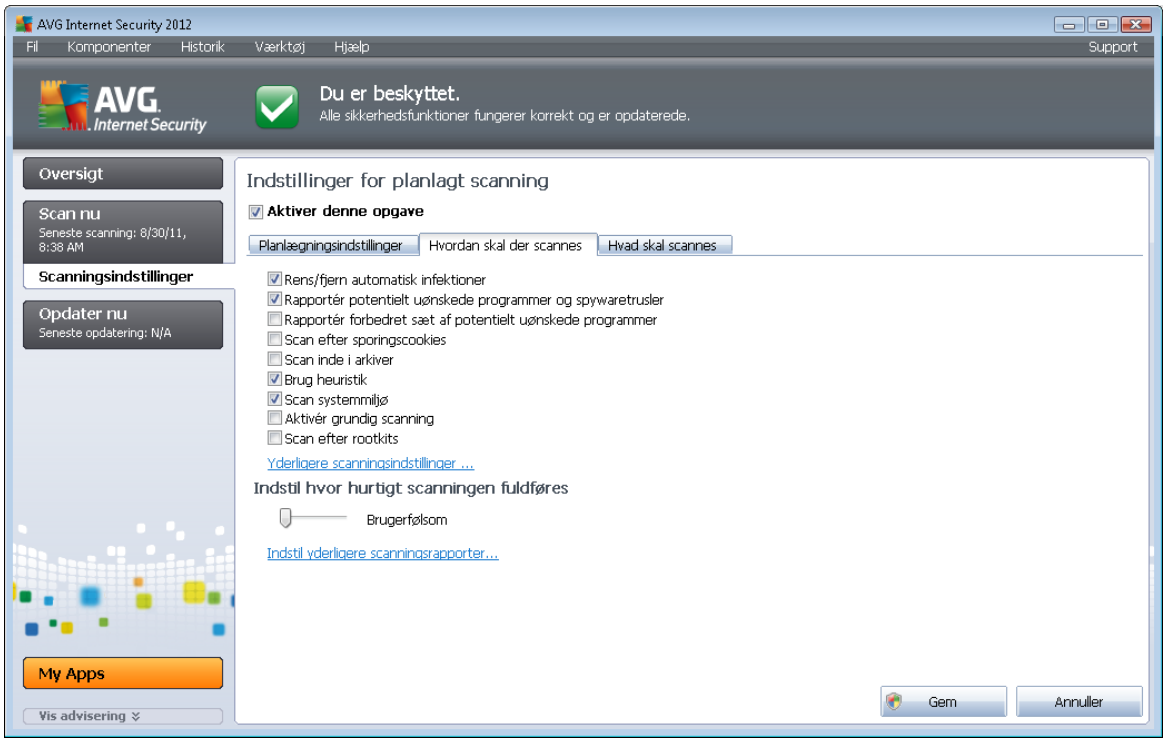
Betjeningsknapper i dialogen Indstillinger for planlagt scanning

Der er to tilgængelige kontrolknapper på alle tre faner i dialogen ***Indstillinger for planlagt scanning*** *(Planlægningsindstillinger, Hvordan skal der scannes og Hvad skal scannes)*, og disse har den samme funktionalitet, uanset hvilken fane du befinder dig på i øjeblikket:

- ***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.

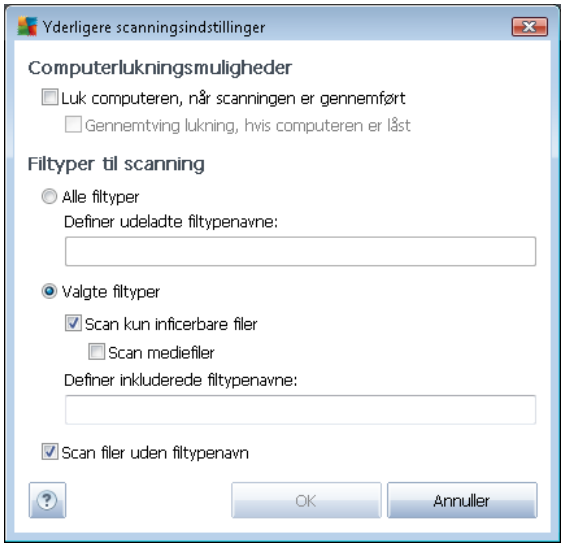
- ***Scan systemmiljø*** (*slået til som standard*): Scanningen kontrollerer også computerens systemområder.

- ***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.

- ***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.

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***).

- ***Filtyper til scanning*** – Du bør også angive, om du vil scanne:

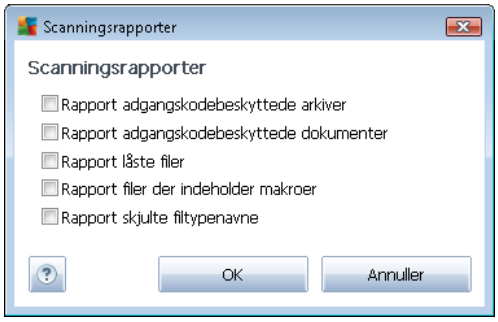
  - ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en kommasepareret liste over filtypenavne, som ikke skal scannes;

  - ***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:



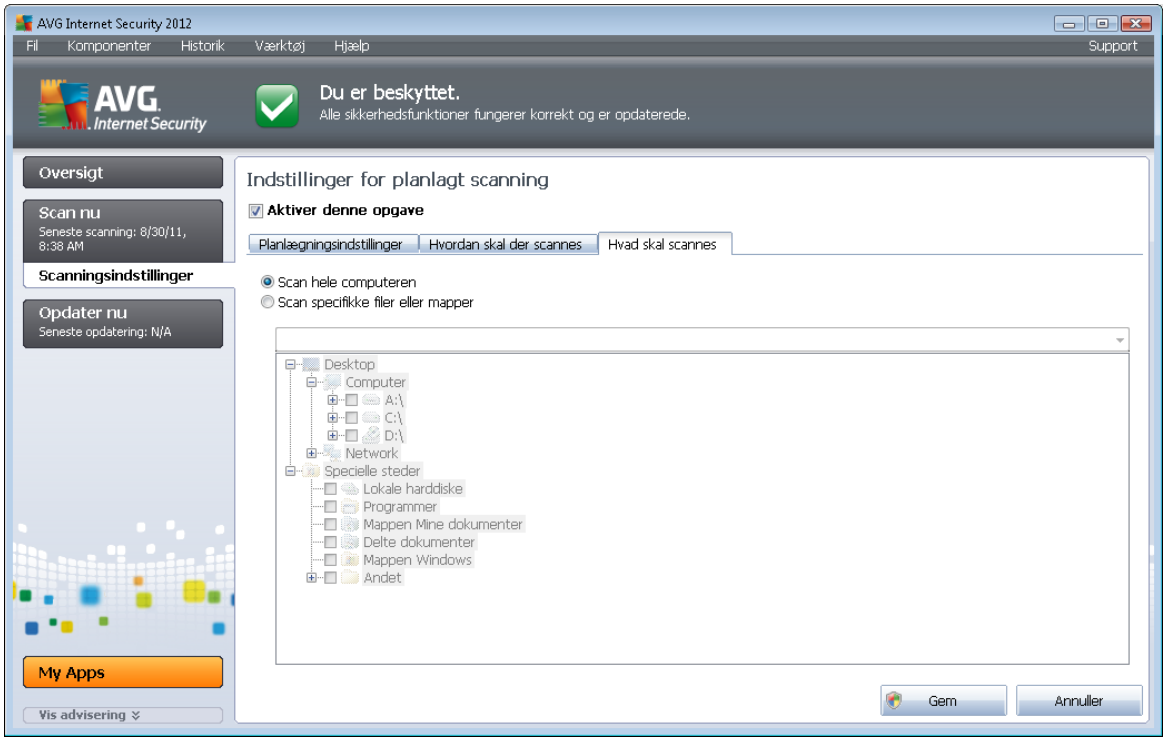
Betjeningsknapper

Der er to tilgængelige kontrolknapper på alle tre faner i dialogen ***Indstillinger for planlagt scanning*** *Planlægningsindstillinger, Hvordan skal der scannes og Hvad skal scannes*, og disse har den samme funktionalitet, uanset hvilken fane du befinder dig på i øjeblikket:

- ***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*)

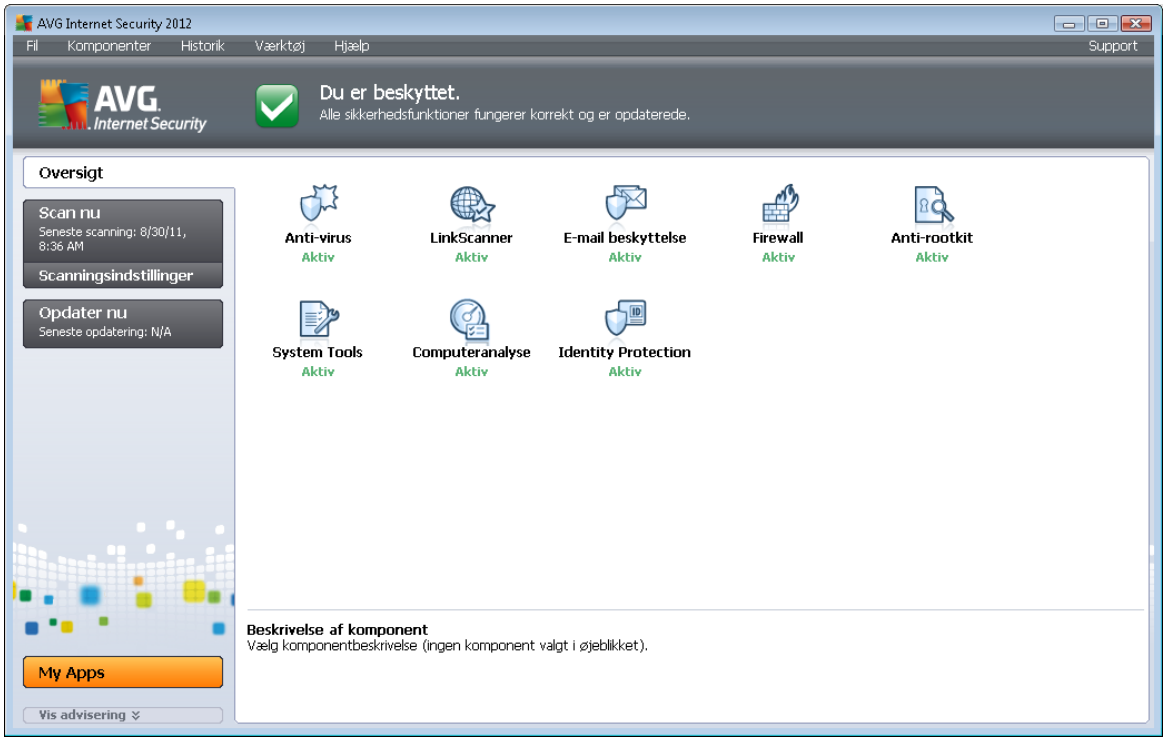
Betjeningsknapper

De samme to kontrolknapper er tilgængelige på alle tre faner i dialogen ***Indstillinger for planlagt scanning*** *(Planlægningsindstillinger, Hvordan skal der scannes og Hvad skal scannes)*:

- ***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 oplysnigner 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

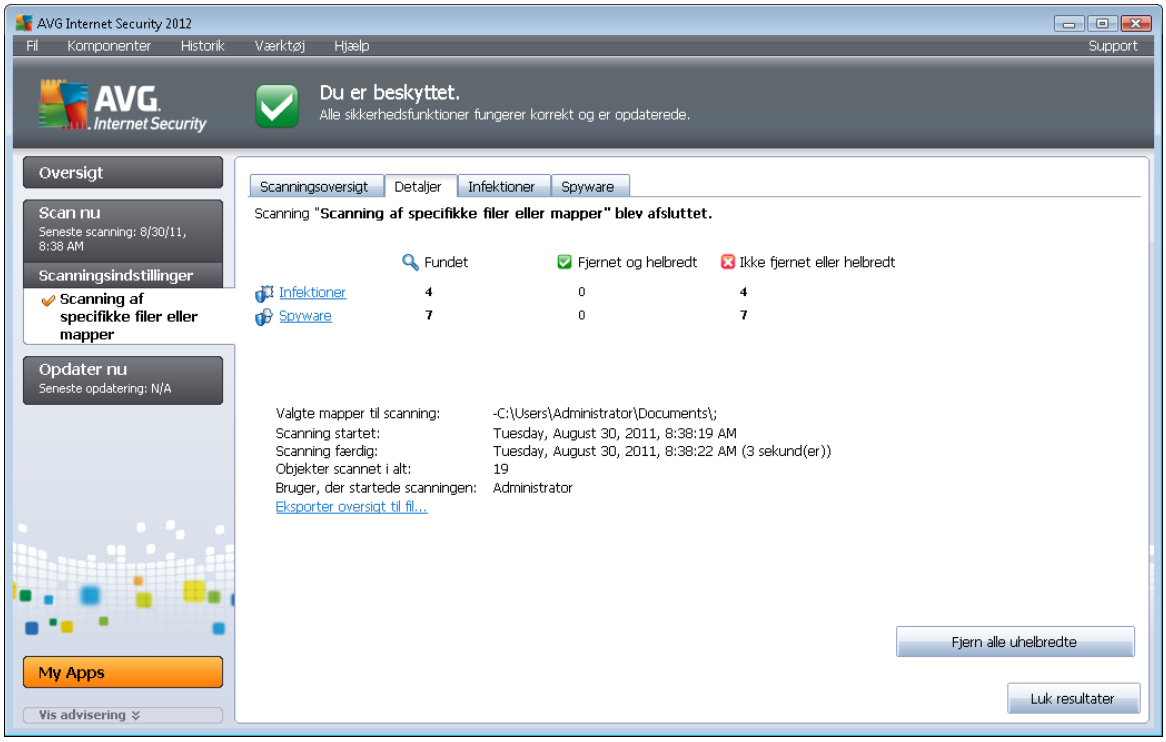
11.7. Scanningsresultatdetaljer

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 kan også finde oplysninger om objekter, der ikke scannes *(f.eks. adgangskodebeskyttede arkiver)*.

11.7.1. Fanen Resultatoversigt



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

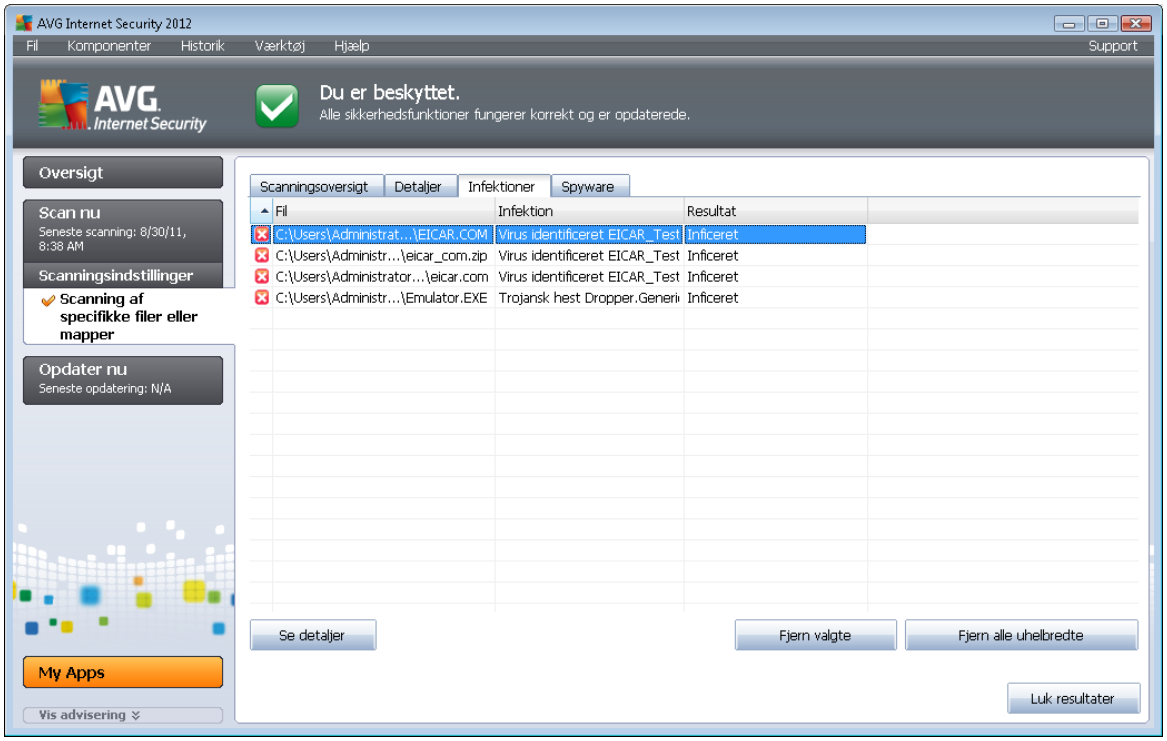
- detekterede virusinfektioner/spywareprogrammer
- fjernede virusinfektioner/spywareprogrammer
- antallet af virusinfektioner / spyware, der ikke kan fjernes eller helbredes

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:

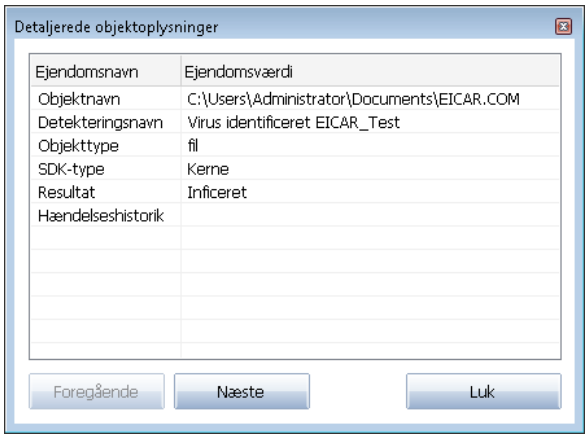
- ***Fil*** - fuld sti til det inficerede objekts oprindelige placering
- ***Infektioner*** - navn på den detekterede virus (*se Virus-opslagsværket online for yderligere oplysninger om specifikke vira*)
- ***Resultat*** - definerer den aktuelle status for det inficerede objekt, der blev detekteret under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

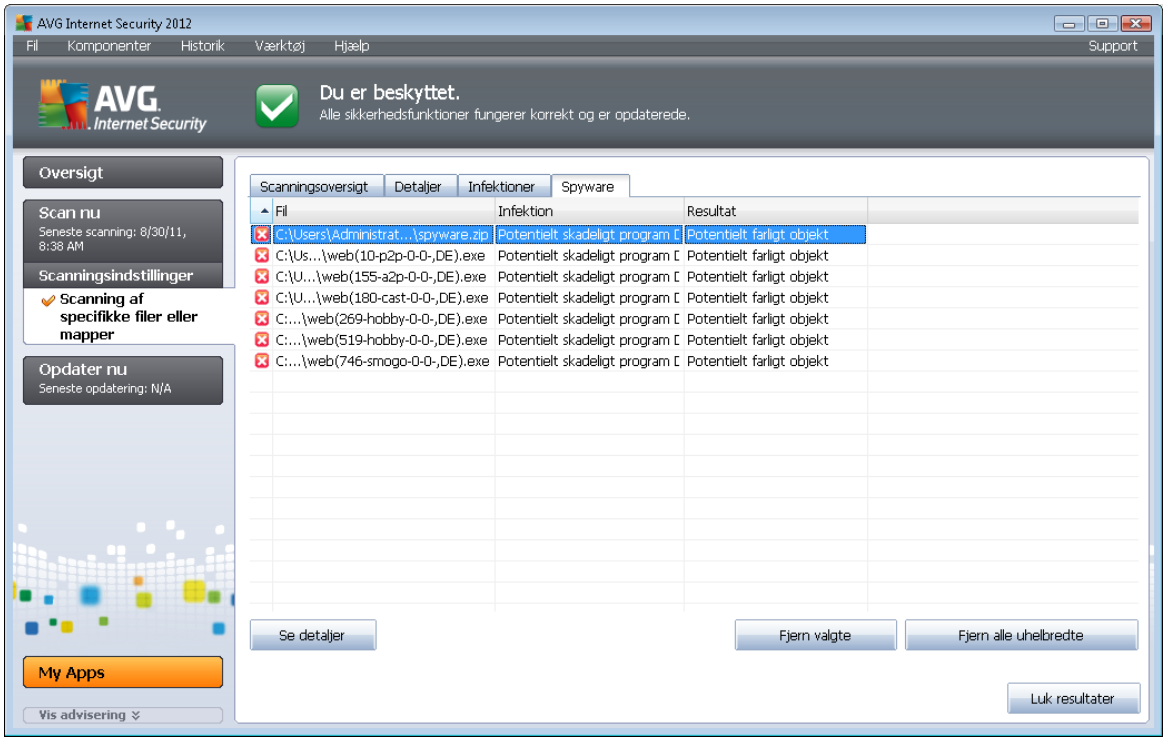


  I denne dialog kan du finde detaljerede oplysninger om det detekterede inficerede objekt (*f.eks. inficeret objektnavn og placering, objekttype, SDK-type, detekteringsresultat og handlingshistorik, der er relateret til det detekterede objekt*). Med knapperne ***Forrige*** / ***Næste*** kan du se oplysninger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

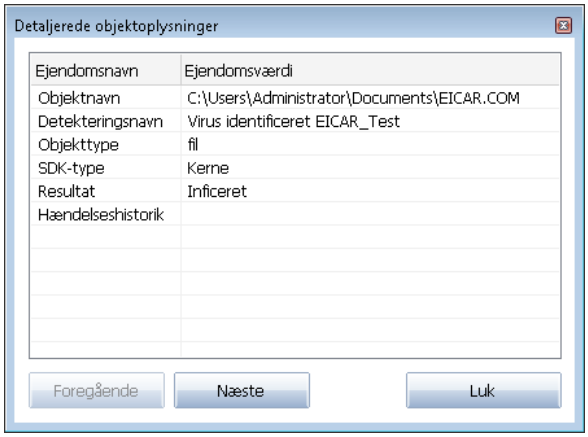
- ***Fil*** - fuld sti til det inficerede objekts oprindelige placering
- ***Infektioner*** – Navnet på den detekterede spyware *(du kan få oplysninger om specifikke virusser ved at se i Virus-opslagsværket på internettet)*
- ***Resultat*** - definerer den aktuelle status for det objekt, der blev detekteret 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 **AVG Internet-sikkerhed 2012** kun har er detekteret advarsler i testresultaterne, kræves der ingen handling.

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 **AVG Internet-sikkerhed 2012** rapporterer en skjult fil, som kan være skadelig, kan du flytte den til 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 Internet-sikkerhed 2012**-scanningen kan registrere filer, der 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 hverken scannes af **AVG Internet-sikkerhed 2012** (*eller generelt set af andre anti-malware-programmer*).

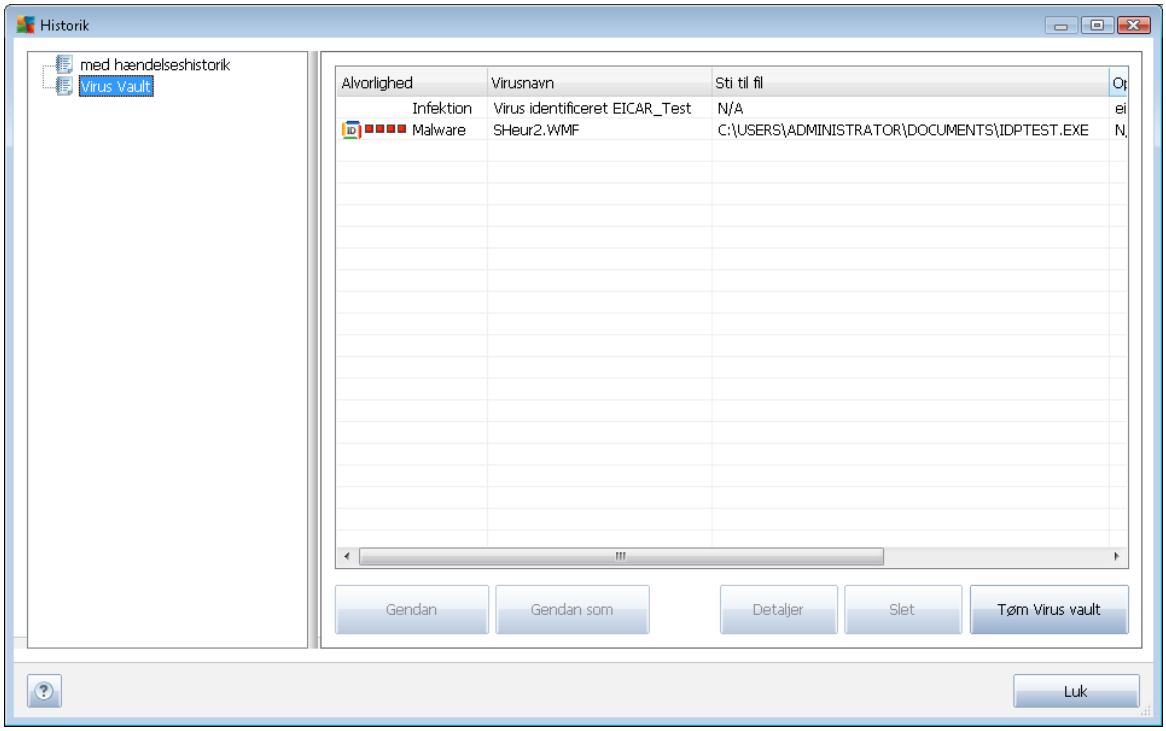
- ***Dokument med makroer*** - Det rapporterede dokument indeholder makroer, som kan være skadelige.

- ***Skjult filtypenavn*** - Filer med skjult filtypenavn kan se ud som f.eks. billeder men i virkeligheden være eksekverbare filer (*f.eks. billede.jpg.exe*). Den anden udvidelse er som standard ikke synlig i Windows, og **AVG Internet-sikkerhed 2012** rapporterer om 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 denne afvigelse. **AVG Internet-sikkerhed 2012** 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 Internet-sikkerhed 2012**. 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.

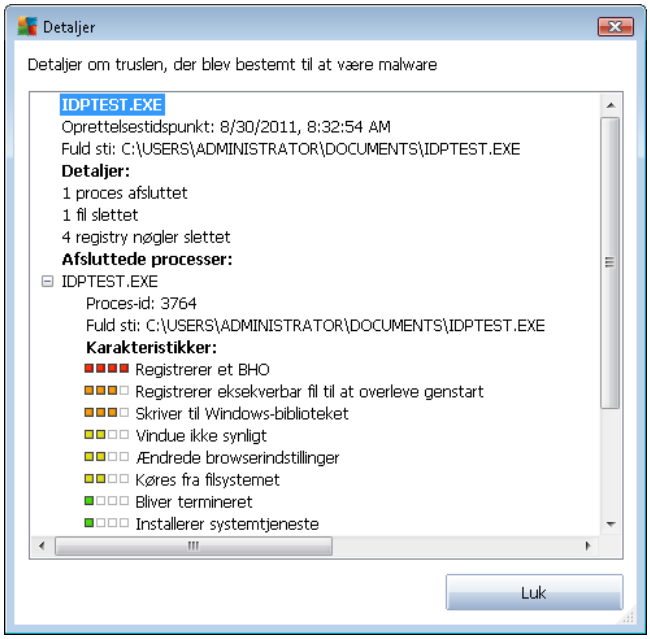
Virus Vault-grænsefladen åbnes i et separat vindue og indeholder en oversigt over oplysninger om inficerede objekter:

- ***Alvorlighed*** - hvis du bestemmer dig for at installere Identitetsbeskyttelse-komponenten i din **AVG Internet-sikkerhed 2012**, 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

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.

Med henblik på alle de aktuelle computertrusler og den hastighed, de spreder sig med, er det altafgørende, at du opdaterer din **AVG Internet-sikkerhed 2012** med jævne mellemrum. Den bedste løsning er at bibeholde programmets standardindstillinger, hvor automatisk opdatering er konfigureret. Bemærk, at hvis virusdatabasen for **AVG Internet-sikkerhed 2012** ikke er opdateret, kan programmet ikke detektere de seneste trusler!

Det er afgørende at AVG opdateres regelmæssigt! Vigtige opdateringer af virusdefinitioner bør om muligt foretages dagligt. Mindre vigtige programopdateringer kan foretages ugentligt.

12.1. Start af opdatering

For at sikre den bedst mulige sikkerhed er **AVG Internet-sikkerhed 2012** som standard planlagt til at se efter nye opdateringer hver fjerde time. Da AVG-opdateringer ikke frigives efter en fast tidsplan, men i stedet som svar på mængden og alvorligheden af nye trusler, er denne kontrol meget vigtig for at sikre, at AVG-virusdatabasen hele tiden er opdateret.

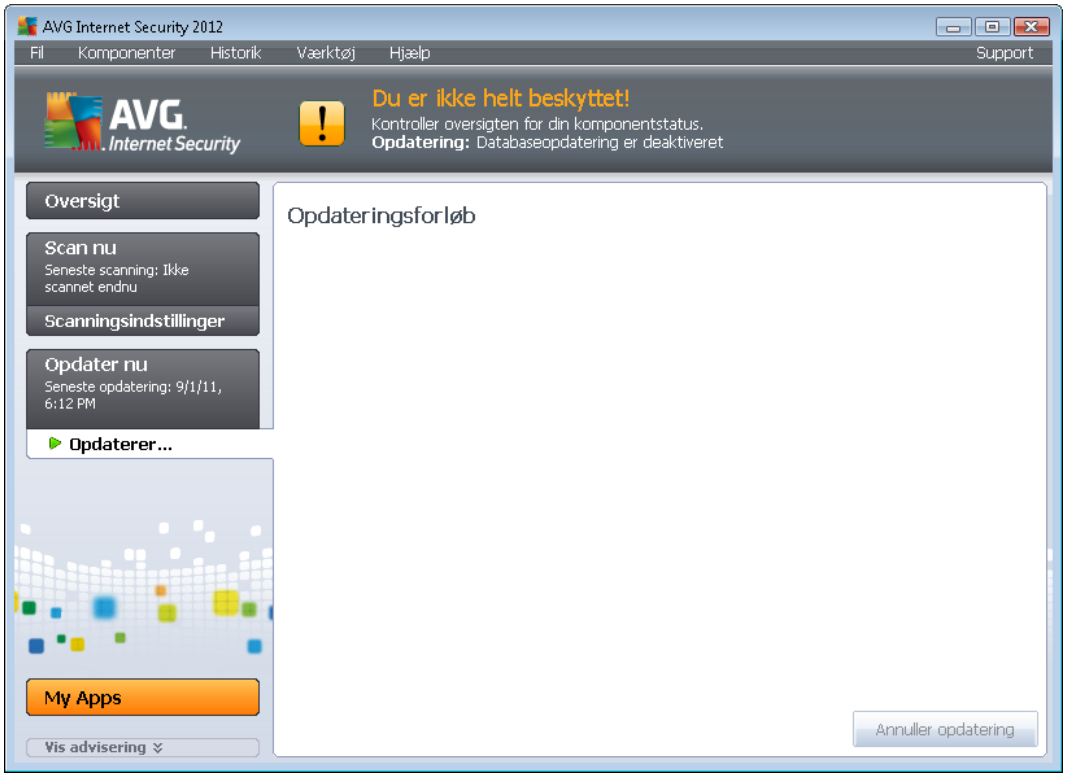
Hvis du ønsker at reducere antallet af opdateringsstarter, kan du konfigurere dine egne parametre for opdateringsstart. Det anbefales imidlertid på det kraftigste at starte opdateringen mindst en gang om dagen! Konfigurationen kan redigeres i sektionen Avancerede indstillinger/Planlægning og især i de følgende dialoger:

- Plan over definitionsopdatering
- Programopdateringsplan
- Anti-spam-opdateringsplan

Hvis du med det samme vil tjekke, om der er nye opdateringsfiler, skal du bruge lynlinket Opdater nu i hovedbrugergrænsefladen. Dette link er altid tilgængeligt via enhver dialog i brugergrænsefladen.

12.2. Opdateringsforløb

Når du har startet opdateringen, verificerer AVG først, om der er nye tilgængelige opdateringer. Hvis ja, starter **AVG Internet-sikkerhed 2012** download og starter selve opdateringsprocessen. Under opdateringen bliver du omdirigeret til grænsefladen ***Opdatering***, hvor du kan se en grafik gengivelse af processen sammen med en oversigt over relevante statistiske parametre (*størrelse af opdateringsfil, modtagne data, downloadhastighed, tidsforbrug...*):



***Bemærk**: Før hver opdateringsstart for AVG-programmet, oprettes der et systemgendannelsespunkt. Hvis opdateringsprocessen mislykkes, og operativsystemet går ned, kan du altid gendanne operativsystemet til dets oprindelige konfiguration fra dette sted. Denne indstilling er tilgængelig via Windows-menuen: Start/Alle programmer/Tilbehør/Systemværktøjer/ Systemgendannelse. Anbefales kun for erfarne brugere!*

12.3. Opdateringsniveauer

AVG Internet-sikkerhed 2012 har to opdateringsniveauer, der kan vælges imellem:

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

- ***Programopdatering*** indeholder diverse programændringer, rettelser og forbedringer.

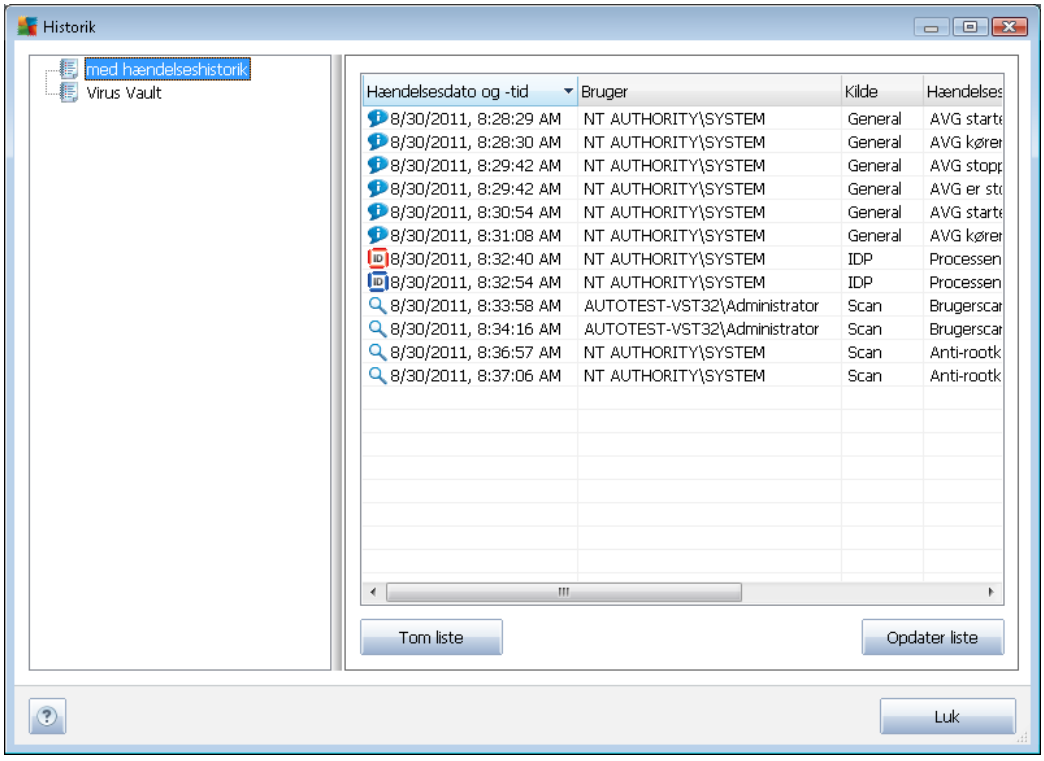
Når du planlægger en opdatering, er det muligt at definere specifikke parametre for begge opdateringsniveauer:

- Plan over definitionsopdatering

- Programopdateringsplan

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

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 2012**. ***Historik*** registrerer følgende typer hændelser:

- Information om opdateringer af AVG-applikationen
- Oplysninger om start, afslutning eller stop af scanning (*herunder test, der udføres automatisk*)
- Oplysninger om hændelser i forbindelse med virusdetektering (*enten af Resident Shield eller ved scanning*), herunder placering af hændelser
- Andre vigtige hændelser

For hver hændelse vises følgende oplysninger:

- ***Dato og tidspunkt for hændelse*** – Angiver den eksakte dato og tidspunkt for hændelsen
- ***Brugeren*** angiver navnet på den bruger, der er logget på på det tidspunkt, hvor hændelsen sker
- ***Kilde*** giver oplysninger om en kildekomponent eller den anden del af AVG-systemet, der udløste hændelsen
- ***Hændelsesbeskrivelse*** giver en kort sammenfatning af hvad der egentlig skete

Betjeningsknapper

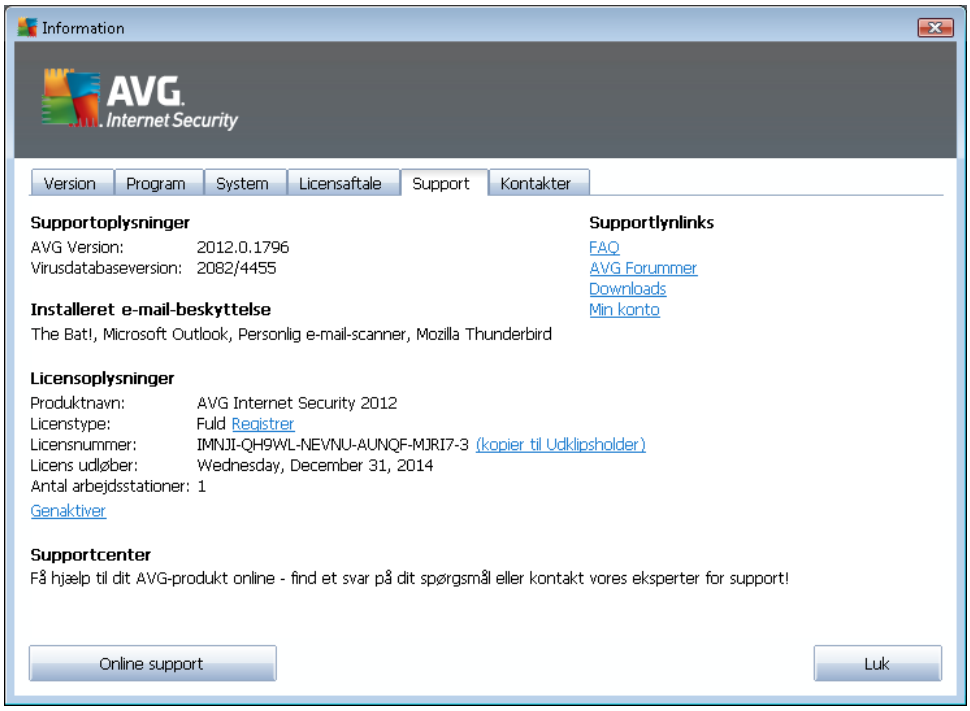
- ***Tøm liste*** – Tryk på denne knap for at slette alle poster fra listen over hændelser
- ***Opdater liste*** – Tryk på denne knap for at opdatere alle poster fra listen over hændelser

14. FAQ og teknisk support

Hvis du har problemer i forbindelse med salg eller tekniske spørgsmål med **AVG Internet-sikkerhed 2012** -applikationen, kan du få hjælp på flere måder. Vælg mellem følgende valgmuligheder:

- ***Kontakt kundesupport***: Du kan kontakte vores professionelle kundesupport direkte via AVG-applikationen. Vælg indstillingen ***Hjælp/Få hjælp online*** i hovedmenuen for at blive omdirigeret til onlinekontaktformularen, så du kan kommunikere med AVG's kundesupport 24 timer i døgnet. Licensnummeret udfyldes automatisk. Hvis du vil fortsætte, skal du følge instruktionerne på websiden.

- ***Support (link i hovedmenu)***: AVG-applikationsmenuen (*øverst i hovedgrænsefladen*) omfatter linket ***Support***, der åbner en ny dialog med alle de typer oplysninger, du skal bruge, hvis du har brug for hjælp. Dialogen indeholder grundlæggende data om det installerede AVG-program (*program/databaseversion*), licensoplysninger og en liste over lynlink til support:



- ***Fejlfinding i hjælpfil***: Der er et nyt afsnit om ***Fejlfinding*** tilgængeligt direkte i hjælpfilen, der indgår i **AVG Internet-sikkerhed 2012**. I dette afsnit er der en liste over situationer, der ofte opstår, når en bruger ønsker professionel hjælp til at få løst et teknisk problem. Vælg den situation, der bedst beskiver problemet, og klik på den for at få detaljerede oplysninger, der kan løse problemet.

- ***Supportcenter på AVG-webstedet***: Du kan også slå løsningen på problemet på AVG-webstedet (http://www.avg.com/). I sektionen ***Supportcenter*** kan du finde en struktureret oversigt over temabaserede grupper, der håndterer spørgsmål i forbindelse med både salg og tekniske problemstillinger.

- ***Ofte stillede spørgsmål***: På AVG-webstedet (http://www.avg.com/) kan du også finde et

separat og meget udførligt struktureret afsnit med ofte stillede spørgsmål. Dette afsnit er tilgængeligt via menuindstillingen ***Supportcenter/FAQ***. Endnu en gang opdeles alle spørgsmål på en fornuftig arrangeret måde inden for kategorier med salg, teknik og virus.

- ***Om virus og trusler***: Et bestemt kapitel på AVG-webstedet (http://www.avg.com/) er dedikeret virusproblemer. Vælg ***Supportcenter/Om virus og trusler*** i menuen for at gå til en side med et struktureret overblik over de oplysninger, der er relateret til onlinetrusler. Du kan også finde instruktioner i at fjerne virus, spyware og rådgivning om, hvordan beskyttelsen bevares.

- ***Diskussionsforum***: Du kan også bruge AVG-diskussionforummet for brugere på http://forums.avg.com.