AVG Internet Security 2013

Brugervejledning

Dokumentrevision 2013.01 (30.8.2012)

Indhold

1. Introduktion

Denne brugervejledning indeholder omfattende brugerdokumentation til **AVG Internet Security 2013**.

AVG Internet Security 2013 yder flere lag af beskyttelse i forbindelse med alt, hvad du foretager dig på internettet. Det betyder, at du ikke skal bekymre dig om identitetstyveri, 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 shoppe online og bruge netbank sikkert samt få glæde af de sociale netværk eller surfe og søge, velvidende at du har beskyttelse i realtid.

2. AVG Installationskrav

2.1. Understøttede operativsystemer

AVG Internet Security 2013 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**: Komponenten Identitet understøttes ikke i Windows XP x64. På dette operativsystem kan du installere AVG Internet Security 2013, men kun uden IDP-komponenten.*

2.2. Minimum og anbefalede hardwarekrav

Minimum hardwarekrav for **AVG Internet Security 2013**:

- Intel Pentium CPU 1,5 GHz eller hurtigere
- 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7) RAM
- 1,3 GB ledig plads på harddisken *(af installationsgrunde)*

Anbefalede hardwarekrav for **AVG Internet Security 2013**:

- Intel Pentium CPU 1,8 GHz eller hurtigere
- 1024 MB RAM
- 1,6 GB ledig plads på harddisken *(af installationsgrunde)*

3. AVG Installationsproces

Hvor kan jeg finde installationsfilen?

For at installere **AVG Internet Security 2013** på din computer skal du hente den nyeste installationsfil. Hvis du vil være sikker på, at du installerer den opdaterede version af **AVG Internet Security 2013**, anbefales det at downloade installationsfilen fra AVG's websted (http://www.avg.com/). Sektionen ***Support / Downloads*** indeholder en struktureret oversigt over installationsfilerne til hver AVG-udgave.

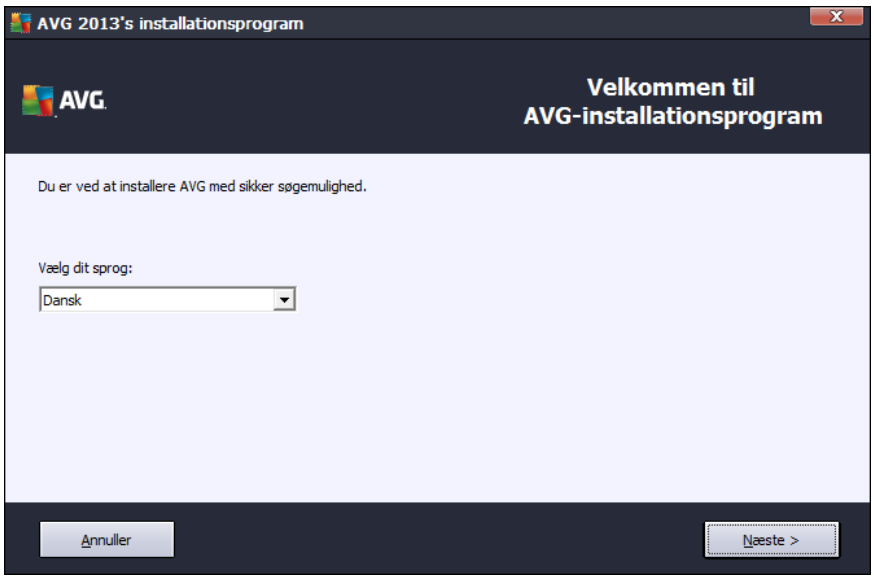
Hvis du ikke er sikker på, hvilke filer du skal downloade og installere, kan du benytte tjenesten ***Vælg produkt*** nederst på websiden. Når du har besvaret tre enkle spørgsmål, definerer denne tjeneste lige præcis de filer, du skal bruge. Tryk på knappen ***Fortsæt*** for at blive omdirigeret til en 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. Vi giver en detaljeret forklaring af hver dialogboks nedenfor:

3.1. Velkommen: valg af sprog

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



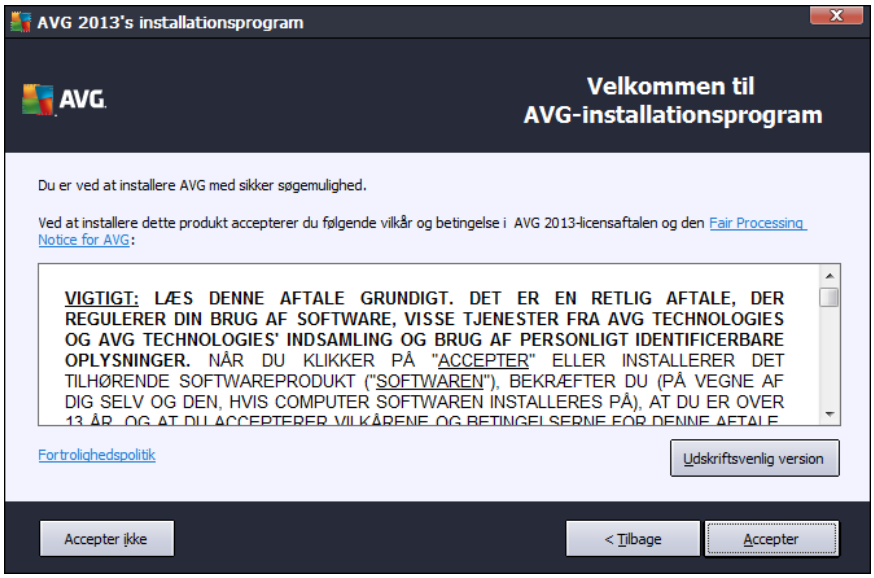
Her i dialogboksen kan du vælge det sprog, der blev brugt under installationsprocessen. Klik på kombinationsfeltet for få vist sprogmenuen. Vælg det ønskede sprog, og installationsprocessen fortsætter på det valgte sprog.

NB! I øjeblikket har du kun valgt installationssproget. Applikationen AVG Internet Security

2013 installeres på det valgte sprog samt på engelsk, som altid installeres automatisk. Det er imidlertid muligt, der kan installeres med flere sprog, der kan arbejdes med, i AVG Internet Security 2013. Du opfordres til at bekræfte dit fulde valg af alternative sprog i følgende konfigurationsdialoger, der kaldes Brugerdefinerede indstillinger.

3.2. Velkommen: licensaftale

Dialogboksen ***Velkommen til AVG-installationsprogrammet*** indeholder den fulde ordlyd af AVG-licensaftalen:



Læs hele teksten omhyggeligt. Du bekræfter, at du har læst, forstået og accepteret aftalen ved at trykke på knappen ***Acceptér***. Hvis du ikke er enig i licensaftalen skal du klikke på knappen ***Accepter ikke***, og installationsprocessen bliver afsluttet med det samme.

AVG Fortrolighedspolitik

Foruden licensaftalen giver denne opsætningsdialogboks dig også mulighed for at få mere at vide om ***AVG Rimelig behandlingsnotits*** og ***AVG Fortrolighedspolitik*** *(alle førnævnte funktioner vises i dialogboksen i form af et aktivt hyperlink, der åbner den dedikerede webside, hvor du kan finde detaljerede oplysninger)*. Klik på det respektive link for at blive omdirigeret til AVG's websted (http://www.avg.com/), der indeholder den fulde ordlyd af disse aftaler.

Betjeningsknapper

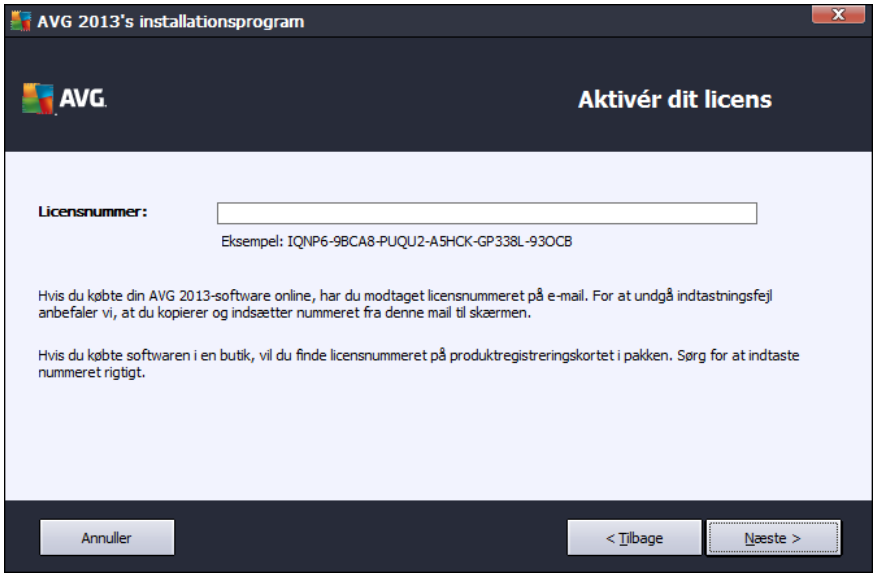
Der findes to betjeningsknapper i den første opsætningsdialogboks:

- ***Udskriftsvenlig version*** – klik på knappen for at få vist den fulde ordlyd af AVG-licensaftalen i en webgrænseflade, der er udskriftsvenlig.
- ***Accepter ikke*** – Klik for at afvise denne licensaftale. Konfigurationsprocessen stopper med det samme. **AVG Internet Security 2013** installeres ikke!

- ***Tilbage*** – Klik for at gå et trin tilbage til den forrige installationsdialogboks.
- ***Accepter*** – Klik for at bekræfte at du har læst, forstået og accepteret licensaftalen. Installation fortsætter, og du går et skridt videre til følgende konfigurationsdialog.

3.3. Aktivér din licens

I dialogboksen ***Aktivér din licens*** kan du indtaste dit licensnummer i det viste tekstfelt:



Her finder du licensnummeret

Salgsnummeret kan findes på cd-emballagen i pakken til **AVG Internet Security 2013**. Licensnummeret kan findes i den bekræftelsesmail, du modtag, efter du købte **AVG Internet Security 2013** online. Du skal indtaste nummeret, nøjagtig som det er vist. Hvis licensnummerets digitale formular er tilgængelig (*i e-mailen*), anbefales det at bruge kopiér/sæt ind-metoden til at indsætte det.

Sådan anvendes metoden med kopiering og indsættelse

Hvis du bruger metoden ***Kopiér og indsæt*** til at angive dit **AVG Internet Security 2013**-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.

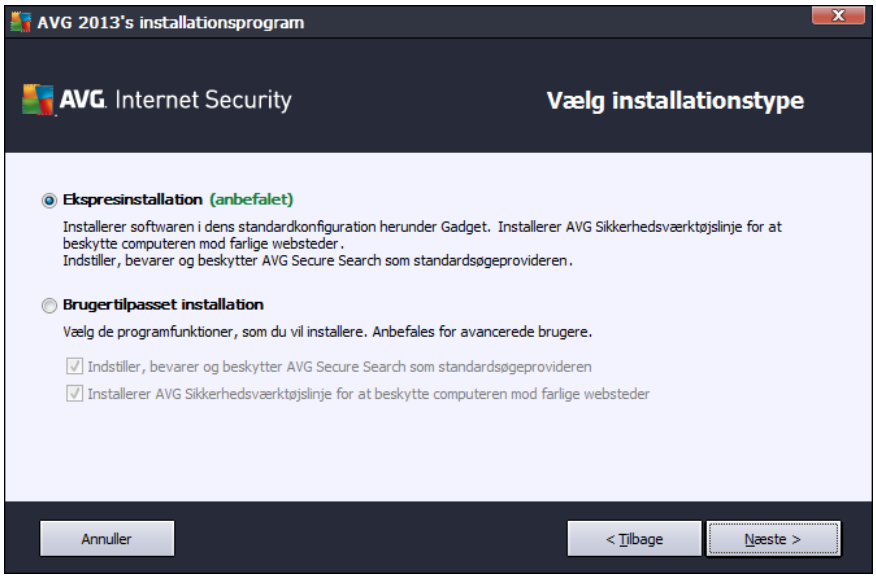
Betjeningsknapper

Som i de fleste indstillingsdialogbokse er der tre tilgængelige kontrolknapper:

- ***Annuller*** – klik for at afslutte opsætningen. **AVG Internet Security 2013** installeres ikke.
- ***Tilbage*** – klik for at gå et skridt tilbage til den forrige opsætningsdialog.
- ***Næste*** – klik for at fortsætte installationen og gå et skridt fremad.

3.4. Vælg installationstype

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



Lyninstallation

For de fleste brugeres vedkommende anbefales det på det kraftigste, at du bevarer standardinstallationen ***Lyninstallation***. På den måde installerer du **AVG Internet Security 2013** i en fuldautomatisk tilstand med indstillinger, der er defineret af programleverandøren, herunder AVG Gadget, AVG Sikkerhedsværktøjslinje, og AVG Secure Search konfigureres som standardssøgeprovideren. Denne konfiguration giver maksimal sikkerhed kombineret med optimal anvendelse af ressourcer. Hvis der på et senere tidspunkt opstår behov for at ændre konfigurationen, har du altid mulighed for at gøre det direkte i **AVG Internet Security 2013**-programmet.

Tryk på knappen ***Næste*** for at fortsætte til den følgende dialogboks i installationsprocessen.

Brugerdefineret installation

Brugerdefineret installation bør kun anvendes af erfarne brugere, der har en god grund til at installere **AVG Internet Security 2013** uden standardindstillingerne, f.eks. for at passe til specifikke systemkrav. I dette afsnit kan du bestemme, om de følgende funktioner skal installeres *(begge funktioner er markeret til at blive installeret og installeres automatisk, medmindre du fravælger det)*:

- ***Indstiller, bevarer og beskytter AVG Secure Search som din standardsøgeprovider*** - sørg for, at indstillingen er markeret for at bekræfte, at du vil bruge AVG Secure Search-programmer, der arbejder tæt sammen med Link Scanner Surf Shield om at give dig maksimal beskyttelse, når du er online.

- ***Installerer AVG Sikkerhedsværktøjslinje for at beskytte din computer mod skadelige websteder*** - sørg for, at indstillingen er markeret for at få installeret AVG Sikkerhedsværktøjslinje, som giver dig maksimal sikkerhed, når du surfer på internettet.

Hvis du vælger denne indstilling, vises en ny sektion ved navn ***Destinationsmappe*** i dialogboksen. Her skal du angive den placering, hvor **AVG Internet Security 2013** skal installeres. **AVG Internet Security 2013** er som standard installeret i programmappen på C-drevet, som vist i tekstfeltet i dialogboksen. Hvis du vil ændre denne placering, skal du bruge knappen ***Gennemse*** til at vise drevstrukturen og vælge den pågældende mappe. Du kan gendanne standardkonfigurationen, der er forudindstillet af softwareleverandøren, ved at bruge knappen ***Standard***.

Derefter skal du trykke på knappen ***Næste*** for at fortsætte til dialogboksen Brugerdefinerede indstillinger.

Betjeningsknapper

Som i de fleste installationsdialoger er der tre tilgængelige kontrolknapper:

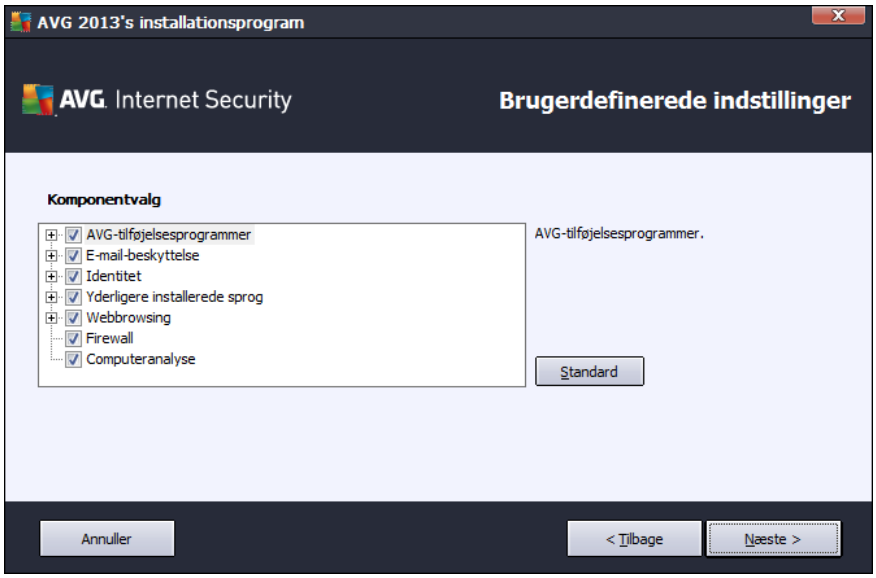
- ***Annuller*** – klik for at afslutte opsætningen. **AVG Internet Security 2013** installeres ikke.

- ***Tilbage*** – klik for at gå et skridt tilbage til den forrige opsætningsdialog.

- ***Næste*** – klik for at fortsætte installationen og gå et skridt fremad.

3.5. Brugerdefinerede indstillinger

Dialogboksen ***Brugerdefinerede indstillinger*** giver dig mulighed for at indstille detaljerede parametre for installationen:



Afsnittet ***Valg af komponenter*** indeholder en oversigt over alle **AVG Internet Security 2013**-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***.

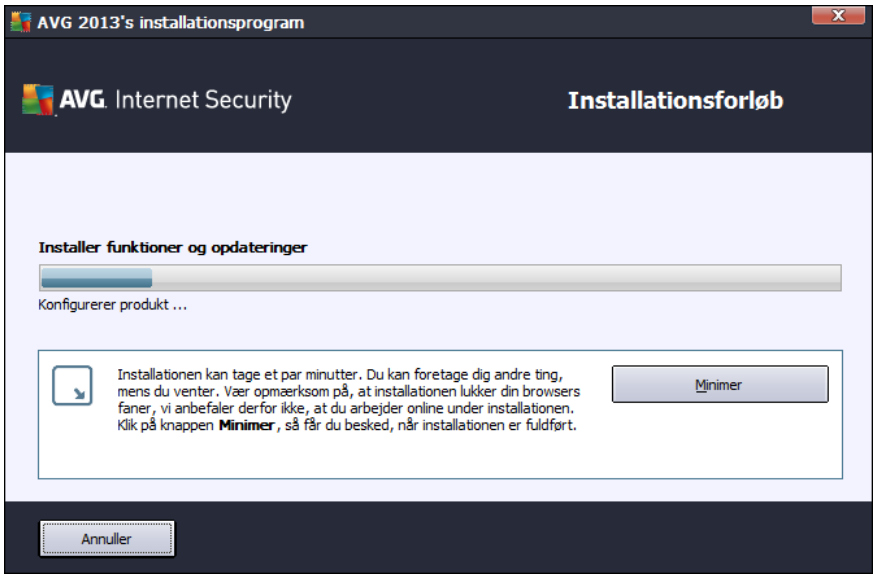
Betjeningsknapper

Som i de fleste indstillingsdialogbokse er der tre tilgængelige kontrolknapper:

- ***Annuller*** – klik for at afslutte opsætningen. **AVG Internet Security 2013** installeres ikke.
- ***Tilbage*** – klik for at gå et skridt tilbage til den forrige opsætningsdialog.
- ***Næste*** – klik for at fortsætte installationen og gå et skridt fremad.

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.

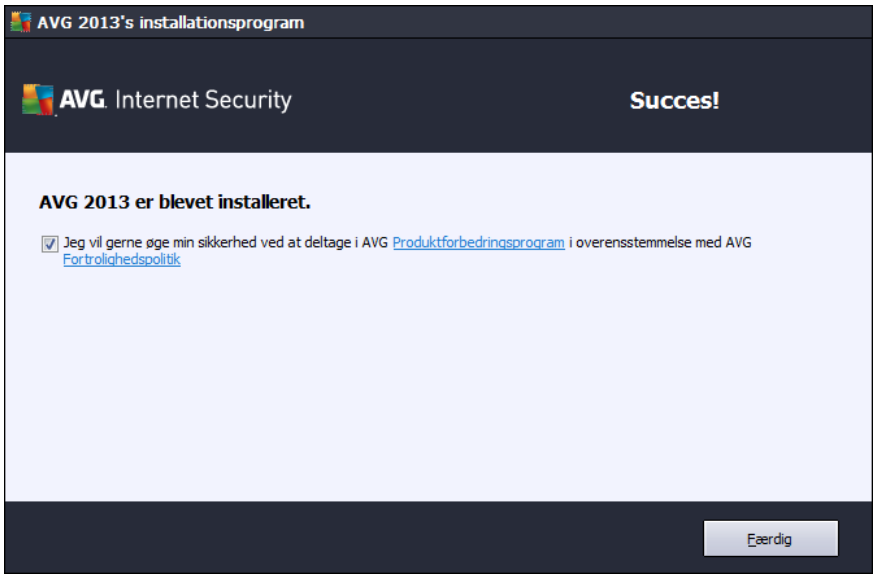
Betjeningsknapper

Der er to kontrolknapper i denne dialogboks:

- ***Minimer*** – installationen kan vare flere minutter. Klik på knappen for at minimere dialogvinduet til et ikon, der er synligt på proceslinjen. Dialogboksen vises igen, når installationen er fuldført.
- ***Annuller*** – denne knap bør kun bruges, hvis du vil afbryde den aktuelle installationsproces. Husk på, at i det tilfælde bliver **AVG Internet Security 2013** ikke installeret.

3.7. Installationen blev fuldført

Dialogen ***Installationen blev fuldført*** bekræfter, at din **AVG Internet Security 2013** er blevet installeret og konfigureret:



AVG Produktforbedringsprogram og AVG Fortrolighedspolitik

Her kan du afgøre, om du vil deltage i ***Produktforbedringsprogrammet*** (*få flere detaljer i kapitlet AVG Avancerede indstillinger / Produktforbedringsprogram*), der indsamler anonyme oplysninger for detekterede trusler for at forbedre det overordnede sikkerhedsniveau på internettet. Alle data behandles fortroligt og i overensstemmelse med AVG Fortrolighedspolitik. Klik på linket ***Fortrolighedspolitik*** for at blive omdirigeret til AVG's websted (http://www.avg.com/), der indeholder den fulde ordlyd af AVG Fortrolighedspolitik. Hvis du accepterer betingelserne, skal du lade denne indstilling være markeret *(indstillingen bekræftes som standard)*.

Genstart af computer

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

4. Efter installationen

4.1. Produktregistrering

Når installationen af **AVG Internet Security 2013** er fuldført, skal du registrere dit produkt online på AVG's websted *(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 Security 2013**. Vælg menupunktet øverste navigationsmenu / Valgmuligheder / Registrer nu. Du vil blive omdirigeret til siden ***Registrering*** på AVG's websted *(http://www.avg.com/)*. Følg instruktionerne 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
- i menuen ***Start/Alle programmer/AVG/AVG 2013***

4.3. Scanning af hele computeren

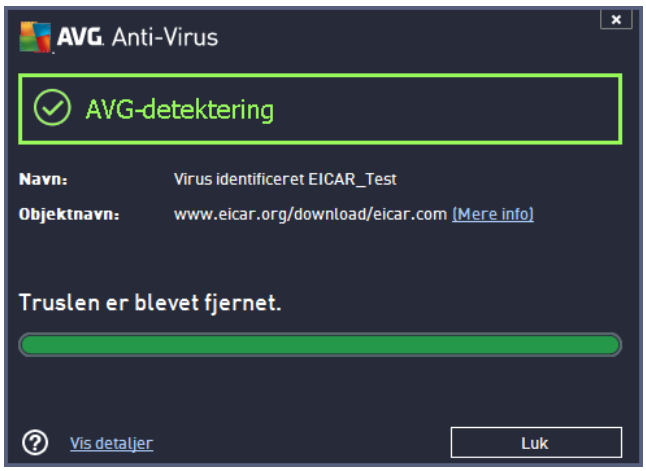
Der er en potentiel risiko for, at en computervirus er blevet overført til din computer inden installationen af **AVG Internet Security 2013**. Derfor bør du køre en Scanning af hele computeren for at sikre, at der ikke er infektioner på din pc. Den første scanning tager måske noget tid *(cirka en time)*, men det anbefales, at du starter den for at sikre dig, at computeren ikke kompromitteres af en trussel. Du kan få instruktioner i Scanning af hele computeren i kapitlet AVG-scanning.

4.4. Eicar-test

For at bekræfte, at **AVG Internet Security 2013** er blevet installeret korrekt, kan du udføre EICAR-testen.

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

Prøv at downloade filen *eicar.com*, og gem den på din lokale disk. Umiddelbart efter at du har bekræftet downloading af testfilen, vil din **AVG Internet Security 2013** reagere med en advarsel. Denne notits demonstrerer, at AVG er korrekt installeret på din computer.



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

4.5. AVG standardkonfiguration

Standardkonfigurationen (*dvs. hvordan applikationen indstilles lige efter installationen*) for **AVG Internet Security 2013** indstilles af softwareleverandøren, så alle komponenter og funktioner er justeret til at give den optimale 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 vil ændre AVG-konfigurationen, så den bedre opfylder dine behov, skal du gå til AVG Avancerede indstillinger: Vælg *elementet Hovedmenu/ Avancerede indstillinger* , og rediger AVG-konfigurationen i den nyligt åbnede dialogboks for AVG Avancerede indstillinger.

5. AVG-brugerflade

AVG Internet Security 2013 åbner med hovedvinduet:

Hovedvinduet er opdelt i flere sektioner:

- ***Øverste navigationsmenu*** består af fire aktive links, der står på en linje i hovedvinduets øvre sektion *(som AVG, Rapporter, Support, Indstillinger).* Detaljer >>
- ***Info om sikkerhedsstatus*** indeholder de grundlæggende oplysninger om den aktuelle status for din **AVG Internet Security 2013**. Detaljer >>
- ***Oversigt over installerede komponenter*** kan findes på en vandret stribe af blokke i hovedvinduets midterste sektion. Komponenterne vises som lysegrønne blokke, der hver har et relevant komponentikon, og kommer med oplysninger om komponentens status. Detaljer >>
- ***My Apps*** afbildes grafisk i nederste del af den midterste stribe i hovedvinduet og giver dig en oversigt over applikationer, der supplerer **AVG Internet Security 2013** , der enten allerede er installeret på din computer eller anbefales at blive det. Detaljer >>
- ***Scan/Opdater lynlinks*** er placeret i nederste linje af blokkene i hovedvinduet. Disse knapper giver direkte adgang til de vigtigste og hyppigst anvendte funktioner i AVG. Detaljer >>

Uden for hovedvinduet for **AVG Internet Security 2013** er der to ekstra kontrolelementer, som du kan bruge til at åbne applikationen:

- ***Systeminformation*** findes nederst i højre side af skærmen *(på proceslinjen)* og angiver den aktuelle status for **AVG Internet Security 2013**. Detaljer >>

- ***AVG gadget*** kan åbnes via Windows sidebar (*understøttes kun i Windows Vista/7/8*) og giver hurtig adgang til scanning og opdatering i **AVG Internet Security 2013**. Detaljer >>

5.1. Øverste navigationsmenu

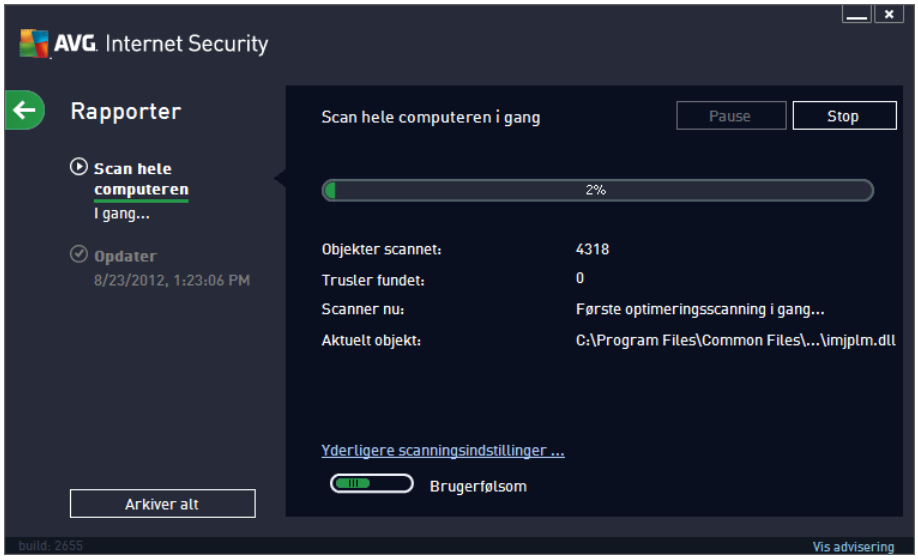
Øverste navigationsmenu består af flere aktive links, der er placeret i den øverste del af hovedvinduet. Navigationen omfatter følgende knapper:

5.1.1. Kan du lide AVG

Klik en enkelt gang på linket for at oprette forbindelse til AVG Facebook-fællesskabet og for at dele AVG's seneste information, nyheder, tips og tricks, der er med til at give den bedst mulige internetsikkerhed.

5.1.2. Rapporter

Åbner en ny dialogboks for ***Rapporter*** med en oversigt over alle relevante rapporter om tidligere kørte scanninger og opdateringsprocesser. Hvis scanningen er i gang i øjeblikket, vises der en roterende cirkel ud for teksten ***Rapporter*** i øverste navigationsmenu for hovedbrugerfladen. Klik på denne cirkel for at åbne den dialogboks, der viser statussen på kørselsprocessen:



5.1.3. Support

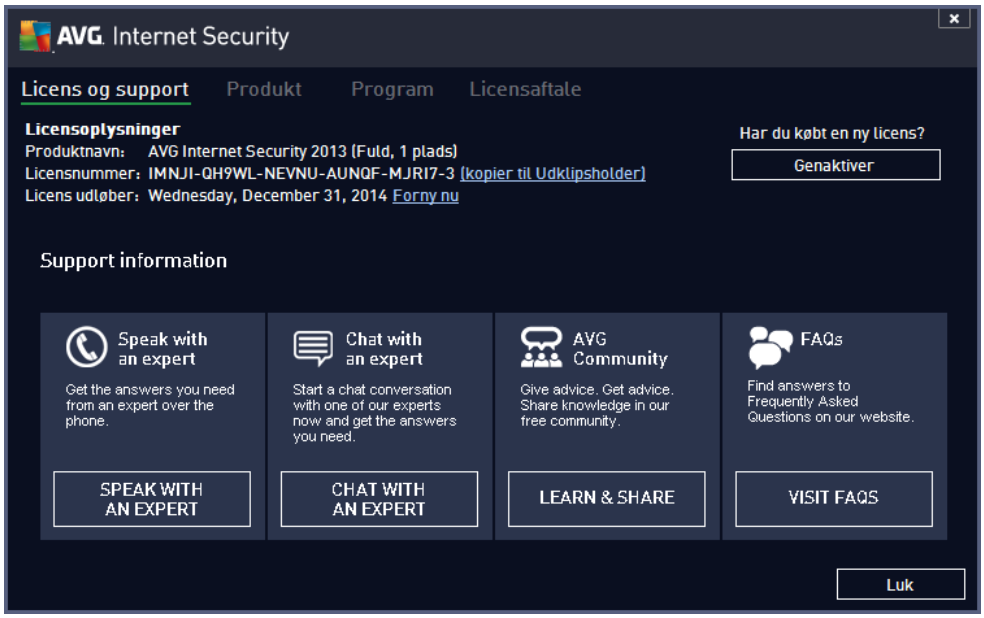
Åbner en ny dialogboks, der indeholder fire faner, hvor du kan finde alle relevante oplysninger om **AVG Internet Security 2013**:

- ***Licens og support*** – denne fane indeholder oplysninger om produktnavnet, licensnummeret og udløbsdatoen. I den nederste del af denne dialogboks finder du også en let overskuelig oversigt over alle de tilgængelige kontakter til kundesupport. Følgende aktive links og knapper er tilgængelige på fanen:
    - *(Gen)aktiver* – klik for at åbne den nye dialogboks ***AVG Activate Software***. Angiv dit licensnummer i det relevant felt for enten at erstatte dit salgsnummer *(som du bruger under AVG Internet Security 2013 installationen)* eller for at ændre dit aktuelle

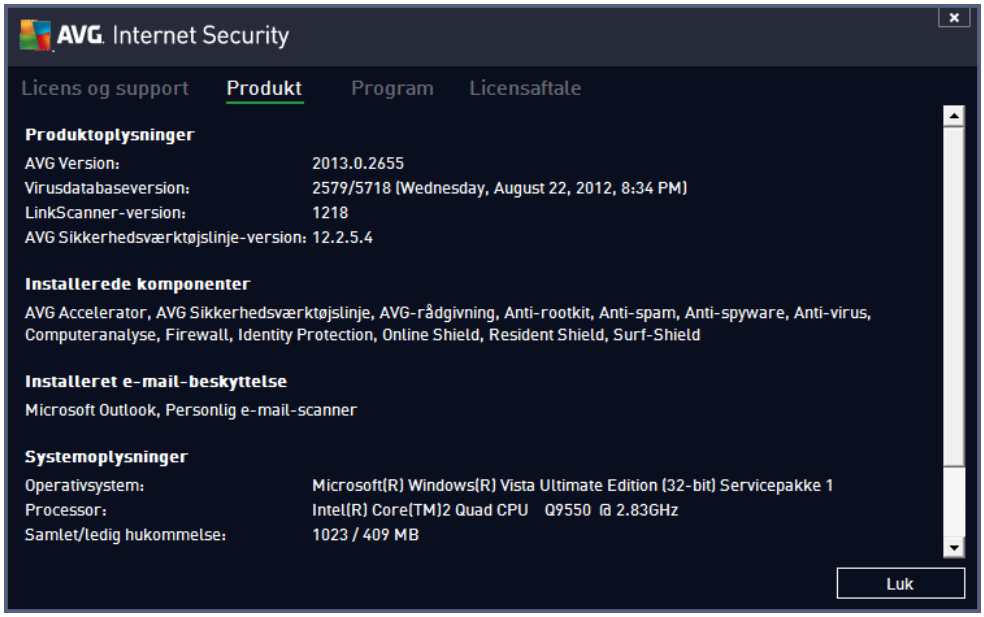
licensnummer til et andet *(f.eks. når du opgraderer til et nyere AVG-produkt)*.

- *Kopier til Udklipsholder* – Brug dette link til at kopiere licensnummeret og indsætte det, hvor det er nødvendigt. På den måde kan du sikre dig, at licensnummeret er angivet korrekt.

- *Forny nu* – vi anbefaler, at du køber din **AVG Internet Security 2013** licensfornyelse i god tid, hvilket vil sige, mindst en måned før udløbet af din aktuelle licens. Du får besked om udløbsdatoen, der nærmer sig. Klik på dette link for at blive omdirigeret til AVG's websted *(http://www.avg.com/)*, hvor du kan finde detaljerede oplysninger om din licensstatus, udløbsdatoen og tilbuddet om fornyelse/opgradering.



- ***Produkt*** – fanen giver et overblik over de **AVG Internet Security 2013** vigtigste tekniske data med hensyn til produktoplysninger, installerede komponenter, installeret e-mail-beskyttelse og systemoplysninger:



- ***Program*** – på denne fane kan du finde oplysninger om versionen af programfilen og den tredjepartskode, der bruges i produktet:

- ***Licensaftale*** – fanen indeholder den fulde ordlyd af licensaftalen mellem dig og AVG Technologies:

5.1.4. Valgmuligheder

Der er adgang til vedligeholdelse af **AVG Internet Security 2013** via elementet ***Indstillinger***. Klik på pilen for at åbne rullemenuen:

- ***Scan computer*** 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...*** – giver dig mulighed for at køre en on-demand-test af en enkelt specifik fil. Klik på denne valgmulighed for at åbne et nyt vindue med diskens træstruktur. Vælg den ønskede fil og bekræft scanningen.
- ***Opdater*** – starter automatisk opdateringsprocessen for **AVG Internet Security 2013**.
- ***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 et netværk uden adgang til internettet, osv.). I det nyåbnede vindue skal du vælge den mappe, hvor du tidligere placerede opdateringsfilen, og starte opdateringsprocessen.
- ***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.
- ***Historik*** – giver flere specifikke muligheder for undermenuen:
  - *Scanningsresultater* – åbner en dialogboks, der indeholder en oversigt over scanningsresultater.

- *Resident Shield-detektering* – åbner en dialogboks med en oversigt over trusler, som Resident Shield har fundet.
- *Detektering af e-mailbeskyttelse* – åbner en dialogboks med en oversigt over vedhæftede filer i e-mailmeddelelser, der detekteres som farlige af komponenten E-mailbeskyttelse.
- *Resident Shield-fund* – åbner en dialogboks med en oversigt over trusler, som Online Shield har fundet.
- *Log med hændelseshistorik* – åbner historikloggrænsefladen med en oversigt over alle loggede **AVG Internet Security 2013** handlinger.
- *Firewall-log* – åbner en dialogboks med en detaljeret oversigt over alle Firewall-handlinger.

- ***Avancerede indstillinger...*** – åbner AVG-dialogboksen for avancerede indstillinger, hvor du kan redigere **AVG Internet Security 2013** konfigurationen. Generelt anbefales det, at du beholder standardindstillingerne for applikationen, der er defineret af softwareleverandøren.
- ***Indstillinger for Firewall...*** – åbner en selvstændig dialogboks for avanceret konfiguration af Firewall-komponenten.
- ***Indhold i hjælp*** – åbner AVG-hjælpefiler.
- ***Få support*** – åbner AVG's websted *(http://www.avg.com/)* på kundesupportcentrets side.
- ***Dit AVG Web*** – åbner AVG's websted *(http://www.avg.com/).*
- ***Om virus og trusler*** – åbner det online virusleksikon, hvor du kan finde detaljerede oplysninger om den identificerede virus.
- ***(Gen)aktivér*** – åbner dialogboksen ***Aktivér AVG*** med de data, du angav under installationsprocessen. I denne dialogboks kan du indtaste dit licensnummer for enten at erstatte salgsnummeret (*som du har installeret AVG med*) eller for at erstatte det gamle licensnummer (*f.eks. ved at opgradere til et nyt AVG-produkt*).
- ***Registrer nu*** – opretter forbindelse til registreringssiden på AVG's websted (http://www.avg.com/). Angiv dine registreringsdata. Det er kun kunder, der registrerer deres AVG-produkt, som kan få gratis teknisk support. Hvis du bruger prøveversionen af **AVG Internet Security 2013**, vises de to sidste elementer som ***Køb nu*** og ***Aktivér***, så du kan købe den fulde version af programmet med det samme. Hvis du har **AVG Internet Security 2013** installeret med et salgsnummer, vises elementerne som ***Registrer*** og ***Aktivér***.
- ***Om AVG*** – åbner en ny dialogboks med fire faner, der indeholder data om din købte licens og tilgængelig support, produkt- og programoplysninger samt den fulde ordlyd af licensaftalen.

5.2. Info om sikkerhedsstatus

Afsnittet ***Info om sikkerhedsstatus*** er placeret i den øverste del af hovedvinduet i **AVG Internet Security 2013**. I denne sektion kan du altid finde oplysninger om den aktuelle sikkerhedsstatus for **AVG Internet Security 2013**. Herunder er en oversigt over ikoner, der kan være afbilledet i denne sektion, og deres betydning:

 - det grønne ikon angiver, at ***AVG Internet Security 2013 er fuldt funktionelt***. Din computer er fuldstændigt beskyttet, opdateret, og alle installerede komponenter arbejder, som de skal.

 - det gule ikon advarer om, at ***en eller flere komponenter ikke er konfigureret korrekt*** , og du skal kontrollere deres egenskaber/indstillinger. Der er ingen kritiske problemer med **AVG Internet Security 2013**, og du har sikkert valgt at slå en komponent fra af en eller anden årsag. Du er stadig beskyttet! Vær dog opmærksom på indstillingerne i den pågældende komponent! Den komponent, der er konfigureret forkert, vises med et orange advarselsbånd i hovedbrugergrænsefladen.

Det gule ikon vises, hvis du af en eller anden årsag har besluttet dig for at ignorere en komponents fejlstatus. Indstillingen ***Ignorér fejlstatus*** er tilgængelig i grenen Avancerede indstillinger/Ignorér fejlstatus. Der har du mulighed for at angive, at du er klar over komponentens fejltilstand, men at du af en eller anden årsag ønsker at bevare **AVG Internet Security 2013** på denne måde, og at du ikke ønsker at få en advarsel om det. Det kan være nødvendigt at bruge denne indstilling i en bestemt situation, men det anbefales på det kraftigste, at du skifter indstillingen ***Ignorér fejlstatus*** så hurtigt som muligt!

Der kan også blive vist et gult ikon, hvis dit **AVG Internet Security 2013** kræver, at computeren genstartes (***Der skal genstartes***). Vær opmærksom på denne advarsel, og genstart computeren.

 - det orange ikon angiver, at ***AVG Internet Security 2013 har en kritisk status***! En eller flere komponenter fungerer ikke korrekt, og **AVG Internet Security 2013** 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 Security 2013 ikke er indstillet til den optimale ydelse, vises knappen Klik for at reparere (du kan også klikke på Klik for at reparere alle, hvis problemet omhandler mere end én komponent) ud for oplysningerne om sikkerhedsstatussen. Tryk på knappen for at starte en automatisk proces med at kontrollere og konfigurere programmet. Dette er en nem måde at indstille AVG Internet Security 2013 på, så du opnår den bedst mulige ydelse og får det maksimale sikkerhedsniveau!

Det anbefales på det kraftigste, at du er opmærksom på ***Info om sikkerhedsstatus***, og hvis rapporten angiver problemer, skal du straks gå videre og løse problemet. Ellers er din computer i fare!

Bemærk: *AVG Internet Security 2013-statusoplysninger kan også når som helst fås fra ikonet på proceslinjen.*

5.3. Komponentoversigt

Oversigt over installerede komponenter kan findes i en vandret række af blokke i midterste del af hovedvinduet. Komponenterne vises som grønne blokke, der har det relevante komponentikon. Hver blok indeholder oplysninger om den aktuelle beskyttelsesstatus. Hvis komponenten er korrekt konfigureret og fuldt funktionsdygtig, vises oplysningerne i grønne bogstaver. Hvis komponenten stoppes, begrænses dens funktionalitet, eller komponenten er i en fejltilstand, bliver du informeret af en advarselstekst, der vises i et orange tekstfelt. ***Det anbefales på det kraftigste, at du er opmærksom på den relevante komponents indstillinger.***

Flyt musen over komponenten for at få vist en kort tekst nederst i hovedvinduet. Teksten indeholder en elementær introduktion til komponentens funktionalitet. Den angiver også komponentens aktuelle status og specificerer, hvilke af komponentens tjenester der ikke er konfigureret korrekt.

Liste over installerede komponenter

I **AVG Internet Security 2013** indeholder sektionen ***Komponentoversigt*** oplysninger om følgende komponenter:

- ***Computer*** – denne komponent dækker to tjenester: ***Anti-Virus Shield*** detekterer vira, spyware, orme, trojanske heste, uønskede eksekverbare filer eller biblioteker i dit system og beskytter dig imod ondsindet adware, og ***Anti-Rootkit*** scanner for farlige rootkits, der er skjulte i applikationer, drivere eller biblioteker. Detaljer >>
- ***Webbrowsing*** – beskytter dig mod webbaserede angreb, mens du søger og surfer på internettet. Detaljer >>
- ***Identitet*** –komponenten kører tjenesten ***Identity Shield***, der konstant beskytter dine digitale aktiver mod nye og ukendte trusler på internettet . Detaljer >>
- ***E-mails*** – kontrollerer dine indgående e-mailmeddelelser for SPAM og blokerer vira, phising-angreb eller andre trusler. Detaljer >>
- ***Firewall*** – styrer al kommunikation i hver netværksport, hvilket beskytter dig mod ondsindede angreb og blokerer alle indtrængningsforsøg. Detaljer >>

Tilgængelige handlinger

- ***Hold musen over et komponentikon*** for at fremhæve det i komponentoversigten. Samtidig vises komponentens grundlæggende funktioner i nederste del af brugergrænsefladen.
- ***Klik en enkelt gang på komponentens ikon*** for at åbne komponentens egen grænseflade med oplysninger om komponentens aktuelle status, og få adgang til dens konfiguration og statistikdata.

5.4. My Apps

I området for ***My Apps*** *(rækken af grønne blokke under komponentens sæt)* er der en oversigt over yderligere AVG-applikationer, der enten allerede er installeret på din computer, eller som det anbefales at installere. Blokkene vises betingelsesvis og kan repræsentere en eller flere af følgende applikationer:

- ***Mobilbeskyttelse*** er en applikation, der beskytter din mobiltelefon mod vira og malware. Den giver dig også mulighed for at spore din smartphone fra et eksternt sted i tilfælde af, du taber den e.l.

- ***LiveKive*** er dedikeret til onlinesikkerhedskopiering af data på sikre servere. LiveKive sikkerhedskopierer automatisk alle dine filer, fotos og musik til 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.

- ***Family Safety*** hjælper dig med at beskytte dine børn mod upassende websteder, medieindhold og online søgninger, og viser dig rapporter om deres online aktivitet. AVG Family Safety anvender logningsteknologi for at overvåge dit barns aktiviteter i chatrum og på sider med sociale netværk. Hvis den opfanger ord, sætninger eller sprogbrug, som typisk bruges til at komme i kontakt med børn online, underrettes du straks herom via sms eller e-mail. Du kan indstille det passende beskyttelsesniveau for hvert barn og overvåge dem særskilt via unikke logins.

- ***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.

- ***MulitMi*** samler alle dine e-mailkonti og sociale konti et sikkert sted, så det er nemmere at få kontakt med familie og venner, søge på internettet, dele fotos, videoer og filer. MultiMi indeholder tjenesten LinkScanner, der beskytter dig mod det stigende antal trusler på internettet ved at analysere websiderne bag alle links på enhver webside, du besøger, og sørger for, at siderne er sikre.

- ***AVG Toolbar*** er tilgængelig direkte i din internetbrowser og sørger for, du har maksimal sikkerhed, når du søger på internettet.

Få flere oplysninger om ***My Apps***-applikationer ved at klikke på den respektive blok. Du bliver omdirigeret til dendedikerede AVG-webside, hvor du også med det samme kan downloade komponenten.

5.5. Scan/opdater lynlinks

Lynklinks er placeret i venstre side af grænsefladen i **AVG Internet Security 2013**. 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:

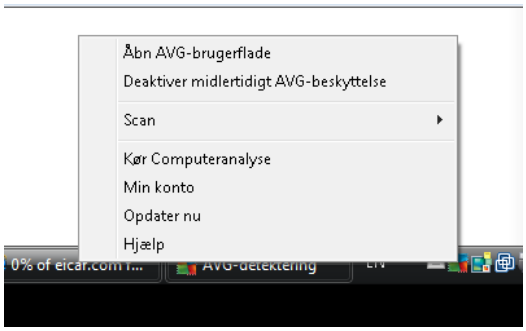
- ***Scan nu*** – knappen er grafisk opdelt i to sektioner. Følg linket ***Scan nu*** for at igangsætte Scan hele computeren med det samme og se dens forløb og resultater i det automatisk oprettede vindue Rapporter. Knappen ***Indstillinger*** åbner dialogboksen ***Scanningsindstillinger***, hvor du kan administrere planlagte scanninger og redigere parametre for Scan hele computeren/Scanning af specifikke filer eller mapper. *(Du kan få*

flere oplysninger i kapitlet AVG-scanning)

- ***Opdater nu*** – tryk på knappen for at starte produktopdateringen med det samme. Du kan følge opdateringens forløb og resultater i det automatisk oprettede vindue ***Rapporter***. *(Du kan få flere oplysninger i kapitlet AVG-opdateringer)*

5.6. Proceslinjeikon

AVG-proceslinjeikonet *(på proceslinjen i Windows, i nederste højre hjørne af skærmen)* angiver den aktuelle status på dit **AVG Internet Security 2013**. Det er altid synlig på din proceslinje, uanset om brugergrænserfladen til dit **AVG Internet Security 2013** er åbnet eller lukket:



Visning af AVG-systembakkeikon

- Hvis ikonet er i fuld farve og uden ekstra elementer, angiver det, at alle **AVG Internet Security 2013**-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. *(Når du har bekræftet indstillingen til ignorering af komponentstatussen, viser du, at du er klar over komponentens fejlstatus, men at du af en eller anden årsag ønsker at bevare indstillingen, og at du 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 sådanne advarsler, og forsøg at fjerne konfigurationsproblemet for en komponent, der ikke er konfigureret korrekt. For at kunne udføre ændringerne i komponentens konfiguration skal du dobbeltklikke på proceslinjeikonet for at åbne programmets 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, at en **AVG Internet Security 2013** scanning er i gang.

Oplysninger om AVG-systembakkeikonet

AVG-proceslinjeikonet oplyser også om aktuelle aktiviteter i dit **AVG Internet Security 2013** og om mulige statusændringer i programmet (*f.eks. automatisk start af en planlagt scanning eller opdatering, skift af Firewall-profil, ændring af status for en komponent, forekomst af fejlstatus, ...*) via et pop op-vindue, der åbnes via proceslinjeikonet:

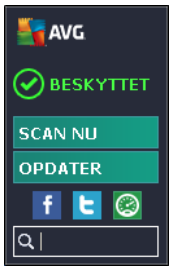
Handlinger, der er tilgængelige fra AVG-systembakkeikonet

AVG-proceslinjeikon kan også bruges som et hurtigt link til at få adgang til brugergrænsefladen i **AVG Internet Security 2013**. Bare dobbeltklik på ikonet. Ved at højreklikke på ikonet åbner du en kort kontekstmenu med følgende indstillinger:

- ***Åbn AVG-brugergrænseflade*** – klik for at åbne brugergrænsefladen i **AVG Internet Security 2013**.
- ***Deaktivér midlertidigt AVG-beskyttelse*** – denne indstilling gør det muligt at slå hele beskyttelsen, der leveres af dit **AVG Internet Security 2013**, på én gang. Husk, at du kun skal vælge denne mulighed, når det er absolut nødvendigt! I de fleste tilfælde er det ikke nødvendigt at deaktivere **AVG Internet Security 2013**, 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 er midlertidigt nødt til at deaktivere **AVG Internet Security 2013**, 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..
- ***Scan*** – klik for at åbne kontekstmenuen til prædefinerede scanninger (*Scan hele computeren* og *Scan specifikke filer eller mapper*), og vælg den ønskede scanning. Den startes med det samme.
- ***Scanning kører ...*** – det element vises kun, hvis der er en scanning i gang på computeren. For denne scanning kan du indstille prioriteten, eller stoppe eller afbryde den igangværende scanning. Der er også adgang til følgende handlinger: *Angiv prioritet for alle scanninger, Afbryd alle scanninger midlertidigt* eller *Stop alle scanninger*.
- ***Kør computeranalyse*** - klik for at starte Computeranalyse-komponenten.
- ***Min konto*** – åbner startsiden for min konto, hvor du kan administrere dine abonnementsprodukter, købe ekstra beskyttelse, hente installationsfiler, kontrollere dine tidligere ordrer og fakturaer og administrere dine personlige oplysninger.
- ***Opdater nu*** – kører en omgående opdatering.
- ***Hjælp*** – åbner hjælpefilen på startsiden.

5.7. AVG-gadget

AVG gadget vises på Windows skrivebordet (*Windows Sidebar*). Denne applikation understøttes kun i operativsystemerne Windows Vista og Windows 7/8. ***AVG gadget*** giver direkte adgang til den vigtigste funktion i **AVG Internet Security 2013** , dvs. scanning og opdatering**:**

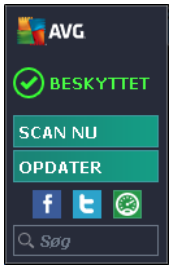


AVG gadgetkontroller

Hvis det er nødvendigt, giver AVG gadget dig mulighed for at køre en scanning eller opdatering med det samme. Den indeholder også et lynlink, der forbinder dig til store sociale netværk og giver dig hurtige søgninger:

- ***Scan nu*** - klik på linket ***Scan nu*** for at starte scanning af hele computeren direkte. Du kan følge scanningsprocessen i den alternative brugergrænseflade for gadgetten. En kort statistisk oversigt viser oplysninger om antallet af scannede objekter, detekterede trusler og helbredte trusler. Under scanningen kan du altid pause eller stoppe 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 Security 2013** opdateringen direkte i gadgeten:



- ***Twitter-link*** – åbner en ny grænseflade til ***AVG gadget***, der viser en oversigt over de seneste AVG-feeds, som er blevet sendt til Twitter. Følg linket ***Vis alle AVG Twitter-feeds*** for at åbne din internetbrowser i et nyt vindue, så viderestilles du direkte til Twitters websted, nærmere betegnet den side, der er dedikeret til AVG-nyheder.

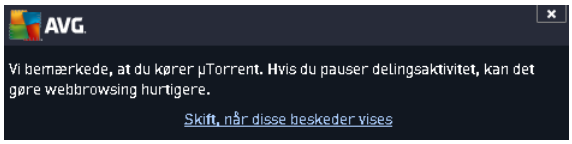
- ***Facebook-link*** – åbner din internetbrowser på Facebook-webstedet, dvs. på siden for ***AVG-fællesskabet***.

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

5.8. AVG Advisor

AVG Advisor er udviklet til at detektere problemer, der kan gøre din computer langsommere eller udsætte den for risici, og til at foreslå en handling, der kan løse problemet. Hvis din computer pludselig bliver langsommere *(internetbrowsing, samlede ydelse)*, er det ikke altid åbenlyst, hvad problemet er, og dernæst hvordan det løses. Det er her, ***AVG Advisor*** kommer ind i billedet: Den viser en meddelelse på proceslinjen, der gør dig opmærksom på, hvad problemet kunne være, og hvordan det kan løses. ***AVG Advisor*** overvåger hele tiden dine kørende processer på din PC og søger efter mulige problemer og giver dig tip til, hvordan problemet kan undgås.

AVG Advisor er synlig i form af et glidende pop op-vindue over systembakken:



Helt konkret overvåger ***AVG Advisor*** følgende:

- ***Status for den aktuelle webbrowser***. Webbrowsere kan overbelaste hukommelsen, især hvis flere faner eller vinduer har været åbne i længere tid og bruger for mange systemressourcer, hvilket nedsætter computerens hastighed. Det hjælper som regel at genstarte webbrowseren i disse tilfælde.

- ***Kørende peer to peer-forbindelser***. Når du har brugt P2P-protokollen til deling af filer, kan forbindelsen sommetider forblive aktiv og bruge en vis del af båndbredden. På den måde kan du se, at webbrowsing bliver langsommere.

- ***Ukendt netværk med et bekendt navn***. Dette gælder oftest kun for brugere, der opretter forbindelse til forskellige netværk, typisk via bærbare: Hvis et nyt ukendt netværk har samme navn som et velkendt og hyppigt anvendt netværk *(f.eks. Hjemme eller MitWifi)*, kan det skabe forvirring, og du kan ved en fejl komme til at oprette forbindelse til et fuldstændigt ukendt og potentielt usikkert netværk. ***AVG Advisor*** kan forhindre dette ved at advare dig om, at det kendte navn faktisk repræsenterer et nyt netværk. Hvis du afgør, at det ukendte netværk er sikkert, kan du selvfølgelig gemme det på en liste i ***AVG Advisor*** over kendte netværk, så det ikke rapporteres igen i fremtiden.

I hver af disse situationer advarer ***AVG Advisor*** dig om potentielle problemer og angiver navnene og ikonerne for de modstridende processer eller applikationer. ***AVG Advisor*** kommer også med forslag til, hvad du kan gøre for at undgå eventuelle problemer.

Understøttede webbrowsere

Funktionen virker med følgende webbrowsere: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.9. AVG Accelerator

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.

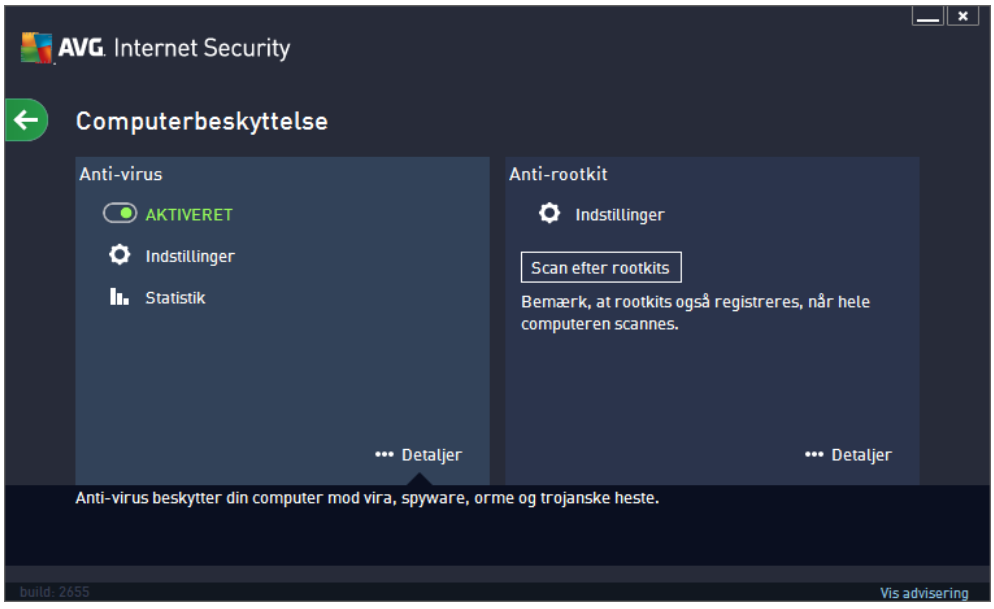
6. AVG Komponenter

6.1. Computer

Computerkomponenten dækker to hovedsikkerhedstjenester: ***Anti-Virus*** og ***Anti-Rootkit***:

- ***Anti-Virus*** består af en scanningsmaskine, der beskytter alle filer, computerens systemområder og flytbare medier *(flashdrev osv.)* og scanner for kendte vira. Alle detekterede vira blokeres fra at foretage en handling og renses eller sættes i karantæne i Virus Vault bagefter. Du bemærker ikke engang processen, da denne såkaldte indbyggede beskyttelse kører "i baggrunden". Anti-Virus anvender også heuristisk scanning, hvor alle filer scannes for typiske viruskarakteristika. Det betyder, at Anti-Virus kan detektere en ny, ukendt virus, hvis den nye virus indeholder nogle typiske karakteristika for eksisterende vira. **AVG Internet Security 2013** kan også analysere og detektere eksekverbare applikationer og DLL-biblioteker, der er potentielt uønskede i systemet *(forskellige slags spyware, adware osv.)*. Yderligere scanner Anti-Virus din systemregistreringsdatabase for mistænkeligt indhold, midlertidige internet-filer og sporingscookies og gør det muligt for dig at behandle alle potentielt skadelige elementer på samme måde som enhver anden infektion.

- ***Anti-rootkit*** er et specialiseret værktøj, der detekterer og effektivt fjerner farlige rootkits, dvs. programmer og teknologier, der kan camouflere tilstedeværelsen af skadelig software på computeren. Et rootkit er udviklet til at tage kontrollen over et computersystem uden autorisation fra systemets ejere og legitime administratorer. Anti-rootkit kan detektere rootkits baseret på et foruddefineret sæt af regler. Hvis Anti-Rootkit finder et rootkit, betyder det ikke nødvendig, at rootkit'et er inficeret. Nogle gange bruges rootkits som drivere, eller de er en del af rigtige applikationer.



Kontrolelementer i dialogboks

Du kan skifte mellem begge sektioner i dialogboksen ved blot at klikke et tilfældigt sted i det relevante tjenestepanel. Derefter fremhæves panelet i en lysere blå farve. I dialogboksens sektioner kan du finde følgende kontrolelementer. Deres funktionalitet er den samme, uanset om de tilhører en sikkerhedstjeneste eller en anden tjeneste *(Anti-Virus eller Anti-Rootkit)*:

 ***Aktiveret / deaktiveret*** – knappen kan minde om et trafiklys i både udseende og funktionalitet. Klik en enkelt gang for at skifte mellem to positioner. Den grønne farve står for ***Aktiveret***, hvilket betyder, at sikkerhedstjenesten Anti-Virus er aktiveret og fuldt funktionsdygtig. Den røde farve angiver, at tjenesten er ***Deaktiveret***. Hvis du ikke har en god grund til at deaktivere tjenesten, anbefaler vi på det kraftigste, at du beholder standardindstillinger for hele sikkerhedskonfigurationen. Standardindstillingerne garanterer maksimal sikkerhed, og at applikationen yder sit maksimale. Hvis du af en eller anden årsag vil deaktivere tjenesten, vil du med det samme blive advaret om den mulige risiko af det røde ***advarselstegn*** og få besked om, at du i øjeblikket ikke er fuldt beskyttet. ***Bemærk dog, at du bør aktivere tjenesten igen så snart som muligt.***

 ***Indstillinger*** – klik på knappen for at blive omdirigeret til grænsefladen for avancerede indstillinger. Helt nøjagtigt åbnes den relevante dialogboks, og du kan konfigurere den valgte tjeneste, dvs. Anti-Virus eller Anti-Rootkit. I grænsefladen for avancerede indstillinger kan du redigere hele konfigurationen for hver sikkerhedstjeneste i **AVG Internet Security 2013,** men enhver konfiguration kan indstilles til kun at anbefales til erfarne brugere.

 ***Statistik*** – klik på knappen for at blive omdirigeret til den dedikerede side på AVG-webstedet (http://www.avg.com/). På denne side finder du en detaljeret statistisk oversigt over alle **AVG Internet Security 2013**-aktiviteter, der blev udført på din computer inden for en bestemt tidsperiode og samlet set.

 ***Detaljer*** – klik på knappen, så vises der en kort beskrivelse af den markerede tjeneste nederst i dialogboksen.

 – Brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til hovedbrugerfladen med oversigten over komponenterne.

I sektionen Anti-Rootkit finder du også en specifik knap til ***Scan efter rootkits*** , som du kan bruge til at starte det uafhængige rootkit direkte *(dog er rootkitscanningen en implicit del af Scan hele computeren)*.

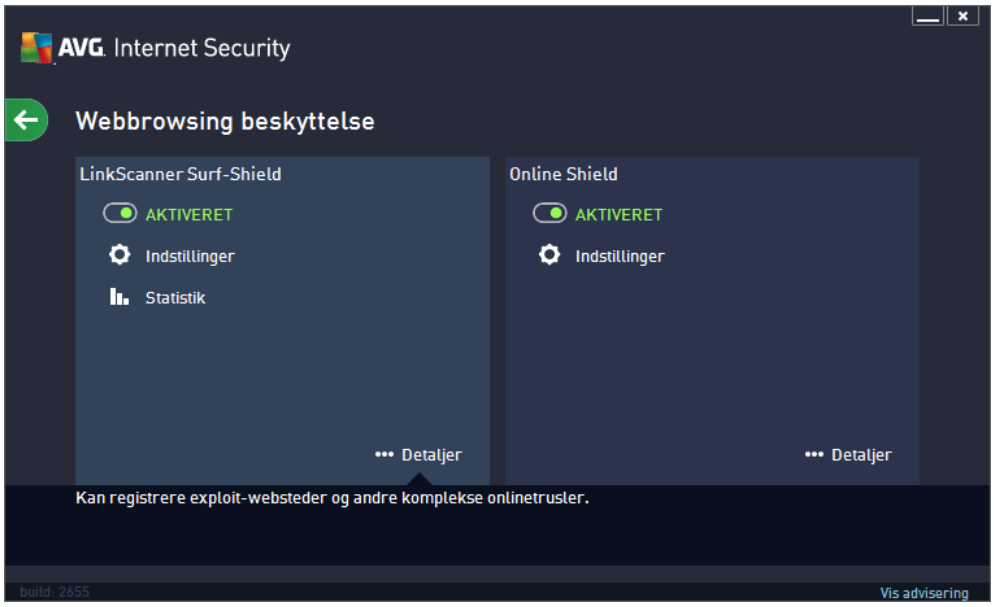
6.2. Webbrowsing

Beskyttelsen med ***Webbrowsing*** består af to tjenester: ***LinkScanner Surf-Shield*** og ***Online Shield***:

- ***LinkScanner Surf-Shield*** beskytter dig imod det stigende antal kortvarige 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 Surf-Shield er ikke beregnet til beskyttelse af serverplatforme!***

- ***Online Shield*** er en form for indbygget realtidsbeskyttelse. Det scanner indholdet på

besøgte websider (og evt. filer på dem), før de vises i din webbrowser eller downloades til din computer. Online Shield detekterer om siden, du vil besøge, indeholder farligt javascript, og forhindrer at siden vises. Det genkender også malware på en side, og stopper øjeblikkeligt download af den, så det aldrig når frem til din computer. Denne effektive beskyttelse blokerer skadeligt indhold på websider, du forsøger at åbne, og forhindrer at det overføres 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, at udnyttede websider kan inficere din computer, ved at du blot er inde på det ramte websted. ***Online Shield er ikke beregnet til beskyttelse af serverplatforme!***



Kontrolelementer i dialogboks

Du kan skifte mellem begge sektioner i dialogboksen ved blot at klikke et tilfældigt sted i det relevante tjenestepanel. Derefter fremhæves panelet i en lysere blå farve. I dialogboksens sektioner kan du finde følgende kontrolelementer. Deres funktionalitet er den samme, uanset om de hører til den ene sikkerhedstjeneste eller den anden *(LinkScanner Surf-Shield eller Online Shield)*:

Aktiveret/deaktiveret – knappen kan minde om et trafiklys i både udseende og funktionalitet. Klik en enkelt gang for at skifte mellem to positioner. Den grønne farve står for ***Aktiveret***, hvilket betyder, at LinkScanner Surf-Shield-/Online Shield-sikkerhedstjenesten er aktiv og fuldt funktionsdygtig. Den røde farve angiver, at tjenesten er ***Deaktiveret***. Hvis du ikke har en god grund til at deaktivere tjenesten, anbefaler vi på det kraftigste, at du beholder standardindstillingerne for hele sikkerhedskonfigurationen. Standardindstillingerne garanterer maksimal sikkerhed, og at applikationen yder sit maksimale. Hvis du af en eller anden årsag vil deaktivere tjenesten, vil du med det samme blive advaret om den mulige risiko af det røde ***advarselstegn*** og få besked om, at du i øjeblikket ikke er fuldt beskyttet. ***Bemærk dog, at du bør aktivere tjenesten igen så snart som muligt.***

Indstillinger – klik på knappen for at blive omdirigeret til grænsefladen for avancerede indstillinger. Den relevante dialogboks åbnes, og du kan konfigurere den valgte tjeneste, dvs.

LinkScanner Surf-Shield eller Online Shield. I grænsefladen for avancerede indstillinger kan du redigere hele konfigurationen for hver sikkerhedstjeneste i **AVG Internet Security 2013,** men enhver konfiguration kan indstilles til kun at anbefales til erfarne brugere.

Statistik – klik på knappen for at blive omdirigeret til den dedikerede side på AVG-webstedet (http://www.avg.com/). På denne side finder du en detaljeret statistisk oversigt over alle **AVG Internet Security 2013**-aktiviteter, der blev udført på din computer inden for en bestemt tidsperiode og samlet set.

Detaljer – klik på knappen, så vises der en kort beskrivelse af den markerede tjeneste nederst i dialogboksen.

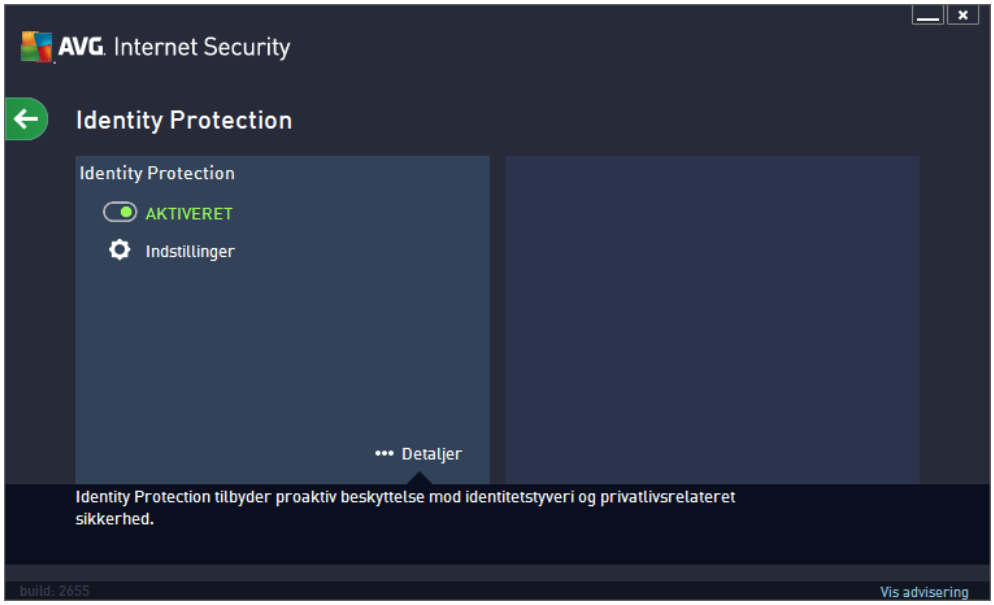
– Brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til hovedbrugerfladen med oversigten over komponenterne.

6.3. Identitet

Komponenten ***Identitetsbeskyttelse*** består af to tjenester: ***Identitetsbeskyttelse*** og ***Identity Alert***:

- ***Identitetsbeskyttelse*** er en tjeneste mod malware, der beskytter dig mod al slags malware (*spyware, bots, identitetstyveri, ...*) ved hjælp af adfærdsteknologi og yder beskyttelse mod nye vira fra dag nul. Identitetsbeskyttelse fokuserer på at forhindre indentitetstyve i at sjæle dine adgangskoder, bankkontooplysninger, kreditkortnumre og andre personlige digitale værdier fra alle former for ondsindet software *(malware)*, der retter sig mod din pc. Der sørges for, at alle programmer, som kører på din computer eller på dit delte netværk, 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 filen bestemmes som værende ondsindet, fjerner Identitetsbeskyttelse koden og flytter den til Virus Vault og gendanner alle ændringer, der er foretaget i systemet *(kodeindsættelser, ændringer i registreringsdatabasen, åbning af porte osv.)*. Du behøver ikke starte en scanning for at være beskyttet. Teknologien er meget proaktiv, kræver sjældent opdatering og er altid på vagt.

- ***Identity Alert*** giver adgang til en webbaseret tjeneste, der er designet til diskret at overvåge dine personlige oplysninger online. Oplysningerne kan omfatte følgende: kreditkortnummer, e-mailadresse, telefon-/*mobil*nummer osv. Overvågningen sker regelmæssigt ved at bekræfte, at disse oplysninger ikke har været udsat for potentielt misbrug. Når servicen detekterer noget mistænkeligt, vil du blive informeret via e-mail. Vær opmærksom på, at idet denne service er webbaseret og kun kører online, skal du være tilsluttet internettet for at kunne få adgang til Identity Alert.



Kontrolelementer i dialogboks

Du kan skifte mellem begge sektioner i dialogboksen ved blot at klikke et tilfældigt sted i det relevante tjenestepanel. Derefter fremhæves panelet i en lysere blå farve. I dialogboksens sektioner kan du finde følgende kontrolelementer. Deres funktionalitet er den samme, uanset om de tilhører en sikkerhedstjeneste eller en anden *(Identitetsbeskyttelse eller Identity Alert)*:

Aktiveret/deaktiveret – knappen kan minde om et trafiklys i både udseende og funktionalitet. Klik en enkelt gang for at skifte mellem to positioner. Den grønne farve står for ***Aktiveret***, hvilket betyder, at sikkerhedstjenesten Identitetsbeskyttelse er aktiv og fuldt funktionsdygtig. Den røde farve angiver, at tjenesten er ***Deaktiveret***. Hvis du ikke har en god grund til at deaktivere tjenesten, anbefaler vi på det kraftigste, at du beholder standardindstillingerne for hele sikkerhedskonfigurationen. Standardindstillingerne garanterer maksimal sikkerhed, og at applikationen yder sit maksimale. Hvis du af en eller anden årsag vil deaktivere tjenesten, vil du med det samme blive advaret om den mulige risiko af det røde ***advarselstegn*** og få besked om, at du i øjeblikket ikke er fuldt beskyttet. ***Bemærk dog, at du bør aktivere tjenesten igen så snart som muligt.***

Indstillinger – klik på knappen for at blive omdirigeret til grænsefladen for avancerede indstillinger. Helt nøjagtigt åbnes den respektive dialogboks, og du kan konfigurere den valgte tjeneste, f.eks. Identitetsbeskyttelse. I grænsefladen for avancerede indstillinger kan du redigere hele konfigurationen for hver sikkerhedstjeneste i **AVG Internet Security 2013,** men enhver konfiguration kan indstilles til kun at anbefales til erfarne brugere.

Detaljer – klik på knappen, så vises der en kort beskrivelse af den markerede tjeneste nederst i dialogboksen.

– Brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til hovedbrugerfladen med oversigten over komponenterne.

I sektionen Identity Alert kan du finde en anden knap: ***Vis og opsæt min Identity Alert-konto***. Brug

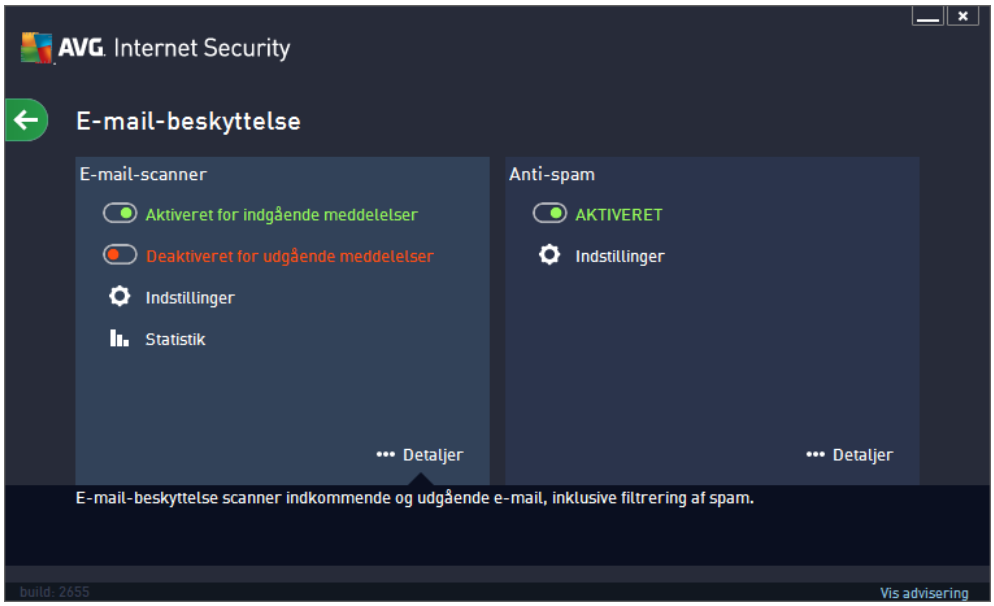
denne knap til at blive omdirigeret til websiden, der er dedikeret til Identity Alert, hvor du skal aktivere tjenesten.

6.4. E-mails

Komponenten ***E-mailbeskyttelse*** dækker følgende to sikkerhedstjenester: ***E-mail-scanner*** og ***Anti-Spam***:

- ***E-mail-scanner***: En af de mest udbredte kilder til vira og trojanske heste er via e-mail. Phishing og spam gør e-mail til en endnu større risikokilde. Gratis e-mailkonti er mere tilbøjelige til at modtage sådanne ondsindede e-mails *(da de sjældent gør brug af anti-spam-teknologi)*, og hjemmebrugere benytter sig i høj grad af disse e-mails. Hjemmebrugere, der surfer på ukendte websteder og udfylder onlineformularer med personlige oplysninger *(som f.eks. deres e-mailadresse)*, 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-mailbeskyttelse er ansvarlig for scanning af alle e-mailmeddelelser, der sendes eller modtages. Når en virus detekteres i en e-mail, flyttes den straks til Virus Vault. Komponenten kan også frasortere visse typer vedhæftede filer i e-mails, og tilføje en certificeringstekst til infektionsfrie beskeder. ***E-mailscanneren er ikke beregnet til serverplatforme!***

- ***Anti-Spam*** kontrollerer alle indkommende e-mailmeddelelser og markerer uønskede e-mails som spam *(Spam er uopfordret e-mail, for det meste annoncering af et produkt eller en service, der masseudsendes til et enormt antal e-mailadresser ad gangen, og fylder modtagernes indbakker op. Spam er ikke legitim, kommerciel e-mail, som forbrugeren har givet tilladelse til.)*. Anti-Spam kan modificere emnet i en e-mail *(der er blevet identificeret som spam)* ved at tilføje en speciel tekststreng. Så kan du nemmere filtrere dine e-mails i e-mail-klienten. Anti-Spam-komponenten anvender flere analysemetoder til at behandle hver e-mailmeddelelse, hvilket giver den bedst mulige beskyttelse mod uønskede e-mailmeddelelser. anti-spam bruger en regelmæssigt opdateret database til detektering af spam. Det er også muligt at bruge RBL-servere *(offentlige databaser for e-mailadresser til "kendte spammere")* og manuelt føje e-mailadresser til din Hvidliste *(markér aldrig som spam)* og Sortliste *(markér altid som spam)*.



Kontrolelementer til dialogboks

Du kan skifte mellem begge sektioner i dialogboksen ved blot at klikke et tilfældigt sted i det relevante tjenestepanel. Derefter fremhæves panelet i en lysere blå farve. I dialogboksens sektioner kan du finde følgende kontrolelementer. Deres funktionalitet er den samme, uanset om de tilhører en sikkerhedstjeneste eller en anden tjeneste *(E-mail-scanner eller Anti-Spam)*:

 ***Aktiveret/deaktiveret*** – knappen kan minde om et trafiklys i både udseende og funktionalitet. Klik en enkelt gang for at skifte mellem to positioner. Den grønne farve står for ***Aktiveret***, hvilket betyder, at sikkerhedstjenesten er aktiveret og fuldt funktionsdygtig. Den røde farve angiver, at tjenesten er ***Deaktiveret***. Hvis du ikke har en god grund til at deaktivere tjenesten, anbefaler vi på det kraftigste, at du beholder standardindstillingerne for hele sikkerhedskonfigurationen. Standardindstillingerne garanterer maksimal sikkerhed, og at applikationen yder sit maksimale. Hvis du af en eller anden årsag vil deaktivere tjenesten, vil du med det samme blive advaret om den mulige risiko af det røde ***advarselstegn*** og få besked om, at du i øjeblikket ikke er fuldt beskyttet. ***Bemærk dog, at du bør aktivere tjenesten igen så snart som muligt.***

I sektionen E-mail-scanner kan du se to "trafiklys"-knapper. På denne måde kan du angive separat, om E-mail-scanner skal kontrollere indgående, udgående eller alle meddelelser. Som standard er scanning af indgående meddelelser slået til, mens scanning af udgående mail er slået fra, hvor risikoen for infektioner er ganske lille.

 ***Indstillinger*** – klik på knappen for at blive omdirigeret til grænsefladen for avancerede indstillinger. Helt nøjagtigt åbnes den relevante dialogboks, og du kan konfigurere den valgte tjeneste, dvs. E-mail-scanner eller Anti-Spam. I grænsefladen for avancerede indstillinger kan du redigere hele konfigurationen for hver sikkerhedstjeneste i **AVG Internet Security 2013,** men enhver konfiguration kan indstilles til kun at anbefales til erfarne brugere.

 ***Statistik*** – klik på knappen for at blive omdirigeret til den dedikerede side på AVG-webstedet (http://www.avg.com/). På denne side finder du en detaljeret statistisk oversigt over alle **AVG Internet Security 2013**-aktiviteter, der blev udført på din computer inden for en bestemt tidsperiode og samlet set.

 ***Detaljer*** – klik på knappen, så vises der en kort beskrivelse af den markerede tjeneste nederst i dialogboksen.

 – Brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til hovedbrugerfladen med oversigten over komponenterne.

6.5. Firewall

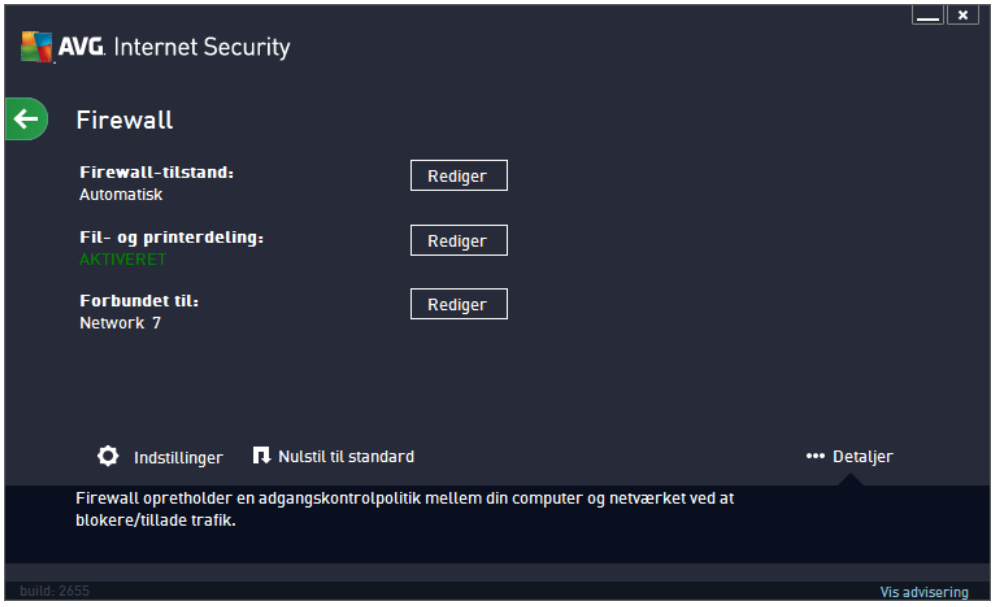
Firewall er et system, der gennemtvinger en adgangskontrol-politik mellem to eller flere netværk, ved at blokere/tillade trafik. Firewall indeholder et sæt regler, der beskytter det interne netværk mod angreb *udefra (typisk fra internettet)* og styrer al kommunikation på hver eneste netværksport. Kommunikationen evalueres i henhold til de definerede regler, og er enten tilladt eller forbudt. Hvis Firewall genkender et indtrængningsforsøg, "blokerer" den forsøget og tillader ikke indtrængeren at få adgang til computeren. Firewall er konfigureret til at tillade eller afvise intern/ekstern kommunikation *(begge veje, ind eller ud)* gennem definerede porte og for definerede softwareapplikationer. 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. 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 Firewall også enkelte computere mod angreb, der iværksættes af interne brugere på andre computere i netværket.

I **AVG Internet Security 2013** styrer ***Firewall*** al trafik på alle din computers 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 vil Firewall'en derefter enten tillade eller forbyde kommunikationen via netværksportene. Hvis applikationen er ukendt *(dvs. den har ingen definerede Firewall-regler)*, vil Firewall som standard spørge dig, om du vil tillade eller blokere kommunikationsforsøget.

AVG Firewall er ikke beregnet som beskyttelse til serverplatforme.

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.*



Tilgængelige Firewall-tilstande

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 tilstande. Kort sagt er en Firewall-tilstand en specifik konfiguration af Firewall-komponenten, og du kan bruge et antal af disse foruddefinerede konfigurationer.

- ***Automatisk*** – i denne tilstand håndterer Firewall al netværkstrafik automatisk. Du får ikke mulighed for at foretage noget valg. Firewall tillader forbindelse for hver kendt applikation, og

på samme tid oprettes der en regel til applikationen, der specificerer, at applikationen altid kan oprette forbindelse i fremtiden. For andre applikationer beslutter Firewall, om forbindelsen skal tillades eller blokeres baseret på applikationens adfærd. I sådan en situation vil regler dog ikke blive oprettet, og applikationen vil blive kontrolleret igen, når den prøver at oprette forbindelse. Den automatiske tilstand er ganske diskret og anbefales til de fleste brugere.

- ***Interaktiv*** – denne tilstand er nyttig, hvis du vil have fuld kontrol over al netværkstrafik til og fra din computer. Firewall overvåger den for dig og giver dig besked om hvert forsøg på at kommunikere eller overføre data, så du kan tillade eller blokere forsøget, som du ser passende. Anbefales kun for avancerede brugere.

- ***Bloker adgang til internettet*** – forbindelse til internettet blokeres fuldstændigt. Du kan ikke få adgang til internettet, og ingen udefra kan få adgang til din computer. Kun til særligt og kortvarigt brug.

- ***Slå Firewall-beskyttelse fra*** – hvis Firewall slås fra, tillades al netværkstrafik til og fra din computer. Dette gør din computer sårbar over for fremtidige hackerangreb. Overvej altid denne mulighed nøje.

Vær opmærksom på, at der også er en specifik automatisk tilstand tilgængelig i Firewall. Denne tilstand aktiveres, hvis enten komponenten Computer eller Identitetsbeskyttelse slås fra, og din computer er derfor mere sårbar. I sådanne tilfælde tillader Firewall automatisk kun kendte og fuldstændigt sikre applikationer. For alle andre bliver du spurgt, hvad der skal gøres. Dette er for at kompensere for de deaktiverede beskyttelseskomponenter og for at holde din computer sikker.

Kontrolelementer i dialogboks

Dialogboksen indeholder en oversigt over de grundlæggende oplysninger om statussen for Firewall-komponenten:

- ***Firewall-tilstand*** – indeholder oplysninger om den aktuelt valgte Firewall-tilstand. Brug knappen ***Skift*** , der findes ud for de viste oplysninger, for at skifte grænsefladen for Firewall-indstillinger, hvis du vil skifte den aktuelle tilstand til en anden *(se forrige afsnit for at få en beskrivelse og anbefaling af brugen af Firewall-profiler)*.

- ***Fil- og printerdeling*** – oplyser, om fil- og printerdeling *(i begge retninger)* er tilladt på nuværende tidspunkt. Fil- og printerdeling betyder faktisk deling af alle filer og mapper, som du har markeret som "Delt" i Windows, fælles diskenheder, printere, scannere og alle lignende enheder. Deling af sådanne elementer bør kun ske i netværk, der er sikre*(f.eks. hjemme, på arbejde eller i skolen)*. Men hvis du har forbindelse til et offentligt netværk (som f.eks. et Wi-Fi i lufthavnen eller en internetcafé), kan det være en dårlig idé at dele noget.

- ***Forbundet til*** – indeholder oplysninger om navnet på det netværk, du i øjeblikket har forbindelse til. I Windows XP svarer netværksnavnet på den betegnelse, du valgte til det bestemte netværk, da du første gang oprettede forbindelse til det. I Windows Vista og nyere tages netværksnavnet automatisk fra Netværks- og delingscentret.

Dialogboksen indeholder følgende kontrolelementer:

Skift – knappen giver dig mulighed for at skifte statussen for et respektivt parameter. Hvis du vil have flere oplysninger om statusændringen, skal du læse beskrivelsen af det specifikke

parameter i afsnittet ovenfor.

Indstillinger – klik på knappen for at blive omdirigeret til grænsefladen for Firewall-indstillinger, hvor du kan redigere hele Firewall-konfigurationen. Enhver konfiguration bør kun udføres af erfarne brugere.

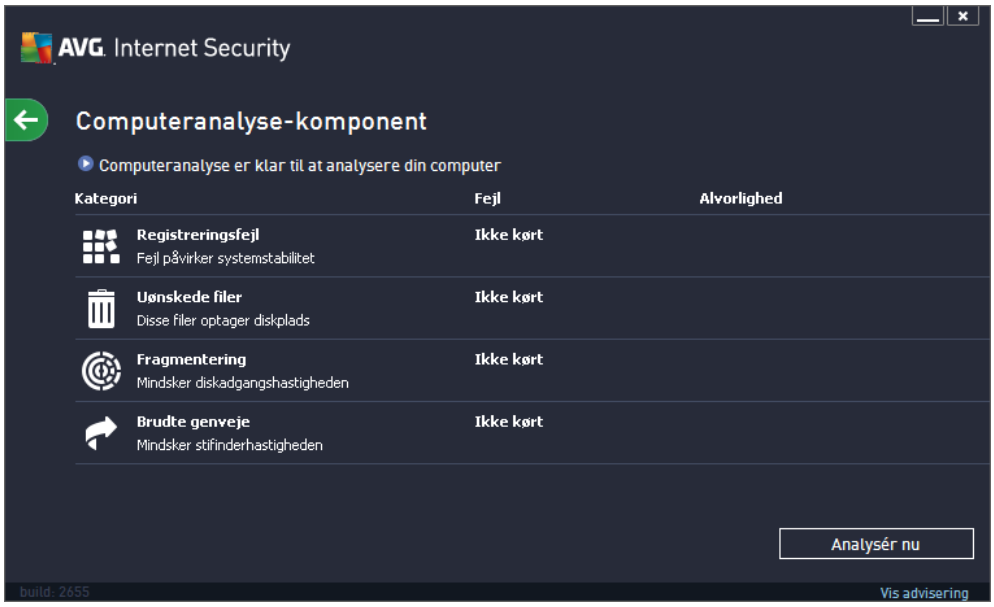
Nulstil til standard – tryk på denne knap for at overskrive den aktuelle Firewall-konfiguration og for at gendanne standardkonfigurationen baseret på automatisk detektering.

Detaljer – klik på knappen, så vises der en kort beskrivelse af den markerede tjeneste nederst i dialogboksen.

– Brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til hovedbrugerfladen med oversigten over komponenterne.

6.6. 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

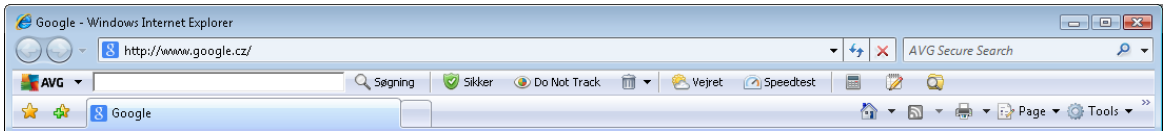
- ***Analyser nu*** (*vises inden analysen starter*) – tryk på denne knap for at starte den øjeblikkelige analyse af computeren

- ***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

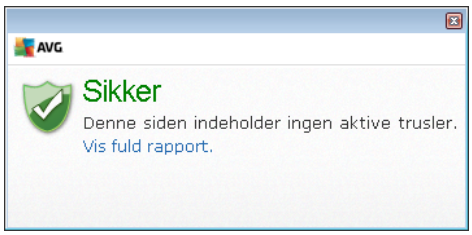
7. AVG sikkerhedsværktøjslinje

AVG Sikkerhedsværktøjslinje er et værktøj, der i tæt samarbejde med tjenesten LinkScanner SurfShield beskytter din sikkerhed, mens du browser på internettet. I **AVG Internet Security 2013** 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 bruger en alternativ internetbrowsere som f.eks. Avant Browser, kan du opleve uventet adfærd).*



AVG-sikkerhedsværktøjslinjen består af følgende elementer:

- ***AVG-logo*** med rullemenuen:
    - ***Brug AVG Secure Search*** – giver dig mulighed for at søge direkte fra ***AVG Sikkerhedsværktøjslinje*** ved hjælp af søgemaskinen ***AVG Secure Search***.
    - ***Aktuelt trusselsniveau*** – åbner viruslaboratoriets webside med en grafisk visning af det aktuelle trusselsniveau på nettet.
    - ***AVG Threat Labs*** – åbner det specifikke websted for ***AVG Threat Lab*** *(på http://www.avgthreatlabs.com)*, hvor du kan finde oplysninger om sikkerheden på forskellige websteder og det aktuelle trusselsniveau online.
    - ***Værktøjslinjen Hjælp*** – åbner onlinehjælp, der gennemgår alle funktioner i ***AVG Sikkerhedsværktøjslinje***.
    - ***Send produkttilbagemelding*** – åbner en webside med en formular, som du kan udfylde og dermed fortælle os, hvad du synes om ***AVG Sikkerhedsværktøjslinje***.
    - ***Afinstaller AVG Sikkerhedsværktøjslinje*** – åbner en webside, der indeholder en detaljeret beskrivelse af, hvordan man deaktiverer ***AVG Sikkerhedsværktøjslinje*** i hver af de understøttede webbrowsere.
    - ***Om...*** – åbner et nyt vindue med oplysninger om versionen af den aktuelt installerede ***AVG Sikkerhedsværktøjslinje***.
- ***Søgefelt*** – søg på internettet ved hjælp af ***AVG Sikkerhedsværktøjslinje*** for at være fuldstændigt sikker og tryg, idet alle søgeresultater er hundrede procent sikre. Indtast søgeordet eller en sætning i søgefeltet, og tryk på knappen ***Søg*** *(eller Enter)*.
- ***Webstedssikkerhed*** – denne knap åbner en ny dialogboks, der indeholder oplysninger om det aktuelle trusselsniveau (*i øjeblikket sikkert*) for den side, du i øjeblikket besøger. Den korte oversigt kan udvides, så alle oplysningerne om alle sikkerhedsaktiviteter, der er relateret til denne side, vises direkte i browservinduet (*Vis fuld rapport*):



- ***Slet*** – knappen "Papirkurv" viser en rullemenu, hvor du kan vælge, om der skal slettes oplysninger om din browsing, dine downloads og dine onlineformularer, eller om hele dine søgehistorik skal slettes på én gang.

- ***Vejr*** – knappen åbner en ny dialogboks, der indeholder oplysninger om, hvordan vejret er der, hvor du befinder dig, og giver dig vejrudsigten for de næste to dage. Disse oplysninger opdateres jævnligt – 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***.

- ***Hastighedstest*** – denne knap viderestiller dig til en onlieapplikation, der kan hjælp dig med at bekræfte kvaliteten på din internetforbindelse *(ping)* og på din hastighed for download og upload.

- Genvejstaster til hurtig adgang til disse applikationer: ***Lommeregner***, ***Notesblok***, ***Windows Stifinder***.

8. AVG Do Not Track

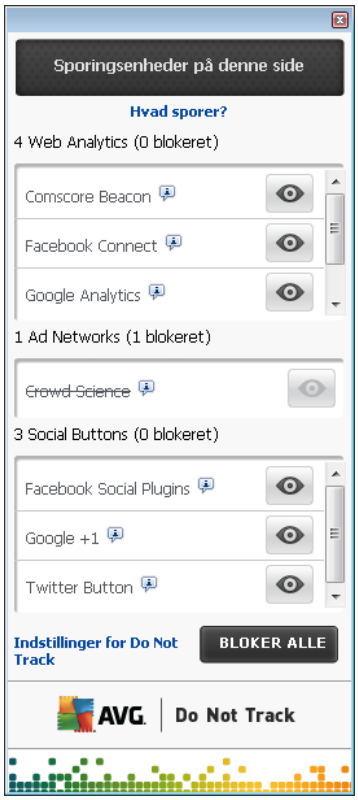
AVG Do Not Track gør det muligt at identificere websteder, der indsamler data om dine onlineaktiviteter. Et ikon i din browser viser de websteder og annoncører, der indsamler data om din aktivitet, og giver dig mulighed for at tillade eller blokere dataindsamling.

- ***AVG Do Not Track*** giver dig flere oplysninger om hver tjenestes politik om beskyttelse af private oplysninger samt et direkte link til fravalg af tjenesten, hvis det er tilgængeligt.
- Desuden understøtter ***AVG Do Not Track*** W3C DNT-protokollen, der automatisk giver besked til websteder, som du ikke ønsker skal spores. Denne meddelelse er aktiveret som standard, men kan ændres når som helst.
- ***AVG Do Not Track*** stilles til rådighed i henhold til disse vilkår og betingelser.
- ***AVG Do Not Track*** er aktiveret som standard, men kan nemt deaktiveres når som helst. Under Ofte stillede spørgsmål i artiklen Deaktivering af funktionen AVG Do Not Track finder du en vejledning.
- Få flere oplysninger om ***AVG Do Not Track*** på vores websted.

I øjeblikket understøttes funktionen ***AVG Do Not Track*** i browserne Mozilla Firefox, Chrome og Internet Explorer. *(I Internet Explorer er Do Not Track-ikonet placeret til højre for kommandolinjen. Hvis du får problemer med at se AVG Do Not Track-ikonet ved hjælp af browserens standardindstillinger, skal du sørge for, at kommandolinjen er aktiveret. Hvis du stadig ikke kan se ikonet, skal du blot trække kommandolinjen til venstre for at vise alle de ikoner og knapper, der er tilgængelige på denne værktøjslinje.)*

8.1. AVG Do Not Track-grænseflade

Når du er online, advarer ***AVG Do Not Track*** dig, så snart den mindste dataindsamlingsaktivitet registreres. Følgende dialog vises:



Alle registrerede tjenester, der indsamler data, opstilles på en liste efter navn på oversigten ***Sporingsfunktioner på denne side***. Der er tre typer dataindsamlingsaktiviteter, som genkendes af ***AVG Do Not Track***:

- ***Webanalyse*** *(tilladt som standard):* Tjenester, der bruges til at forbedre ydelsen for og oplevelsen af det relevante websted. Denne kategori indeholder tjenester såsom Google Analytics, Omniture eller Yahoo Analytics. Vi anbefaler, at du ikke blokerer webanalysetjenester, da webstedet så muligvis ikke fungerer som tiltænkt.

- ***Sociale Knapper*** *(tilladt som standard):* Elementer, der er udviklet til at forbedre oplevelsen med sociale netværk. Sociale knapper vises fra sociale netværk til det websted, som du besøger. De kan indsamle data om din onlineaktivitet, mens du er logget på. Eksempler på Sociale knapper er: Facebook Social Plugins, Twitter Button, Google +1.

- ***Reklamenetværk*** *(som standard er nogle blokeret):* Tjenester, der indsamler eller deler data om din onlineaktivitet på flere sider enten direkte eller indirekte, tilbyder dig tilpassede annoncer i stedet for indholdsbaserede annoncer. Dette afgøres ud fra hver reklamenetværks politik om beskyttelse af private oplysninger, som er tilgængelig på deres websted. Nogle reklamenetværk er blokeret som standard.

Bemærk: *Afhængigt af hvilke tjenester der kører i baggrunden af webstedet, vises nogle af de tre ovenstående sektioner muligvis ikke i AVG Do Not Track-dialogboksen.*

Dialogboksen indeholder også to hyperlink:

- ***Hvad sporer?*** - klik på dette link øverst i dialogboksen for at blive omdirigeret til en dedikeret webside, der detaljeret forklarer sporingsprincipperne og beskriver specifikke sporingstyper.

- ***Indstillinger*** - klik på dette link nederst i dialogboksen for at blive omdirigeret til en dedikeret webside, hvor du kan konfigurere forskellige ***AVG Do Not Track***-parametre *(se kapitlet Indstillinger for AVG Do Not Track for at få flere oplysninger)*

8.2. Oplysninger om sporingsprocesser

Listen over registrerede dataindsamlingstjenester angiver blot navnet på den angivne tjeneste. Hvis du ønsker at træffe en fornuftig beslutning om, hvorvidt den relevante tjeneste skal blokeres eller tillades, kan det være en idé at vide mere om det. Flyt markøren over det relevante listeelement. Der vises en oplysningsboble med detaljerede data om tjenesten. Du får mere at vide om, hvorvidt tjenesten indsamler personlige data eller blot nogle af de tilgængelige data, om dataene deles med tredjepart, og om de indsamlede data sendes videre til eventuel yderligere brug.

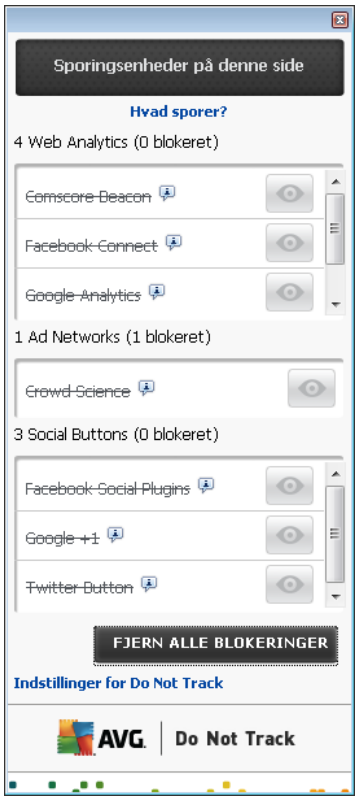
I den nederste del af oplysningsboblen kan du se linket ***Fortrolighedspolitik***, der omdirigerer dig til webstedet med fortrolighedspolitikken for den relevante registrerede tjeneste

8.3. Blokering af sporingsprocesser

Med listen over alle reklamenetværk/sociale knapper/webanalyser har du nu mulighed for at kontrollere, hvilke tjenester der skal blokeres. Du kan gøre det på to måder:

- ***Bloker alt***– Klik på denne knap nederst i dialogboksen for at angive, at du slet ikke ønsker nogen dataindsamlingsaktivitet. *(Dog skal du være opmærksom på, at denne handling kan bevirke, at den relevante webside, hvor tjenesten kører, ikke virker.)*

-  – Hvis du ikke vil blokere alle de registrerede tjenester med det samme, kan du angive individuelt, om tjenesten skal tillades eller blokeres. Du kan vælge at køre nogle af de registrerede systemer *(f.eks. webanalyser):* disse systemer bruger de indsamlede data til deres egen optimering af webstedet og er på den måde med til at forbedre det fælles internetmiljø for alle brugerne. Samtidigt kan du imidlertid blokere dataindsamlingsaktiviteterne for alle de processer, der klassificeres som reklamenetværk. Klik blot på  -ikonet ud for den relevante proces for at blokere dataindsamlingen *(procesnavnet vises som overkrydset)* eller for at tillade dataindsamlingen igen.

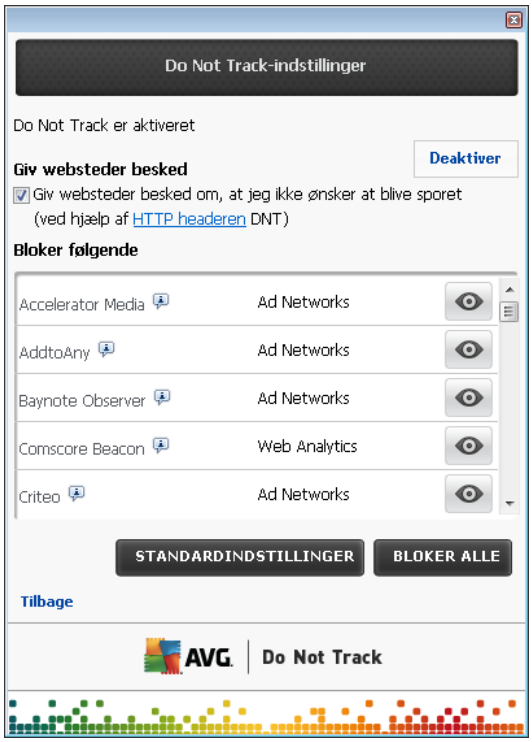


8.4. Indstillinger for AVG Do Not Track

Direkte i dialogboksen ***AVG Do Not Track*** er der kun én konfigurationsmulighed: Nederst kan du se ***Giv besked, når der registreres aktive sporingsfunktioner*** -afkrydsningsfeltet. Dette element er fravalgt som standard Markér afkrydsningsfeltet for at bekræfte, at du vil have besked, hver gang du kommer ind på en webside, der indeholder en ny dataindsamlingstjeneste, der endnu ikke er blevet blokeret. Når indstillingen er markeret, og hvis ***AVG Do Not Track*** registrerer en ny dataindsamlingstjeneste på den side, du i øjeblikket besøger, vises en beskeddialogboks på

skærmen. Ellers vil du kun kunne se den netop registrerede tjeneste ved hjælp af ikonet ***AVG Do Not Track*** *(placeret på kommandolinjen i browseren)*, som skifter farve fra grøn til gul.

I den nederste del af dialogboksen ***AVG Do Not Track*** kan du imidlertid finde linket ***Indstillinger***. Klik på linket for at blive omdirigeret til en dedikeret webside, hvor du kan vise dine detaljerede ***indstillinger for AVG Do Not Track***:



Giv mig besked

- ***Placering af beskeder*** *(øverst til højre som standard)* - Åbn rullemenuen for at angive, hvor ***AVG Do Not Track***-dialogboksen skal vises på skærmen.

- ***Vis besked for*** *(10 som standard)* - I dette felt skal du angive, i hvor lang *(i sekunder)* du ønsker at se ***AVG Do Not Track***-beskeden på skærmen. Du kan angive et tal fra 0 til 60 sekunder*(hvis det er 0, vises beskeden slet ikke på skærmen)*.

- ***Giv besked, når der registreres aktive sporingsfunktioner*** *(slået fra som standard)* - Markér afkrydsningsfeltet for at bekræfte, at du vil have besked, hver gang du kommer ind på en webside, der indeholder en ny dataindsamlingstjeneste, der endnu ikke er blevet blokeret. Når indstillingen er markeret, og hvis AVG Do Not Track registrerer en ny dataindsamlingstjeneste på den side, du i øjeblikket besøger, vises en beskeddialogboks på skærmen. Ellers vil du kun kunne se den netop registrerede tjeneste ved hjælp af ikonet ***AVG Do Not Track*** *(placeret på kommandolinjen i browseren)*, som skifter farve fra grøn til gul.

- ***Giv websteder besked om, at jeg ikke ønsker at blive sporet*** *(aktiveret som standard)* - Sørg for, at denne indstilling er markeret for at bekræfte, at du ønsker, at ***AVG Do Not Track*** skal oplyse udbyderen af en registreret dataindsamlingstjeneste om, at du ikke

ønsker at blive sporet.

Bloker følgende

I denne sektion kan du se en boks med en liste over kendte tjenester til dataindsamling, der kan klassificeres som annoncenetværk. ***AVG Do Not Track*** blokerer som standard nogle af reklamenetværkene automatisk, og det er din beslutning, om resten også skal blokeres eller tillades. Det gør du ved at klikke på knappen ***Bloker alt*** under listen.

Betjeningsknapper

De kontrolknapper, der er tilgængelige på siden ***Indstillinger for AVG Do Not Track*** er følgende:

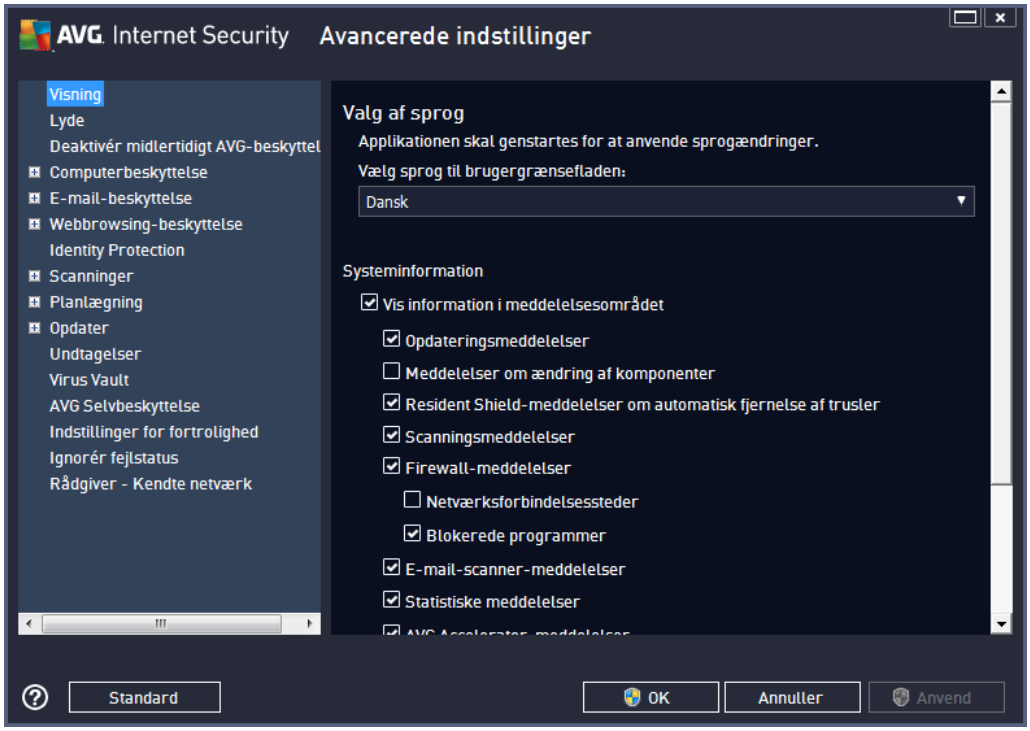
- ***Bloker alt*** – klik for med det samme at blokere alle de tjenester, der er angivet i feltet herover, der er klassificeret som reklamenetværk;
- ***Tillad alt*** – klik for med det samme at fjerne blokeringen af alle tidligere blokerede tjenester, der er i feltet herover, og som er klassificeret som reklamenetværk;
- ***Standardindstillinger*** – klik for at slette alle dine tilpassede indstillinger og vende tilbage til standardkonfigurationen;
- ***Gem*** – klik for at anvende og gemme alle dine angivne konfigurationer;
- ***Annuller*** – klik for at annullere alle de indstillinger, du har angivet tidligere.

9. AVG Avancerede indstillinger

Den avancerede konfigurationsdialog for **AVG Internet Security 2013** 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 for (*eller dens specifikke del*) for at åbne redigeringsdialogboksen i den højre sektion i vinduet.

9.1. Udseende

Det første element i navigationstræet, ***Udseende***, refererer til de generelle indstillinger for **AVG Internet Security 2013-**brugergrænsefladen og nogle få elementære indstillinger omkring applikationens adfærd:



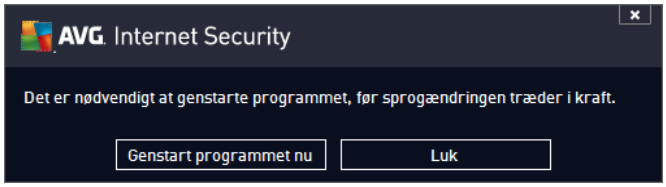
Valg af sprog

I sektionen ***Sprogvalg*** kan du vælge det ønskede sprog i rullemenuen. Det ønskede sprog vil herefter blive brugt i hele **AVG Internet Security 2013-**brugergrænsefladen. Rullemenuen indeholder kun de sprog, du valgte at installere under installationsprocessen, samt engelsk (*engelsk installeres som standard altid automatisk*). Hvis du er færdig med at ændre **AVG Internet Security 2013** 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 Security 2013**

- 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 deaktivere visning af systeminformation om statussen for **AVG Internet Security 2013**-applikationen. Systembeskederne bliver som standard vist. Det anbefales kraftigt, at du beholder denne konfiguration. Systemadviseringer informerer eksempelvis om kørsel af scanninger eller opdateringer, eller om statusændringer for en **AVG Internet Security 2013** -komponent. 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 meddelelser *(der er relateret til en specifik AVG Internet Security 2013-komponent)*, kan du angive og specificere dine præferencer ved at markere eller fjerne markeringen fra følgende indstillinger:

- ***Vis systeminformation*** *(slået til som standard)* – som standard vises alle tekstbobler. 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 systeminformation om opdateringer*** *(slået til som standard)* – afgør, om oplysninger for opdateringens **AVG Internet Security 2013** igangsætning, forløb og fuldførelse skal vises.

    - ***Vis information om statusændring i komponenter*** *(slået fra som standard)* – afgør, om oplysninger vedrørende komponentens aktivitet/inaktivitet eller dens mulige problem skal vises. Når du rapporterer en komponents fejlstatus, svarer denne indstilling til informationsfunktionen for proceslinjeikonet, der rapporterer et problem i hvilken som helst **AVG Internet Security 2013** komponent.

    - ***Vis systeminformation vedrørende Resident Shield (automatisk handling)*** *(slået til som standard)* – afgør, om oplysninger vedrørende lagring, kopiering og åbning af filer skal vises eller tilsidesættes (*denne konfiguration vises kun, hvis funktionen til automatisk helbredelse til Resident Shield er slået til*).

    - ***Vis systeminformation om scanning*** *(slået til som standard)* – afgør, om der skal vises oplysninger ved automatisk start af den planlagte scanning, dens forløb og resultaterne.

    - ***Vis systeminformation vedrørende Firewall*** *(slået til som standard)* – afgør, om der skal vises oplysninger om Firewall-status og -processer, dvs. advarsler om

aktivering/deaktivering af komponenten, mulige blokeringer af trafik osv. skal vises. Dette element indeholder to ekstra specifikke valgindstillinger *(du kan få en detaljeret forklaring af dem begge ved at se kapitlet om Firewall i dette dokument)*:

– ***Vis adviseringer om profilændringer*** *(slået til som standard)* – informerer dig om automatiske ændringer af Firewall-profiler.

– ***Vis meddelelser om nyoprettet applikationsregel*** *(slået fra som standard)* – giver dig besked om den automatiske oprettelse af Firewall-regler til nye applikationer baseret på en sikker liste.

- ***Vis systeminformation vedrørende E-mail-scanner*** *(slået til som standard)* – afgør, om der skal vises oplysninger om scanning af alle indgående og udgående e-mailmeddelelser.

- ***Vis statistikoplysninger*** *(slået til som standard)* – lad indstillingen være markeret for at tillade, at der regelmæssigt vises informationsmeddelelser om statistik på proceslinjen.

- ***Vis systeminformation om AVG Accelerator*** *(slået til som standard)* – afgør, om der skal vises oplysninger om aktiviteter i ***AVG Accelerator***. Tjenesten ***AVG Accelerator*** giver en mere glidende afspilning af video på nettet og gør det nemmere at downloade.

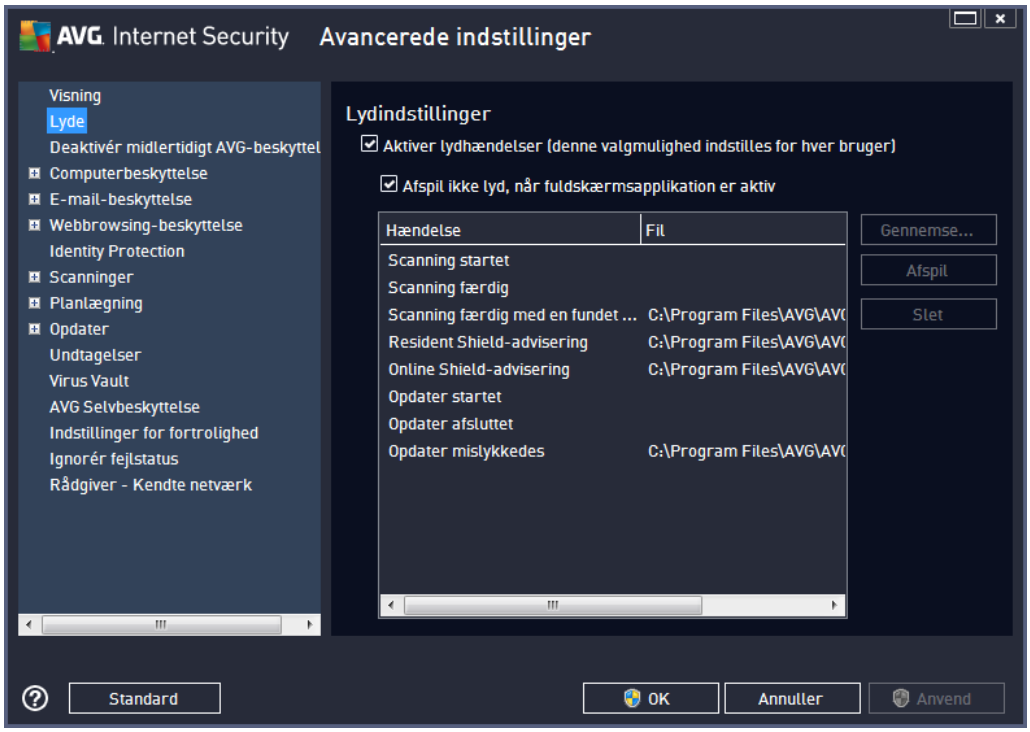
- ***Vis adviseringer fra AVG Advisor*** *(slået til som standard* – afgør, om der skal vises oplysninger ved aktiviteter i AVG Advisor på rullepanelet på proceslinjen.

Gamingtilstand

Denne AVG-funktion er beregnet til applikationer i fuld skærm, hvor AVG-tekstbobler (*vises, f.eks. når en planlagt scanning startes*) vil virke forstyrrende (*de kan minimere applikationen eller ødelægge grafikken*). Du kan undgå dette ved lade afkrydsningsfeltet for funktionen ***Aktiver gamingtilstand, når en fuldskærmsapplikation køres*** være markeret (*standardindstilling*).

9.2. Lyde

I dialogen ***Lyde*** kan du angive, om du ønsker at få oplysninger om bestemte **AVG Internet Security 2013**-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. Det kan også være en god ide at markere indstillingen ***Afspil ikke lyd, når fuldskærmsapplikation er aktiv*** for at undertrykke lydbeskeden i situationer, hvor den kan være forstyrrende *(se også sektionen om gaming-tilstand i kapitlet Avancerede indstillinger/Visning i dette dokument)*.

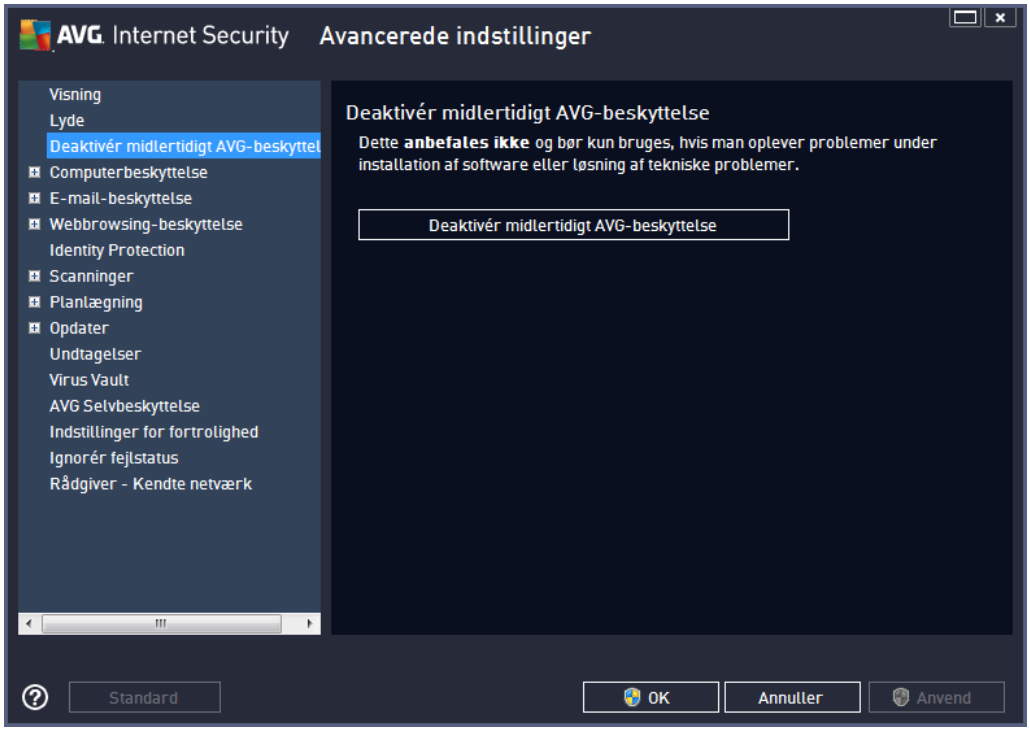
Betjeningsknapper

- ***Gennemse*** – når du har valgt den relevante hændelse på listen, kan du bruge knappen ***Gennemse*** for at søge på disken efter den lydfil, du vil tildele den til. *(Bemærk, at det kun er *.wav-lyde, der understøttes i øjeblikket!)*
- ***Afspil*** – hvis du vil lytte til den valgte lyd, kan du markere hændelsen på listen og trykke på knappen ***Afspil***.
- ***Slet*** – brug knappen ***Slet*** til at fjerne den lyd, der er tildelt til 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 Security 2013** 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 Security 2013**, 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 skulle komme ud for nogle problemer under installationen, kan du forsøge at deaktivere Resident-beskyttelsen (*Aktivér Resident Shield*) først. Hvis du midlertidigt skal deaktivere **AVG Internet Security 2013**, skal du genaktivere den, så snart du er færdig. Hvis du har forbindelse til internettet eller et netværk, når din antivirussoftware er deaktiveret, er din computer sårbar over for angreb.

Sådan deaktiveres AVG-beskyttelsen

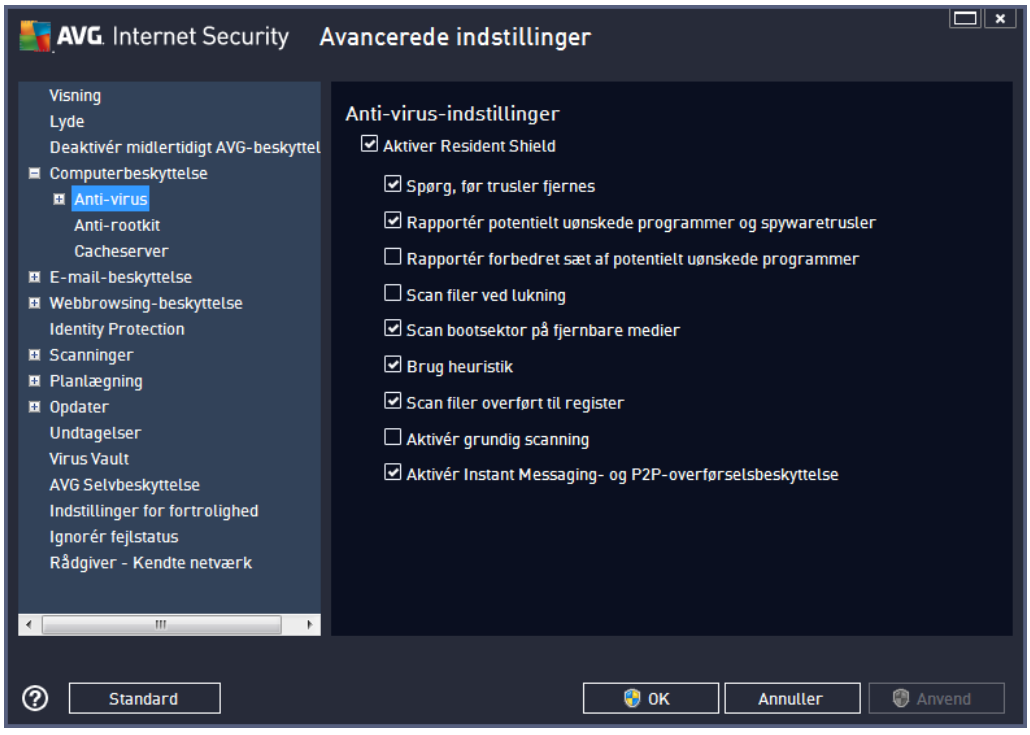
Markér feltet ***Deaktivér midlertidigt AVG-beskyttelse***, og bekræft dit valg ved at trykke på knappen ***Anvend***. I den netop åbnede dialogboks ***Deaktivér midlertidigt AVG-beskyttelse*** skal du angive, i hvor lang tid du vil deaktivere dit **AVG Internet Security 2013**. Denne beskyttelse slås 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. Du kan bestemme dig for en længere tidsperiode, men denne indstilling anbefales ikke, medmindre det er absolut nødvendigt. Derefter aktiveres alle deaktiverede komponenter igen automatisk. Du kan højst deaktivere AVG-beskyttelsen til næste genstart af computeren. Der er en separat indstilling deaktivering af komponenten ***Firewall*** findes i

dialogboksen ***Deaktivér midlertidigt AVG-beskyttelse***. Markér ***Deaktiver firewallbeskyttelse*** for at gøre dette.

9.4. Computerbeskyttelse

9.4.1. Anti-virus

Anti-Virus sammen med ***Resident Shield*** giver din computer uafbrudt beskyttelse mod alle kendte typer vira, spyware og malware generelt *(inklusive såkaldt sovende og inaktiv malware, dvs. malware, der er downloadet, men endnu ikke aktiveret)*.



I dialogboksen ***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 integrerede beskyttelse der skal aktiveres:

- ***Spørg, før trusler fjernes*** (*er slået til som standard*) – markér afkrydsningsfeltet for at sikre, at Resident Shield ikke udfører handlinger automatisk. I stedet vises en dialogboks, der beskriver den registrerede trussel og giver dig mulighed for at beslutte, hvad du vil foretage dig. Hvis du ikke markerer afkrydsningsfeltet, eliminerer **AVG Internet Security 2013** infektionen automatisk, og hvis det ikke er muligt, flyttes objektet til Virus Vault.

- ***Scan efter sporingscookies*** (*slået fra som standard*) – denne parameter definerer, at cookies skal detekteres under scanningen. (*HTTP-cookies bruges til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på webstedet eller indholdet i deres elektroniske indkøbsvogne.*)

- ***Rapportér potentielt uønskede programmer og spywaretrusler*** (*slået til som standard*) – markér for at aktivere scanning efter spyware og vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler, at denne funktion holdes aktiveret, da den forstærker 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 erhverves direkte fra producenten, men som senere kan misbruges til skadelige formål. Dette er en ekstra funktion, der forstærker din computersikkerhed endnu mere, men den kan dog risikere at blokere lovlige programmer og er derfor som standard slået fra.

- ***Scan filer ved lukning*** (*slået fra 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*)

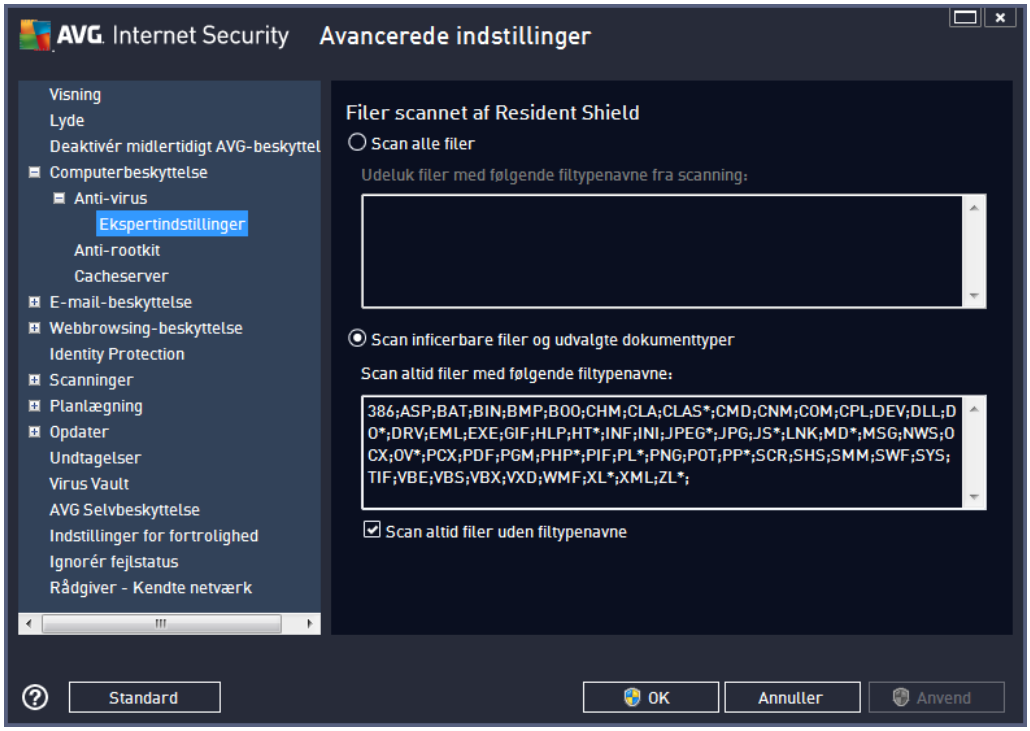
- ***Brug heuristik*** (*slået til som standard*) – heuristisk analyse bruges til detektering (*dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø*).

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

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

- ***Aktivér beskyttelse af instant messaging og P2P-download*** (*slået til som standard*) – markér dette element, hvis du vil bekræfte, at kommunikation via instant messaging (*f.eks. AIM, Yahoo!, ICQ, Skype, MSN Messenger, …*) og data, der er downloadet via peer to peer-netværk *(netværk, der tillader direkte forbindelse mellem klienter uden en server, hvilket kan være farligt, og som typisk bruges til at dele musikfiler)*, er virusfri.

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

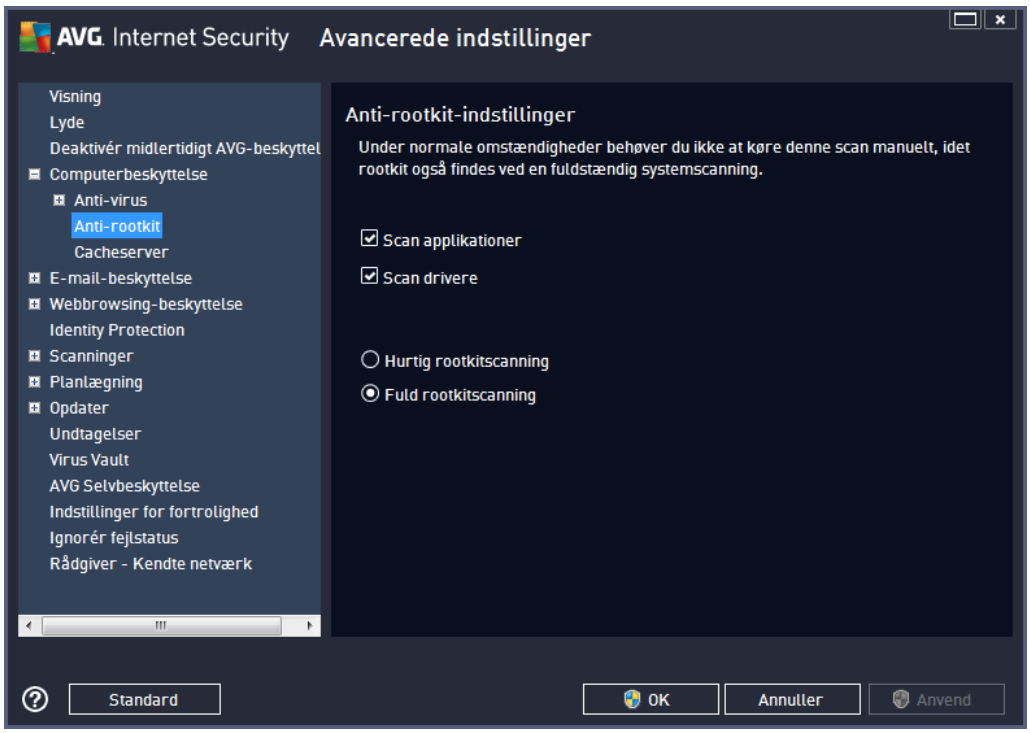


Markér det pågældende afkrydsningsfelt for at angive, hvad der skal scannes: ***Scan alle filer*** eller kun ***Scan inficerbare filer og udvalgte dokumenttyper***. Hvis du vil gøre scanningen hurtigere og give maks. beskyttelse på samme tid, anbefaler vi, at du beholder standardindstillingerne. Dermed scannes kun inficérbare filer. I den pågældende sektion i dialogboksen finder du også en redigerbar liste over filtypenavne, der definerer de filer, som medtages i scanningen.

Markér ***Scan altid filer uden filtypenavne*** (*som standard*)for at sikre, at filer uden filtypenavn og i ukendt format bliver scannet af Resident Shield. Vi anbefaler, at denne funktion er slået til, da filer uden filtypenavn er mistænkelige.

9.4.2. Anti-rootkit

I dialogboksen ***Anti-rootkit-indstillinger*** kan du redigere konfigurationen af ***Anti-rootkit***-tjenesten og særlige parametre i anti-rootkit-scanningen. Anti-rootkit-scanning er en standardproces, der indgår i Scan hele computeren:

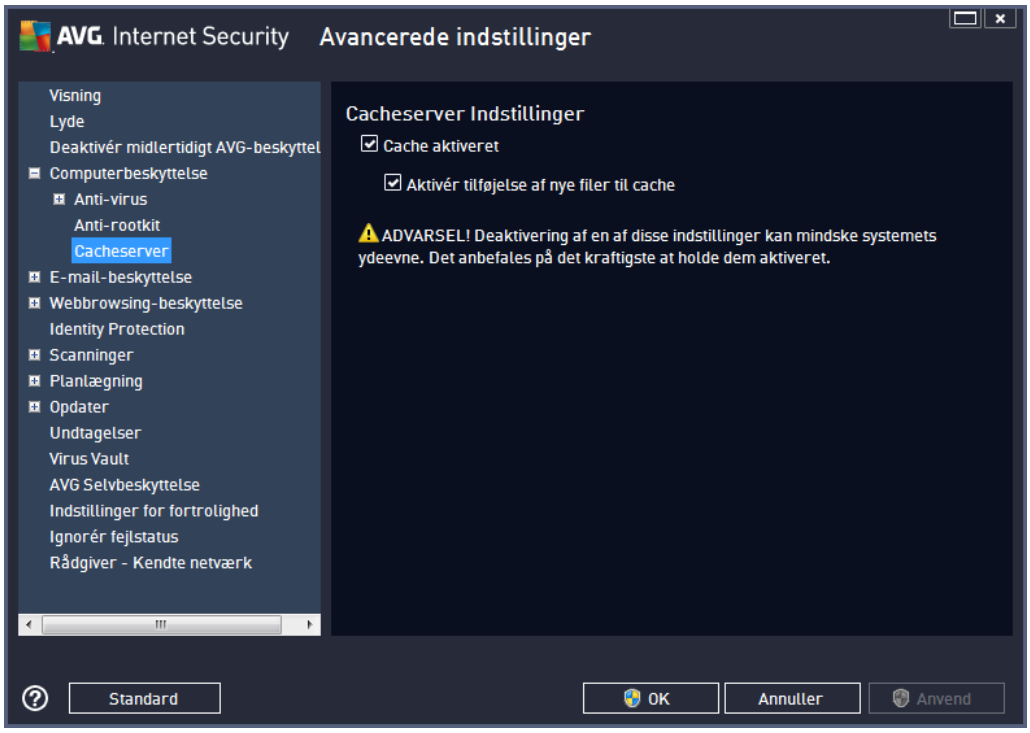


Scan applikationer og ***Scan drivere*** gør det muligt at angive, hvad der skal medtages i anti-rootkit-scanningen. Disse indstillinger er beregnede til avancerede brugere. Vi anbefaler, at du lader alle indstillinger være slået til. Du kan også vælge rootkit-scanningstilstanden:

- ***Hurtig rootkit-scanning*** – scanner alle igangværende processer, indlæste drivere og systemmappen (*typisk c:\Windows*)
- ***Fuld rootkit-scanning*** – scanner alle igangværende processer, indlæste drivere, systemmappen (*typisk c:\Windows*), samt alle lokale drev (*inklusive flashdrev, men ikke floppydrev/CD-drev*)

9.4.3. Cacheserver

Dialogen ***Cacheserverindstillinger*** viser den cacheserverproces, der er beregnet til at fremskynde alle typer **AVG Internet Security 2013**-scanninger:



Cacheserveren indsamler og gemmer oplysninger om pålidelige filer (*en fil betragtes som pålidelig, hvis den har en digital signatur fra en pålidelig kilde*). Disse filer betragtes per automatik som sikre og behøver ikke at blive scannet igen. Derfor springes disse filer over under scanning.

Dialogboksen for ***Indstillinger for cacheserver*** har 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.

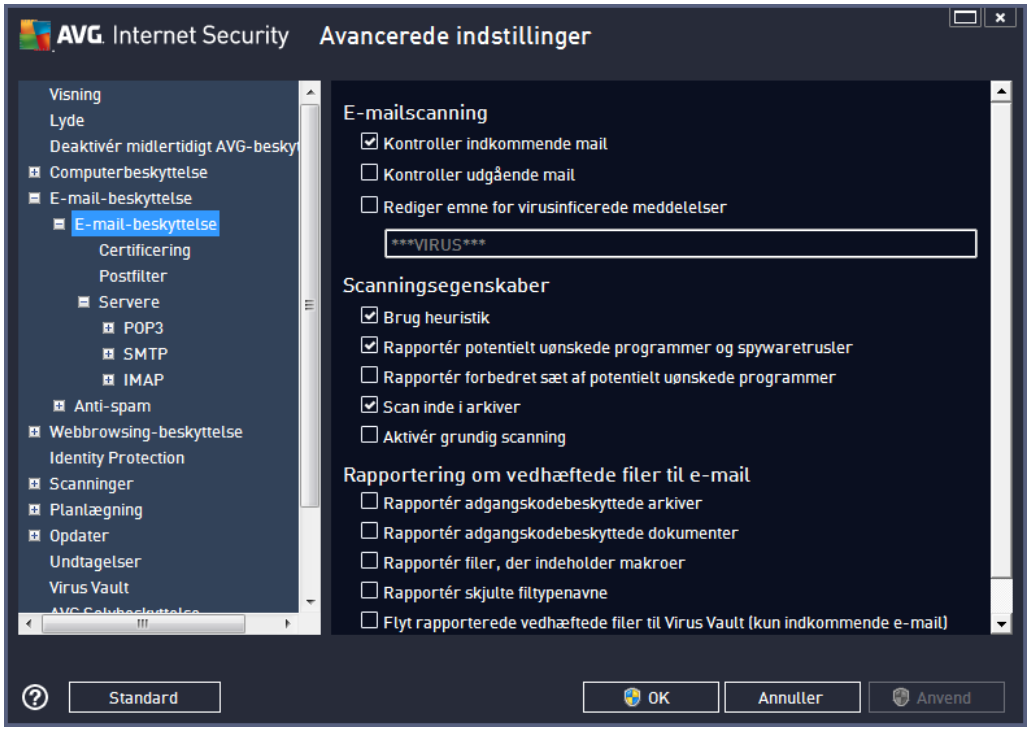
Medmindre du har en god grund til at deaktivere cacheserveren, anbefaler vi på det kraftigste, at du beholder standardindstillingerne og lader begge indstillinger være slået til. Ellers kan du komme til at opleve en betydelig forringelse af dit systems hastighed og ydeevne.

9.5. E-mail-scanner

I denne sektion kan du redigere den detaljerede 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-mailmeddelelse blev detekteret som inficeret, skal du markere dette element og skrive 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 du beholder.

Scanningsegenskaber

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

- ***Brug heuristik*** (*slået til som standard*) – markér afkrydsningsfeltet for at anvende metoden til heuristikdetektering, når der scannes e-mailmeddelelser. Hvis denne indstilling er slået til, kan du filtrere vedhæftede filer i e-mails 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*** (*slået til som standard*) – markér afkrydsningsfeltet for at aktivere scanning efter spyware såvel som 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 du lader denne funktion være aktiveret, da den øger computersikkerheden.

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*) – markér afkrydsningsfeltet for at detektere udvidede pakker: 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 (*f.eks. når der er mistanke om, at din computer er inficeret med en virus eller et angreb*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, som stort set aldrig bliver inficeret, bare for at være helt sikker. Husk på, at denne metode kræver meget tid.

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 advarselsdialogboks. Der føjes kun en certificeringstekst til slutningen af e-mailmeddelelsen, og alle sådanne rapporter vises på en liste i dialogboksen E-mail-scanner-detektering:

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

- ***Rapportér adgangskodebeskyttede dokumenter*** – dokumenter, der er beskyttet med adgangskode, er ikke mulige at scanne for vira. Markér afkrydsningsfeltet for at rapportere disse som potentielt farlige.

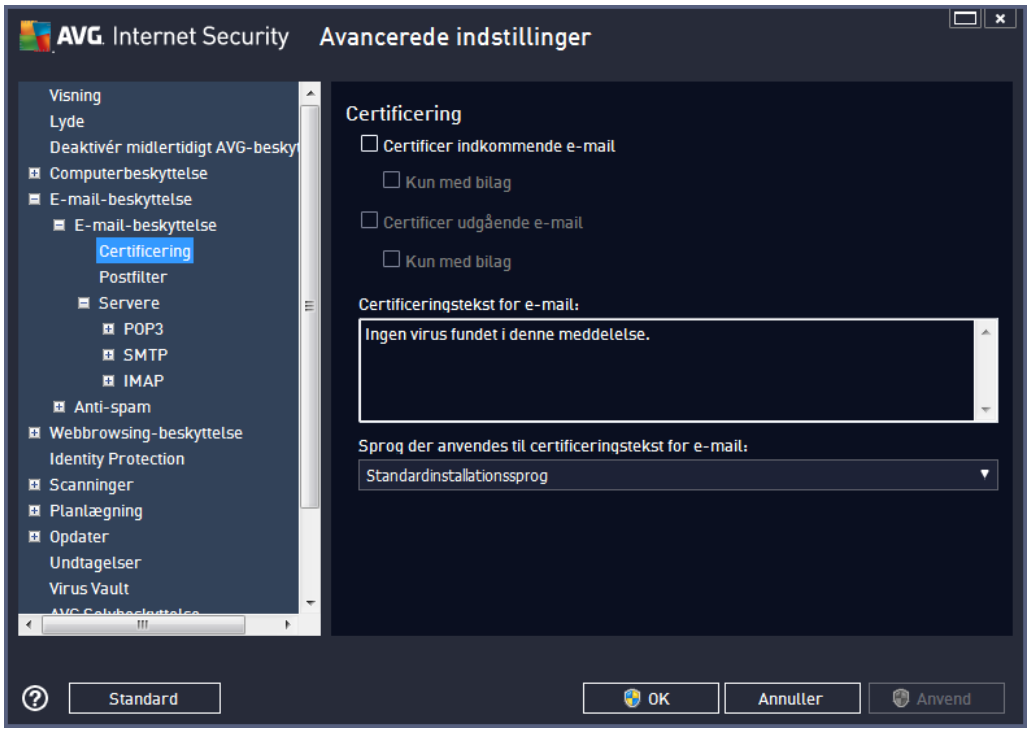
- ***Rapportér filer med makroer*** – En makro er en foruddefineret række trin, der er beregnet til at gøre bestemte opgaver nemmere for en bruger (*MS Word-makroer er almindeligt kendte*). Som sådan kan en makro indeholde potentielt farlige instruktioner, og det er muligvis relevant for dig at markere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

- ***Rapportér skjulte filtypenavne*** – et skjult filtypenavn kan f.eks. få en mistænkelig eksekverbar fil "something.txt.exe" til at se ud som en harmløs almindelig tekstfil "something.txt". Markér afkrydsningsfeltet for at rapportere dem som potentielt farlige.

- ***Flyt rapporterede vedhæftede filer til Virus Vault*** – angiv, om du vil have besked via e-

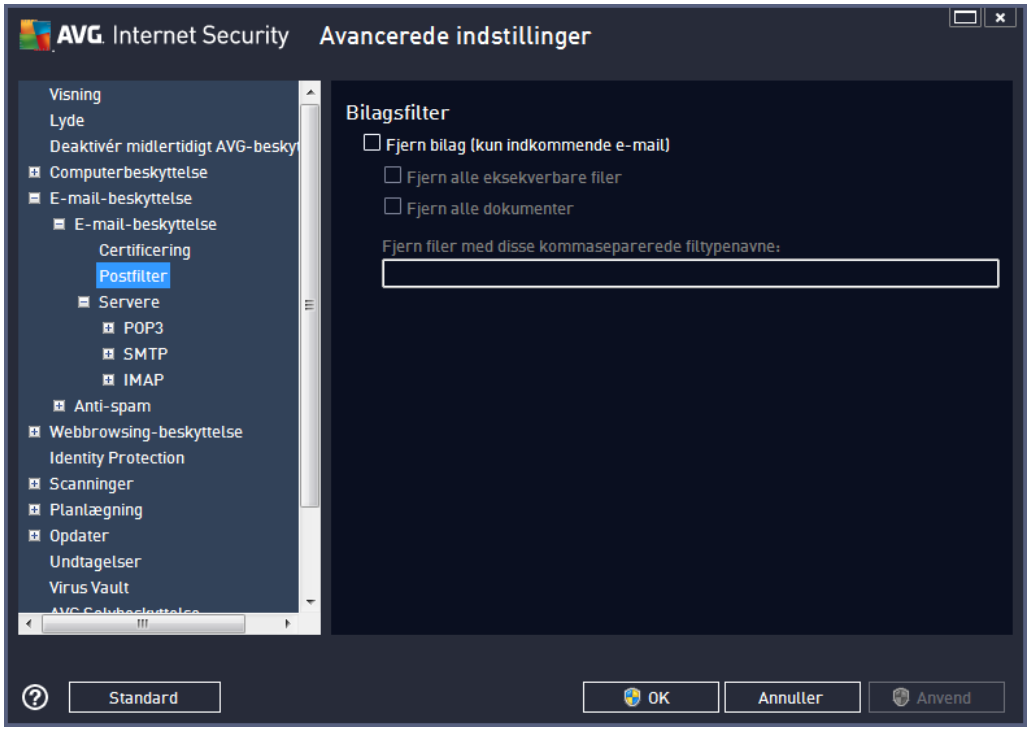
mail om adgangskodebeskyttede arkiver, adgangskodebeskyttede dokumenter, filer der indeholder makroer og/eller filer med skjulte filtypenavne, der detekteres som en vedhæftet fil til den scannede e-mailmeddelelse. Hvis der identificeres en sådan meddelelse under scanningen, skal du definere, om det detekterede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

I dialogboksen ***Certificering*** kan du markere specifikke afkrydsningsfelter for at afgøre, om du vil certificere indgående mail (***certificer indgående e-mail***) og/eller udgående e-mail (***certificer udgående e-mail***). For hver af disse indstillinger kan du specificere parameteren ***Kun med bilag*** yderligere, så certificeringen kun føjes til e-mailmeddelelser med 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, der er anvendt til e-mailcertificeringstekst*** kan du definere yderligere, på hvilket sprog den automatisk genererede del af certificeringen (*ingen virus fundet i denne meddelelse*) skal vises.

Bemærk: *Vær opmærksom på, at det kun er standardteksten, der vises på det ønskede sprog, og din brugerdefinerede tekst oversættes ikke automatisk.*



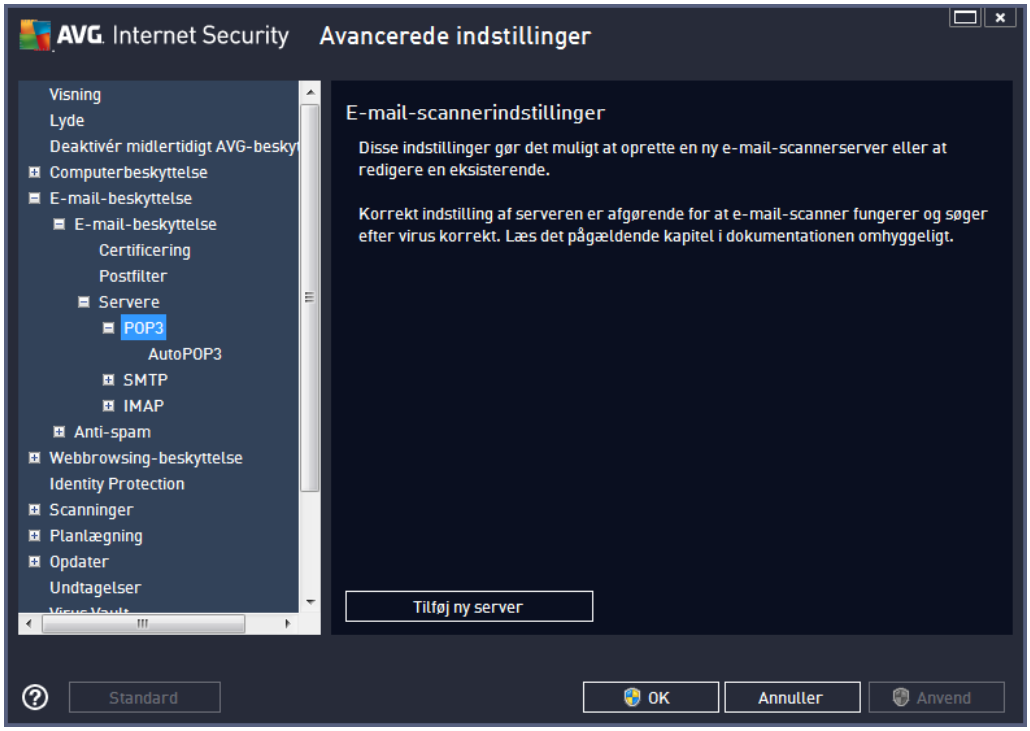
I dialogboksen ***Bilagsfilter*** kan du indstille parametre for scanning af vedhæftede filer i e-mailmeddelelser.Som standard er indstillingen ***Fjern vedhæftede filer*** slået fra. Hvis du beslutter at aktivere den, bliver alle vedhæftede filer i e-mailmeddelelser, der detekteres som inficerede eller 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 parametre for E-mail-scanner-servere:

- POP3-server
- SMTP-server
- IMAP-server

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

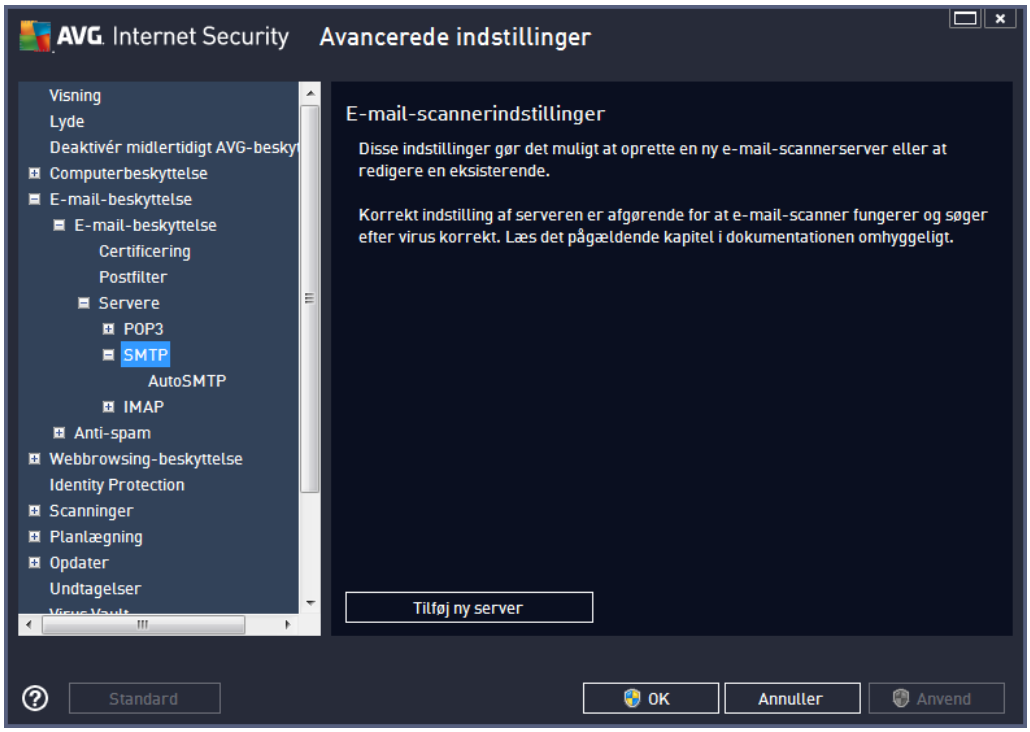


I denne dialogboks (*åbnes via **Servere / POP3***) kan du konfigurere en ny E-mail scanner-server vha. POP3-protokollen for indkommende e-mail:

- ***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*). Dette felt er deaktiveret for automatisk oprettede "AutoPOP3"-servere.
- ***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 (*f.eks. 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*). Når det gælder automatisk oprettede "AutoSMTP"-servere, bliver 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

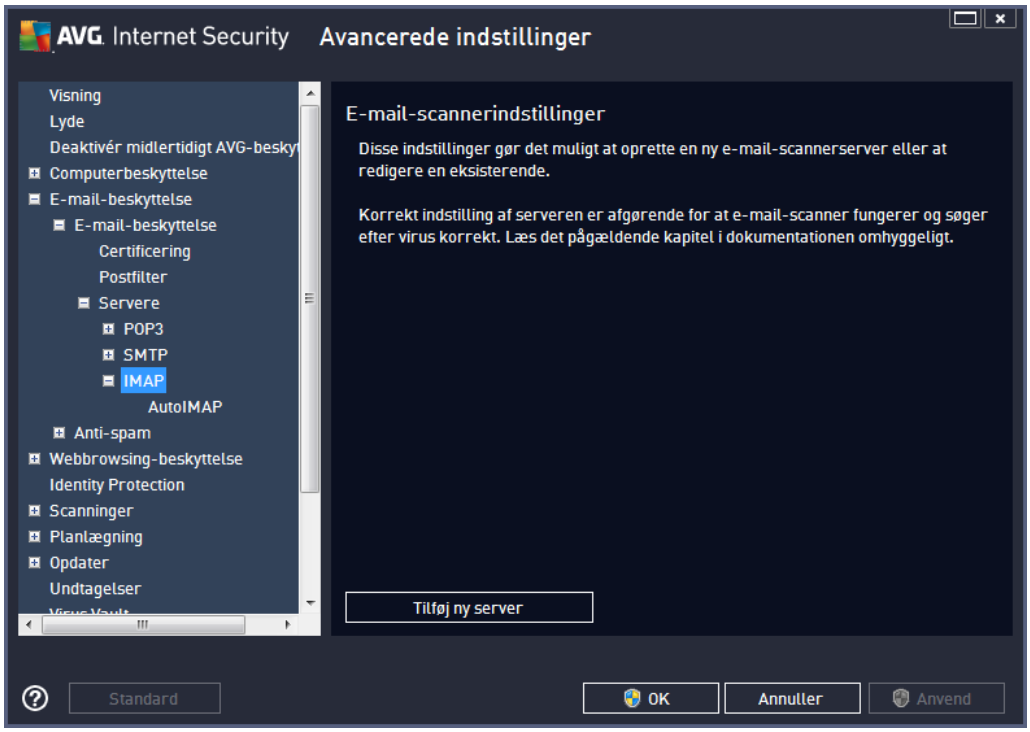
  - ***Fast vært*** – i dette tilfælde anvender programmet altid den server, der er angivet her. Angiv adressen eller navnet på din mailserver. Du kan bruge et domænenavn (*for eksempel smtp.acme.com*) eller en IP-adresse (*for eksempel 123.45.67.89*) som navn. Hvis mailserveren ikke benytter en standardport, 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.

- ***SMTP-serveraktivering for e-mail-klient*** – markér/fjern markering af dette felt for at aktivere/deaktivere den SMTP-server, 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*). Dette felt er deaktiveret for automatisk oprettede "AutoIMAP"-servere.

- ***Logintype*** - definerer metoden til at bestemme mailserveren, der anvendes til udgående e-mail:

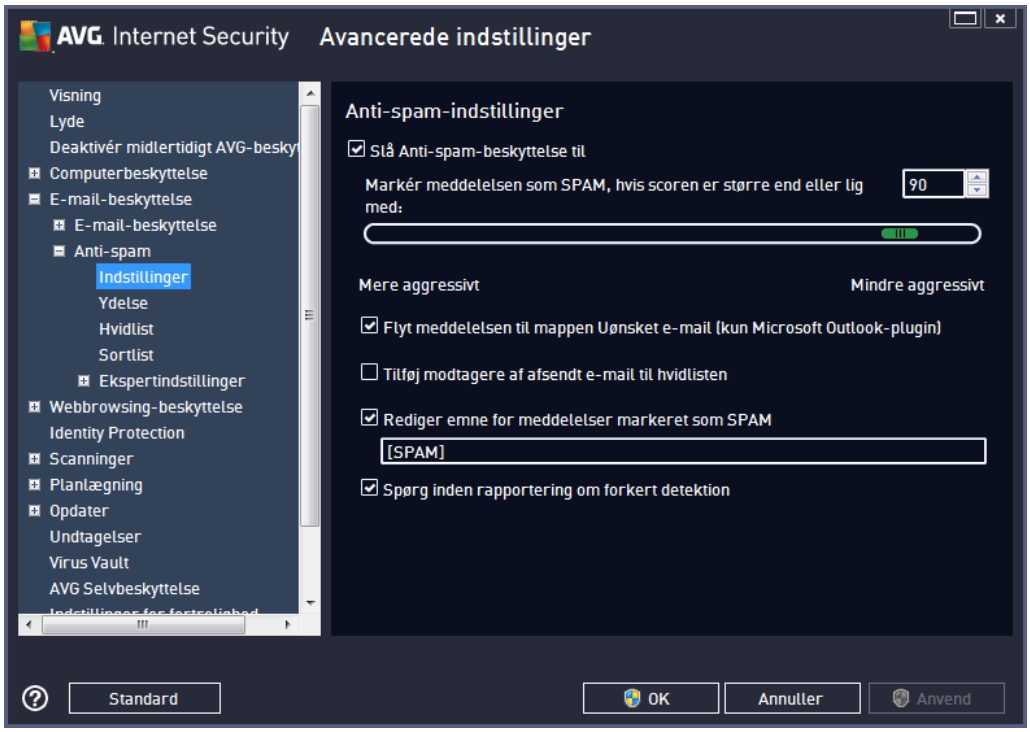
  - ***Automatisk*** – login udføres automatisk i henhold til indstillingerne i din e-mail-klient

  - ***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 en 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.
- ***E-mail-klient IMAP serveraktivering*** – markér eller fjern markeringen fra dette afkrydsningsfelt for at aktivere/deaktivere IMAP-serveren, der er specificeret ovenfor

9.5.2. Anti-spam



I dialogboksen ***Indstillinger for Anti-Spam*** kan du markere eller fjerne markeringen fra afkrydsningsfeltet ***Slå Anti-Spam-beskyttelse til*** for at tillade/blokere anti-spam-scanning af e-mailkommunikation. 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*).

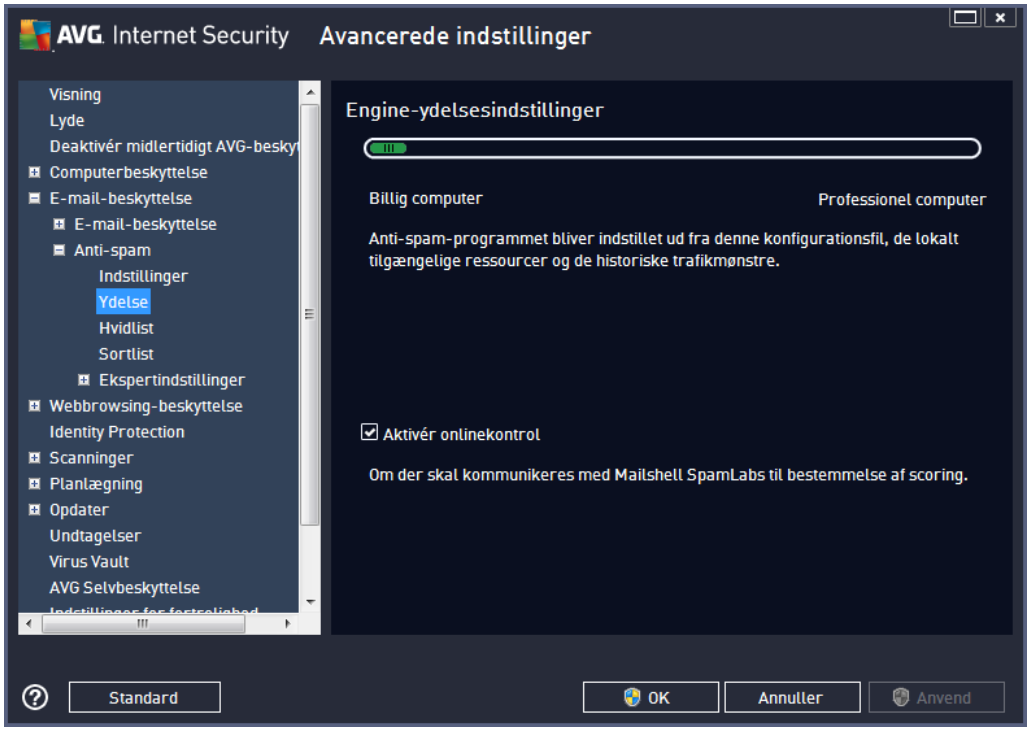
Generelt anbefaler vi, at tærsklen indstilles mellem 50 – 90, eller hvis du er meget i tvivl, til 90. Her er en generel vurdering af scoringstærsklen:

- ***Værdi 80-90*** – e-mailmeddelelser, der sandsynligvis er spam, vil blive filtreret ud. Visse ikke-spam meddelelser kan også blive filtreret fra.
- ***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 blive 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*** *(kun Microsoft Outlook-plugin)* – markér dette afkrydsningsfelt for at angive, at alle detekterede spammeddelelser automatisk skal flyttes til mappen med uønsket e-mail i din MS Outlook e-mail-klient. For tiden understøttes funktionen ikke i andre e-mail-klienter.
- ***Føj modtagere af sendte e-mails til hvidliste*** – markér dette afkrydsningsfelt for at bekræfte, at alle modtagere af sendte e-mails er pålidelige, og at alle e-mailmeddelelser, der modtages fra deres e-mailkonti, kan leveres.
- ***Rediger emne for meddelelser markeret som SPAM*** – markér dette afkrydsningsfelt, hvis du vil have, at alle meddelelser, der detekteres som spam, skal mærkes med et bestemt ord eller tegn i e-mailens emnelinje. Den ønskede tekst kan indtastes i det aktiverede tekstfelt.
- ***Spørg inden rapportering om forkert detektion*** – forudsat at du under installationsforløbet accepterede at deltage i projektet med fortrolighedsindstillinger. I så fald har du tilladt rapportering af detekterede trusler til AVG. Rapporten oprettes 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.

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 eller højre for at ændre scanningens ydelsesniveau mellem tilstandene ***Computer med høj ydelse*** / ***Computer med lav ydelse***.

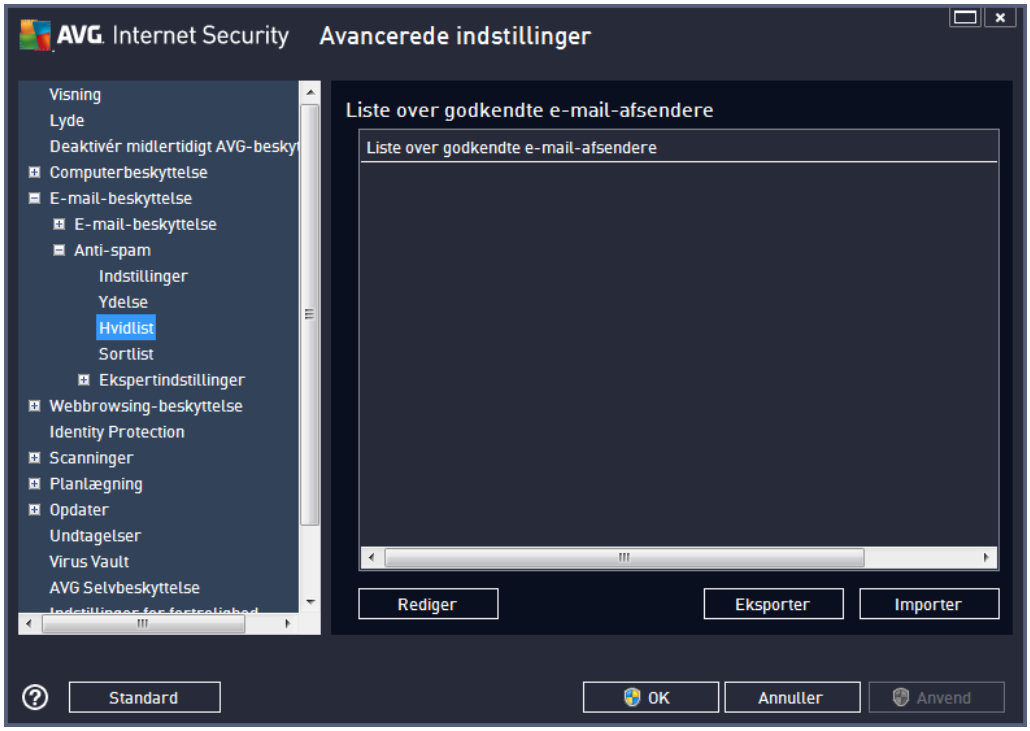
- ***Computer med lav ydelse*** – under scanningsprocessen vil der ikke blive brugt nogen regler til at identificere spam. Kun træningsdata bruges til identifikation. Denne tilstand anbefales ikke til almindelig brug, medmindre computerhardwaren er virkelig dårlig.

- ***Computer med høj ydelse*** – denne tilstand forbruger en stør 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. Kun erfarne brugere bør foretage ændringer i denne konfiguration.

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.



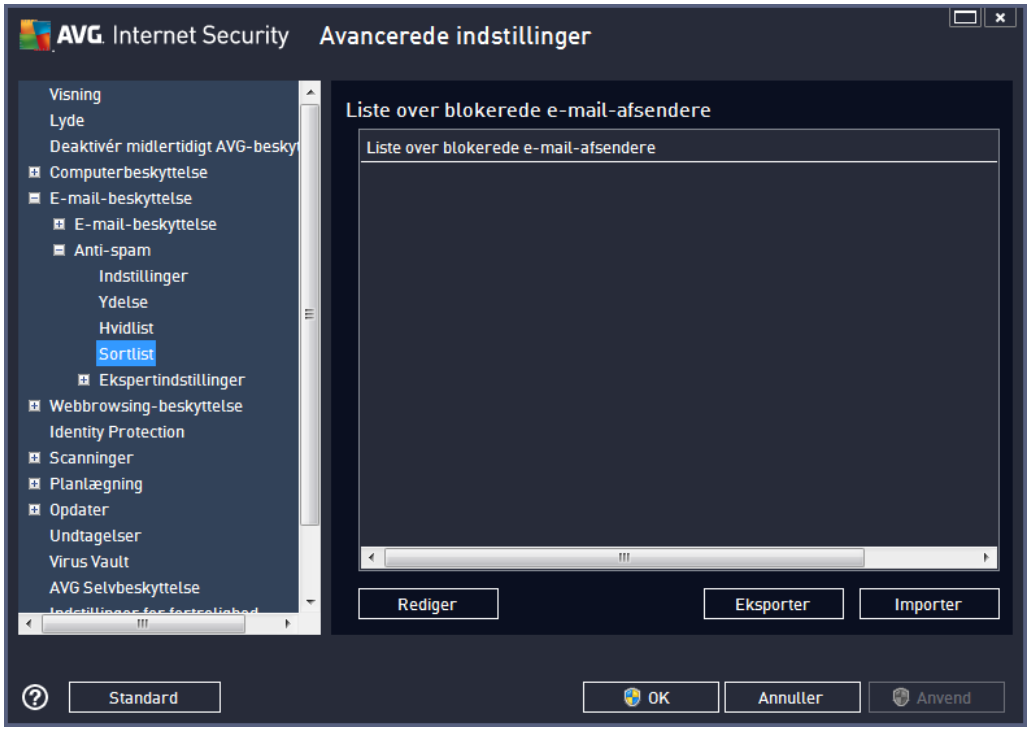
I redigeringsgrænsefladen kan du sammensætte en liste over afsendere, som du er sikker på aldrig vil sende dig uønskede meddelelser (spam). Du kan også sammensætte en liste med domænenavne (*f.eks. avg.com*), som du ved ikke genererer spammeddelelser. Når du har klargjort en sådan liste over afsendere og/eller domænenavne, kan du indtaste dem ved at bruge følgende metoder: direkte indtastning af hver e-mailadresse eller import af hele listen over adresser på én 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 har klargjort en sådan liste over afsendere og/eller domænenavne, kan du indtaste dem ved at bruge følgende metoder: direkte indtastning af hver e-mailadresse eller import af hele listen over adresser på én 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.

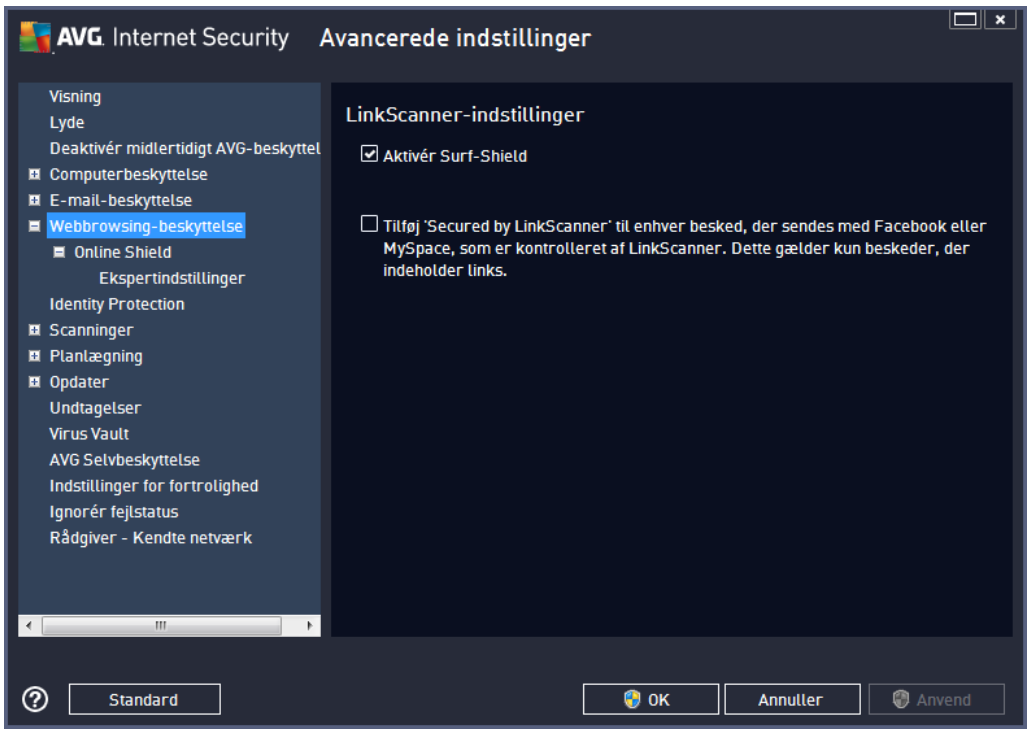
Grenen Ekspertindstillinger indeholder udvidede indstillingsmuligheder for Anti-spam-funktionen. Disse indstillinger er udelukkende beregnet til erfarne brugere, typisk netværksadministratorer, der har behov for at konfigurere antispam-beskyttelsen i detaljer for at beskytte e-mail-servere bedst muligt. 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 alle 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. I hver dialogboks finder du generelt en enkelt specifik funktion, som du kan redigere. Dens beskrivelse inkluderes altid i selve dialogboksen. Følgende parametre kan redigeres:

- ***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. Webbrowsing beskyttelse

Dialogboksen ***LinkScanner-indstillinger*** gør det muligt at markere/fjerne markering af følgende funktioner:

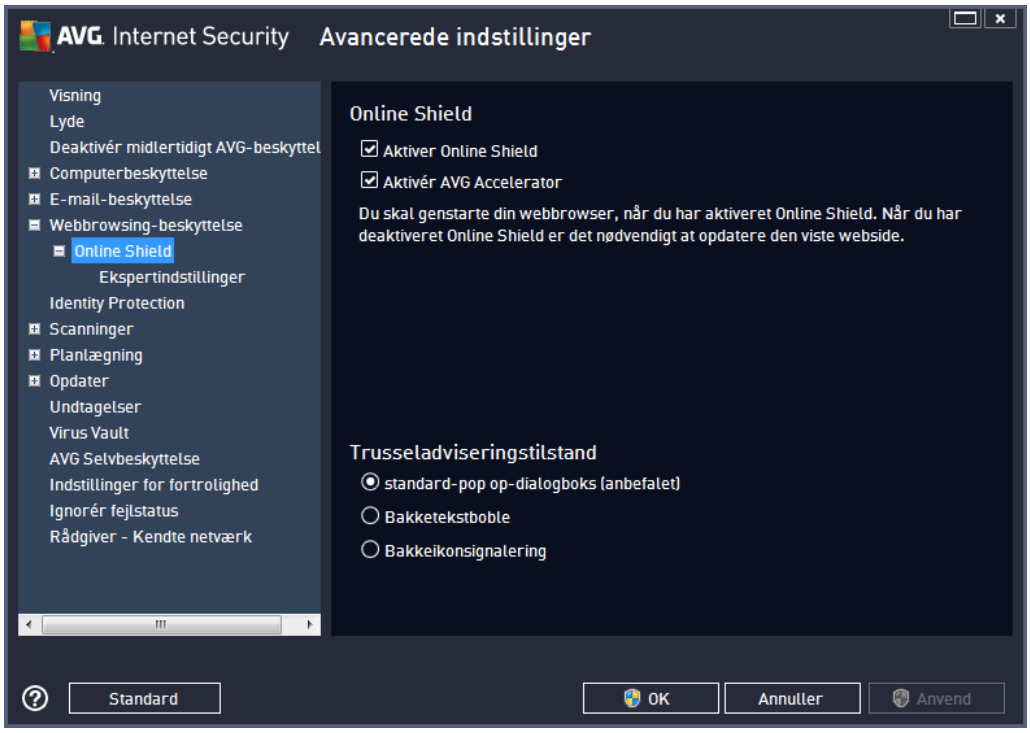


- ***Aktivér Surf-Shield*** - (*slået til som standard*): aktiv (*realtid*) beskyttelse mod udnyttende

websteder, når de besøges. Kendte skadelige webstedsforbindelser og deres udnyttende indhold blokeres, når de åbnes af brugeren via en webbrowser (*eller et andet program, der bruger HTTP*).

- ***Tilføj "Secured by LinkScanner"...*** - (*slået fra som standard*): bekræft denne indstilling for at sikre, at alle meddelelser, der sendes fra de sociale netværk Facebook/MySpace, som indeholder aktive links, certificeres som værende kontrolleret af LinkScanner.

9.6.1. Online Shield



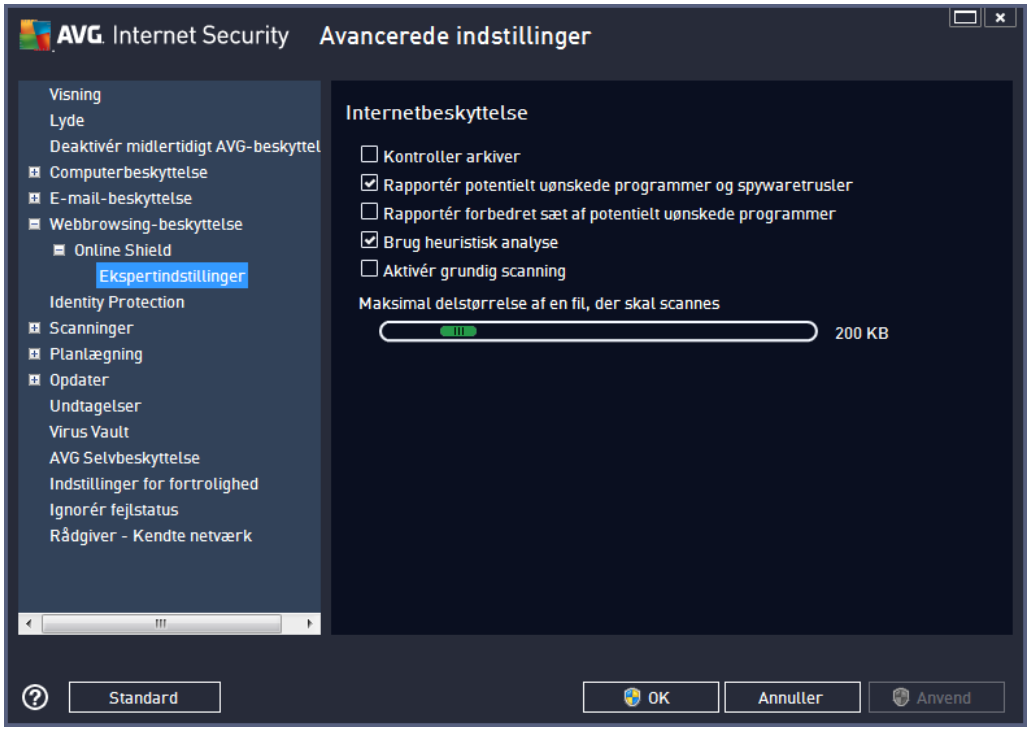
Dialogboksen ***Online Shield*** har følgende indstillinger:

- ***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*** *(slået til som standard)* – Aktivér/deaktiver AVG Accelerator-tjenesten. 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:

Trusselnotifikationstilstand

I den nederste del af dialogboksen skal du vælge den metode, der skal bruges til at give dig besked om en mulig detekteret trusse: via standard-pop-op-dialogboks, via bakketekstboble eller via proceslinjeoplysninger.



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

- ***Aktivér Internetbeskyttelse*** – denne indstilling bekræfter, at ***Online Shield*** skal foretage en scanning af internetsidens indhold. Under forudsætning af at denne indstilling er slået til (*som standard*) kan du også slå disse elementer til og 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 du lader denne funktion være 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 bestemte situationer (*mistanke om at din computer er ved at blive inficeret*) kan du markere denne indstilling for a aktivere de mest grundige scanningsalgoriter, som vil scanne selv de områder af din computer, der sjældent bliver inficeret, bare for at være helt sikker. Husk på, at denne metode kræver meget tid.

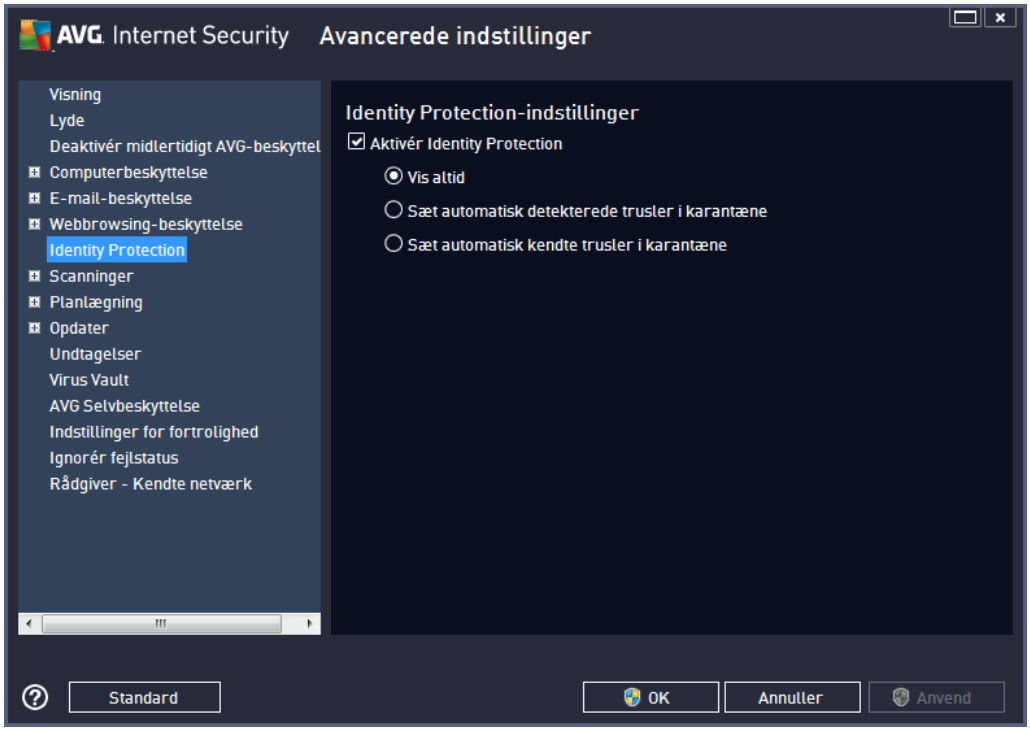
- ***Maksimal delstørrelse af en fil, der skal scannes*** – hvis der er filer på den viste side, kan du også scanne deres indhold, før de downloades til din computer. Men scanning af store filer tager lang tid, og download af websiden kan blive markant langsommere. Du kan bruge skyderen til at angive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

- ***Undlad vært/IP/domæne*** – du kan skrive 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*** i tekstfeltet. Udeluk derfor kun værter, som du er helt sikker på, aldrig ville indeholde skadeligt webstedsindhold.

9.7. Identitetsbeskyttelse

Identitetsbeskyttelse er en antimalware-komponent, der beskytter dig mod alle former for malware (*spyware, bots, identitetstyveri, ...*) ved hjælp af adfærdsteknologi og yder beskyttelse mod nye vira fra dag nul *(du kan få en detaljeret beskrivelse af komponentens funktionalitet ved at se kapitlet Identitetsbeskyttelse*).

Dialogboksen til indstillingerne for ***Identitetsbeskyttelse*** giver dig mulighed for at slå de elementære funktioner i komponenten Identitetsbeskyttelse til/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 angive, at alle muligt detekterede trusler skal flyttes til den sikre del af Virus Vault med det samme. Hvis du bevarer standardindstillingerne, bliver du, når en trussel detekteres, spurgt, om den skal flyttes i karantæne, for at sikre at ingen applikationer, du ønsker at køre, bliver fjernet.
- ***Sæt automatisk kendte trusler i karantæne*** – hold dette element markeret, hvis alle programmer, der detekteres som potentiel malware, automatisk og øjeblikkeligt skal flyttes til Virus Vault.

9.8. Scanninger

De avancerede scanningsindstillinger inddeles i fire kategorier, der angiver bestemte scanningstyper, sådan som de er defineret af softwareleverandøren:

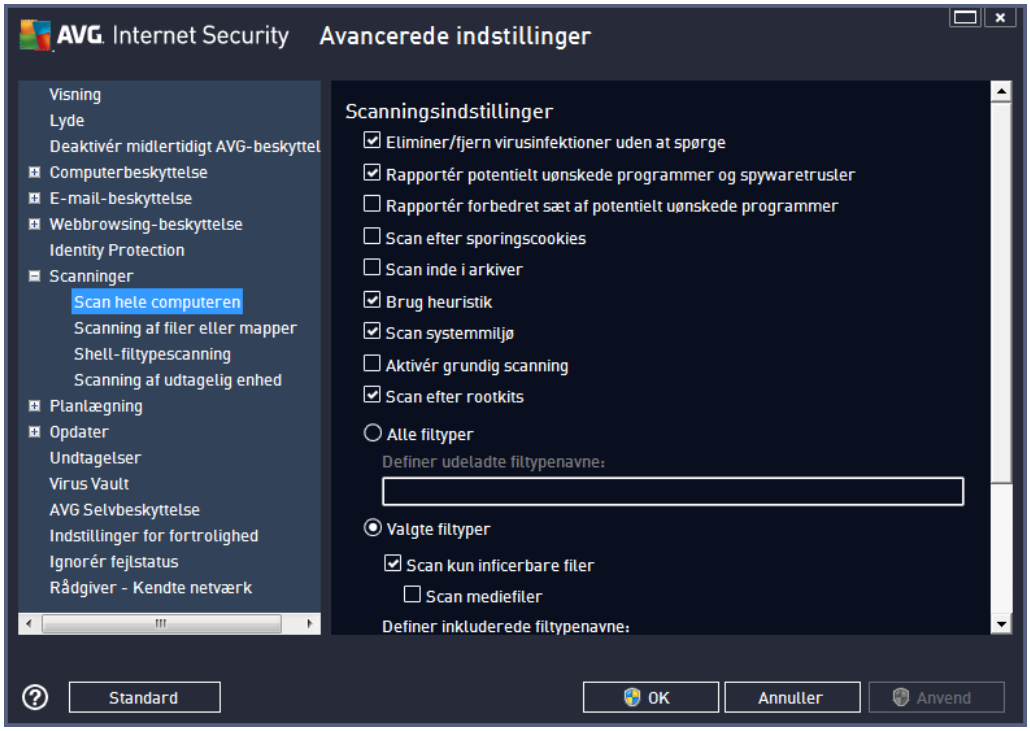
- ***Scan hele computeren*** – foruddefineret standardscanning af hele computeren
- ***Shell-udvidelsesscanning*** – bestemt scanning af et udvalgt objekt direkte fra Windows

Stifinder

- ***Scanning af filer eller mapper*** – foruddefineret standardscanning af udvalgte områder på computeren
- ***Scanning af udtagelig enhed*** – bestemt scanning af udtagelige enheder, der er sat i computeren

9.8.1. 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 virusinfektion uden at spørge mig*** (*slået til som standard*) – Hvis en virus identificeres under scanningen, kan den helbredes automatisk, hvis der findes en kur. Hvis den inficerede fil ikke kan helbredes automatisk, flyttes det inficerede objekt til Virus Vault.
- ***Rapportér potentielt uønskede programmer og spywaretrusler*** (*slået til som standard*) – markér for at aktivere scanning efter spyware og vira. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler, at du lader denne funktion være aktiveret, da den øger computersikkerheden.

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*) – markér indstillingen for at registrere udvidede spywarepakker: 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 angiver, at cookies skal detekteres; (*HTTP-cookies bruges til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på webstedet eller indholdet i deres elektroniske indkøbsvogne*)

- ***Scan inde i arkiver*** (*slået fra som standard*) – denne parameter angiver, at scanningen skal kontrollere alle filer, der er gemt 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 bestemte situationer (*mistanke om at din computer er ved at blive inficeret*) kan du markere denne indstilling for at aktivere de mest grundige scanningsalgoritmer, som vil scanne selv de områder af din computer, der sjældent bliver inficeret, bare for at være helt sikker. Husk på, at denne metode kræver meget tid.

- ***Scan efter rootkits*** (*slået til som standard*) – Anti-Rootkit-scan søger i din computer efter mulige rootkits, f.eks. programmer eller teknologier, som kan skjule malware i 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.

Du skal også beslutte, om der skal scannes

- ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en liste over kommaseparerede (*efter lagringen ændres kommaerne til semikoloner*) filtypenavne, der ikke skal scannes;

- ***Valgte filtyper*** – Du kan angive, om du vil scanne filer, der kan inficeres(*filer, der ikke kan inficeres, scannes ikke, det kan f.eks. være visse filer, som er almindelig tekst, eller visse ikke-eksekverbare filer*), herunder mediefiler (*video-, lydfiler – hvis du ikke markerer dette felt, reducerer det scanningstiden endnu mere, fordi disse filer ofte er ret store og sandsynligvis ikke er inficeret med virus*). Igen kan du angive ud fra filtypenavne, hvilke filer der altid skal scannes.

- 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

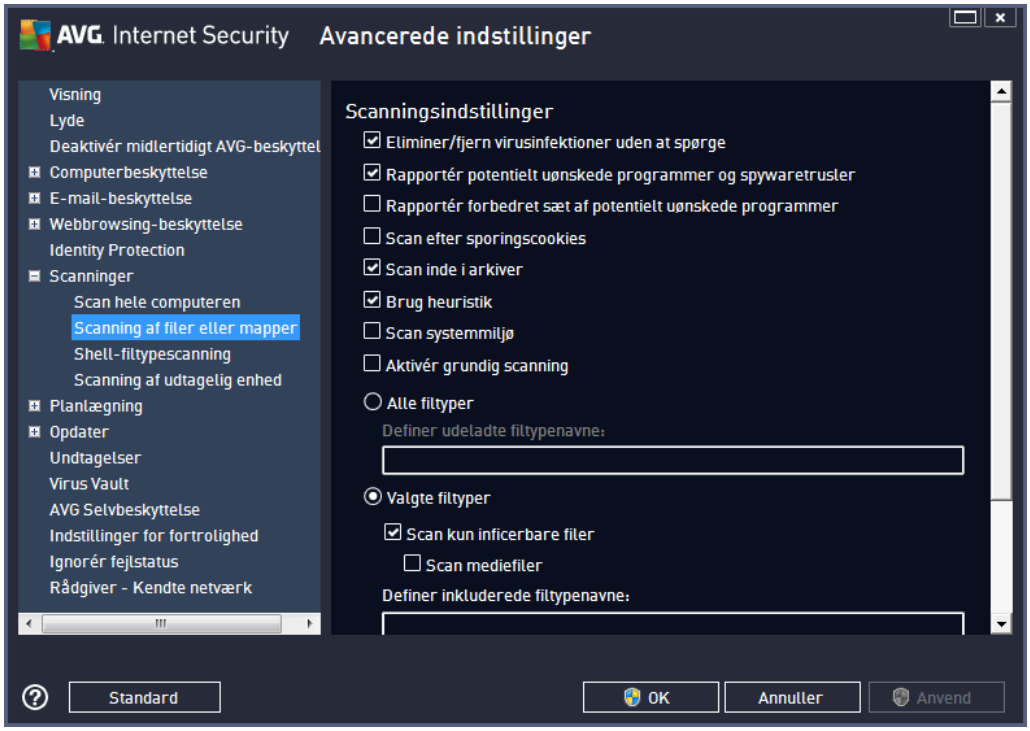
I sektionen ***Indstil hvor hurtigt scanningen fuldføres*** kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne indstillingsværdi sat til *brugerfølsomt* niveau af automatisk ressourceforbrug. Hvis du ønsker at scanningen skal køre hurtigere, tager den kortere tid, men de anvendte systemressourcer vil blive øget markant under scanningen og gøre dine andre aktiviteter på pc'en langsommere (*denne indstilling kan bruges, når din computer er tændt, men ingen arbejder på den i øjeblikket*). Omvendt kan du også reducere de anvendte systemressourcer ved at udvide varigheden af scanningen.

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:

9.8.2. Scanning af 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:

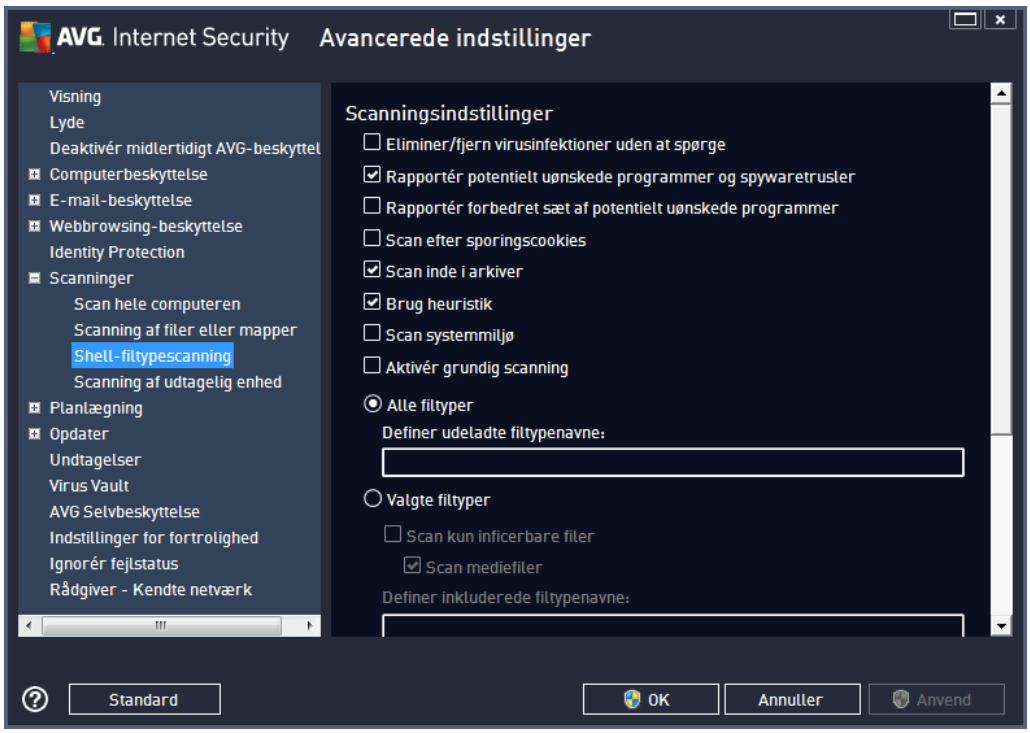


Alle de parametre, der er angivet i denne konfigurationsdialogboks, gælder kun for de områder, der er udvalgt til scanning ved hjælp af Scanning af specifikke filer eller mapper!

Bemærk: *Du kan få en beskrivelse af specifikke parametre i kapitlet AVG Avancerede indstillinger/ Scanninger/Scan hele computeren.*

9.8.3. 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 er konfigurationen relateret til scanning af specifikke objekter, der startes direkte fra Windows Stifinder-miljøet (*shell-udvidelse*), se kapitlet Scanning i Windows stifinder:



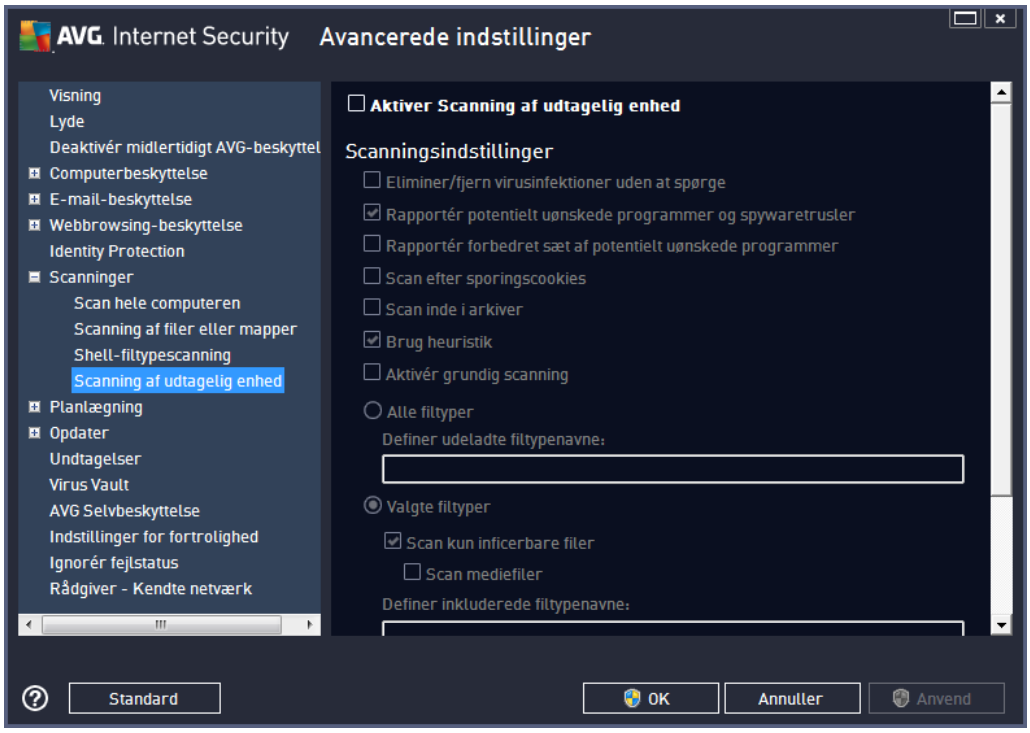
Parameterlisten er magen til listerne for Scanning af hele computeren. Standardindstillingerne varierer imidlertid (*f.eks. kontrollerer Scanning af hele computeren som standard ikke arkiverne, men den scanner systemmiljøet, og det samme gælder for Shell-udvidelsesscanning*).

Bemærk: *Du kan få en beskrivelse af specifikke parametre i kapitlet AVG Avancerede indstillinger/ Scanninger/Scan hele computeren.*

Sammenlignet med dialogboksen Scan hele computeren indeholder dialogboksen ***Shell-udvidelsesscanning*** også sektionen ***Andre indstillinger, der er relateret til AVG-brugergrænsefladen***, hvor du kan angive, om scanningsstatussen og scanningsresultaterne er tilgængelige i AVG-brugergrænsefladen. Du kan også angive, at scanningsresultatet kun vises, hvis der er detekteret en infektion under scanningen.

9.8.4. 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. Hvis denne scanning skal være klar og igangsættes automatisk, når der er brug for det, skal du markere indstillingen ***Aktivér scanning af flytbar enhed***.

Bemærk: *Du kan få en beskrivelse af specifikke parametre i kapitlet AVG Avancerede indstillinger/ Scanninger/Scan hele computeren.*

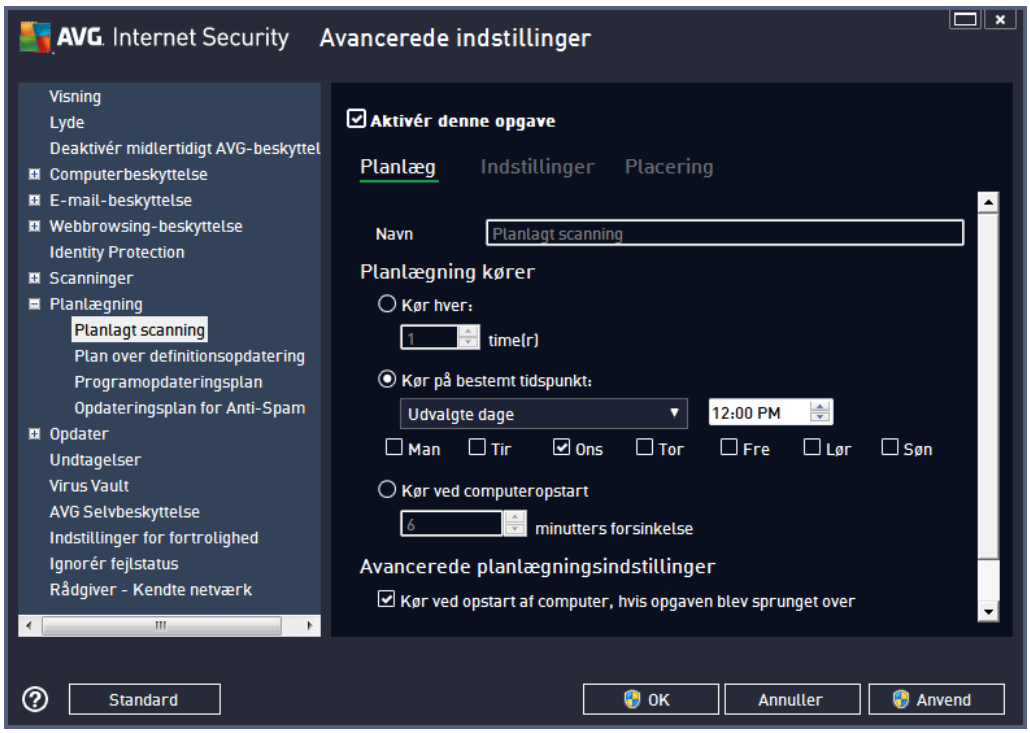
9.9. Planlægning

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

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

9.9.1. Planlagt scanning

Parametrene for den planlagte scanning kan redigeres (*eller en ny planlægning kan konfigureres*) op 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:



Derefter angiver tekstfeltet ***Navn*** (*deaktiveret for alle standardplaner*) det navn, som programleverandøren har tildelt til netop denne plan. Når det gælder planer, der er tilføjet for nylig (*du kan tilføje en ny plan ved at højre klikke over punktet* ***Planlagt scanning*** *i det venstre navigationstræ*), kan du angive dit eget navn, og i dette tilfælde kan du redigere tekstfeltet. Prøv altid at bruge korte, beskrivende og passende navne til scanninger, så det senere er nemme at skelne mellem scanningerne.

Eksempel: *Det er ikke en god ide at kalde scanningen "Ny scanning" eller "Min scanning", fordi disse navne ikke angiver, hvad scanningen rent faktisk kontrollerer. På den anden side kunne et eksempel på et godt beskrivende navn være "Systemområdescanning" osv. I scanningsnavnet er det heller ikke nødvendigt at angive, om det er en scanning af hele computeren eller blot en scanning af bestemte filer eller mapper – dine egne scanninger vil altid være en bestemt udgave af Scan specifikke filer eller mapper.*

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

Planlægning kører

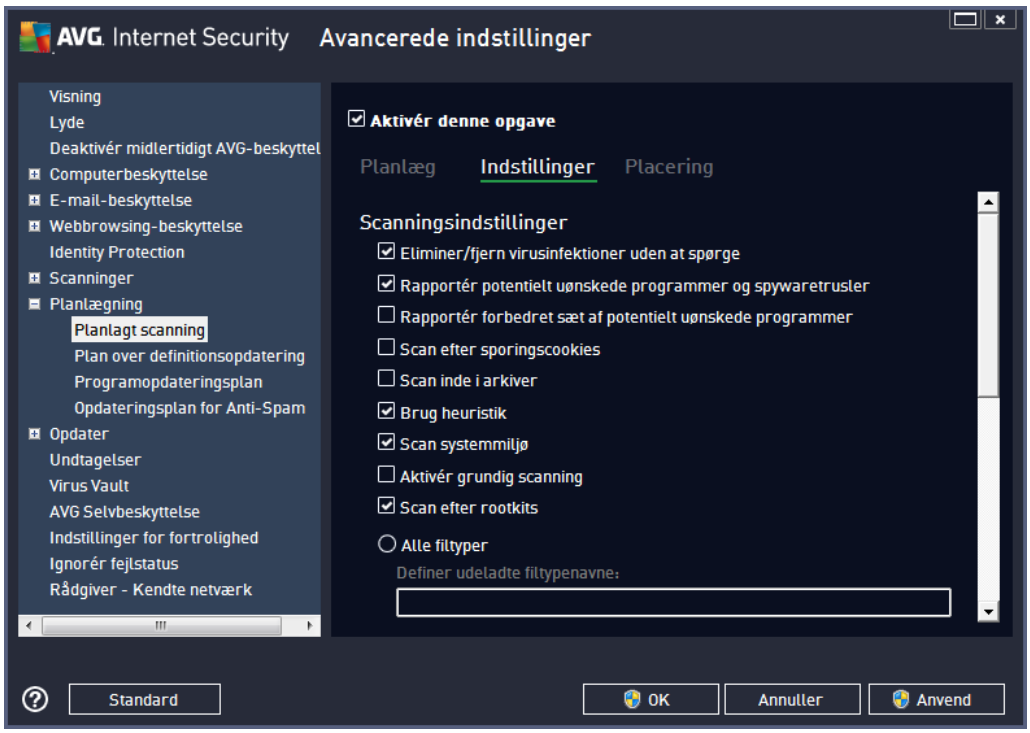
Her kan du angive tidsintervaller for kørsel af den nyplanlagte scanning. Tidsindstillingen kan enten defineres via den gentagne scanningsstart efter et bestemt tidsrum (***Kør hver ...***) eller ved at definere en præcis dato og et bestemt klokkeslæt (***Kør med bestemte mellemrum...***) eller muligvis 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 ***Indstillinger*** er der en liste over scanningsparametre, der valgfrit kan slås til/fra. Som standard er de fleste parametre slået til, og funktionaliteten anvendes under scanningen. ***Medmindre du har en god grund til at ændre disse indstillinger, anbefaler vi at bevare den forudindstillede konfiguration***:

- ***Helbred/fjern virusinfektion uden at spørge mig*** *(slået til som standard):* Hvis en virus identificeres under scanningen, kan den helbredes automatisk, hvis der findes en kur. Hvis den inficerede fil ikke kan helbredes automatisk, flyttes det inficerede objekt til Virus Vault.

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

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*): markér afkrydsningsfeltet 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*): dette parameter definerer, at cookies skal detekteres under scanningen (*HTTP-cookies bruges til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på webstedet eller indholdet i deres elektroniske indkøbsvogne*).

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

- ***Brug heuristik*** (*slået til som standard*): Heuristisk analyse (*dynamisk emulering af det scannede 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 (*hvis der er mistanke om, at din computer er inficeret*) kan du markere denne valgmulighed for at aktivere de mest dybdegående scanningsalgoritmer, som vil scanne selv de områder på computeren, der egentlig ikke kan blive inficeret, men bare for at være sikker. Husk på, at denne metode kræver meget tid.

- ***Scan efter rootkits*** *(slået til som standard):* Anti-rootkit-scan søger i din computer efter mulige rootkits, f.eks. programmer eller teknologier, som kan skjule malware i 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.

Du skal også beslutte, om der skal scannes

- ***Alle filtyper*** med mulighed for at definere undtagelser fra scanningen ved at angive en liste over kommaseparerede (*efter de er blevet gemt, ændres kommaerne til semikolonner*) filtypenavne, der ikke skal scannes;

- ***Valgte filtyper*** – du kan specificere, at der kun skal scannes efter filer, der kan blive inficeret (*filer, der ikke kan blive inficeret, scannes ikke, f.eks. almindelige tekstfiler eller andre ikke-eksekverbare filer*), herunder mediefiler (*video, lydfiler – hvis du ikke markerer dette felt, reduceres scanningstiden yderligere, fordi disse filer ofte er meget store og typisk ikke er inficeret med en virus*). Igen kan du angive ud fra filtypenavne, hvilke filer der altid skal scannes.

- 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

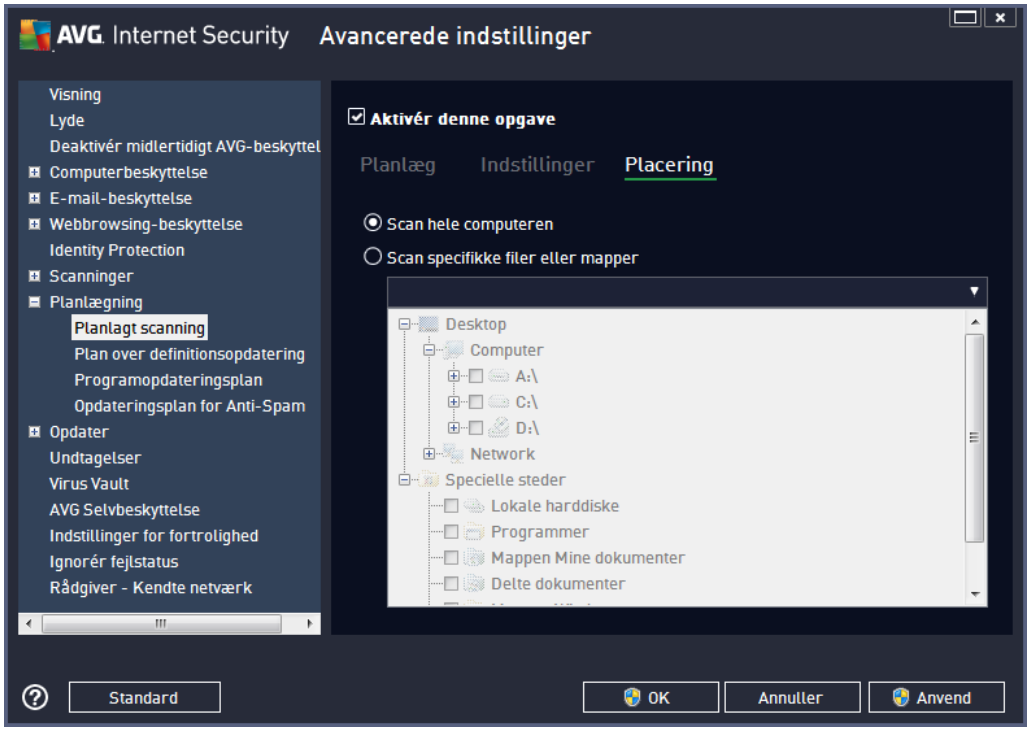
I denne sektion kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne værdi indstillet til niveauet *brugerfølsom* af automatisk ressourceforbrug. Hvis du vil have scanningen til at køre hurtigere, tager det kortere tid, men forbruget af systemressourcer øges markant under scanningen og gør de andre aktiviteter på pc'en langsommere (*denne indstilling kan anvendes, når computeren er tændt, uden der i øjeblikket 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:

Computerlukningsmuligheder

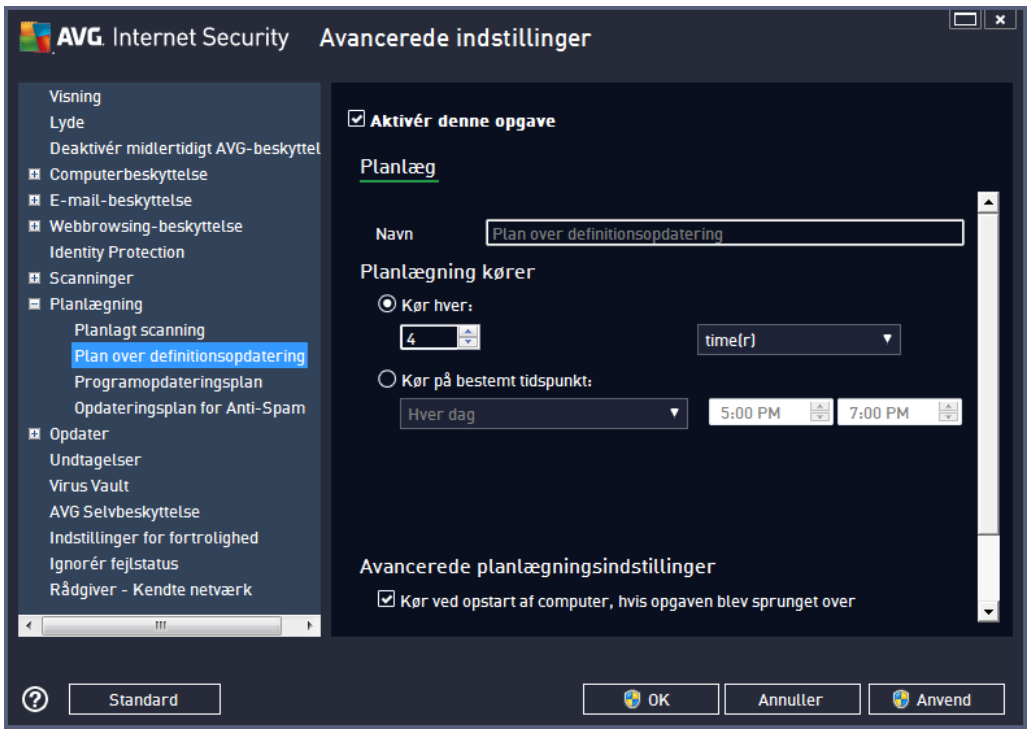
I sektionen ***Computerlukningsmuligheder*** kan du angive, om computeren skal lukkes automatisk, når scanningsprocessen er gennemført. Når denne indstilling er bekræftet (***Luk computeren, når scanningen er gennemført***), aktiveres en ny indstilling, som gør det muligt at lukke computeren, selvom den i øjeblikket er låst (***Gennemtving lukning, hvis computeren er låst***).



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

9.9.2. 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 dialogboks kan du konfigurere visse detaljerede parametre for plan for definitionsopdatering. Tekstfeltet ***Navn*** (*slået fra for alle standardplaner*) viser det navn, som programleverandøren har 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

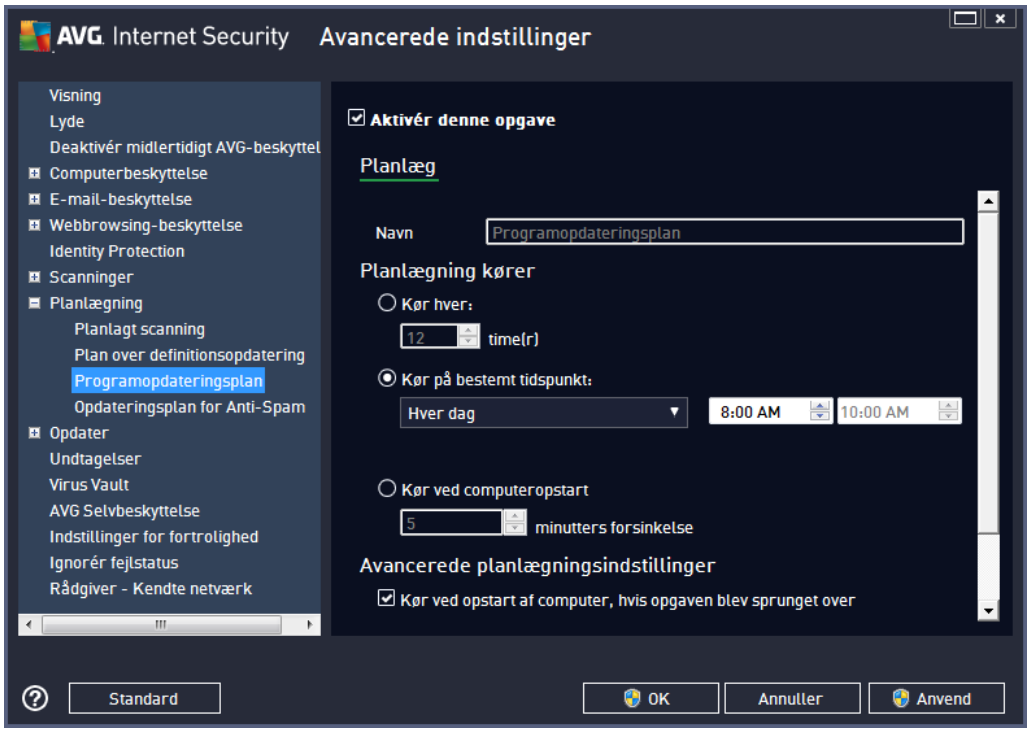
I denne sektion kan du definere, under hvilke betingelser definitionsopdateringen skal/ikke skal starte, hvis computeren er i strømsparetilstand eller helt slukket.

Andre opdateringsindstillinger

Markér til sidst indstillingen ***Kør opdateringen igen, så snart der er forbindelse til internettet*** for at sikre, at hvis internetforbindelse afbrydes, og opdateringsprocessen mislykkes, så startes den igen med det samme, når internetforbindelsen er genoprettet. Når den planlagte opdatering er startet på det angivne tidspunkt, får du en besked om dette via et pop op-vindue, der åbnes over AVG-proceslinjeikonet (*under forudsætning af at du har bevaret standardkonfigurationen i dialogboksen Avancerede indstillinger/Visning*).

9.9.3. 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:



Tekstfeltet ***Navn*** (*deaktiveret for alle standardplaner*) viser navnet, der er tildelt netop denne plan af programleverandøren.

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

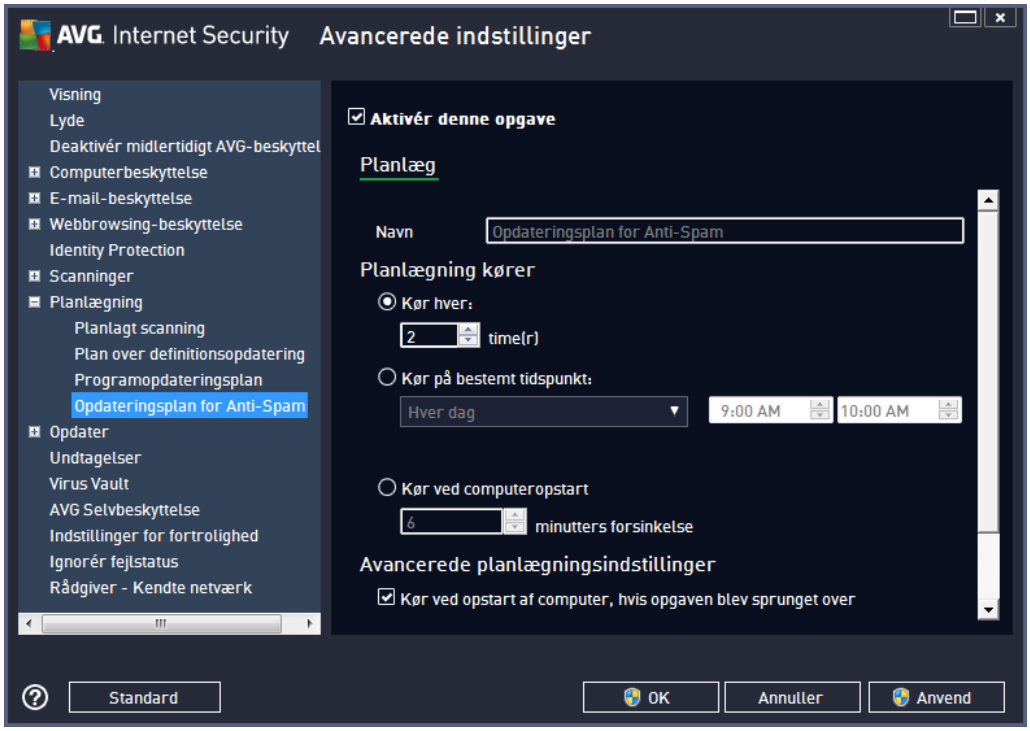
Kontrollér indstillingen ***Kør opdateringen igen, så snart der er forbindelse til internettet,*** for at sikre, at hvis internetforbindelse afbrydes, og opdateringen mislykkes, startes den igen, så snart internetforbindelsen er genoprettet. Når den planlagte opdatering køres på det angivne tidspunkt,

bliver du informeret om det med et popup-vindue, der åbnes over AVG-proceslinjeikonet (*forudsat du har bevaret standardkonfigurationen i dialogboksen Avancerede indstillinger/Visning*).

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

9.9.4. 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. Tekstfeltet, der hedder ***Navn*** (*deaktiveret for al standardplanlægning*) angiver det navn, der er knyttet til denne bestemte planlægning af softwareleverandøren.

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.

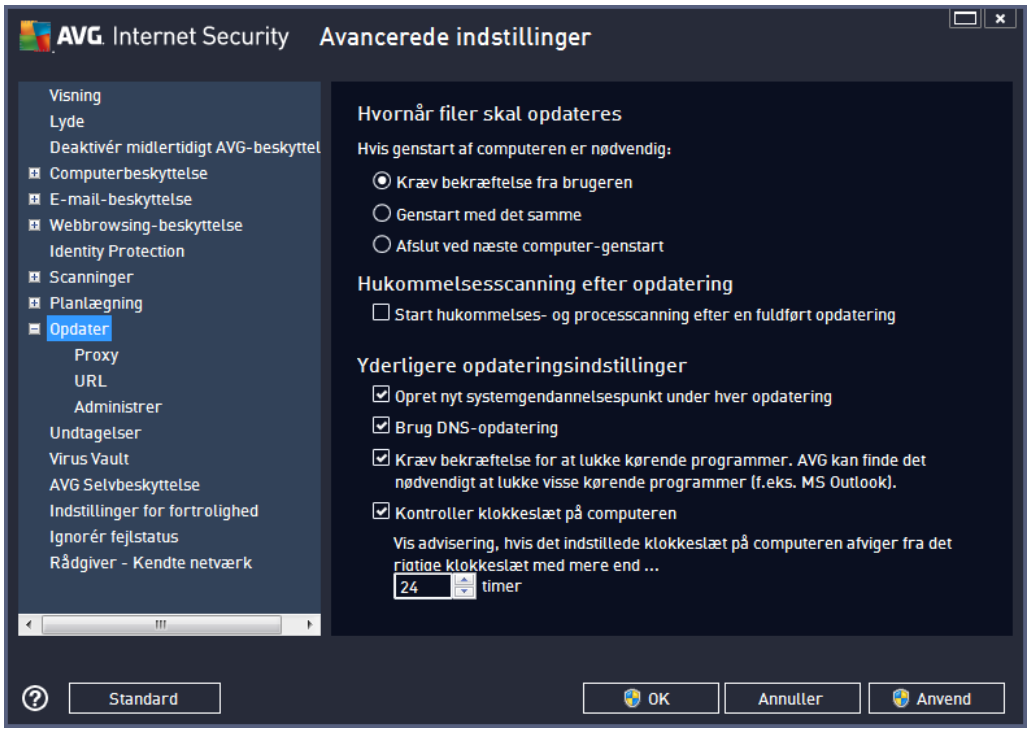
Andre opdateringsindstillinger

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 herom med et pop op-vindue, der åbnes over AVG-procesikonet (*forudsat at du har bevaret standardkonfigurationen i dialogboksen Avancerede indstillinger/Visning*).

9.10. 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 tre forskellige indstillinger, der kan bruges, hvis opdateringsprocessen kræver, at din pc skal genstartes. 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. Husk, at denne indstilling kun anbefales, hvis du er sikker på, at computeren genstartes regelmæssigt, mindst én gang om dagen!

Hukommelsesscanning efter opdatering

Markér dette afkrydsningsfelt for at angive, at du vil starte en ny hukommelsesscanning, hver gang der er udført en opdatering. Den senest hentede opdating kan indeholde nye virusdefinitioner, og disse kunne anvendes med det samme under scanningen.

Yderligere opdateringsindstillinger

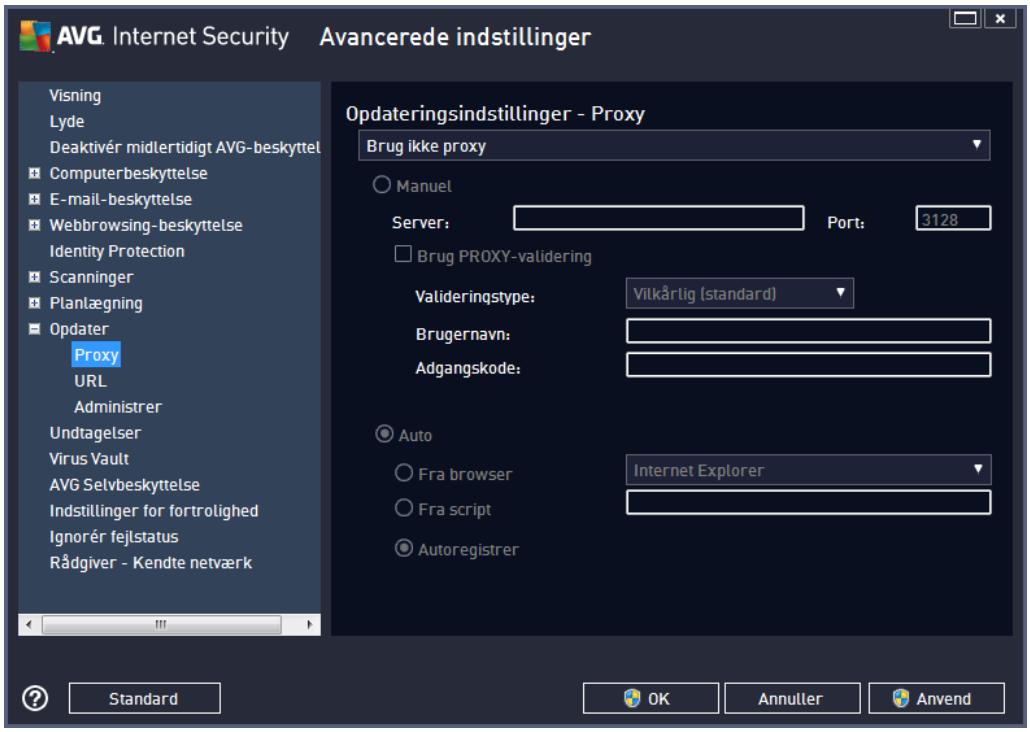
- ***Opret nyt systemgendannelsespunkt i løbet af hver programopdatering*** – før hver AVG programopdatering oprettes et systemgendannelsespunkt. Hvis opdateringsprocessen mislykkes, og operativsystemet bryder ned, kan du altid gendanne dit operativsystem til dets oprindelige konfiguration fra dette sted. Denne indstilling er tilgængelig via Start/Alle programmer/Tilbehør/Systemværktøjer/Systemgendannelse, men det anbefales, at eventuelle ændringer kun foretages af erfarne brugere! Hold dette afkrydsningsfelt markeret, hvis du ønsker at bruge denne funktion.

- ***Brug DNS-opdatering*** (*slået til som standard*) – når denne indstilling er markeret, vil dit **AVG Internet Security 2013** søge efter oplysninger om den seneste virusdatabaseversion og den 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 programmer*** (*slået til som standard*) – denne indstilling gør det muligt at sikre, at programmer, der aktuelt er åbne, ikke kan lukkes uden din tilladelse – hvis det er nødvendigt for at færdiggøre opdateringsprocessen.

- ***Kontroller klokkeslæt på computeren*** – markér denne indstilling for at angive, at du ønsker at få vist en besked, hvis computerens tid afviger fra den rigtige tid med mere end et angivet antal timer.

9.10.1. 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 ikke proxy*** – standardindstillinger
- ***Brug proxy***
- ***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.

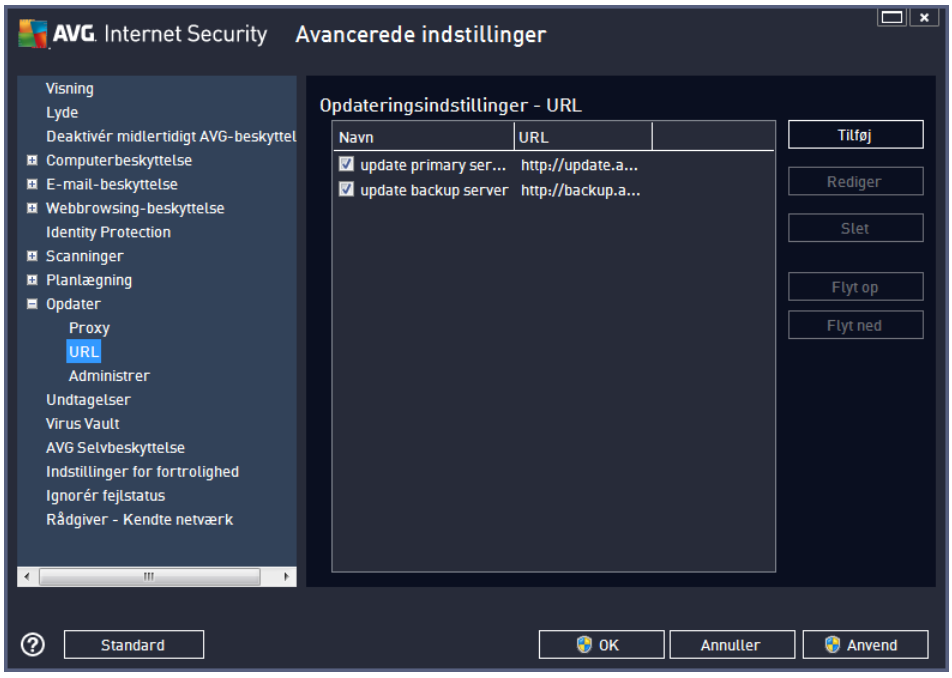
Automatisk konfiguration

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

9.10.2. URL

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



Betjeningsknapper

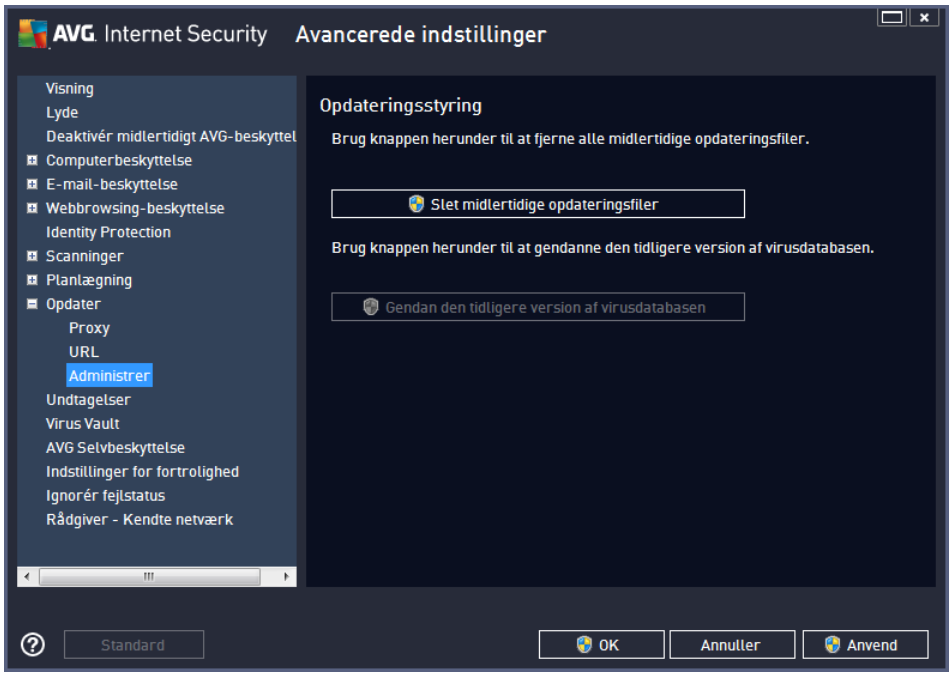
Listen og dens elementer kan ændres vha. nedenstående betjeningsknapper:

- ***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

9.10.3. Administrer

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

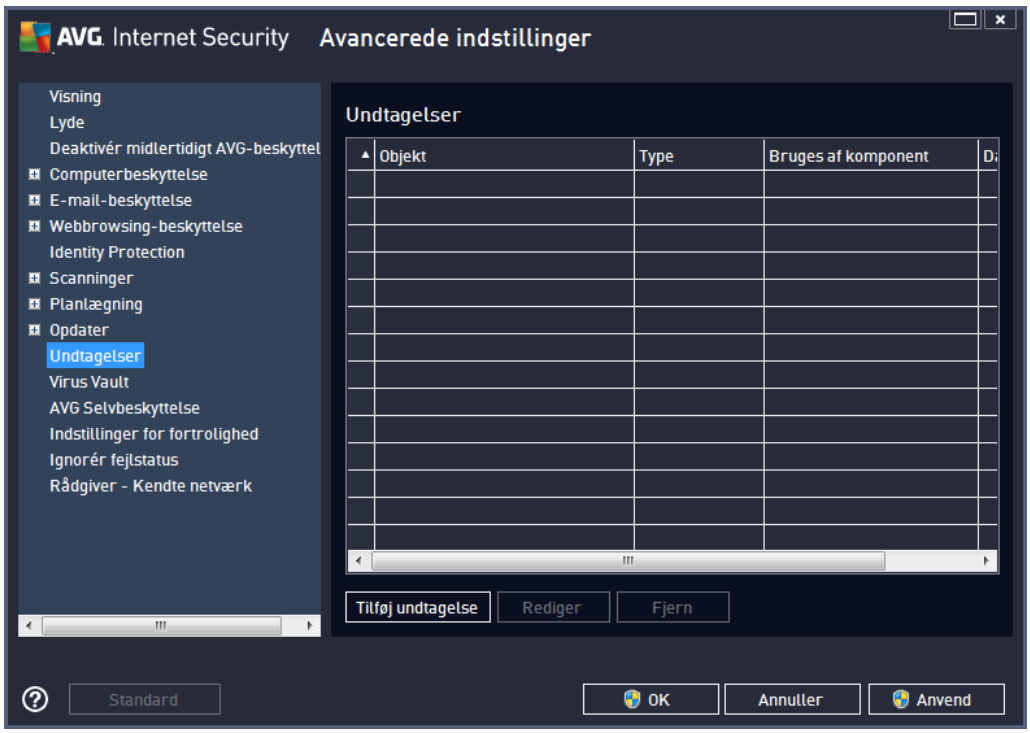


- ***Slet midlertidige opdateringsfiler*** – tryk på denne knap for at slette alle unødvendige opdateringsfiler fra din harddisk (*som standard gemmes disse filer i 30 dage*)
- ***Gendan tidligere version af virusdatabasen*** – tryk på denne knap for at slette den seneste virusdatabaseversion fra din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

9.11. Undtagelser

I dialogboksen ***Undtagelser*** kan du definere undtagelser, dvs. elementer som **AVG Internet Security 2013** vil ignorere. Typisk skal du skulle definere en undtagelse, hvis AVG bliver ved med at detektere et program eller en fil som en trussel eller blokere et sikkert websted som farligt. Føj en sådan fil eller websted til undtagelseslisten, så vil AVG ikke længere rapportere eller blokere den.

Du bør altid sikre dig, at den pågældende fil, program eller website er fuldstændigt sikkert!



Tabellen i dialogboksen viser en liste over undtagelser, hvis en eller flere allerede er blevet defineret. Der er et afkrydsningfelt ud for hvert element. Hvis afkrydsningsfeltet er markeret, er undtagelsen aktiv. Hvis ikke, er undtagelsen kun defineret, men ikke anvendt. Ved at klikke på kolonneoverskriften kan du sortere de tilladte elementer iht. de pågældende kriterier.

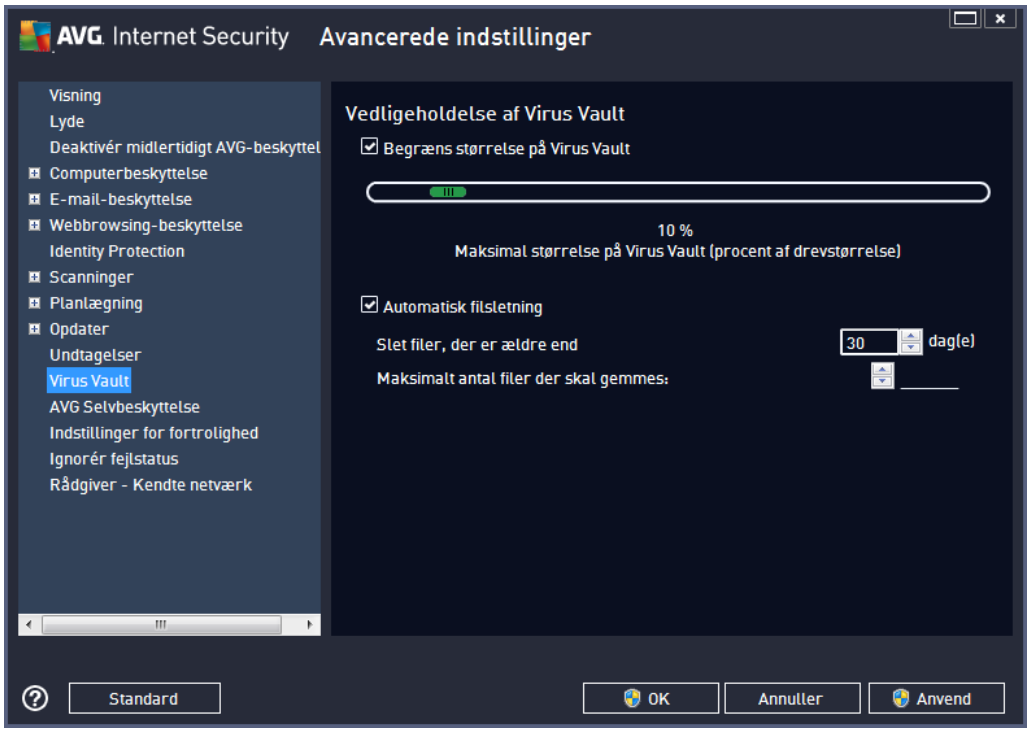
Betjeningsknapper

- ***Tilføj undtagelse*** – klik for at åbne en ny dialogboks, hvor du kan angive det element, der skal ekskluderes fra AVG-scanningen. Først inviteres du til at definere objektets type, dvs. om det er en fil, en mappe eller en URL. Derefter skal du gennemse din disk for at angive stien til det pågældende objekt eller indtaste URL-adressen. Til sidst kan du vælge, hvilke AVG-funktioner der skal ignorere det valgte objekt *(Resident Shield, Identity, Scan, Anti-Rootkit)*.

- ***Rediger*** – denne knap er kun aktiv, hvis der allerede er blevet defineret nogle undtagelser, og de vises på tabellen. Derefter kan du bruge knappen til at åbne redigeringsdialogboksen over en valgt undtagelse og konfigurere parametrene for undtagelsen.

- ***Fjern*** – brug denne knap til at annullere en tidligere defineret undtagelse. Du kan enten fjerne dem en efter en eller markere en blok af undtagelser på listen og annullere de definerede undtagelser. Efter at undtagelsen er blevet annulleret, kontrollerer AVG den pågældende fil, mappe eller URL igen. Bemærk, at det kun er undtagelsen, der fjernes, ikke selve filen eller mappen!

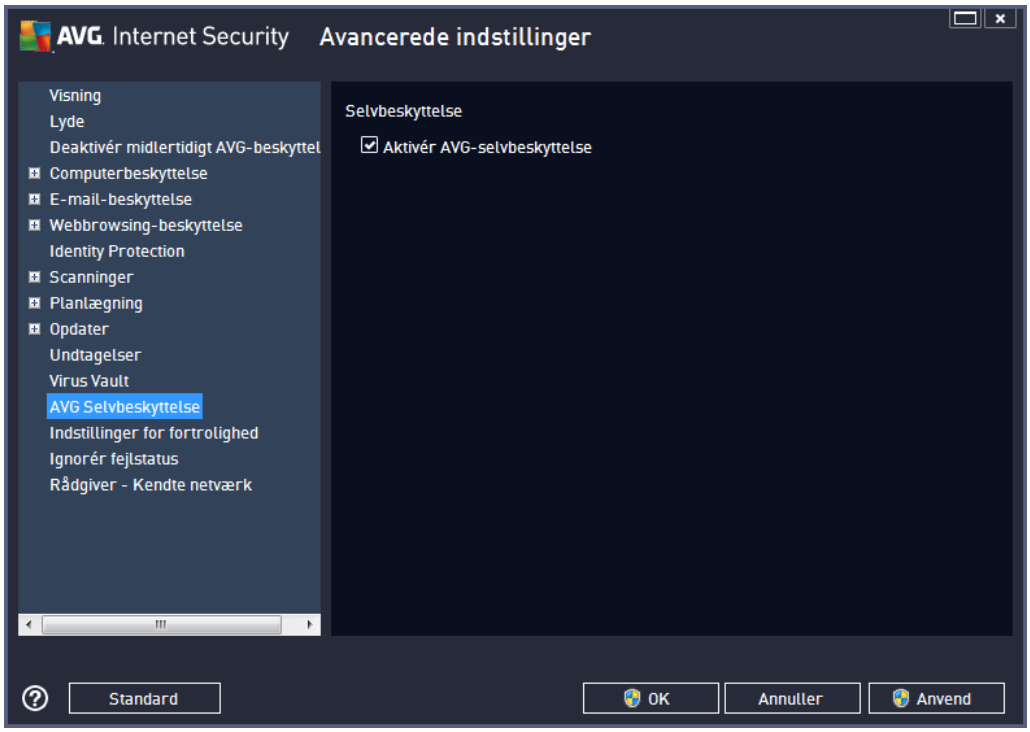
9.12. Virus Vault



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

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

9.13. AVG Self Protection

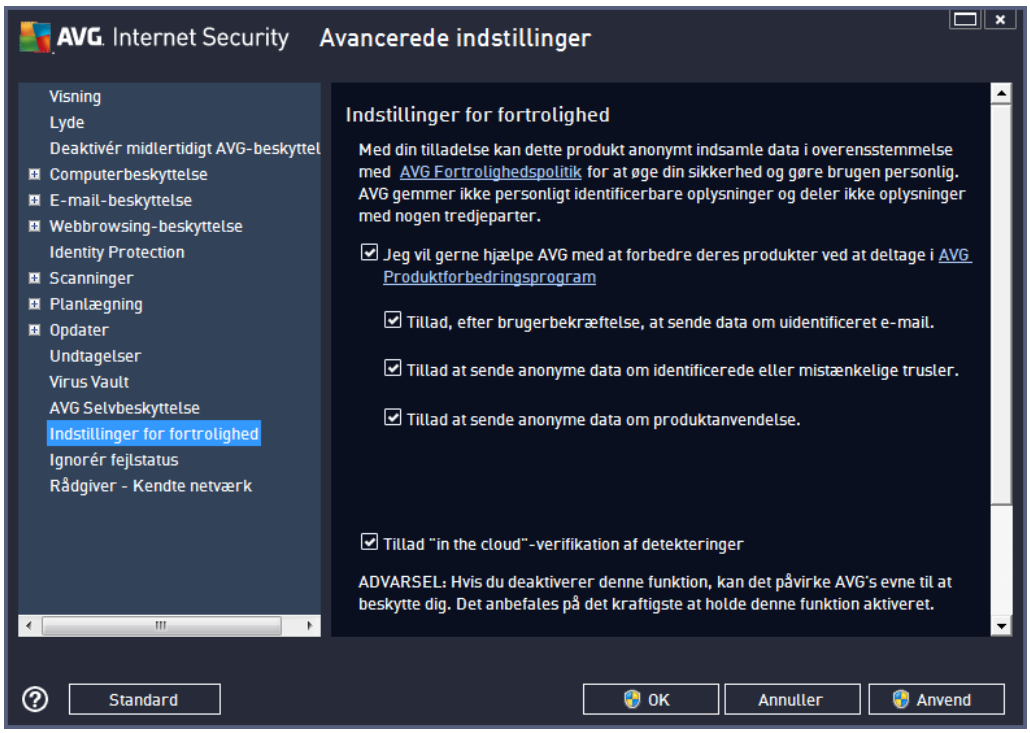


AVG Self Protection giver **AVG Internet Security 2013** mulighed for at beskytte dens egne processer, filer, registreringsdatabasenøgler og drivere mod at blive ændret eller deaktiveret. Den primære årsag til denne type beskyttelse er, at nogle sofistikerede trusler forsøger at afvæbne anti-virusbeskyttelsen for derefter frit at beskadige din computer.

Vi anbefaler, at denne funktion er aktiveret!

9.14. Indstillinger for fortrolighed

Dialogboksen ***Indstillinger for fortrolighed*** inviterer dig til at deltage i AVG-produktforbedring og hjælpe os med at forbedre den overordnede internetsikkerhed. Din rapportering hjælper os med at indsamle opdaterede oplysninger fra alle deltagere verden over om de seneste trusler, så vi til gengæld kan forbedre beskyttelsen for alle. Rapporteringen sker automatisk og er derfor ikke til ulejlighed for dig. Der inkluderes ingen personlige data i rapporterne. Rapportering af detekterede trusler er valgfri, men vi anmoder om, at du lader denne funktion være slået til. Det gør det muligt at forbedre beskyttelsen for dig og andre AVG-brugere.



I dialogboksen er der følgende indstillingsmuligheder:

- ***Jeg vil gerne hjælpe AVG med at forbedre deres produkter ved at deltage i AVG Produktforbedringsprogram*** *(slået til som standard)* – hvis du vil hjælpe os med fortsat at blive bedre **AVG Internet Security 2013**, skal du lade dette afkrydsningsfelt være markeret. Dette vil muliggøre rapportering af alle trusler til AVG, så vi vil kunne indsamle opdaterede oplysninger om malware fra deltagere verden over og derved forbedre beskyttelse for alle. Rapporten oprettes automatisk og er derfor ikke til gene for dig, og der medtages ikke personlige data i rapporterne.
    - ***Tillad, efter brugerbekræftelse, at sende data om uidentificeret e-mail*** *(slået til som standard)* – send oplysninger om e-mailmeddelelser, der ved en fejl er identificeret som spam, eller om spammeddelelser, der ikke blev detekteret af anti-spam-tjenesten. Ved afsendelse af denne slags oplysninger vil du blive bedt om bekræftelse.
    - ***Tillad, at der sendes anonyme data om identificerede eller mistænkelige trusler*** *(slået til som standard)* – send oplysninger om al mistænkelig eller farlig kode eller adfærdsmønster *(kan være en virus, spyware eller skadeligt websted du forsøger at få adgang til)*, der detekteres på din computer.
    - ***Tillad, at der sendes anonyme data om produktbrug*** *(slået til som standard)* – Send grundlæggende statistik om applikationsbrugen såsom antallet af detekteringer, scanninger, fuldførte eller mislykkede opdateringer osv.
- ***Tillad "in the cloud"-verifikation af detekteringer*** *(slået til som standard)* – detekterede trusler kontrolleres, hvis de er inficerede, for at frasortere falske positive.

De mest almindelige trusler

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 andre 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 behøver et "bærer"-objekt at knytte sig til. 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 at infiltrere en computer, så angriberen kan kontrollere den eksternt. Naturligvis uden computerejerens viden eller tilladelse.

- ***Potentielt uønskede programmer*** er en type spyware, der kan være farlig for din computer, men nødvendig ikke er det. 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, en 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 derpå 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.

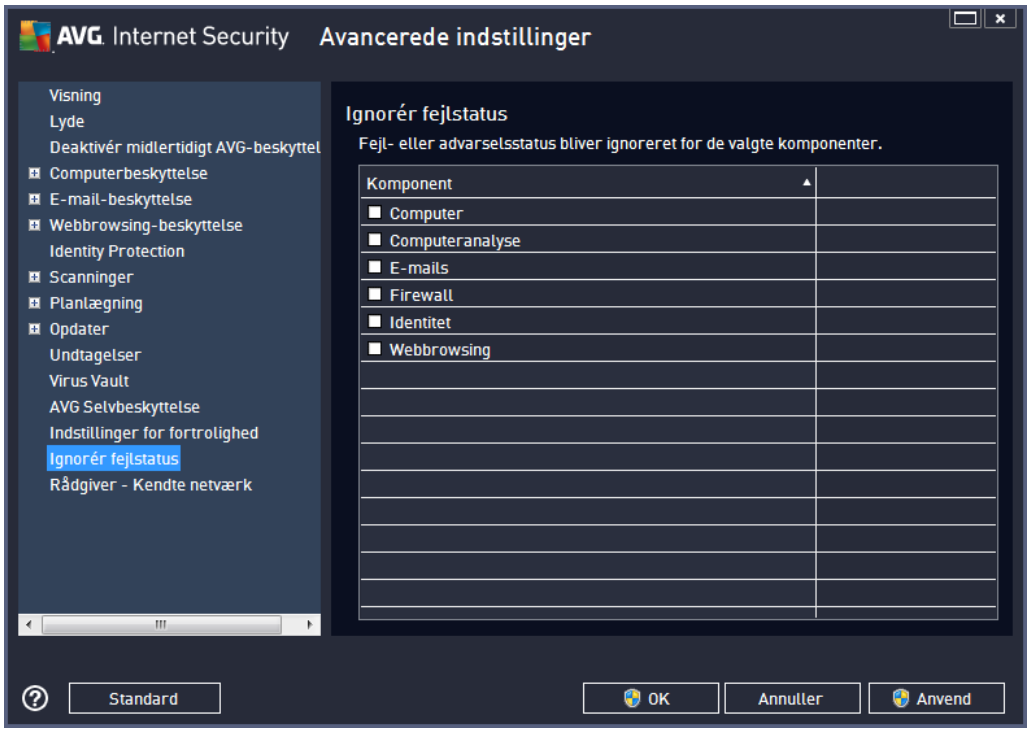
- ***Ondsindede websteder*** er websteder, som bevidst installerer ondsindet software på din computer, og hackede websteder gør nøjagtig det samme, disse er blot legitime websteder, der er blevet kompromitteret til at inficere besøgende.

For at beskytte dig mod alle disse forskellige former for trusler omfatter AVG Internet Security 2013 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

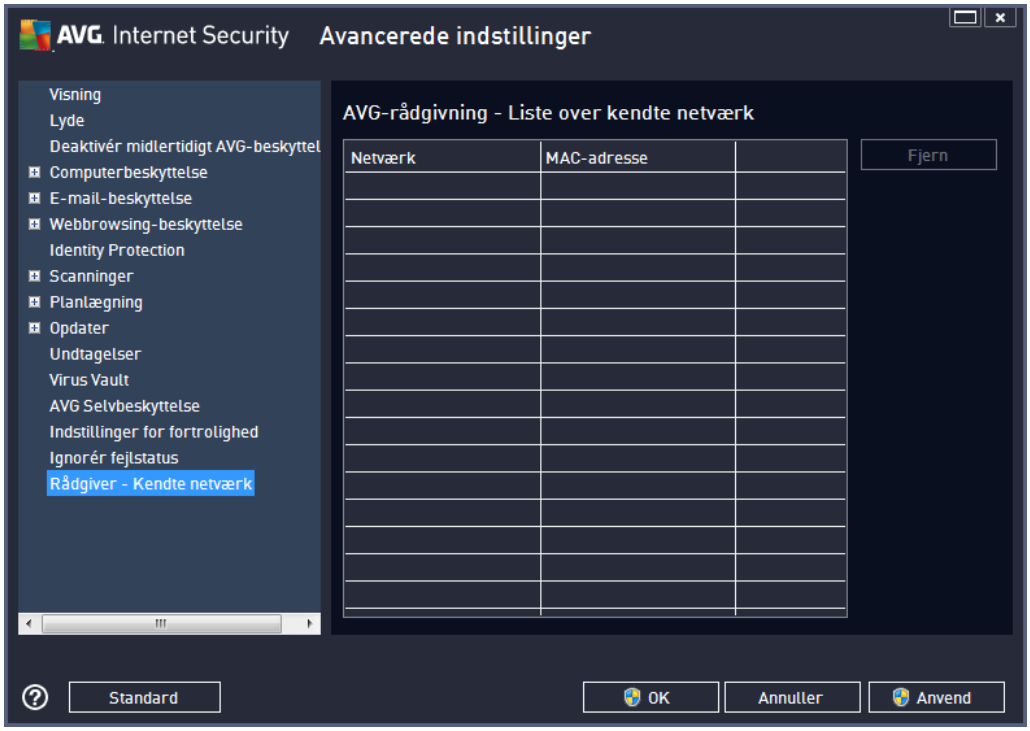
Der kan opstå en situation, hvor du kan være nødt til at slå komponenten fra midlertidigt. ***Dette anbefales ikke. Du bør forsøge at holde alle komponenter aktive permanent og i standardkonfigurationen***, men det kan ske. I dette tilfælde rapporterer proceslinjeikonet automatisk komponentens fejltilstand. 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.

I denne situation kan du i dialogboksen ***Ignorer fejlstatus*** vælge komponenter, der kan være i en fejltilstand (*eller slået fra*), og du vil ikke modtage oplysninger om det. Tryk på knappen ***OK*** for at bekræfte.

9.16. Rådgiver – Kendte netværk

AVG Advisor omfatter en funktion, der overvåger de netværk, du har forbindelse til, og hvis der findes et netværk *(med et netværksnavn, der allerede er brugt, hvilket kan være forvirrende)*, får du besked, og det anbefales, at du kontrollerer netværkssikkerheden. Hvis du har tillid til, at det nye netværk er sikkert at oprette forbindelse til, kan du også gemme det på denne liste *(via linket i systeminformation for AVG Advisor, der glider over proceslinjen, så snart der registreres et ukendt netværk). Få detaljer ved at se kapitlet om AVG Advisor)*. AVG Advisor husker derefter netværkets unikke attributter *(MAC-adressen specifikt)* og viser ikke meddelelsen næste gang. Hvert netværk, som du opretter forbindelse til, betragtes automatisk som et kendt netværk og føjes til listen. Du kan fjerne de enkelte elementer ved at klikke på knappen ***Fjern***, hvorefter det pågældende netværk betragtes som ukendt og potentielt usikkert igen.

I denne dialogboks kan du markere de netværk, der betragtes som kendte:



Bemærk: *Den kendte netværksfunktion i AVG Advisor understøttes ikke til Windows XP 64-bit.*

10. Firewall-indstillinger

Firewall-konfigurationen åbner i et nyt vindue, hvor du i flere dialogbokse kan indstille avancerede parametre for komponenten. Firewall-konfigurationen åbner i et nyt vindue, hvor du kan redigere de avancerede parametre for komponenten i flere konfigurationsdialogbokse. Konfigurationen kan alternativt blive vist i enten basis- eller eksperttilstand. Når du første gang åbner konfigurationsvinduet, åbner det i basisversionen og indeholder muligheder for redigering af følgende parametre:

- Generelt
- Applikationer
- Fil- og printerdeling

Nederst i dialogboksen finder du knappen ***Eksperttilstand***. Tryk på knappen for at få vist yderligere elementer i dialogboksens navigation for den meget avancerede Firewall-konfiguration:

- Avancerede indstillinger
- Definerede netværk
- Systemservices
- Logs

Softwareleverandører har imidlertid konfigureret alle AVG Internet Security 2013-komponenter til at yde det optimale. Medmindre du har en reel grund til det, skal du ikke ændre standardkonfigurationen. Ændringer i indstillingerne bør kun udføres af en erfaren bruger!

10.1. Generelt

Dialogboksen ***Generel information*** indeholder en oversigt over alle tilgængelige Firewall-tilstande. Det aktuelle valg af Firewall-tilstand kan ændres ved blot at vælge en anden tilstand i menuen.

Softwareleverandører har imidlertid konfigureret alle AVG Internet Security 2013-komponenter til at yde det optimale. Medmindre du har en reel grund til det, skal du ikke ændre standardkonfigurationen. Ændringer i indstillingerne bør kun udføres af en erfaren bruger!

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 tilstande. Kort sagt er en Firewall-tilstand en specifik konfiguration af Firewall-komponenten, og du kan bruge et antal af disse foruddefinerede konfigurationer:

- ***Automatisk*** – i denne tilstand håndterer Firewall al netværkstrafik automatisk. Du får ikke mulighed for at foretage nogen valg. Firewall tillader forbindelse for hver kendt applikation, og på samme tid oprettes der en regel til applikationen, der specificerer, at applikationen altid kan oprette forbindelse i fremtiden. For andre applikationer beslutter Firewall, om forbindelsen skal tillades eller blokeres baseret på applikationens adfærd. I sådan en situation vil regler dog ikke blive oprettet, og applikationen vil blive kontrolleret igen, når den prøver at oprette forbindelse. ***Den automatiske tilstand er ganske diskret og anbefales til de fleste brugere.***

- ***Interaktiv*** – denne tilstand er nyttig, hvis du vil have fuld kontrol over al netværkstrafik til og fra din computer. Firewall overvåger den for dig og giver dig besked om hvert forsøg på at kommunikere eller overføre data, så du kan tillade eller blokere forsøget, som du ser passende. Anbefales kun for avancerede brugere.

- ***Bloker adgang til internettet*** – forbindelse til internettet blokeres fuldstændigt. Du kan ikke få adgang til internettet, og ingen udefra kan få adgang til din computer. Kun til særligt og kortvarigt brug.

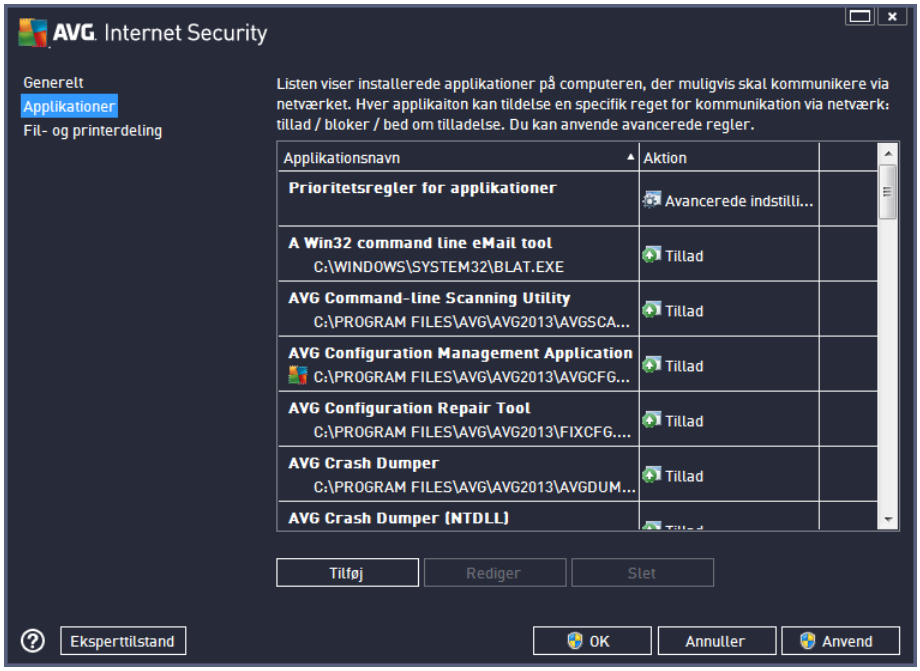
- ***Slå Firewall-beskyttelse fra*** – hvis Firewall slås fra, tillades al netværkstrafik til og fra din computer. Dette gør din computer sårbar over for fremtidige hackerangreb. Overvej altid denne mulighed nøje.

Vær opmærksom på, at der også er en specifik automatisk tilstand tilgængelig i Firewall. Denne tilstand aktiveres, hvis enten komponenten Computer eller Identitetsbeskyttelse slås fra, og din computer er derfor mere sårbar. I sådanne tilfælde tillader Firewall automatisk kun kendte og

fuldstændigt sikre applikationer. For alle andre bliver du spurgt, hvad der skal gøres. Dette er for at kompensere for de deaktiverede beskyttelseskomponenter og for at holde din computer sikker.

10.2. Applikationer

Dialogboksen til ***applikationen*** indeholder en liste over de applikationer, der indtil videre har forsøgt at kommunikere over netværket, 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
- – bloker kommunikation
- – vis spørgedialog (*brugeren afgør, om kommunikation skal tillades eller blokeres, når applikationen forsøger at kommunikere over netværket*)
- – avancerede indstillinger defineret

Bemærk, at det kun er installerede applikationer, der kan detekteres. Når den nye applikation forsøger at oprette forbindelse over netværket for første gang, vil Firewall som standard enten automatisk oprette en regel til den i henhold til den pålidelige database eller spørge dig, om kommunikationen skal tillades eller blokeres. I sidstnævnte tilfælde kan du gemme dit svar som en pemanent regel (som så bliver anført i dialogboksen).

Du kan selvfølgelig også definere regler til den nye applikation med det samme – i denne dialogboks skal du trykke på ***Tilføj*** og udfylde 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 en individuel

applikation. ***Andre applikationsregler*** (*nederst på listen*) bruges som "sidste udkald", hvis der ikke gælder specifikke regler, f.eks. for en ukendt og udefineret applikation. Vælg den handling, der skal udføres, når en sådan applikation forsøger at kommunikere over netværket: Bloker *(kommunikation blokeres altid)*, Tillad *(kommunikation tillades på alle netværk)*, Spørg *(du vil blive spurgt, om du vil tillade eller blokere kommunikation)*. ***Disse elementer har andre indstillingsmuligheder end almindelige applikationer og er kun beregnet til erfarne brugere. Vi anbefaler på det kraftigste, at du ikke ændrer indstillingerne!***

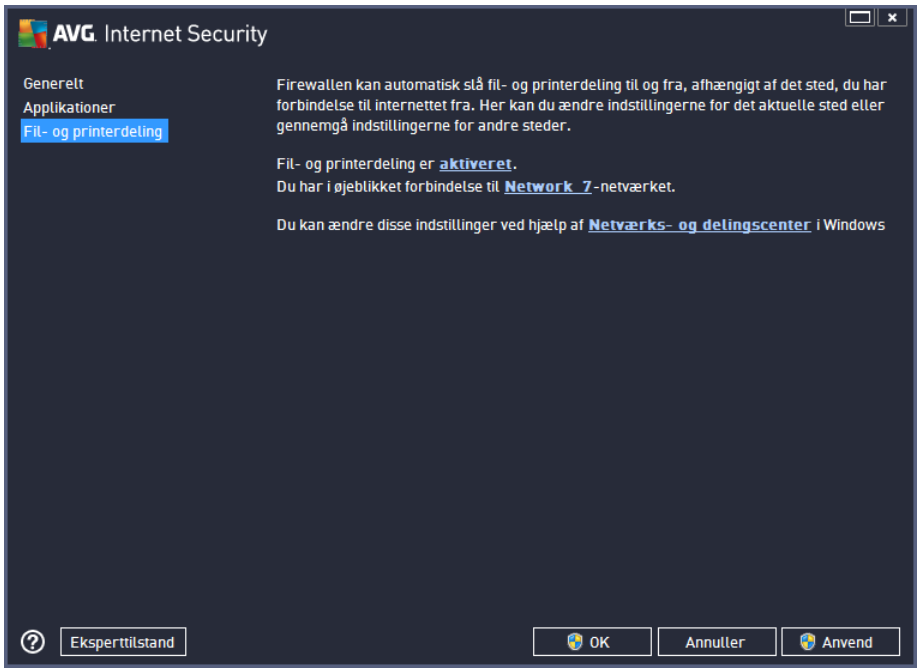
Betjeningsknapper

Denne liste kan redigeres ved hjælp af følgende betjeningsknapper:

- ***Tilføj*** – åbner en tom dialogboks til angivelse af nye applikationsregler.
- ***Rediger*** – åbner den samme dialogboks med data til redigering af en eksisterende applikations regelsæt.
- ***Slet*** – fjerner den valgte applikation fra listen.

10.3. Fil- og printerdeling

Fil- og printerdeling betyder faktisk deling af alle filer og mapper, som du har markeret som "Delt" i Windows, fælles diskenheder, printere, scannere og alle lignende enheder. Deling af sådanne elementer bør kun ske i netværk, der er sikre *(f.eks. hjemme, på arbejde eller i skolen)*. Men hvis du har forbindelse til et offentligt netværk *(som f.eks. et Wi-Fi i lufthavnen eller en internetcafé)*, kan det være en dårlig idé at dele noget. AVG Firewall kan nemt blokere eller tillade deling og giver dig mulighed for at gemme dit valg for allerede besøgte netværk.

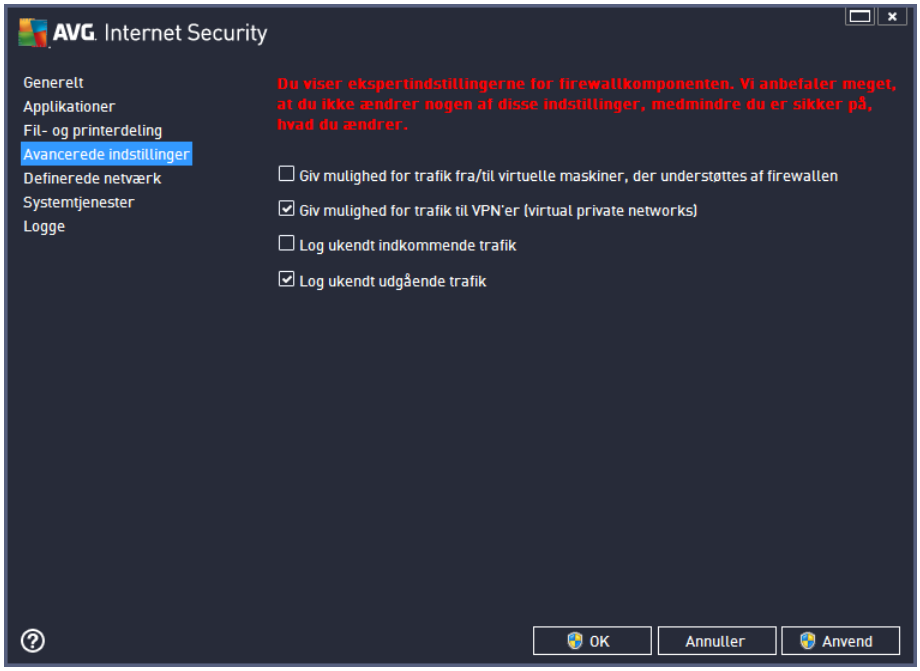


I dialogboksen ***Fil- og printerdeling*** kan du redigere konfigurationen for fil- og printerdeling samt

netværk, der i øjeblikket er tilsluttede. I Windows XP svarer netværksnavnet på den betegnelse, du valgte til det bestemte netværk, da du første gang oprettede forbindelse til det. I Windows Vista og nyere tages netværksnavnet automatisk fra Netværks- og delingscentret.

10.4. Avancerede indstillinger

Enhver redigering i dialogboksen Avancerede indstillinger er KUN TILTÆNKT ERFARNE BRUGERE!

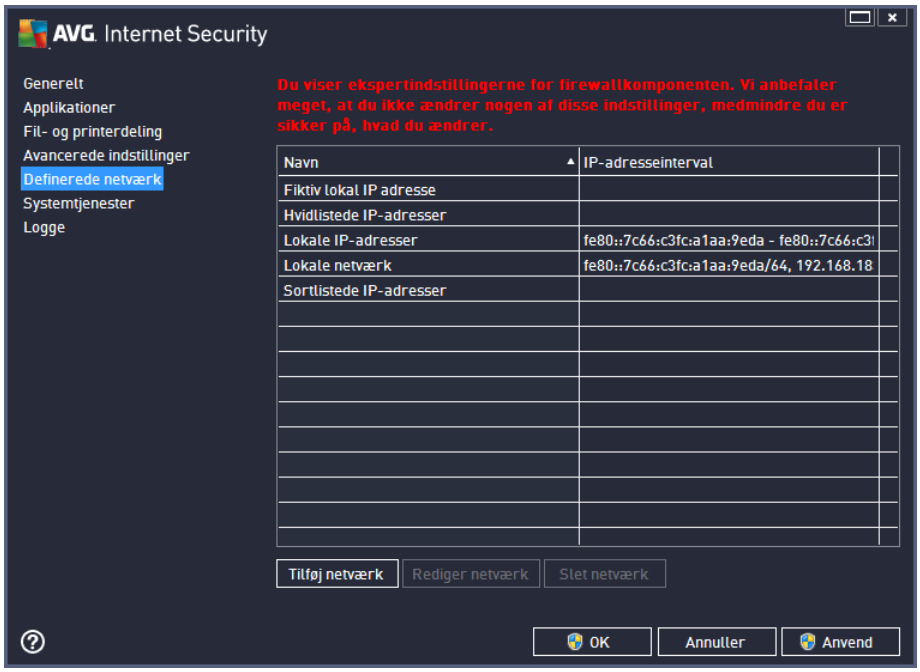


Dialogboksen ***Avancerede indstillinger*** giver dig mulighed for at til- eller framelde dig følgende Firewall-parametre:

- ***Tillad trafik fra/til virtuelle maskiner, der understøttes af Firewall*** – understøttelse for netværksforbindelse i virtuelle maskiner såsom VMWare.
- ***Tillad trafik til virtuelle privatnetværk (VPN)*** – understøttelse for VPN-forbindelser *(bruges til at oprette forbindelse til fjerncomputere)*.
- ***Log ukendt indkommende/udgående trafik*** – alle kommunikationsforsøg *(ind/ud)* af ukendte applikationer registreres i Firewall-loggen.

10.5. Definerede netværker

Redigering i dialogboksen Definerede netværk er KUN BEREGNET FOR ERFARNE BRUGERE!

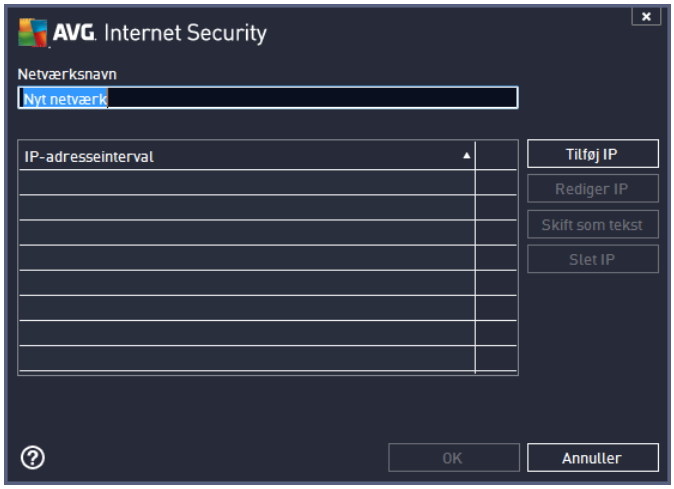


Dialogboksen ***Definerede netværk*** indeholder en liste over alle netværk, som din computer er tilsluttet. Listen indeholder følgende oplysninger om alle detekterede netværk:

- ***Netværk*** – indeholder en navneliste over alle netværk, som computeren er forbundet til.
- ***IP-adresseinterval*** – hvert netværk detekteres og specificeres automatisk i form af IP-adresseintervaller.

Betjeningsknapper

- ***Tilføj netværk*** – åbner et nyt dialogvindue, hvor du kan redigere parametre for det nyligt definerede netværk, dvs. at angive ***netværksnavnet*** og specificere ***IP-adresseintervallet***:



- ***Rediger netværk*** – åbner dialogvinduet ***Netværksegenskaber*** (*se ovenfor*), hvor du kan redigere parametrene for et allerede defineret netværk (*dialogboksen er identisk med dialogboksen til tilføjelse af nye netværk. Se beskrivelsen i forrige afsnit.*).

- ***Slet netværk*** – fjerner referencen til et valgt netværk fra listen over netværk.

10.6. 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. Diagrammet består af følgende kolonner:

- ***Systemtjeneste og -protokoller*** – denne kolonne viser navnet på den relevante systemtjeneste.
- ***Handling*** – I denne kolonne vises et ikon for den tildelte handling:
  - Tilladkommunikation for alle netværk
  - Blokér kommunikation

Hvis du vil registere et element i listen (*inklusive de tildelte handlinger*), skal du højreklikke på elementet og vælge ***Redigér***. ***Redigering af systemreglerne må imidlertid kun udføres af øvede brugere, og det anbefales på det kraftigste, at du ikke redigere systemreglerne!***

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 samme dialogboks åbnes, hvis du beslutter at redigere konfigurationen af et af de eksisterende elementer på listen over systemtjenester og protokoller. Den øverste del af dialogboksen giver et overblik over alle detaljerne for den systemregel, der redigeres i øjeblikket, mens den nederste del viser den valgte detalje. Du kan redigere, tilføje eller slette regeloplysninger vha. den relevante knap:

Husk, at indstillingerne for de detaljerede regler er avancerede og primært er tiltænkt til netværksadministratorer, der har brug for fuld kontrol over firewallkonfigurationen. 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.

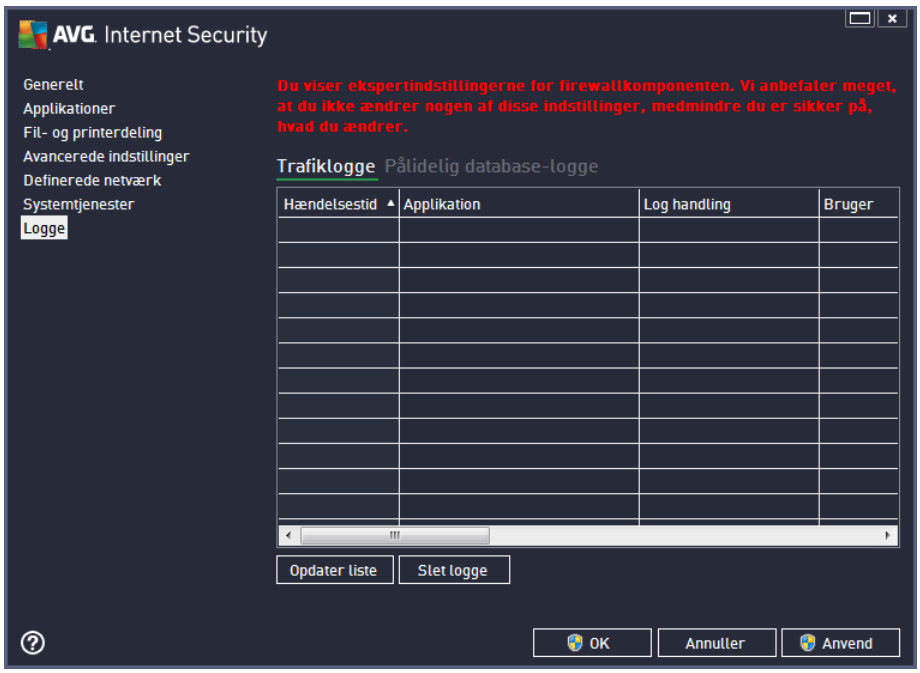
10.7. Logge

Redigering i dialogboksen Logge er KUN BEREGNET FOR ERFARNE BRUGERE!

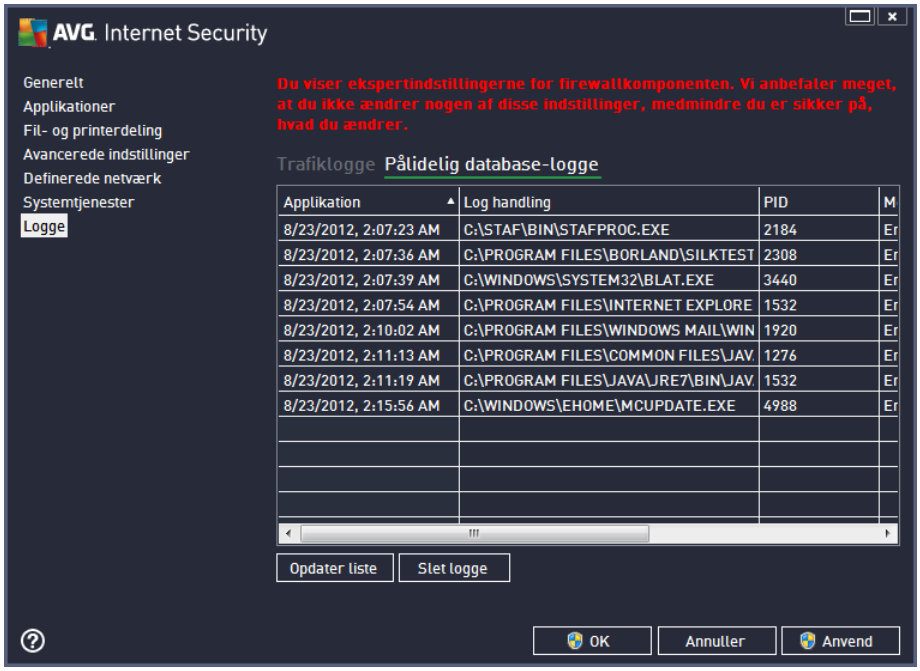
I dialogboksen ***Logge*** kan du gennemse listen over alle loggede Firewall-handlinger og hændelser

med en detaljeret beskrivelse af relevante parametre, der vises på to faner :

- ***Trafiklogge*** – denne fane indeholder oplysninger om aktivitet i alle applikationer, der har forsøgt at oprette forbindelse til netværket. For hvert element finder du oplysninger om hændelsestid, applikationsnavn, pågældende loghandling, brugernavn, PID, trafikretning, protokoltype, numre på eksterne og lokale porte og oplysninger om lokale og eksterne IP-adresser.



- ***Database, der er tillid til-logge*** – en *pålidelig database* er AVG's interne database til indsamling af oplysninger om certificerede og pålidelige applikationer, der altid kan få tilladelse til at kommunikere online. Den første gang en ny applikation forsøger at oprette forbindelse til netværket (*dvs. hvor der endnu ikke er specificeret en firewall-regel for denne applikation*), er det nødvendigt at afgøre, om der skal tillades netværkskommunikation for den respektive 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 dialogboks spurgt, om du vil give applikationen adgang til netværket.



Betjeningsknapper

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

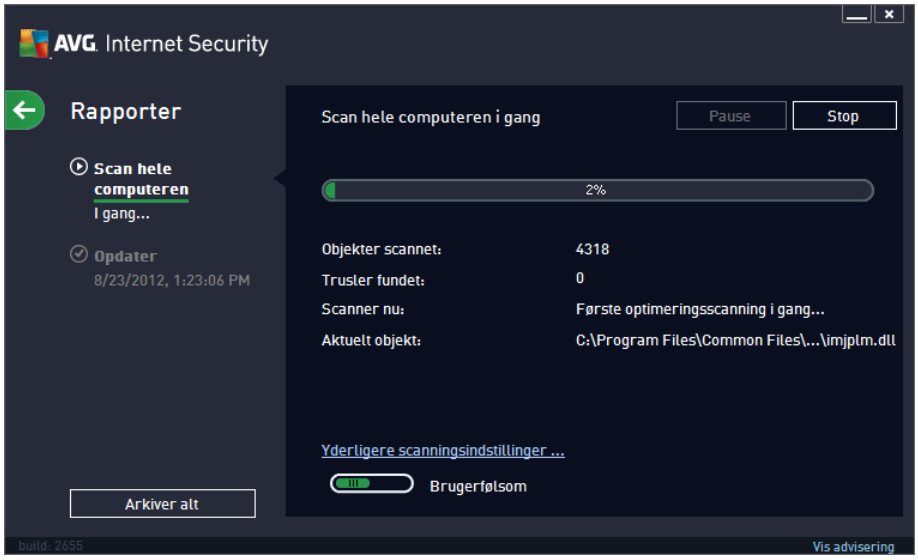
- ***Slet logge*** – tryk for at slette alle poster i tabellen.

11. AVG Scanning

AVG Internet Security 2013 kører som standard ingen scanninger, fordi du efter den første *(som du bliver spurgt, om du vil køre*) burde være fuldt beskyttet af de integrerede komponenter i **AVG Internet Security 2013**, der altid er på vagt og ikke lader en eneste ondsindet kode få adgang til din computer. Du kan selvfølgelig planlægge en scanning til at køre med jævne mellemrum eller starte en scanning manuelt, som passer til dine aktuelle behov.

Grænsefladen for AVG-scanning kan åbnes fra grænsefladen for hovedbrugeren via knappen, der grafisk er inddelt i to sektioner: 

- ***Scan nu*** – tryk på knappen for at linke til at starte Scan hele computeren med det samme og se dens forløb og resultater, der automatisk åbnes i vinduet Rapporter:



- ***Indstillinger*** – vælg denne knap *(vis med grafik som tre vandrette linjer i et grønt felt)* for at åbne dialogboksen ***Scanningsindstillinger***, hvor du kan administrere planlagte scanninger og redigere parametrene for Scan hele computeren / Scanning af filer eller mapper:

I dialogboksen ***Scanningsindstillinger*** kan du se tre hovedsektioner for scanningskonfigurationer:

- ***Administrer planlagte scanninger*** – klik på denne indstilling for at åbne en ny dialogboks med en oversigt over alle scanningsplaner. Inden du definerer dine egne scanninger, kan du kun se én planlagt scanning, der er prædefineret af softwareleverandøren, som er anført i tabellen. Scanningen er slået fra som standard. Du kan slå den til ved at højreklikke på den og vælge indstillingen *Aktivér opgave* i kontekstmenuen. Når den planlagte scanning er slået til, kan du redigere dens konfiguration via knappen *Rediger scanningsplan*. Du kan også klikke på knappen *Tilføj scanningsplan* for at oprette din egen nye scanningsplan.

- ***Scan hele computeren / Indstillinger*** – knappen er inddelt i to sektioner. Klik på indstillingen *Scan hele computeren* for at starte en scanning af hele din computer med det samme *(få flere oplysninger om scanning af hele computeren ved at se det relevante kapitel kaldet Prædefinerede scanninger / Scan hele computeren)*. Hvis du klikker på sektionen *Indstillinger* i bunden, vises konfigurationsdialogboksen for scanning af hele computeren.

- ***Scan specifikke filer eller mapper / Indstillinger*** – igen er knappen inddelt i to sektioner. Klik på indstillingen *Scan specifikke filer eller mapper* for at starte en scanning af de valgte områder i din computer med det samme *(få flere oplysninger om de valgte filer og mapper ved at se det relevante kapitel kaldet Prædefinerede scanninger / Scan specifikke filer)*. Hvis du klikker på sektionen *Indstillinger* i bunden, vises konfigurationsdialogboksen for scanning af de specifikke filer eller mapper.

11.1. Foruddefinerede scanninger

En af hovedfunktionerne i **AVG Internet Security 2013** 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.

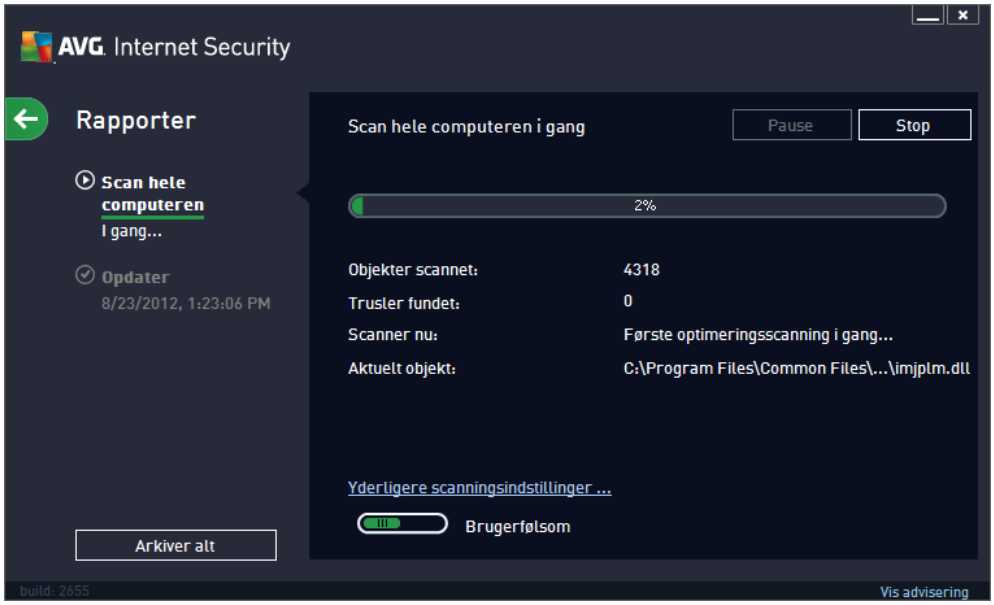
I **AVG Internet Security 2013** vil du finde følgende typer scanning, der er foruddefineret af softwareleverandøren:

11.1.1. Scan hele computeren

Scan hele computeren scanner hele din computer for at finde mulige infektioner og/eller potentielt uønskede programmer. Denne test scanner alle harddisk på din computer, detekterer og helbreder de virusser, der findes, eller flytter den detekterede infektion til Virus Vault. Der skal planlægges en scanning af hele computeren mindst én gang om ugen.

Scanningskørsel

Scan hele computeren kan startes direkte fra hovedbrugergrænsefladen ved at klikke på ikonet ***Scan nu***. Der skal ikke konfigureres flere indstillinger for denne type scanning. Scanningen starter med det samme. I dialogboksen med ***statussen for scanning af hele computeren*** (*se skærmbillede*) kan du se dens status og resultater. Scanningen kan afbrydes midlertidigt (***Pause***) eller annulleres (***Stop***), hvis det er nødvendig.



Redigering af scanningskonfiguration

Du kan ændre konfigurationen af ***Scan hele computeren*** i dialogboksen ***Scan hele computeren – Indstillinger*** *(dialogboksen kan åbnes via indstillingslinket for Scan hele computeren i dialogboksen Scanningsindstillinger).* ***Det anbefales, at du bevarer standardindstillingerne, medmindre du har en god grund til at ændre dem!***

På listen over scanningsparametre kan du slå bestemte parametre til/fra efter behov:

- ***Helbred/fjern virusinfektion uden at spørge mig*** *(slået til som standard)* – hvis en virus identificeres under scanningen, kan den renses automatisk, hvis der er en kur mod den. Hvis den inficerede fil ikke kan helbredes automatisk, flyttes det inficerede objekt til Virus Vault.

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

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** *(slået fra som standard)* – markér indstillingen for at detektere udvidede pakker af spyware. Det vil sige programmer, der er helt OK og skadesløse, når de fås direkte fra producenten, men senere kan misbruges til skadelige 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 efter sporingscookies*** *(slået fra som standard)* – Denne parameter angiver, at cookies skal detekteres; *(HTTP-cookies bruges til godkendelse, sporing og vedligeholdelse af bestemte oplysninger om brugerne, f.eks. webstedspræferencer eller indholdet deres elektroniske indkøbsvogne).*

- ***Scan inde i arkiver*** *(slået fra som standard)* – denne parameter angiver, at scanningen skal kontrollere alle filer, der er gemt i arkiver, f.eks. ZIP, RAR, ...

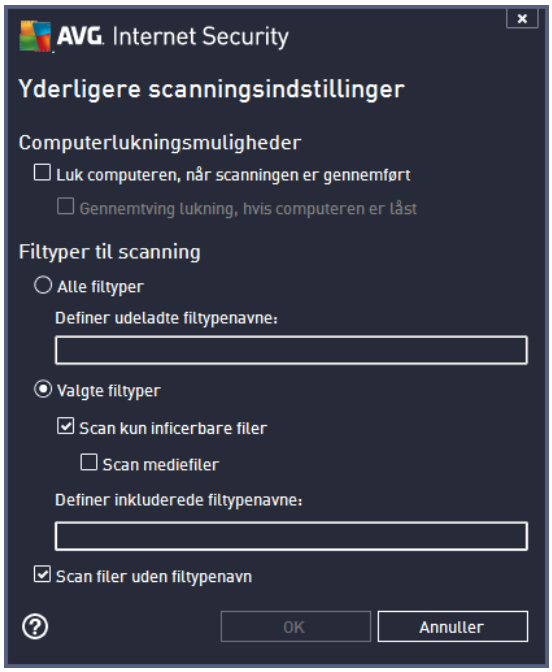
- ***Brug heuristik*** *(slået til som standard)* – Heuristisk analyse *((dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø)* vil være en af de metoder, der bruges til virusdetektering under scanning.

- ***Scan systemmiljø*** *(slået til som standard)* – Scanningen kontrollerer også computerens

systemområder.

- ***Aktivér grundig scanning*** *(slået fra som standard)* – I bestemte situationer *(mistanke om at din computer er ved at blive inficeret)* kan du markere denne indstilling for at aktivere de mest grundige scanningsalgoritmer, som vil scanne selv de områder af din computer, der sjældent bliver inficeret, bare for at være helt sikker. Husk på, at denne metode kræver meget tid.

- ***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 skal også finde ud af, om du vil scanne:

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

    - ***Valgte filtyper*** – Du kan angive, om du vil scanne filer, der kan inficeres(*filer, der ikke kan inficeres, scannes ikke, det kan f.eks. være visse filer, som er almindelig tekst, eller visse ikke-eksekverbare filer*), herunder mediefiler (*video-, lydfiler – hvis du ikke markerer dette felt, reducerer det scanningstiden endnu mere, fordi disse filer ofte er ret store og sandsynligvis ikke er inficeret med virus*). Igen kan du angive ud fra filtypenavne, hvilke filer der altid skal scannes.

    - Du kan også markere ***Scan filer uden filtypenavn*** - denne indstilling er aktiveret som standard, og det anbefales, at du ikke ændrer dette, medmindre du har en

god grund til det. Filer uden filtypenavn er ret mistænkelige og bør altid scannes.

- ***Indstil hvor hurtigt scanningen fuldføres*** – du kan bruge skyderen til at ændre prioriteten af scanningsprocessen. Værdien af denne indstilling er som standard angivet til niveauet *brugerfølsom* vedrørende automatisk ressourceforbrug. Du kan også køre scanningsprocessen langsommere, hvilket betyder, at systemressourcebelastningen minimeres (*det er nyttigt, når du har brug for at arbejde på computeren, men ikke bekymrer dig om, hvor lang tid scanningen varer*), eller hurtigere med øget krav til systemressourcerne (*f.eks. når computeren midlertidigt er uden opsyn*).

- ***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 identiske med parametrene for en scanning, der er defineret for nylig – sådan som det er beskrevet i kapitlet AVG-scanning/Scanningsplanlægning/ Sådan scanner du. Hvis du beslutter dig for at ændre standardkonfigurationen af* ***Scan hele computeren****, kan du derefter gemme din nye indstilling som standardkonfigurationen, så den bruges til alle efterfølgende scanninger af hele computeren.*

11.1.2. Scan specifikke filer eller mapper

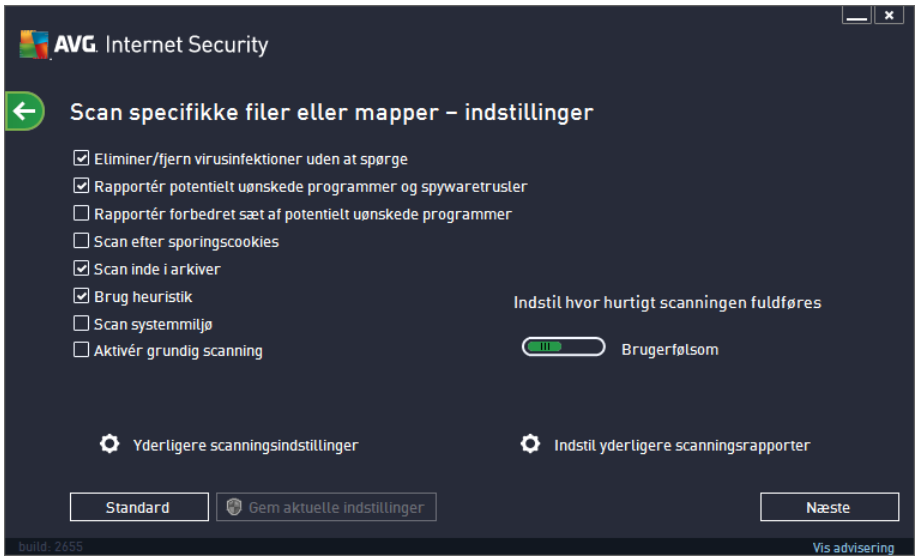
Scan specifikke filer eller mapper – scanner kun de områder af computeren, som du har valgt skal scannes (*valgte mapper, harddiske, disketter, cd'er osv.*). Scanningsprocessen i tilfælde af detektering af virus og behandlingen af den er den samme, som når hele computeren scannes.: alle virusser renses eller flyttes til Virus Vault. Scanning af 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 startes direkte fra dialogboksen Scanningsindstillinger ved at klikke på knappen **Scan specifikke filer eller mapper**. En ny dialog med navnet ***Vælg specifikke filer eller mapper til scanning*** åbnes. Vælg de mapper, du vil scanne, i computerens træstruktur. Stien til hver enkelt af de valgte mapper oprettes automatisk og vises i tekstfeltet i den øverste del af denne dialogboks. Der er også mulighed for at få scannet en bestemt mappe, mens alle dens undermapper udelukkes fra denne scanning. Det gør du ved at skrive et minustegn "**-**" ud for den automatisk oprettede sti (*se skærmbillede*). Brug parameteren "!" for at undtage hele mappen fra scanning. For at starte scanningen skal du til sidst trykke på knappen ***Start scanning***. Selve scanningsprocessen er grundlæggende set den samme som Scanning af hele computeren.

Redigering af scanningskonfiguration

Du kan også redigere konfigurationen af ***Scan specifikke filer eller mapper*** i dialogboksen ***Scan specifikke filer eller mapper - Indstillinger*** *(du kan åbne dialogboksen via linket Indstillinger til Scan specifikke filer eller mapper i dialogboksen Scanningsindstillinger).* ***Det anbefales, at du bevarer standardindstillingerne, medmindre du har en god grund til at ændre dem!***



På listen over scanningsparametre kan du slå bestemte parametre til/fra efter behov:

- ***Eliminer/fjern virusinfektion uden at spørge*** *(aktiveret som standard)*: Hvis en virus identificeres under scanningen, kan den renses automatisk, hvis der er en kur mod den. Hvis den inficerede fil ikke kan helbredes automatisk, flyttes det inficerede objekt til Virus Vault.

- ***Rapporter potentielt uønskede programmer og spywaretrusler*** *(er aktiveret som standard)*: Markér indstillingen for at aktivere scanning efter spyware samt virus. Spyware repræsenterer en tvivlsom malwarekategori: selvom det normalt repræsenterer en sikkerhedsrisiko, kan nogle af disse programmer være installeret med vilje. Vi anbefaler, at du lader denne funktion være aktiveret, da den øger computersikkerheden.

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** *(deaktiveret som standard)* : Markér indstillingen for at detektere udvidede pakker af spyware. Det vil sige programmer, der er helt OK og skadesløse, når de fås direkte fra producenten, men senere kan misbruges til skadelige 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 efter sporingscookies*** *(deaktiveret som standard)*: Denne parameter angiver, at cookies skal detekteres; *(HTTP-cookies bruges til godkendelse, sporing og vedligeholdelse af bestemte oplysninger om brugerne, f.eks. webstedspræferencer eller indholdet deres elektroniske indkøbsvogne)*.

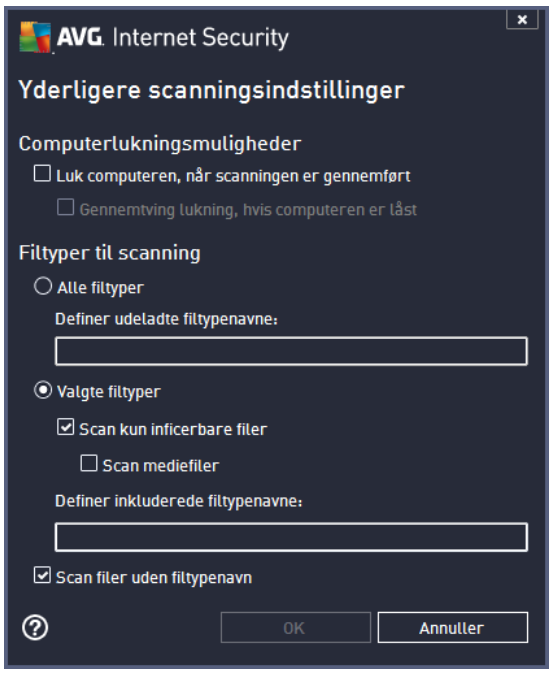
- ***Scan inde i arkiver*** *(aktiveret som standard)*: Denne parameter definerer som standard, at scanningen skal kontrollere alle de filer, der er gemt i arkiver, f.eks. ZIP, RAR, ...

- ***Brug heuristik*** *(slået til som standard)*: Heuristisk analyse *(dynamisk emulering af det scannede objekts instruktioner i et virtuelt computermiljø)* vil være en af de metoder, der bruges til virusdetektering under scanning.

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

- ***Aktivér grundig scanning*** *(slået fra som standard)*: I bestemte situationer *(mistanke om at din computer er ved at blive inficeret)* kan du markere denne indstilling for at aktivere de mest grundige scanningsalgoritmer, som vil scanne selv de områder af din computer, der sjældent bliver inficeret, bare for at være helt sikker. Husk på, at denne metode kræver meget tid.

- ***Yderligere scanningsindstillinger*** – Linket åbner en ny dialogboks ***Yderligere scanningsindstillinger***, hvor du kan angive 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 skal også finde ud af, om du vil scanne:

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

  - ***Valgte filtyper*** – Du kan angive, om du vil scanne filer, der kan inficeres(*filer, der ikke kan inficeres, scannes ikke, det kan f.eks. være visse filer, som er almindelig tekst, eller visse ikke-eksekverbare filer*), herunder mediefiler (*video-, lydfiler – hvis du ikke markerer dette felt, reducerer det scanningstiden endnu mere, fordi disse filer ofte er ret store og sandsynligvis ikke er inficeret med virus*). Igen kan du angive ud fra filtypenavne, hvilke filer der altid skal scannes.

  - Du kan også markere ***Scan filer uden filtypenavn*** – denne indstilling er aktiveret som standard, og det anbefales, at du ikke ændrer dette, medmindre du har en god grund til det. Filer uden filtypenavn er ret mistænkelige og bør altid scannes.

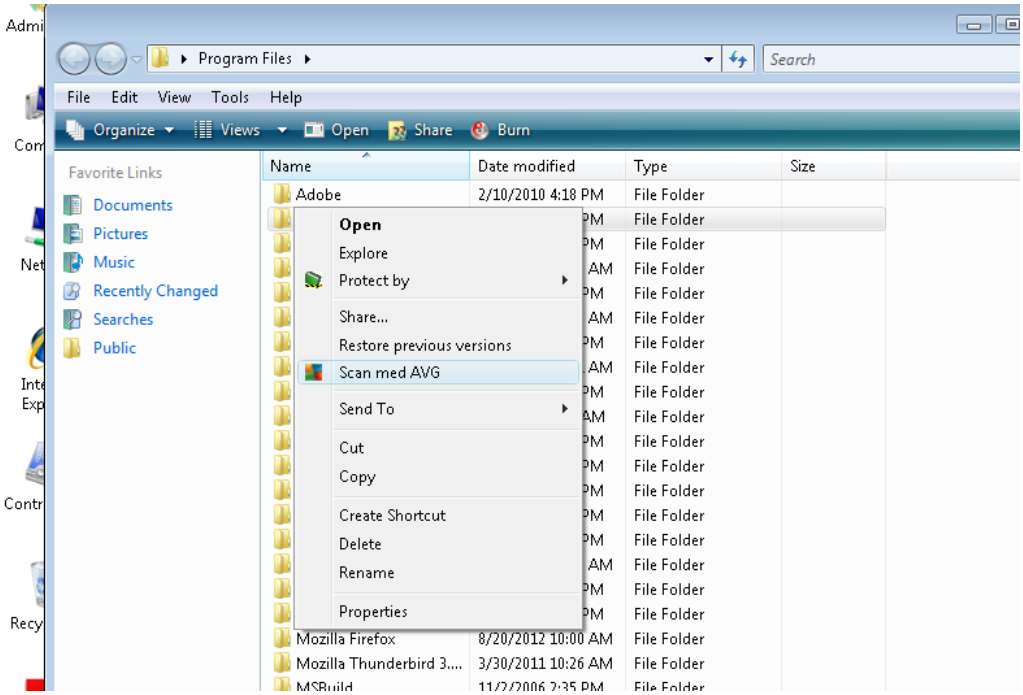
- ***Indstil hvor hurtigt scanningen fuldføres*** – du kan bruge skyderen til at ændre prioriteten af scanningsprocessen. Værdien af denne indstilling er som standard angivet til niveauet *brugerfølsom* vedrørende automatisk ressourceforbrug. Alternativt kan du køre scanningen langsommere, hvilket betyder, 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 dialogboks ***Scanningsrapporter***, hvor du kan vælge, hvilke typer mulige resultater der skal rapporteres:

Advarsel: *Disse scanningsindstillinger er identiske med parametrene for en netop defineret scanning – sådan som det er beskrevet i kapitlet AVG-scanning/Scanningsplanlægning/Sådan scannes der. 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. Scanning i Windows stifinder

Udover de foruddefinerede scanninger af hele computeren eller udvalgte områder af den, giver **AVG Internet Security 2013** 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 Security 2013**

11.3. Kommandolinjescanning

I **AVG Internet Security 2013** 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.

Du kan køre AVG-scanning fra kommandolinjen ved at 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 burde disse blive stillet op på en række og adskilt af et mellemrum og en skråstreg
- hvis et parameter kræver, at en specifik værdi angives (f.eks. parameteren ***/scan***, der 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 starter computeren i Windows Fejlsikret tilstand, er der også mulighed for at køre kommandolinjescanningen fra den grafiske brugerflade. Selve scanningen køres fra kommandolinjen,

dialogen ***Kommandolinjeforfatter*** gør det kun muligt at angive de fleste scanningsparametre i den komfortable grafiske brugerflade.

Idet denne dialogboks kun er tilgængelig i Windows Fejlsikret tilstand, skal du se i hjælpefilen, der åbnes direkte fra dialogboksen for at få en detaljeret beskrivelse af den.

11.3.1. CMD-scanningsparametre

Derefter følger en liste over alle parametre, der er tilgængelige for scanning af kommandolinje:

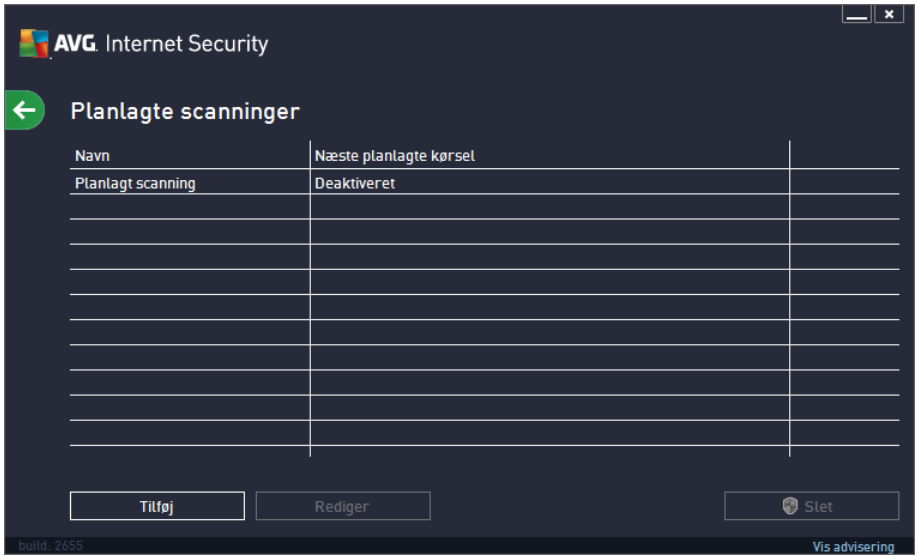
- /SCAN Scan specifikke filer eller mapper /SCAN=path;path *(f.eks. /SCAN=C:\;D:\)*
- /COMP Scan hele computeren
- /HEUR Brug heuristisk analyse
- /EXCLUDE Udelad sti eller filer fra scanning
- /@ Kommandofil/filnavn/
- /EXT Scan disse filtypenavne /for eksempel EXT=EXE,DLL/
- /NOEXT Scan ikke disse filtypenavne /for eksempel NOEXT=JPG/
- /ARC Scan arkiver
- /CLEAN Rens automatisk
- /TRASH Flyt inficerede filer til Virus Vault
- /QT Lyntest
- /LOG Generer en fil med scanningsresultatet
- /MACROW Rapportér makroer
- /PWDW Rapportér filer, der er beskyttet med adgangskode
- /ARCBOMBSW Rapportér arkivbomber *(arkiver komprimeret flere gange)*
- /IGNLOCKED Ignorer låste filer
- /REPORT Rapportér til fil /filnavn/
- /REPAPPEND Føj til rapportfilen
- /REPOK Rapportér ikke-inficerede filer som OK
- /NOBREAK Tillad ikke afbrydelse med CTRL-BREAK
- /BOOT Aktivér MBR/BOOT-kontrol
- /PROC Scan aktive processer

- /PUP Rapportér potentielt uønskede programmer
- /PUPEXT Rapportér forbedret sæt af potentielt uønskede programmer
- /REG Scan registreringsdatabase
- /COO Scan cookies
- /? Vis hjælp om dette emne
- /HELP Vis hjælp om dette emne
- /PRIORITY Indstil scanningsprioritet /Lav, Auto, Høj/ *(se Avancerede indstillinger / Scanninger)*
- /SHUTDOWN Luk computeren, når scanningen er fuldført
- /FORCESHUTDOWN Gennemtving computerlukning, når scanningen er fuldført
- /ADS Scan alternative datastrømme *(kun NTFS)*
- /HIDDEN Rapportér filer med skjulte filtypenavne
- /INFECTABLEONLY Scan kun filer med inficerbare filtypenavne
- /THOROUGHSCAN Aktivér grundig scanning
- /CLOUDCHECK Kontrollér for falske positive
- /ARCBOMBSW Rapportér genkomprimerede arkivfiler

11.4. Scanningsplanlægning

Med **AVG Internet Security 2013** kan du køre en scanning efter behov *(f.eks. når du har mistanke om, at en infektion er trængt igennem til din computer)* eller ud fra en tidsplan. Det anbefales meget, at du kører scanninger efter en tidsplan. På den måde kan du sikre dig, at din computer er beskyttet mod risikoen for en infektion, og du behøver ikke at skulle bekymre dig om, hvis og hvornår scanningen skal starte. 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 nogle gange er slukket, skal de planlagte scanninger køres ved computerstart, når en opgave ikke er udført.

Den planlagte scanning kan oprettes/redigeres i dialogboksen ***Planlagte scanninger***, der kan åbnes med knappen ***Administrer planlagte scanninger*** i dialogboksen Scanningsindstillinger. I den nye dialogboks ***Planlagt scanning*** kan du få et fuldt overblik over alle de aktuelle planlagte scanninger:

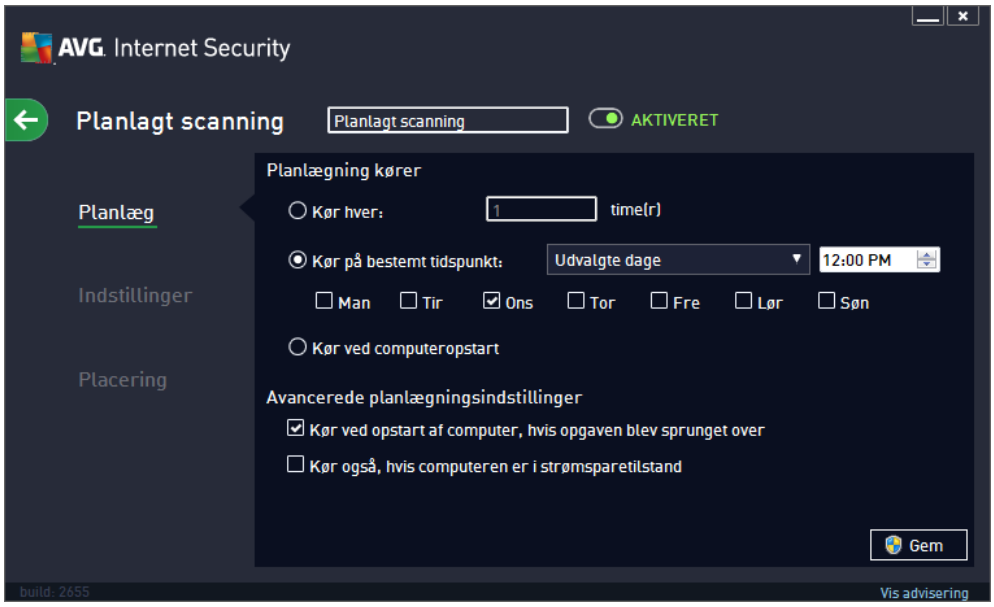


Før du kan definere dine egne scanninger, kan du kun se én planlagt scanning, der er foruddefineret af den softwareleverandør, der er angivet i diagrammet. Scanningen er slået fra som standard. Du kan aktivere den ved at højreklikke på den og vælge indstillingen ***Aktiver opgave*** i kontekstmenuen. Når den planlagte scanning er aktiveret, kan du redigere dens konfiguration via knappen ***Rediger***. Du kan også klikke på knappen ***Tilføj scanningsplan*** for at oprette en ny scanningstidsplan, som er din egen. Parametrene for den planlagte scanning kan redigeres (*eller en ny planlægning kan konfigureres*) på tre faner:

- Planlæg
- Indstillinger
- Placering

På hver fane skal du blot slå knappen "trafiklys" fra  for at deaktivere den planlagte test midlertidigt og slå den til igen, når behovet opstår:

11.4.1. Planlæg



I den øverste del af fanen ***Planlægning*** kan du finde det tekstfelt, hvor du kan angive navnet på den scanningsplan, der defineres i øjeblikket. Prøv altid at bruge korte, beskrivende og passende navne på scanninger for at gøre det nemmere at differentiere scanningen senere. Det er f.eks. 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.

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

- ***Planlægning kører*** – Her kan du angive tidsintervaller for scanning, der er planlagt for nylig. Tidsindstillingen kan enten defineres ved en gentagelse af scanningsstarten efter en bestemt tidsperiode *(Kør hver...)* eller ved at definere en nøjagtig dato og et nøjagtigt tidspunkt *(Kør med bestemte mellemrum...)* eller eventuelt ved at definere en hændelse, som scanningsstarten skal knyttes til *(Kør ved computeropstart)*.

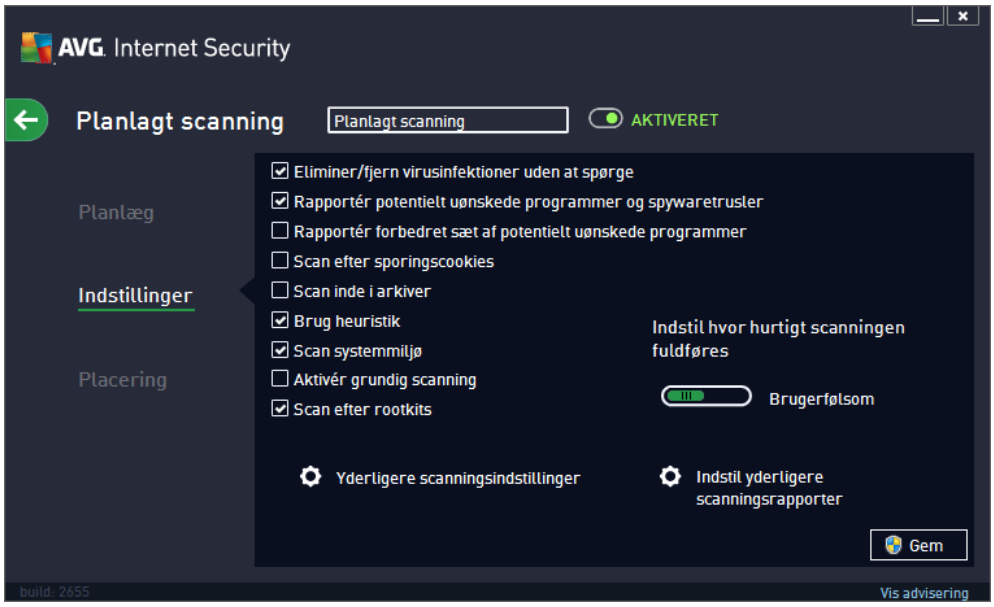
- ***Avancerede planlægningsindstillinger*** – I dette afsnit kan definere, under hvilke betingelser scanningen skal/ikke skal startes, hvis computeren er i strømsparetilstand eller helt slukket. Når den planlagte scanning køres på det tidspunkt, du har angivet, bliver du informeret om det via et popup-vindue, der åbnes over AVG systembakkeikonet. Derefter vises et nyt AVG-ikon på proceslinjen (i fuld farve med et blinkende lys), der angiver, at en planlagt scanning er i gang. 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.

Kontrolelementer i dialogboksen

- ***Gem*** – gemmer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogboksen, og skifter tilbage til oversigten over Planlagte scanninger. 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.

- – brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til oversigten over Planlagte scanninger.

11.4.2. Indstillinger



I øvre del af fanen ***Indstillinger*** kan du finde det tekstfelt, hvor du kan indtaste navnet på den scanningsplan, der i øjeblikket er ved at blive defineret. Prøv altid at bruge korte, beskrivende og passende navne på scanninger for at gøre det nemmere at differentiere scanningen senere. Det er f. eks. 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.

På fanen ***Indstillinger*** er der en liste over scanningsparametre, der valgfrit kan slås til/fra. ***Medmindre du har en god grund til at ændre disse indstillinger, anbefaler vi at bevare den forudindstillede konfiguration***:

- ***Helbred/fjern virusinfektion uden at spørge mig*** *(slået til som standard):* Hvis en virus identificeres under scanningen, kan den helbredes automatisk, hvis der findes en kur. Hvis den inficerede fil ikke kan helbredes automatisk, flyttes det inficerede objekt til Virus Vault.

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

- ***Rapportér forbedret sæt af potentielt uønskede programmer*** (*slået fra som standard*): markér afkrydsningsfeltet 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*): dette parameter definerer, at cookies skal detekteres under scanningen (*HTTP-cookies bruges til validering, sporing og vedligeholdelse af specifikke oplysninger om brugere, som f.eks. foretrukne indstillinger på webstedet eller indholdet i deres elektroniske indkøbsvogne*).

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

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

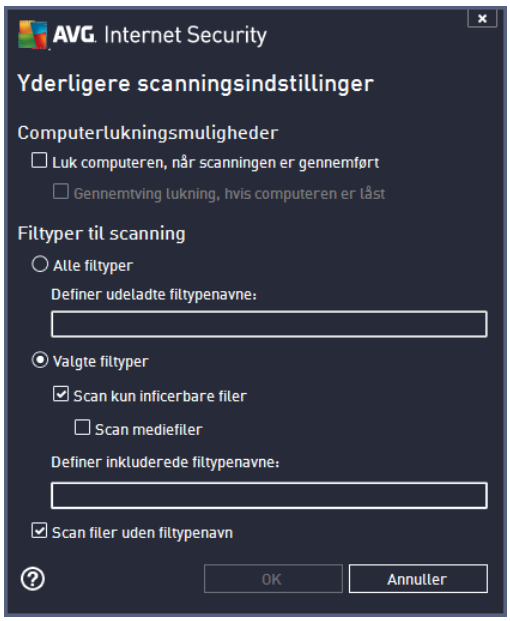
- ***Scan systemmiljø*** (*slået til som standard*): Scanningen kontrollerer også computerens systemområder;

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

- ***Scan efter rootkits*** *(slået til som standard):* Anti-rootkit-scan søger i din computer efter mulige rootkits, f.eks. programmer eller teknologier, som kan skjule malware i 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.

Yderligere scanningsindstillinger

Linket åbner en ny dialogboks, ***Yderligere scanningsindstillinger***, 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 skal også beslutte, om der skal scannes:

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

    - ***Valgte filtyper*** – du kan specificere, at der kun skal scannes efter filer, der kan blive inficeret *(filer, der ikke kan blive inficeret, scannes ikke, f.eks. almindelige tekstfiler eller andre ikke-eksekverbare filer)*, herunder mediefiler (*video, lydfiler – hvis du ikke markerer dette felt, reduceres scanningstiden yderligere, fordi disse filer ofte er meget store og typisk ikke er inficeret med en virus)*. Igen kan du angive ud fra filtypenavne, hvilke filer der altid skal scannes.

    - 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 denne sektion kan du yderligere specificere den ønskede scanningshastighed afhængigt af forbruget af systemressourcer. Som standard er denne værdi indstillet niveauet *brugerfølsom* 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, uden der i øjeblikket er nogen, der arbejder med den*). På den anden side kan du reducere forbruget af systemressourcer ved at forlænge scanningens varighed.

Indstil yderligere scanningsrapporter

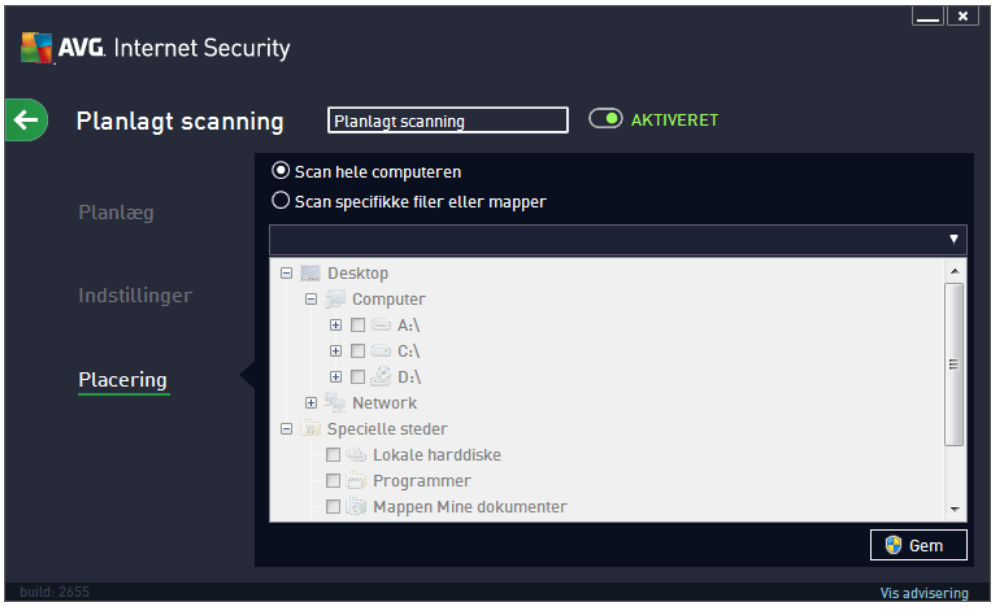
Klik på linket ***Indstil yderligere scanningsrapporter ...*** for at åbne det selvstændige dialogvindue ***Scanningsrapporter***, hvor du kan markere adskillige punkter for at definere, hvilke scanningsfund, der skal rapporteres:

Kontrolelementer i dialogboksen

- ***Gem*** – gemmer alle ændringer, du har udført på denne fane eller enhver anden fane i dialogboksen, og skifter tilbage til oversigten over Planlagte scanninger. 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.

- – brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til oversigten over Planlagte scanninger.

11.4.3. Placering



Under fanen ***Placering*** kan du definere, om du vil planlægge scanning af hele computeren eller scanning af specifikke filer eller mapper. Hvis du vælger at scanne specifikke filer eller mapper, aktiveres den viste træstruktur i den nederste del af dialogboksen, og du kan angive de mapper, der skal scannes (*udvid elementer ved at klikke på plustegnet, 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 dialogboksen, og rullemenuen gemmer din valgte scanningshistorik til senere brug. Du kan også vælge manuelt at angive den fulde sti til den ønskede mappe (*hvis du angiver flere stier, er det nødvendigt at adskille dem med semikolon uden ekstra mellemrum*).

I træstrukturen kan du også se en gren kaldet ***Specielle placeringer***. Herunder er en liste over placeringer, der scannes, når det relevante 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*)

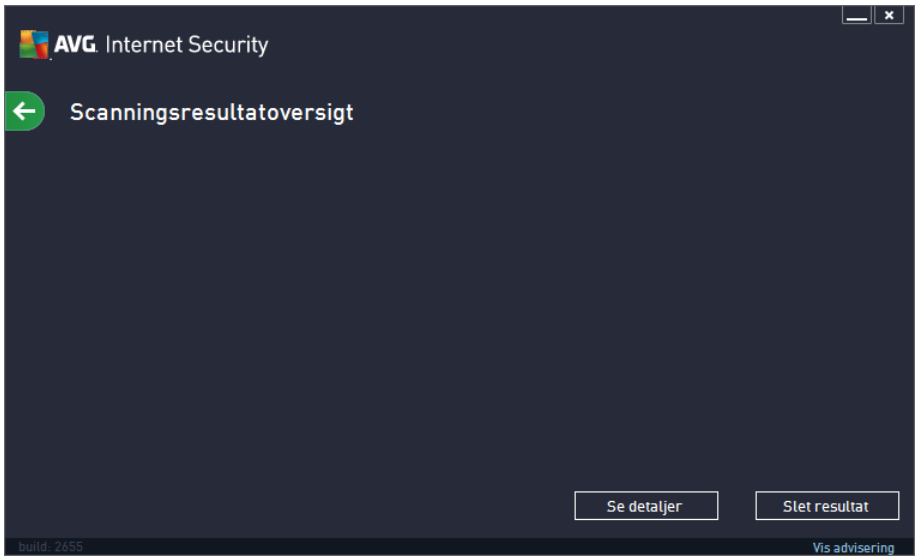
Kontrolelementer i dialogboksen

- ***Gem*** – gemmer alle ændringer, du har udført på denne fane eller enhver anden fane i

dialogboksen, og skifter tilbage til oversigten over Planlagte scanninger. 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.

- – brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til oversigten over Planlagte scanninger.

11.5. Scanningsresultater



Dialogboksen ***Scanningsresultatoversigt*** angiver en liste over resultaterne af de scanninger, der er udført indtil videre. Diagrammet indeholder følgende oplysninger om hvert enkelt scanningsresultat:

- ***Ikonet*** – Den første kolonne viser et oplysningsikon, der beskriver statussen for scanningen:
  - Ingen infektioner fundet, scanning fuldført
  - Ingen infektioner fundet, scanningen blev afbrudt, før den var fuldført
  - Infektioner blev fundet og ikke helbredt, scanning fuldført
  - Infektioner blev fundet og ikke helbredt, scanningen blev afbrudt, før den var fuldført
  - Infektioner fundet og alle blev helbredt eller fjernet, scanning fuldført
  - Infektioner fundet og alle blev helbredt eller fjernet, scanningen blev afbrudt, før den var fuldført
- ***Navn*** – Kolonnen indeholder navnet på den pågældende scanning. Det er enten en af de to prædefinerede scanninger eller din egen planlagte scanning.
- ***Starttidsspunkt*** – Angiver den nøjagtige dato og det nøjagtige klokkeslæt, hvor scanningen blev startet.

- ***Sluttidspunkt*** – Angiver den nøjagtige dato og det nøjagtige klokkeslæt, hvor scanningen blev afsluttet eller afbrudt.
- ***Testede objekter*** – Angiver det samlede antal af alle objekter, der blev scannet.
- ***Infektioner*** – Angiver antallet af fjernede/samlet antal infektioner der blev fundet.
- ***Høj/Mellem/Lav*** – De efterfølgende tre kolonner giver antallet af infektioner, der henholdsvis er kategoriseret med høj, mellem og lav alvorlighedsgrad.
- ***Rootkits*** – Angiver det samlede antal rootkits, der blev fundet under scanningen.

Kontrolelementer i dialogboks

Vis detaljer – Klik på knappen for at se detaljerede oplysninger om en udvalgt scanning *(markeret i diagrammet herover)*.

Slet resultater – Klik på denne knap for at fjerne udvalgte oplysninger om scanningsresultater fra diagrammet.

 – Brug den grønne pil øverst til venstre i dialogboksen for at gå tilbage til hovedbrugerfladen med oversigten over komponenterne.

11.6. Oplysninger om scanningsresultater

Du kan åbne en oversigt med detaljerede oplysninger over udvalgte scanningsresultater ved at klikke på knappen ***Vis detaljer***, der er tilgængelig i dialogboksen Scanningsresultatoversigt. Du bliver omdirigeret til den samme dialogboksgrænseflade, som angiver oplysningerne om et relevant scanningsresultat. Oplysningerne er inddelt på tre faner:

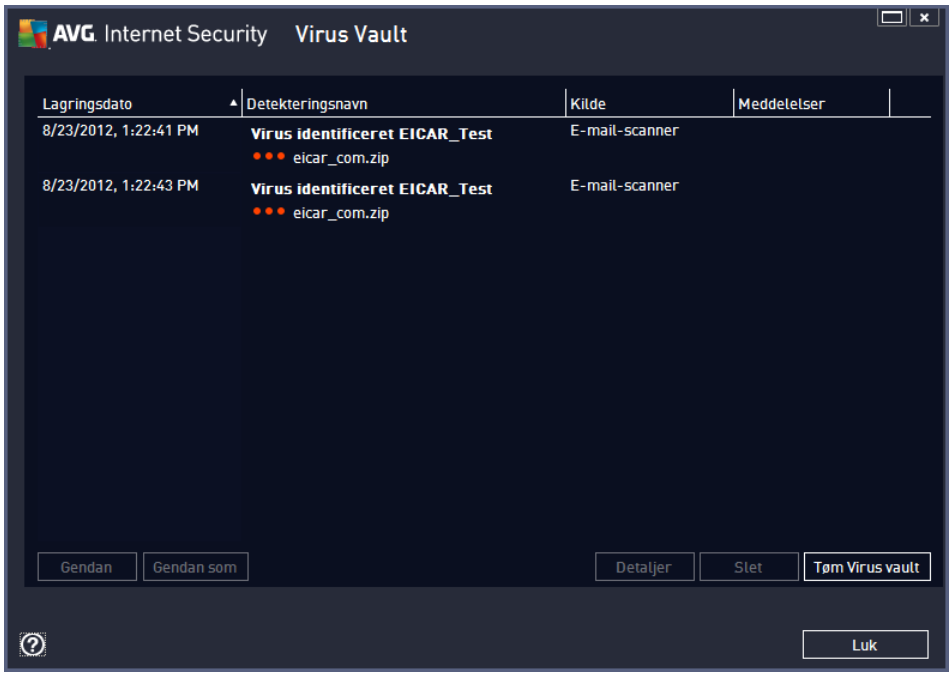
- ***Opsummering*** – Fanen indeholder grundlæggende oplysninger om scanningen: Om den blev gennemført, om der blev fundet trusler, og hvad der skete med dem.
- ***Detaljer*** – Fanen viser alle oplysninger om scanningen, herunder oplysninger om detekterede trusler. Eksporter oversigt til fil giver dig mulighed for at gemme den som en .csv-fil.
- ***Detekteringer*** – Denne fane vises kun, hvis der var trusler under scanningen og indeholder detaljerede oplysninger om truslerne:

   ***Lav alvorlighed***: information eller advarsler, ikke egentlige trusler. Typisk dokumenter, der indeholder makroer, dokumenter eller arkiver beskyttet med adgangskode, låste filer osv.

   ***Middel alvorlighed***: typisk PUP *(potentielt uønskede programmer f.eks. adware)* eller sporingscookies

   ***Høj alvorlighed***: alvorlige trusler som f.eks. virus, trojanske heste, exploits osv. Også objekter detekteret af detekteringsmetoden Heuristik, dvs. trusler, der endnu ikke er beskrevet i virusdatabasen.

12. 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. Hvis du finder ud af, at fraværet af filen giver problemer, kan du sende den pågældende fil til analyse eller gendanne den på dens oprindelige placering.

Virus Vault-grænsefladen åbnes i et separat vindue og giver et overblik over oplysninger om inficerede objekter, der er i karantæne:

- ***Alvorlighedsgrad*** – hvis du beslutter dig for at installere komponenten Identitet i dit **AVG Internet Security 2013**, angives der en grafisk identifikation af det relevante resultat på en firtrinsskala, der går fra problemfri *(tre grønne prikker)* til meget farlig *(tre røde prikker)* i denne sektion samt oplysninger om infektionstypen (*ud fra deres infektionsniveau – alle de viste objekter kan enten helt sikkert være inficeret eller er muligvis inficeret*)
- ***Virusnavn*** – angiver navnet på den detekterede infektion ifølge Virusleksikon
- ***Sti til fil*** – fuld sti til den detekterede inficerede fils oprindelige placering
- ***Lagringsdato*** – dato og klokkeslæt den mistænkelige fil blev detekteret og fjernet til Virus Vault

Betjeningsknapper

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

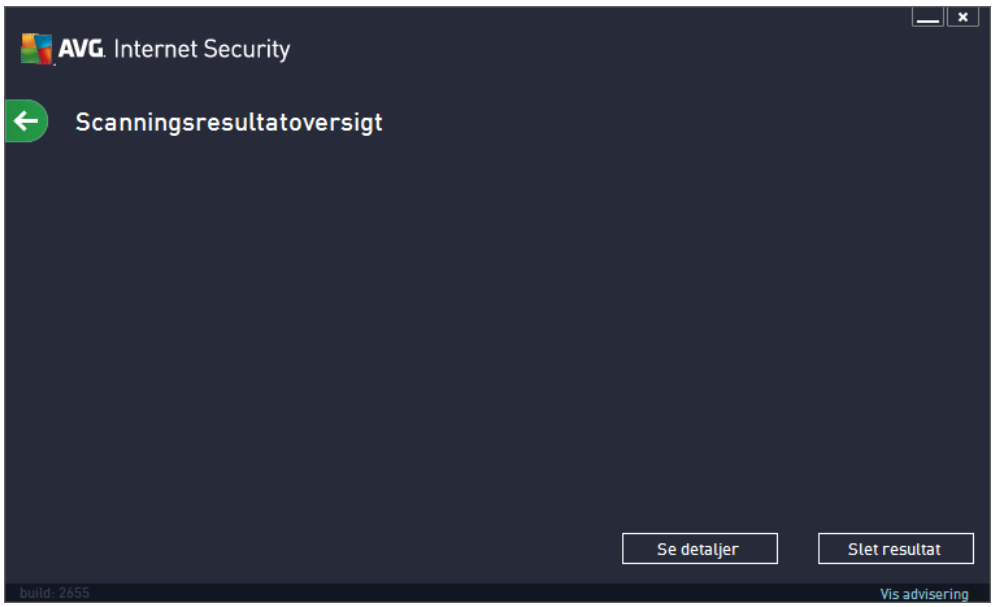
- ***Gendan*** – flytter den inficerede fil tilbage til sin oprindelige placering på disken
- ***Gendan som*** – flytter den inficerede fil til en valgt mappe
- ***Detaljer*** – hvis du ønsker detaljerede oplysninger om specifikke trusler, der er i karantæne i ***Virus Vault*** , kan du markere det valgte element på listen og klikke på knappen ***Detaljer*** for at få vist en ny dialogboks med en beskrivelse af den detekterede trussel.
- ***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*).

13. Historik

Sektionen ***Historik*** indeholder oplysninger om alle tidligere hændelser *(såsom opdateringer, scanninger, detekteringer osv.)* og rapporter om disse hændelser. Der er adgang til denne sektion fra hovedbrugerfladen via menupunktet ***Valgmuligheder / Historik***. Desuden er historikken for alle registrerede hændelser inddelt i følgende:

- Scanningsresultater
- Resident Shield-detektering
- Detektering af e-mailbeskyttelse
- Online Shield-resultater
- Log med hændelseshistorik
- Firewall-log

13.1. Scanningsresultater



Dialogboksen ***Scanningsresultatoversigt*** kan åbnes via menupunktet ***Valgmuligheder / Historik/ Scanningsresultater*** i den øverste navigationsmenu i hovedvinduet i **AVG Internet Security 2013**. Dialogboksen indeholder en liste over tidligere startede scanninger og oplysninger om resultaterne 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
- ***Høj/Mellem*** / ***Lav*** – disse kolonner angiver antallet af fjernede infektioner/infektioner i alt, som er fundet med henholdsvis høj, mellem og lav alvorlighedsgrad
- ***Info*** – oplysninger, der er relateret til scanningsforløbet og resultatet *(typisk afslutning eller afbrydelse af det)*
- ***Rootkits*** – antallet af detekterede rootkits

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
- – du kan skifte tilbage til AVG's primære standarddialogboks *(oversigt over komponenter)* ved at bruge pilen øverst til venstre i denne dialogboks

13.2. Resident Shield-detektering

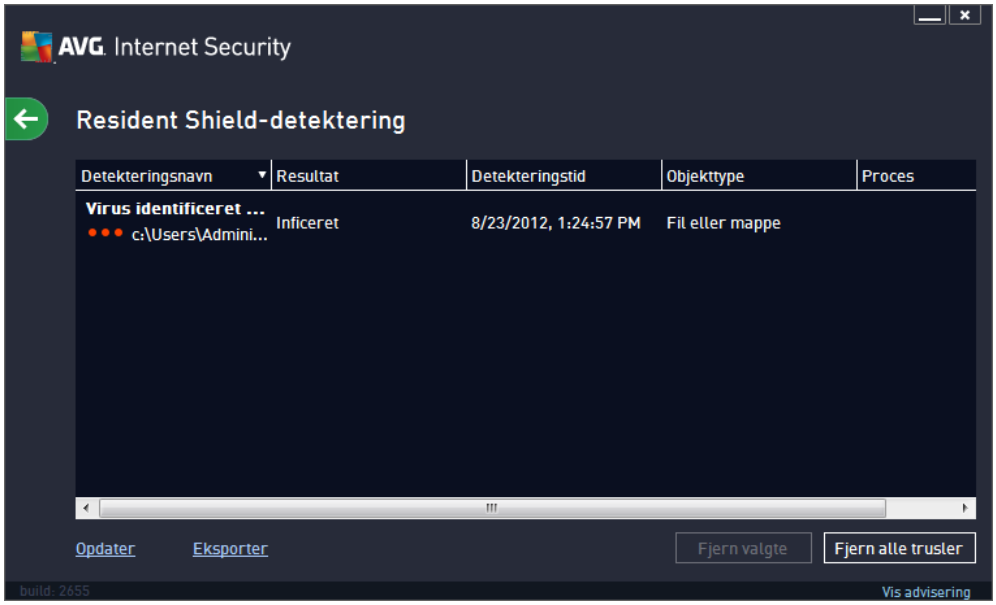
Tjenesten ***Resident Shield*** er en del af komponenten ***Computer*** og scanner filer, idet de kopieres, åbnes eller gemmes. Når en virus eller enhver form for trussel detekteres, bliver du omgående advaret med følgende dialogboks:

I denne advarselsdialogboks er der data om den fil, der blev detekteret og defineret som inficeret (*Navn*), samt beskrivende oplysninger om den genkendte infektion (*Beskrivelse*). Linket Vis detaljer omdirigerer dig til det online virusleksikon, hvor du kan finde detaljerede oplysninger om den detekterede infektion, hvis den kendes. I dialogboksen er der en oversigt over tilgængelige løsninger til, hvor den detekterede trussel kan behandles. En af alternativerne vil være mærket som anbefalet: ***Beskyt mig (anbefalet). Hvis det er muligt, bør du altid holde dig til denne mulighed!***

Bemærk: *Det kan ske, at størrelsen på det detekterede objekt overstiger pladsbegrænsningen i Virus Vault. I dette tilfælde vises pop op-advarsler, 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 den nederste del af dialogboksen finder du linket ***Vis detaljer***. Klik på det for at åbne et nyt vindue med detaljerede oplysninger om den proces, der var i gang, da infektionen blev detekteret, samt identifikation af processen.

En liste over alle detekteringer, Resident Shield har foretaget, er tilgængelig i dialogboksen ***Resident Shield-detektering***. Der er adgang til dialogboksen via menupunktet ***Valgmuligheder / Historik / Resident Shield-detektering*** i øverste navigationsmenu i hovedvinduet til **AVG Internet Security 2013. Dialogboksen viser en oversigt over objekter, der blev detekteret af den integrerede beskyttelse og markeret som farlig samt enten blev kureret eller flyttet til** Virus Vault.



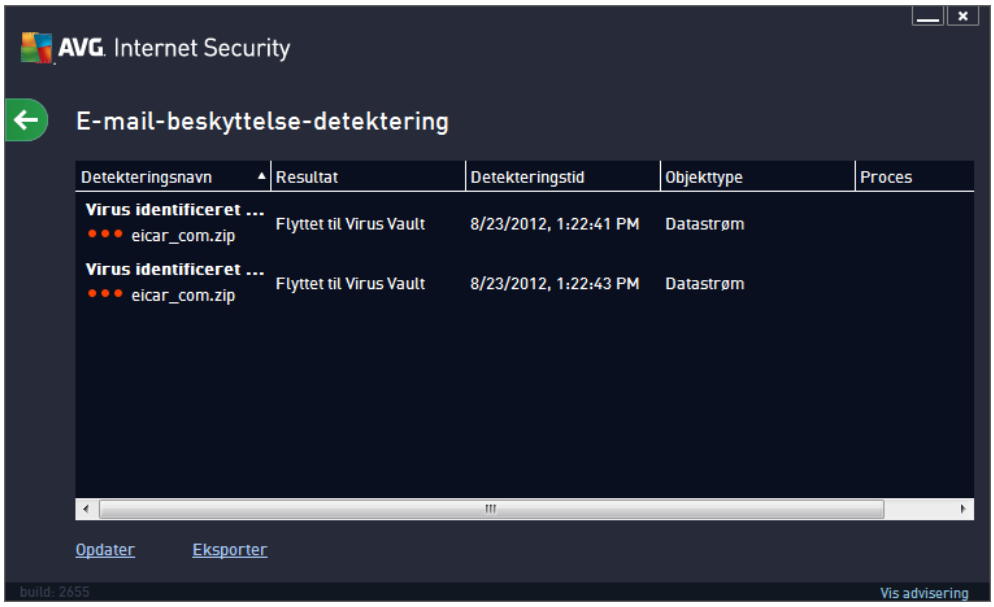
For hvert detekteret objekt findes følgende oplysninger:

- ***Detekteringsnavn*** – beskrivelse (*måske endda navn*) af det detekterede objekt og dens placering
- ***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 få vist det potentielt farlige objekt, så det kunne detekteres

Betjeningsknapper

- ***Opdater*** – opdater listen over fund, der blev detekteret af ***Online Shield***
- ***Eksportér*** – eksporter hele listen over detekterede objekter i en fil
- ***Fjern valgte*** – på listen kan du markere valgte registreringer og bruge denne knap til at slette kun disse valgte elementer
- ***Fjern alle trusler*** – brug knappen til at slette alle registreringer, der vises i denne dialogboks
- – du kan skifte tilbage til AVG's primære standarddialogboks *(oversigt over komponenter)* ved at bruge pilen øverst til venstre i denne dialogboks

13.3. Detektering af e-mailbeskyttelse



E-mail-scanner-detektering Der er adgang til dialogboksen via ***Valgmuligheder / Historik / E-mail-scanner-detekteringMenupunktet*** i øverste navigationsmenu for hovedvinduet til **AVG Internet Security 2013** . Dialogboksen indeholder en liste over alle resultater, der detekteres af komponenten E-mailbeskyttelse . 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 dialogboksen, under listen, finder du oplysninger om det samlede antal detekterede objekter, der er anført ovenfor. Du kan også eksportere hele listen over detekterede objekter i en fil (***Eksportér liste til fil***) og slette alle poster på detekterede objekter (***Tøm liste***).

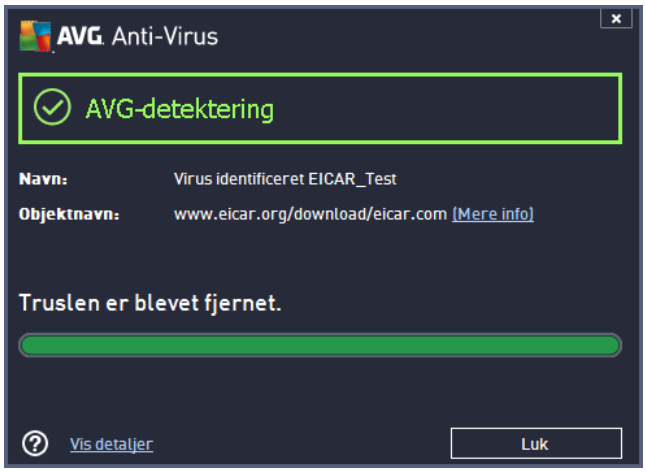
Betjeningsknapper

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

- ***Opdater liste*** – opdaterer listen over detekterede trusler.
- – du kan skifte tilbage til AVG's primære standarddialogboks *(oversigt over komponenter)* ved at bruge pilen øverst til venstre i dialogboksen

13.4. Online Shield-fund

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 advarselsdialogboks er der data om den fil, der blev detekteret og defineret som inficeret (*Navn*), samt beskrivende oplysninger om den genkendte infektion (*Beskrivelse*). Linket Vis detaljer omdirigerer dig til det online virusleksikon, hvor du kan finde detaljerede oplysninger om den detekterede infektion, hvis den kendes. Dialogboksen indeholder følgende kontrolelementer:

- ***Vis detaljer*** – klik på linket for at åbne et nyt pop op-vindue, hvor du vil finde oplysninger om den proces, der var i gang, da infektionen blev detekteret, samt identifikation af processen.
- ***Luk*** - klik på knappen for at lukke advarselsdialogen.

Den mistænkelige webside åbnes ikke, og trusselsdetekteringen logges i listen over ***Online Shield-fund***. Der er adgang til denne oversigt over detekterede trusler via menupunktet ***Valgmuligheder / Historik / Online Shield-fund*** i øverste navigationsmenu i hovedvinduet til **AVG Internet Security 2013**.

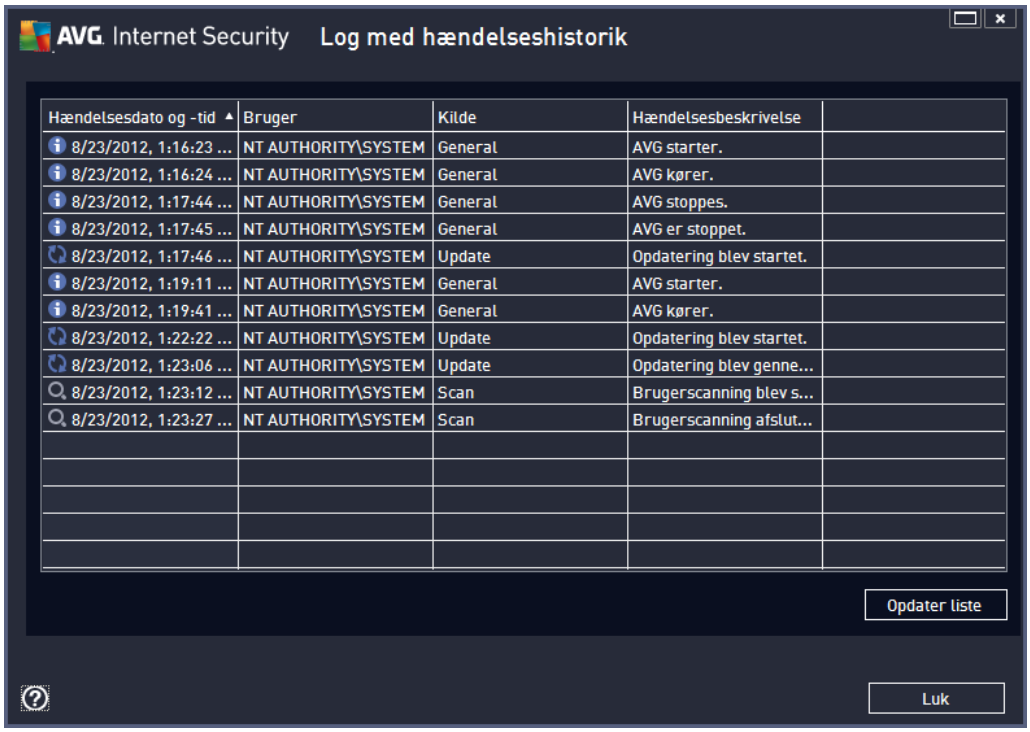
For hvert detekteret objekt findes følgende oplysninger:

- ***Detekteringsnavn*** – beskrivelse (*måske endda navn*) af det detekterede objekt og dens kilde (*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 få vist det potentielt farlige objekt, så det kunne detekteres

Betjeningsknapper

- ***Opdater*** – opdater listen over fund, der blev detekteret af ***Online Shield***
- ***Eksportér*** – eksportér hele listen over detekterede objekter i en fil
- – du kan skifte tilbage til AVG's primære standarddialogboks *(oversigt over komponenter)* ved at bruge pilen øverst til venstre i denne dialogboks

13.5. Log med hændelseshistorik



Der er adgang til dialogboksen for ***Log med hændelseshistorik*** via menupunktet ***Indstillinger / Historik/Log med hændelseshistorik*** i øverste navigationsmenu i hovedvinduet for **AVG Internet Security 2013**. I denne dialogboks findes en oversigt over vigtige hændelser, der er sket under brugen af **AVG Internet Security 2013**. Dialogboksen indeholder registreringer af følgende hændelsestyper: oplysninger om opdateringer af AVG-applikationen, oplysninger om scanningens start, slutning eller stop (*inklusive automatisk udførte test*), oplysninger om hændelser, der er forbundet med virusdetektering (*enten af den indbyggede beskyttelse eller scanning*), inklusive forekomststed og andre vigtige hændelser.

For hver hændelse vises følgende oplysninger:

- ***Hændelsesdato og -tid*** viser den nøjagtige dato og klokkeslæt for, hvornår hændelsen skete
- ***Bruger*** angiver navnet på den bruger, der var logget ind på det tidspunkt, hvor hændelsen skete
- ***Kilde*** angiver kildekomponenten eller en anden del af AVG-systemet, der udløste hændelsen
- ***Hændelsesbeskrivelse*** giver en kort sammenfatning af, hvad der egentlig skete

Betjeningsknapper

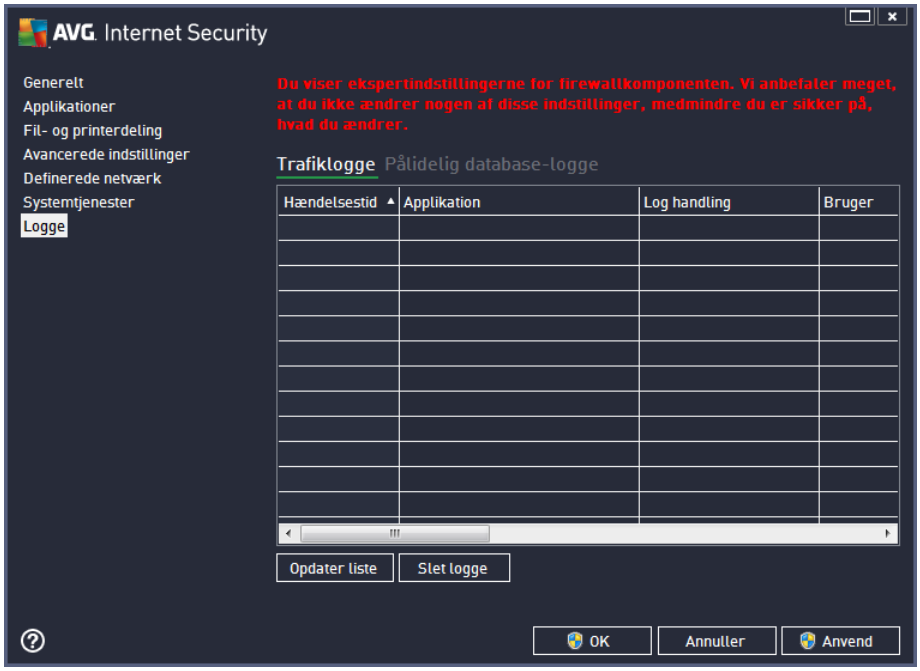
- ***Opdater liste*** – Tryk på denne knap for at opdatere alle poster fra listen over hændelser

- ***Luk*** – tryk på knappen for at gå tilbage til **AVG Internet Security 2013** hovedvinduet

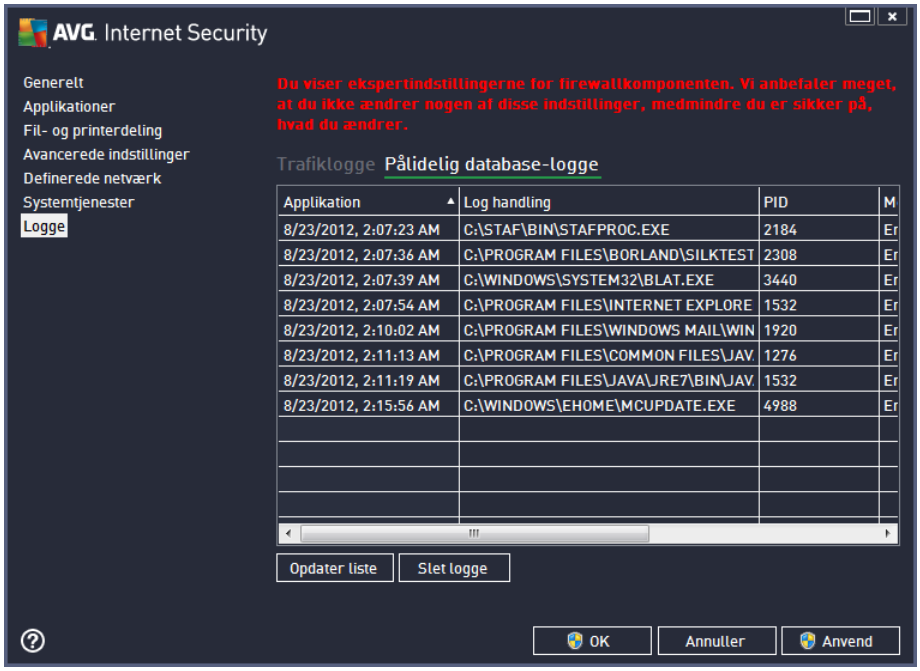
13.6. Firewall -log

I dialogboksen ***Logge*** kan du gennemse listen over alle loggede Firewall-handlinger og hændelser med en detaljeret beskrivelse af relevante parametre, der vises på to faner:

- ***Trafiklogge*** – denne fane indeholder oplysninger om aktivitet i alle applikationer, der har forsøgt at oprette forbindelse til netværket. For hvert element finder du oplysninger om hændelsestid, applikationsnavn, pågældende loghandling, brugernavn, PID, trafikretning, protokoltype, numre på eksterne og lokale porte og oplysninger om lokale og eksterne IP-adresser.



- ***Database, der er tillid til-logge*** – en *pålidelig database* er AVG's interne database til indsamling af oplysninger om certificerede og pålidelige applikationer, der altid kan få tilladelse til at kommunikere online. Den første gang en ny applikation forsøger at oprette forbindelse til netværket (*dvs. hvor der endnu ikke er specificeret en firewall-regel for denne applikation*), er det nødvendigt at afgøre, om der skal tillades netværkskommunikation for den respektive 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 dialogboks spurgt, om du vil give applikationen adgang til netværket.



Betjeningsknapper

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

- ***Slet logge*** – tryk for at slette alle poster i tabellen.

14. 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.

Når man tager alle de nye computertrusler samt den hastighed, hvormed de spredes, i betragtning, er det særdeles vigtigt at opdatere **AVG Internet Security 2013** jævnligt. Den bedste løsning er at holde sig til programmets standardindstillinger, hvor den automatiske opdatering er konfigureret. Husk på, at hvis virusdatabasen i **AVG Internet Security 2013** 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.

14.1. Start af opdatering

For at sikre den størst mulige tilgængelige sikkerhed er **AVG Internet Security 2013** som standard planlagt til at søge efter nye virusdatabaseopdatering hver fjerde time. Da AVG-opdateringer ikke frigives efter nogen fast tidsplan, men i stedet som reaktion på mængden og alvorligheden af nye trusler, er denne kontrol meget vigtig for at sikre, at din AVG-virusdatabase hele tiden er opdateret.

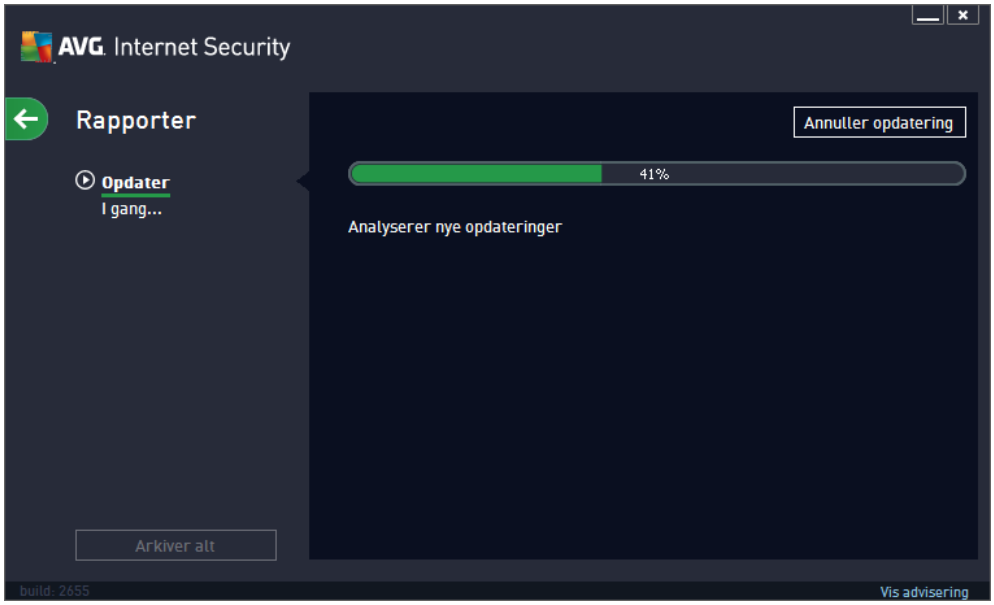
Hvis du ønsker at reducere antallet af opdateringsstarter, kan du konfigurere dine egne parametre for opdateringsstart. Det anbefales imidlertid på det kraftigste, at du starter opdateringen mindst én gang om dagen! Konfigurationen kan redigeres i sektionen Avancerede indstillinger/Planlægning og især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

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

Hvis du ønsker at kontrollere, om der er nye opdateringsfiler med det samme, kan du bruge linket Opdater nu i hovedbrugergrænsefladen. Dette link er altid tilgængeligt via enhver dialog i brugergrænsefladen.

14.2. Opdateringsforløb

Når du har startet opdateringen, verificerer AVG først, om der er nye tilgængelige opdateringer. Hvis det sker, begynder **AVG Internet Security 2013** at hente dem og starter selve opdateringsprocessen. Under opdateringsprocessen bliver du omdirigeret til grænsefladen med ***rapporter***, hvor du kan se en grafisk visning af statussen samt et overblik over relevante statistiske parametre *(størrelse af opdateringsfil, modtaget data, overførselshastighed, forløbet tid, ...)*:



14.3. Opdateringsniveauer

AVG Internet Security 2013 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 forskellige programændringer, -rettelser og -forbedringer.

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

- Plan over definitionsopdatering

- Programopdateringsplan

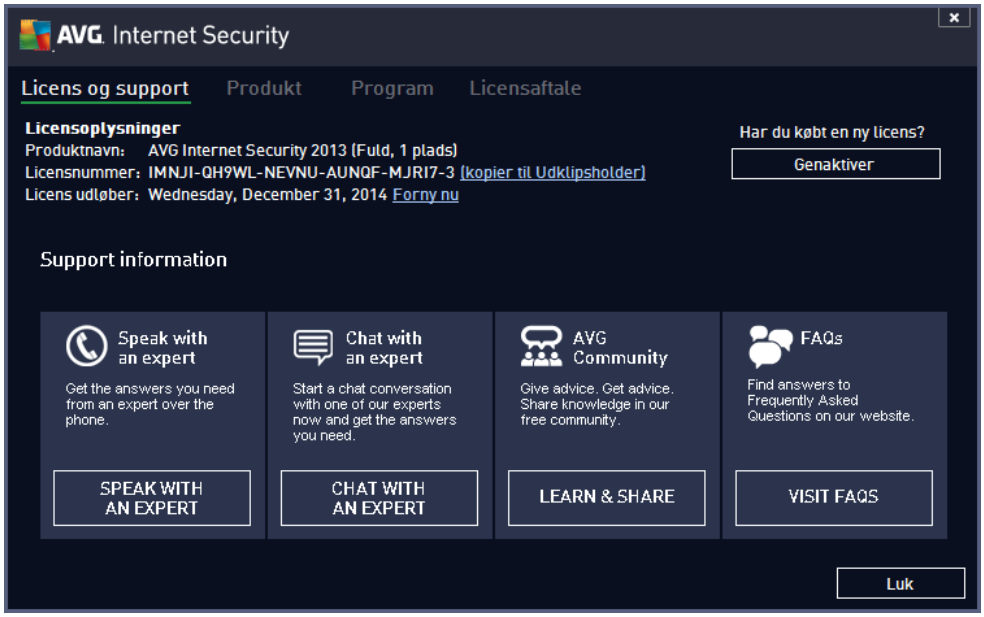
Bemærk: *Hvis en planlagt programopdatering og scanning sker samtidigt, har opdateringsprocessen en højere prioritet, og scanningen afbrydes.*

15. FAQ og teknisk support

Hvis du har salgsmæssige eller tekniske problemer med din **AVG Internet Security 2013**-applikation, kan du få hjælp på flere måder. Vælg mellem følgende valgmuligheder:

- ***Få Support***: I AVG-applikationen kan du gå til en dedikeret side til kundesupport på AVG's websted (http://www.avg.com/). Vælg hovedmenupunktet ***Valgmuligheder / Få support*** for at blive omdirigeret til AVG's websted med tilgængelige supportmuligheder. Følg instruktionerne på websiden for at fortsætte.

- ***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 hjælpefilen***: En ny sektion for ***Fejlfinding*** er tilgængelig direkte i hjælpefilen **AVG Internet Security 2013** *(hjælpefilen åbnes ved at trykke på F1 i en hvilken som helst dialogboks i applikationen)*. Denne sektion indeholder en liste over de situationer, der hyppigst opstår, når en bruger søger professionel hjælp til et teknisk problem. Vælg den situation, der bedst beskriver problemet, og klik på den for at få detaljerede oplysninger, der kan løse problemet.

- ***AVG-webstedets supportcenter***: Alternativt kan du lede efter en løsning til dit problem på AVG's websted (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. Der er adgang til sektionen via menupunktet ***Supportcenter / FAQ***. Igen er alle spørgsmål inddelt på en organiseret måde i kategorierne salg, teknisk og virus.

- ***Om virus og trusler***: En bestemt del af AVG's websted (http://www.avg.com/) er dedikeret til virusproblemer *(der er adgang til websiden fra hovedmenuen via valmuligheden Hjælp / Om virus og trusler)*. I menuen skal du vælge ***Supportcenter / Om virus og trusler*** for at gå til en side, der indeholder en struktureret oversigt over oplysninger, der har med onlinetrusler at gøre. Du kan også finde instruktioner i at fjerne virus og spyware, og rådgivning om, hvordan beskyttelsen bevares.

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