McAfee®

Internet Security

Brugerhåndbog

Indhold

KAPITEL 1

McAfee Internet Security

Internet Security er som et alarmsystem til hjemmet, bare på computeren. Det beskytter dig og din familie mod de nyeste trusler og gør det samtidig sikrere for jer at være på internettet. Du kan bruge Internet Security til at beskytte computeren mod virus, hackere og spyware, overvåge internettrafik for mistænkelig aktivitet, beskytte familiens privatliv, bedømme risikofyldte websteder og meget mere.

I dette kapitel

KAPITEL 2

McAfee SecurityCenter

McAfee SecurityCenter giver dig mulighed for at overvåge computerens sikkerhedsstatus, øjeblikketligt få oplyst, om computerens virus-, spyware-, e-mail- og firewall-beskyttelsestjenester er opdaterede, og reagere over for potentielle sikkerhedssårbarheder. Det indeholder de navigationsværktøjer og kontrolelementer, du skal bruge til at koordinere og administrere alle områder af computerens beskyttelse.

Inden du begynder at konfigurere og administrere computerens beskyttelse, bør du gennemgå grænsefladen i SecurityCenter og sikre, at du forstår forskellen mellem beskyttelsesstatus, beskyttelseskategorier og beskyttelsestjenester. Opdater derefter SecurityCenter for at sikre, at du har den sidste nye beskyttelse fra McAfee.

Når du har udført indledende konfigurationsopgaver, kan du bruge SecurityCenter til at overvåge computerens beskyttelsesstatus. Hvis SecurityCenter registrerer et beskyttelsesproblem, advarer det dig, så du kan løse eller ignorere problemet (afhængigt af dets alvor). Du kan gennemgå SecurityCenter-hændelser, som f.eks. ændringer i konfigurationen af virusscanning, i en hændelseslogfil.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i SecurityCenter

Forenklet beskyttelsesstatus

Se hurtigt computerens beskyttelsesstatus, søg efter opdateringer, og løs beskyttelsesproblemer.

Automatiske opdateringer og opgraderinger

SecurityCenter downloader og installerer opdateringer til dine programmer automatisk. Når en ny version af et McAfee-program er tilgængelig, får du den automatisk i din abonnementsperiode, og du er derved altid sikret opdateret beskyttelse.

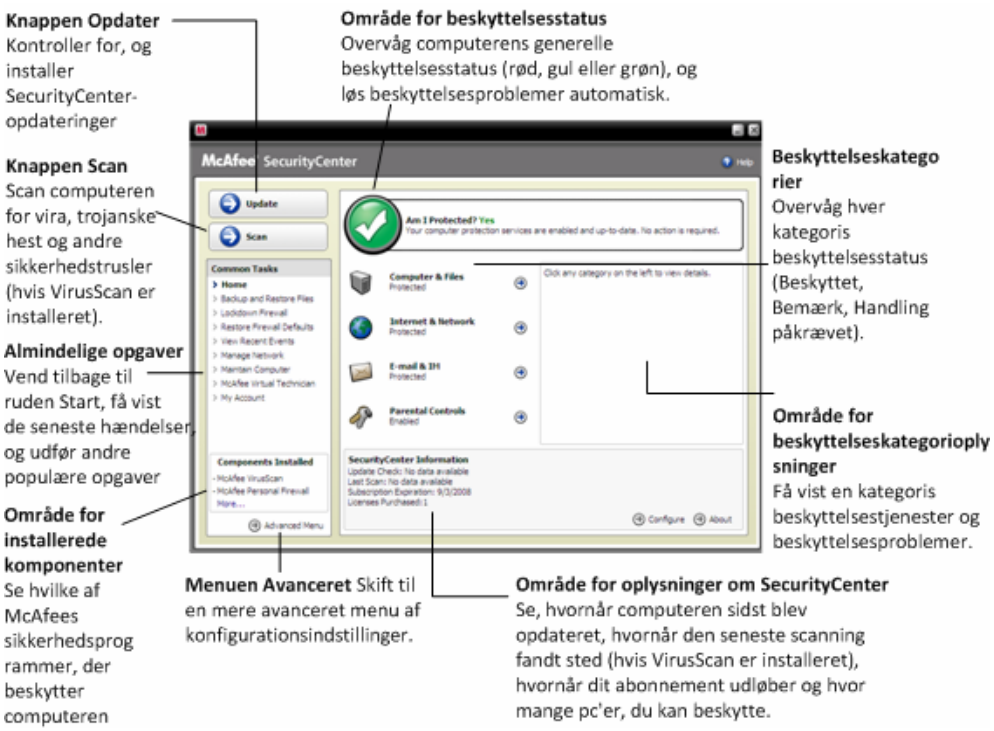
Alarmer i realtid

Sikkerhedsalarmer underretter dig om virusudbrud og sikkerhedstrusler.

KAPITEL 3

Brug af SecurityCenter

Inden du begynder at bruge SecurityCenter, skal du gennemgå de komponenter og konfigurationsområder, du vil bruge til at administrere computerens beskyttelsesstatus. Flere oplysninger om den terminologi, der bruges i dette billede, finder du under Forklaring af beskyttelsesstatus (side 8) og Forklaring af beskyttelseskategorier (side 9). Derefter kan du gennemgå dine McAfee-kontooplysninger og kontrollere gyldigheden af dit abonnement.



I dette kapitel

Forklaring af beskyttelsesstatus

Computerens beskyttelsesstatus vises i beskyttelsesstatusområdet i startruden til SecurityCenter. Det angives, om computeren er fuldt beskyttet mod de seneste sikkerhedstrusler og kan påvirkes af ting, som f.eks. eksterne sikkerhedsangreb, andre sikkerhedsprogrammer og programmer, der benytter internettet.

Computerens beskyttelsesstatus kan være rød, gul eller grøn.

Beskyttelses-status	Beskrivelse
Rød	Din computer er ikke beskyttet. Beskyttelsesstatusområdet i startruden til SecurityCenter er rødt og angiver, at computeren ikke er beskyttet. SecurityCenter rapporterer mindst ét kritisk sikkerhedsproblem. For at opnå fuld beskyttelse skal du løse alle kritiske sikkerhedsproblemer i hver beskyttelseskategori (kategoristatus for problem er indstillet til **Handling påkrævet**, også med rødt). Oplysninger om, hvordan du løser beskyttelsesproblemer, finder du under Løsning af beskyttelsesproblemer (side 18).
Gul	Din computer er delvist beskyttet. Beskyttelsesstatusområdet i startruden til SecurityCenter er gult og angiver, at computeren ikke er beskyttet. SecurityCenter rapporterer mindst ét ikke-kritisk sikkerhedsproblem. For at opnå fuld beskyttelse skal du løse eller ignorere de ikke-kritiske sikkerhedsproblemer i hver beskyttelseskategori. Oplysninger om, hvordan du løser eller ignorerer beskyttelsesproblemer, finder du under Løse eller ignorere beskyttelsesproblemer (side 17).
Grøn	Din computer er fuldt beskyttet. Beskyttelsesstatusområdet i startruden til SecurityCenter er grønt og angiver, at computeren er beskyttet. SecurityCenter rapporterer ingen kritiske eller ikke-kritiske sikkerhedsproblemer. I hver beskyttelseskategori vises de tjenester, der beskytter computeren.

Forklaring af beskyttelseskategorier

Beskyttelsestjenesterne i SecurityCenter er opdelt i fire kategorier: Computer & Filer, Internet & Netværk, E-mail & IM og Forældrestyring. Disse kategorier hjælper dig med at gennemse og konfigurere de sikkerhedstjenester, der beskytter computeren.

Du kan klikke på et kategorinavn for at konfigurere beskyttelsestjenesterne og få vist de sikkerhedsproblemer, der evt. er registreret for disse tjenester. Hvis computerens beskyttelsesstatus er rød eller gul, vises meddelelsen *Handling påkrævet* eller *Bemærk* i en eller flere kategorier for at vise, at SecurityCenter har registreret et problem i kategorien. Flere oplysninger om beskyttelsesstatus finder du under Forklaring af beskyttelsesstatus (side 8).

Beskyttelseskategori	Beskrivelse
Computer & Filer	Kategorien Computer & Filer giver dig mulighed for at konfigurere følgende beskyttelsestjenester: ▪ Virusbeskyttelse ▪ Spywarebeskyttelse ▪ SystemGuards ▪ Windows-beskyttelse ▪ Pc-sundhed
Internet & Netværk	Kategorien Internet & Netværk giver dig mulighed for at konfigurere følgende beskyttelsestjenester: ▪ Firewall-beskyttelse ▪ Phishing-beskyttelse ▪ Identitetsbeskyttelse
E-mail & IM	Kategorien E-mail & IM giver dig mulighed for at konfigurere følgende beskyttelsestjenester: ▪ Beskyttelse mod e-mail-virus ▪ IM-virusbeskyttelse ▪ Beskyttelse mod e-mail-spyware ▪ Beskyttelse mod IM-spyware ▪ Spambeskyttelse
Forældrestyring	Kategorien Forældrestyring giver dig mulighed for at konfigurere følgende beskyttelsestjenester: ▪ Indholdsblokering

Forklaring af beskyttelsestjenester

Beskyttelsestjenester er de forskellige sikkerhedskomponenter i SecurityCenter, som du konfigurerer for at beskytte computeren. Beskyttelsestjenester svarer direkte til McAfee-programmer. Når du installerer VirusScan, bliver følgende beskyttelsestjenester f.eks. tilgængelige: Virus Protection, Spyware Protection, SystemGuards og Script Scanning. Flere oplysninger om disse beskyttelsestjenester finder du i VirusScan Hjælp.

Som standard aktiveres alle de beskyttelsestjenester, der er knyttet til et program, når du installerer programmet. Du kan dog til enhver tid deaktivere en beskyttelsestjeneste. Hvis du f.eks. installerer Forældrestyring, aktiveres både Indholdsblokering og Identitetsbeskyttelse. Hvis du ikke vil bruge beskyttelsestjenesten Indholdsblokering, kan du deaktivere den. Du kan også midlertidigt deaktivere en beskyttelsestjeneste, mens du udfører opsætnings- eller vedligeholdelsesopgaver.

Administrere dine abonnementer

Der følger et abonnement med hvert beskyttelsesprodukt fra McAfee, du køber, som giver dig mulighed for at bruge produktet på et bestemt antal computere og i en bestemt periode. Abonnementets længde afhænger af det, du har købt, men starter som regel, når du aktiverer produktet. Aktivering er nemt og gratis. Du skal blot bruge en internetforbindelse, men det er også vigtigt, fordi den giver dig mulighed for at modtage regelmæssige, automatiske produktopdateringer, der beskytter din computer mod de seneste trusler.

Aktiveringen sker normalt, når produktet installeres, men hvis du beslutter at vente (hvis du f.eks. ikke har en internetforbindelse), har du 15 dage til at aktivere produktet i. Hvis du ikke aktiverer inden 15 dage, modtager du ikke længere vigtige opdateringer til dine produkter eller får foretaget scanninger. Vi underretter dig med jævne mellemrum (med meddelelser på skærmen), når dit abonnement er ved at udløbe. Herved undgår du forstyrrelser i din beskyttelse ved at forny abonnementet tidligt eller konfigurere automatisk fornyelse på vores websted.

Hvis du ser et link i SecurityCenter, der beder dig om at aktivere, så er dit abonnement ikke blevet aktiveret endnu. Du kan se dit abonnements udløbsdato på din kontoside.

Få adgang til din McAfee-konto

Du kan nemt få adgang til dine McAfee-kontooplysninger (din kontoside) fra SecurityCenter.

1 Klik på **Min konto** under **Almindelige opgaver**.

2 Log ind på din McAfee-konto

Aktivere dit produkt

Aktivering sker normalt, når du installerer dit produkt. Men hvis det ikke er sket, vil du se et link i SecurityCenter, der beder dig om at aktivere. Vi underretter dig også med jævne mellemrum.

- Klik på **Forny dit abonnement** under **Oplysninger om SecurityCenter** i startruden til SecurityCenter.

Tip! Du kan også aktivere fra den advarsel, der vises med jævne mellemrum.

Kontrollere dit abonnement

Du skal kontrollere dit abonnement for at sikre, at det endnu ikke er udløbet.

- Højreklik på ikonet SecurityCenter i meddelelsesområdet længst til højre på proceslinjen, og klik derefter på **Bekræft abonnement**.

Forny dit abonnement

Umiddelbart før dit abonnement udløber, vil du se et link i SecurityCenter, der beder dig om at forny abonnementet. Vi underretter dig også med jævne mellemrum om forestående abonnementsudløb med alarmer.

- Klik på **Forny** under **Oplysninger om SecurityCenter** i startruden til SecurityCenter.

Tip! Du kan også forny dit produkt fra den besked, der vises med jævne mellemrum. Eller gå til din kontoside, hvor du kan forny eller konfigurere automatisk fornyelse.

KAPITEL 4

Opdatere SecurityCenter

SecurityCenter sikrer, at dine registrerede McAfee-programmer er aktuelle, ved at søge efter og installere onlineopdateringer hver fjerde time. Afhængigt af de programmer, du har installeret og aktiveret, kan onlineopdateringer indeholde de nyeste virusdefinitioner og opgraderinger af beskyttelse mod virus, hackere, spam og spyware og af dine personlige oplysninger. Hvis du vil søge efter opdateringer mere end hver fjerde time, kan du gøre det på ethvert tidspunkt. Mens SecurityCenter søger efter opdateringer, kan du foretage andre opgaver i programmet.

Selvom det ikke anbefales, kan du ændre den måde, SecurityCenter søger efter og installerer opdateringer på. Du kan f.eks. konfigurere SecurityCenter til at downloade, men ikke installere opdateringer, eller underrette dig før download og installation af opdateringer. Du kan også deaktivere automatisk opdatering.

Bemærk! Hvis du installerede dit McAfee-produkt fra en cd, skal du aktivere det inden for 15 dage, i modsat fald modtager du ikke vigtige opdateringer eller får foretaget scanninger.

I dette kapitel

Søge efter opdateringer

Som standard søger SecurityCenter automatisk efter opdateringer hver fjerde time, når computeren har forbindelse til internettet. Hvis du vil søge efter opdateringer mere end hver fjerde time, kan du gøre det. Hvis du har deaktiveret automatiske opdateringer, er du ansvarlig for regelmæssigt at søge efter opdateringer.

- Klik derefter på **Opdater** i startruden til SecurityCenter.

Tip! Du kan søge efter opdateringer uden at starte SecurityCenter ved at højreklikke på ikonet SecurityCenter i meddelelsesområdet på proceslinjen og derefter klikke på **Opdateringer**.

Konfigurere automatiske opdateringer

Som standard søger SecurityCenter automatisk efter og installerer opdateringer hver fjerde time, når computeren har forbindelse til internettet. Hvis du vil ændre denne standardfunktion, kan du konfigurere SecurityCenter til automatisk at downloade opdateringer og derefter give dig besked, når opdateringerne er parate til at blive installeret, eller give dig besked, inden opdateringerne downloades.

Bemærk! SecurityCenter underretter dig, når opdateringer er parate til at blive downloadet eller installeret, ved hjælp af alarmer. Fra disse alarmer kan du enten downloade eller installere opdateringerne eller udskyde opdateringerne. Når du opdaterer programmer fra en alarm, bliver du bedt om at bekræfte dit abonnement, inden programmerne downloades og installeres. Flere oplysninger finder du under Arbejde med alarmer (side 21).

1. Åbn ruden Konfiguration af SecurityCenter.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.

2. Klik på **Til** under **Automatiske opdateringer er deaktiveret** i ruden Konfiguration af SecurityCenter, og klik derefter på **Avanceret**.
3. Klik på en af følgende knapper:
   - **Installer opdateringerne automatisk, og giv mig besked, når mine tjenester er opdateret (anbefales)**
   - **Download opdateringerne automatisk, og giv mig besked, når de er klar til at blive installeret**
   - **Giv besked før download af opdateringer**
4. Klik på **OK**.

Deaktivere automatiske opdateringer

Hvis du deaktiverer automatiske opdateringer, er du ansvarlig for regelmæssigt at søge efter opdateringer. Ellers har din computer ikke den nyeste sikkerhedsbeskyttelse. Flere oplysninger om at søge efter opdateringer finder du under Søge efter opdateringer (side 13).

1. Åbn ruden Konfiguration af SecurityCenter.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.

2. Klik på **Fra** under **Automatiske opdateringer er aktiveret** i ruden Konfiguration af SecurityCenter.
3. Klik på **Ja** i dialogboksen til bekræftelse.

Tip! Du kan aktivere automatiske opdateringer ved at klikke på knappen **Til** eller fjerne markeringen af **Deaktiver automatisk opdatering, og lad mig kontrollere for opdateringer manuelt** i ruden Opdateringsindstillinger.

KAPITEL 5

Løse eller ignorere beskyttelsesproblemer

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Kritiske beskyttelsesproblemer kræver øjeblikkelig handling og kompromitterer din beskyttelsesstatus (ændrer farven til rød). Ikke-kritiske beskyttelsesproblemer kræver ikke øjeblikkelig handling og muligvis kompromittere din beskyttelsesstatus (afhængigt af typen af problem). For at opnå grøn beskyttelsesstatus skal du løse alle kritiske problemer og enten løse eller ignorere alle ikke-kritiske problemer. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician. Se Hjælp i McAfee Virtual Technician for at få flere oplysninger om McAfee Virtual Technician.

I dette kapitel

Løse beskyttelsesproblemer

De fleste sikkerhedsproblemer kan løses automatisk. Nogle problemer kræver dog, at du foretager en handling. Hvis Firewall-beskyttelse f.eks. er deaktiveret, kan SecurityCenter aktivere den automatisk. Hvis Firewall-beskyttelse ikke er installeret, skal du dog installere den. I følgende tabel beskrives nogle af de handlinger, du kan foretage, når du løser beskyttelsesproblemer manuelt:

Problem	Handling
Der er ikke udført en komplet scanning af computeren inden for de sidste 30 dage.	Scan computeren manuelt. Flere oplysninger findes i VirusScan Hjælp.
Dine virussignaturfiler er forældede.	Opdater beskyttelsen manuelt. Flere oplysninger findes i VirusScan Hjælp.
Et program er ikke installeret.	Installer programmet fra McAfees websted eller en cd.
Komponenter mangler i et program.	Installer programmet igen fra McAfees websted eller en cd.
Et program er ikke aktiveret og kan ikke modtage fuld beskyttelse.	Aktiver programmet på McAfees websted.
Dit abonnement er udløbet.	Kontroller din kontostatus på McAfees websted. Du kan få flere oplysninger under Administrere dine abonnementer (side 11).

Bemærk! Ofte påvirker et enkelt beskyttelsesproblem mere end én beskyttelseskategori. I dette tilfælde fjernes problemet fra alle andre beskyttelseskategorier, når du løser det.

Løse beskyttelsesproblemer automatisk

SecurityCenter kan løse de fleste beskyttelsesproblemer automatisk. De konfigurationsændringer, som SecurityCenter foretager, når beskyttelsesproblemer løses automatisk, registreres ikke i hændelseslogfilen. Flere oplysninger om hændelser finder du under Vise hændelser (side 27).

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Reparer** i i beskyttelsesstatusområdet i startruden til SecurityCenter.

Løse beskyttelsesproblemer manuelt

Hvis et eller flere beskyttelsesproblemer stadig forekommer, når du har forsøgt at løse dem automatisk, kan du løse problemerne manuelt.

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på den beskyttelseskategori, SecurityCenter har rapporteret problemet i, i startruden til SecurityCenter.
3. Klik på linket efter beskrivelsen af problemet.

Ignorere beskyttelsesproblemer

Hvis SecurityCenter registrerer et ikke-kritisk problem, kan du løse det eller ignorere det. Andre ikke-kritiske problemer (hvis f.eks. Anti-Spam eller Forældrestyring ikke er installeret) ignoreres automatisk. Ignorerede problemer vises ikke i området med oplysninger om beskyttelseskategori i startruden til SecurityCenter, medmindre computerens beskyttelsesstatus er grøn. Hvis du ignorerer et problem, men senere beslutter, at det skal vises i området med oplysninger om beskyttelseskategori, selvom computerens beskyttelsesstatus ikke er grøn, kan du få vist det ignorerede problem.

Ignorere et beskyttelsesproblem

Hvis SecurityCenter registrerer et ikke-kritiske problem, som du ikke vil løse, kan du ignorere det. Når et problem ignoreres, fjernes det fra området med oplysninger om beskyttelseskategori i SecurityCenter.

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på den beskyttelseskategori, SecurityCenter har rapporteret problemet i, i startruden til SecurityCenter.
3. Klik på linket **Ignorer** ud for beskyttelsesproblemet.

Vise eller skjule ignorerede problemer

Afhængigt af alvoren kan du vise eller skjule et ignoreret beskyttelsesproblem.

1. Åbn ruden Alarmindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
   3. Under **Alarmer** skal du klikke på **Avanceret**.

2. Klik på **Ignorerede problemer** i ruden Konfiguration af SecurityCenter.
3. I ruden Ignorerede problemer skal du foretage en af følgende handlinger:
   - Marker dets afkrydsningsfelt for at ignorere et problem.
   - Fjern markeringen fra dets afkrydsningsfelt i området med oplysninger om beskyttelseskategori for at rapportere et problem.
4. Klik på **OK**.

Tip! Du kan også ignorere et problem ved at klikke på linket **Ignorer** ud for det rapporterede problem i området med oplysninger om beskyttelseskategori.

KAPITEL 6

Arbejde med alarmer

Alarmer er små pop-up-dialogbokse, som vises i skærmens nederste højre hjørne, når bestemte SecurityCenter-hændelser forekommer. En alarm indeholder detaljerede oplysninger om en hændelse samt anbefalinger og indstillinger, der kan løse de problemer, der evt. er knyttet til hændelsen. Nogle alarmer indeholder også links til yderligere oplysninger om hændelsen. Med disse links kan du gå til McAfees globale websted eller sende oplysninger til McAfee til fejlfinding.

Der findes følgende tre typer alarmer: rød, gul og grøn.

Alarmtype	Beskrivelse
Rød	En rød alarm er en kritisk besked, som kræver, at du reagerer. Røde alarmer forekommer, når SecurityCenter ikke kan afgøre, hvordan et beskyttelsesproblem kan løses automatisk.
Gul	En gul alarm er en ikke-kritisk besked, som ofte kræver, at du reagerer.
Grøn	En grøn alarm er en ikke-kritisk besked, som ikke kræver, at du reagerer. Grønne alarmer giver grundlæggende oplysninger om en hændelse.

Alarmer spiller en vigtig rolle i forbindelse med overvågning og administration af din beskyttelsesstatus, og derfor kan du ikke deaktivere dem. Du kan dog kontrollere, om visse typer oplysningsalarmer skal vises, og konfigurere andre alarmindstillinger (f.eks. om SecurityCenter skal afspille en lyd sammen med en alarm eller vise McAfee-velkomstbilledet ved opstart).

I dette kapitel

Vise og skjule oplysningsalarmer

Oplysningsalarmer giver dig besked om hændelser, som ikke udgør nogen trusler mod din sikkerhed. Hvis du f.eks. har konfigureret Firewall-beskyttelse, vises en oplysningsalarm som standard, når et program på computeren gives adgang til internettet. Hvis du ikke ønsker at få vist en bestemt type oplysningsalarm, kan du skjule den. Hvis du ikke ønsker at få vist nogen oplysningsalarmer, kan du skjule dem alle. Du kan også skjule alle oplysningsalarmer, når du spiller et spil i fuldskærmstilstand på computeren. Når du er færdig med at spille spillet og afslutter fuldskærmstilstand, viser SecurityCenter oplysningsalarmer igen.

Hvis du ved en fejl skjuler en oplysningsalarm, kan du til enhver tid få den vist igen. Som standard viser SecurityCenter alle oplysningsalarmer.

Vise eller skjule oplysningsalarmer

Du kan konfigurere SecurityCenter til at vise nogle oplysningsalarmer og skjule andre eller til at skjule alle oplysningsalarmer.

1. Åbn ruden Alarmindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
   3. Under **Alarmer** skal du klikke på **Avanceret**.

2. Klik på **Oplysningsalarmer** i ruden Konfiguration af SecurityCenter.
3. I Oplysningsalarmer skal du foretage en af følgende handlinger:
   - Hvis du vil vise en oplysningsalarm, skal du fjerne markeringerne i dens afkrydsningsfelt.
   - Hvis du vil skjule en oplysningsalarm, skal du markere dens afkrydsningsfelt.
   - Hvis du vil skjule alle oplysningsalarmer, skal du markere afkrydsningsfeltet **Vis ikke oplysningsalarmer**.
4. Klik på **OK**.

Tip! Du kan også skjule en oplysningsalarm ved at markere afkrydsningsfeltet **Vis ikke denne advarsel igen** i selve alarmen. Hvis du gør det, kan du få vist oplysningsalarmen igen ved at fjerne markeringen i det pågældende afkrydsningsfelt i ruden Oplysningsalarmer.

Vise eller skjule oplysningsalarmer under spil

Du kan også skjule oplysningsalarmer, når du spiller et spil i fuldskærmstilstand på computeren. Når du er færdig med at spille spillet og afslutter fuldskærmstilstand, viser SecurityCenter oplysningsalarmer igen.

1 Åbn ruden Alarmindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
   3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Marker eller fjern markeringen i afkrydsningsfeltet **Vis oplysningsalarmer, når spilletilstand registreres** i ruden Alarmindstillinger.

3 Klik på **OK**.

Konfigurere alarmindstillinger

Alarmernes udseende og frekvens konfigureres af SecurityCenter. Du kan dog justere de grundlæggende alarmindstillinger. Du kan f.eks. afspille en lyd med alarmer eller skjule velkomstbilledalarmen, når Windows startes. Du kan også skjule alarmer, der giver dig besked om virusudbrud og andre sikkerhedstrusler på internettet.

Afspille en lyd med alarmer

Hvis du vil modtage en lydbesked, når en alarm forekommer, kan du konfigurere SecurityCenter til at afspille en lyd med hver alarm.

1 Åbn ruden Alarmindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
   3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Marker afkrydsningsfeltet **Afspil en lyd, når der opstår en alarm** under **Lyd** i ruden Alarmindstillinger.

Skjule velkomstbilledet ved opstart

Som standard vises McAfee-velkomstbilledet kortvarigt, når Windows startes, og giver dig besked om, at SecurityCenter beskytter computeren. Du kan dog skjule velkomstbilledet, hvis du ikke ønsker at få den vist.

1 Åbn ruden Alarmindstillinger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Fjern markeringen i afkrydsningsfeltet **Vis McAfee-velkomstskærmen, når Windows starter** under **Velkomstbillede** i ruden Alarmindstillinger.

Tip! Du kan til enhver tid få vist velkomstbilledet igen ved at markere afkrydsningsfeltet **Vis McAfee-velkomstskærmen, når Windows starter**.

Skjule alarmer om virusudbrud

Du kan skjule alarmer, der giver dig besked om virusudbrud og andre sikkerhedstrusler på internettet.

1 Åbn ruden Alarmindstillinger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Fjern markeringen i afkrydsningsfeltet **Alarmer, når der forekommer en virus eller sikkerhedstrussel** i ruden Alarmindstillinger.

Tip! Du kan til enhver tid få vist alarmer om virusudbrud ved at markere afbrydsningsfeltet **Alarmer, når der forekommer en virus eller sikkerhedstrussel**

Skjule sikkerhedsmeddelelser

Du kan skjule sikkerhedsmeddelelser om beskyttelse af flere computere på dit hjemmenetværk. Disse meddelelser indeholder oplysninger om dit abonnement, det antal computere du kan beskytte med dit abonnement, samt hvordan du udvider abonnementet til at beskytte endnu flere computere.

1 Åbn ruden Alarmindstillinger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Fjern markeringen i feltet **Vis virusmeddelelser eller andre sikkerhedsmeddelelser** i ruden Alarmindstillinger.

Tip! Du kan få vist disse sikkerhedsmeddelelser når som helst ved at markere afkrydsningsfeltet **Vis virusmeddelelser eller andre sikkerhedsmeddelelser**.

KAPITEL 7

Vise hændelser

En hændelse er en handling eller konfigurationsændring, der forekommer inden for en beskyttelseskategori og de tilknyttede beskyttelsestjenester. Forskellige beskyttelsestjenester registrerer forskellige typer hændelser. SecurityCenter registrerer en hændelse, hvis en beskyttelsestjeneste er aktiveret eller deaktiveret. Virusbeskyttelse registrerer en hændelse, hver gang en virus registreres og fjernes. Firewall-beskyttelse registrerer en hændelse, hver gang et forsøg på at oprette forbindelse til internettet blokeres. Flere oplysninger om beskyttelseskategorier finder du under Forklaring af beskyttelseskategorier (side 9).

Du kan få vist hændelser, når du foretager fejlfinding af konfigurationsproblemer og gennemgår handlinger, der er foretaget af andre brugere. Mange forældre bruger hændelseslogfilen til at overvåge børnenes adfærd på internettet. Du kan få vist nylige hændelser, hvis du kun ønsker at undersøge de sidste 30 hændelser, der er forekommet. Du kan få vist alle hændelser, hvis du vil undersøge en omfattende liste over alle de hændelser, der er forekommet. Når du får vist alle hændelser, starter SecurityCenter hændelsesloggen, som sorterer hændelser efter den beskyttelseskategori, de er forekommet i.

I dette kapitel

Vise de seneste hændelser

Du kan få vist nylige hændelser, hvis du kun ønsker at undersøge de sidste 30 hændelser, der er forekommet.

- Klik på **Vis seneste hændelser** under **Almindelige opgaver**.

Vise alle hændelser

Du kan få vist alle hændelser, hvis du vil undersøge en omfattende liste over alle de hændelser, der er forekommet.

1. Klik på **Vis seneste hændelser** under **Almindelige opgaver**.
2. Klik på **Vis logfil** i ruden Seneste hændelser.
3. Klik på den type hændelse, du ønsker at få vist.

KAPITEL 8

McAfee VirusScan

De avancerede registrerings- og beskyttelsestjenester i VirusScan forsvarer dig og din computer mod de nyeste sikkerhedstrusler, herunder virus, trojanske heste, sporingscookies, spyware, adware og andre potentielt uønskede programmer. Beskyttelsen udvides ud over filerne og mapperne på den stationære computer og målrettes mod trusler fra forskellige indgange, herunder e-mail, onlinemeddelelser og internettet.

Med VirusScan beskyttes computeren omgående og hele tiden (der kræves ingen langsommelig administration). Mens du arbejder, spiller, søger på internettet eller tjekker din e-mail, køres programmet i baggrunden og overvåger, scanner og registrerer potentiel skade i real tid. Omfattende scanninger gennemføres efter en plan, så computeren jævnligt kontrolleres ved hjælp af et mere avanceret sæt indstillinger. VirusScan giver dig fleksibilitet til at tilpasse denne funktion, hvis du ønsker det. Hvis du ikke ønsker det, forbliver computeren beskyttet.

Ved normal brug af en computer kan den blive infiltreret med virus, orm og andre potentielle trusler. Hvis det forekommer, giver VirusScan dig besked om truslen, men normalt håndterer programmer truslen for dig og renser eller sætter inficerede elementer i karantæne, inden der opstår skade. Selvom det er sjældent, kan der være nødvendigt med yderligere handling. I disse tilfælde lader VirusScan dig vælge, hvad du vil gøre (scanne igen, næste gang comptueren startes, beholde det registrerede element eller fjerne det registrerede element).

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i VirusScan

Omfattende virusbeskyttelse

Beskyt dig selv og din computer mod de seneste sikkerhedstrusler, herunder virus, trojanske heste, sporingscookies, spyware, adware og andre potentielt uønskede programmer. Beskyttelsen udvides ud over filerne og mapperne på den stationære computer og målrettes mod trusler fra forskellige indgange, herunder e-mail, onlinemeddelelser og internettet. Der kræves ingen langsommelig administration.

Ressourcebevidste scanningsindstillinger

Tilpas scanningsindstillingerne, hvis du vil, men selvom du ikke gør det, er computeren fortsat beskyttet. Hvis du oplever langsom scanningshastighed, kan du deaktivere indstillingen for brug af færrest mulige computerressourcer. Du skal dog være opmærksom på, at virusbeskyttelse prioriteres højere end andre opgaver.

Automatiske reparationer

Hvis VirusScan registrerer en sikkerhedstrussel under en scanning, forsøger programmet at håndtere truslen automatisk i overensstemmelse med trusselstypen. På den måde kan de fleste trusler registreres og neutraliseres uden din medvirken. Selvom det er sjældent, kan VirusScan ikke altid selv neutralisere en trussel. I disse tilfælde lader VirusScan dig vælge, hvad du vil gøre (scanne igen, næste gang computeren startes, beholde det registrerede element eller fjerne det registrerede element).

Afbryde opgaver midlertidigt i fuldskærmstilstand

Når du f.eks. ser film, spiller spil eller udfører andre aktiviteter på computeren, som fylder hele skærmen, standser VirusScan en række opgaver midlertidigt, herunder manuelle scanninger.

KAPITEL 9

Scanne computeren

Første gang du starter SecurityCenter, begynder virusbeskyttelsen i VirusScan at beskytte computeren mod potentielt skadelige virus, trojanske heste og andre sikkerhedstrusler i realtid. Medmindre du deaktiverer virusbeskyttelse i realtid, overvåger VirusScan konstant computeren for virusaktivitet og scanner filer, hver gang du eller din computer forsøger at åbne dem, ved hjælp af de indstillinger for realtidsscanning, du vælger. Hvis du vil sikre, at computeren altid er beskyttet mod de seneste sikkerhedstrusler, skal du lade virusbeskyttelse i realtid være aktiveret og oprette en plan for regelmæssige og mere omfattende manuelle scanninger. Flere oplysninger om konfiguration af scanningsindstillinger finder du under Konfigurere virusbeskyttelse (side 47).

VirusScan indeholder et mere detaljeret sæt scanningsindstillinger for virusbeskyttelse, som giver dig mulighed for regelmæssigt at køre mere omfattende scanninger. Du kan køre komplette, hurtige, brugertilpassede eller planlagte scanninger fra SecurityCenter. Du kan også køre manuelle scanninger direkte i Windows Stifinder, mens du arbejder. Ved scanning i SecurityCenter kan du skifte scanningsindstillinger undervejs. Scanning fra Windows Stifinder gør det dog nemt for dig at beskytte computerens sikkerhed.

Uanset om du kører en scanning fra SecurityCenter eller Windows Stifinder, kan du få vist scanningsresultaterne efter scanningen. Du kan få vist resultaterne af en scanning for at finde ud af, om VirusScan har registreret, repareret eller sat virus, trojanske heste, spyware, adware, cookies og andre potentielt uønskede programmer i karantæne. Du kan få vist resultaterne af en scanning på forskellige måder. Du kan f.eks. få vist et grundlæggende resume af scanningsresultaterne eller detaljerede oplysninger som f.eks. infektionsstatus og -type. Du kan også få vist generel scannings- og registreringsstatistik.

I dette kapitel

Scanne din pc

VirusScan byder på et komplet sæt scanningsindstillinger for virusbeskyttelse, herunder scanning i realtid (som konstant overvåger din pc for trusselsaktivitet), manuel scanning fra Windows Stifinder samt komplette, hurtige, brugertilpassede eller planlagte scanninger fra SecurityCenter.

For at...	Skal du...
Starte scanning i realtid, så computeren konstant overvåges for virusaktivitet og scanner filer, hver gang du eller din computer forsøger at åbne dem.	1. Åbn konfigurationsruden Computer & filer. Hvordan? 1. Klik på menuen **Avanceret** i den venstre rude. 2. Klik på **Konfigurer**. 3. Klik derefter på **Computer & filer** i ruden Konfigurer. 2. Under **Virusbeskyttelse** skal du klikke på **Til**. **Bemærk**! Scanning i realtid er som standard aktiveret.
Starte en hurtig scanning for hurtigt at kontrollere din computer for trusler	1. Klik på **Scan** i menuen Grundlæggende. 2. Klik på **Start** under Hurtig scanning i ruden Scanningsindstillinger.
Starte en komplet scanning for at få foretaget en grundig kontrol af din computer for trusler	1. Klik på **Scan** i menuen Grundlæggende. 2. Klik på **Start** under Komplet scanning i ruden Scanningsindstillinger.

For at...	Skal du...
Starte en brugertilpasset scanning baseret på dine egne indstillinger	1. Klik på **Scan** i menuen Grundlæggende. 2. Klik på **Start** under Lad mig vælge i ruden Scanningsindstillinger. 3. Tilpas en scanning ved at fjerne markeringen ud for eller markere: **Alle trusler i alle filer** **Ukendte virus** **Arkivfiler** **Spyware og potentielle trusler** **Sporingscookies** **Skjulte programmer** 4. Klik på **Start**.
Starte en manuel scanning for at kontrollere filer, mapper og drev for trusler	1. Åbn Windows Stifinder. 2. Højreklik på en fil, en mappe eller et drev, og klik derefter på **Scan**.

For at...	Skal du...
Starte en planlagt scanning, der jævnligt scanner computeren for trusler	1. Åbn ruden Planlagt scanning. Hvordan? 1. Klik på **Start** under **Almindelige opgaver**. 2. Klik på **Computer & filer** i startruden for SecurityCenter. 3. Klik på **Konfigurer** i området Computer & filer. 4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**. 5. Klik på **Planlagt scanning** i ruden Virusbeskyttelse. 2. Vælg **Aktiver planlagt scanning**. 3. Hvis du vil reducere den mængde processorkraft, der normalt bruges til scanning, skal du vælge **Scan ved brug af færrest mulige computerressourcer**. 4. Vælg en eller flere dage. 5. Angiv et starttidspunkt. 6. Klik på **OK**.

Scanningsresultaterne vises i alarmen Scanning fuldført. Resultaterne omfatter antallet af scannede, registrerede og fjernede elementer og antallet af elementer i karantæne. Klik på **Vis scanningsoplysninger** for at få flere oplysninger om scanningsresultaterne eller bearbejde de inficerede elementer.

Bemærk! Du kan få mere at vide om scanningsindstillinger under Scanningstyper. (side 40)

Vise scanningsresultater

Når en scanning er udført, kan du få vist resultaterne for at finde ud af, hvad scanningen har fundet, og for at analysere computerens beskyttelsesstatus. Scanningsresultaterne fortæller dig, om VirusScan har registreret, repareret eller sat virus, trojanske heste, spyware, adware, cookies og andre potentielt uønskede programmer i karantæne.

Klik på **Scan** i menuen Grundlæggende eller Avanceret, og gør derefter følgende:

For at...	Skal du...
Få vist scanningsresultater i alarmen	Se scanningsresultater i alarmen Scanning fuldført.
Få vist flere oplysninger om scanningsresultater	Klikke på **Vis scanningsoplysninger** i alarmen Scanning fuldført.
Få vist en hurtig oversigt over scanningsresultaterne	Pege på ikonet **Scanning fuldført** i meddelelsesområdet på proceslinjen.
Få vist scannings- og registreringsstatistik	Dobbeltklikke på ikonet **Scanning fuldført** i meddelelsesområdet på proceslinjen.
Få vist detaljer om registrerede elementer, infektionsstatus og type	1. Dobbeltklikke på ikonet **Scanning fuldført** i meddelelsesområdet på proceslinjen. 2. Klikke på **Detaljer** i ruden Komplet scanning, Hurtig scanning, Brugertilpasset scanning eller Manuel scanning.
Få vist detaljer om den seneste scanning	Dobbeltklikke på ikonet **Scanning fuldført** i meddelelsesområdet på proceslinjen og få vist detaljerne for den seneste scanning under Din scanning i ruden Komplet scanning, Hurtig scanning, Brugertilpasset scanning eller Manuel scanning.

KAPITEL 10

Arbejde med scanningsresultater

Hvis VirusScan registrerer en sikkerhedstrussel under en scanning, forsøger programmet at håndtere truslen automatisk i overensstemmelse med trusselstypen. Hvis VirusScan f.eks. registrerer en virus, trojansk hest eller sporingscookie på computeren, forsøger programmet at rense den inficerede fil. VirusScan sætter altid en fil i karantæne, før programmet forsøger at rense den. Hvis filen ikke er renset, sættes den i karantæne.

Ved nogle sikkerhedstrusler kan VirusScan evt. ikke rense en fil eller sætte den i karantæne. Hvis det er tilfældet, giver VirusScan dig besked om, at du skal håndtere truslen. Du kan foretage forskellige handlinger, afhængigt af trusselstypen. Hvis VirusScan f.eks. har registreret en virus i en fil, men ikke kan rense den eller sætte den i karantæne, tillades der ikke yderligere adgang til filen. Hvis VirusScan registrerer sporingscookies, men ikke kan rense dem eller sætte dem i karantæne, kan du vælge at fjerne dem eller have tillid til dem. Hvis VirusScan registrerer potentielt uønskede programmer, foretager VirusScan ingen automatiske handlinger. I stedet får du mulighed for at vælge, om programmet skal i karantæne, eller du har tillid til det.

Når VirusScan sætter elementer i karantæne, krypteres og isoleres de i en mappe for at forhindre disse filer, programmer eller cookies i at beskadige computeren. Du kan gendanne eller fjerne elementer i karantæne. I de fleste tilfælde kan du slette en cookie i karantæne, uden at det påvirker systemet. Hvis VirusScan har sat et program, som du genkender og bruger, i karantæne, kan du overveje at gendanne det.

I dette kapitel

Arbejde med virus og trojanske heste

Hvis VirusScan f.eks. registrerer en virus eller en trojansk hest i en fil på computeren, forsøger programmet at rense filen. Hvis VirusScan ikke kan rense filen, sættes den i karantæne. Hvis det mislykkes, tillades adgang til filen ikke (kun ved realtidsscanning).

1 Åbn ruden Scanningsresultater.

   Hvordan?

   1. Dobbeltklik på ikonet **Scanning fuldført** i meddelelsesområdet længst til højre på proceslinjen.
   2. I ruden Status for scanning: Manuel scanning skal du klikke på **Vis resultater**.

2 Klik på **Virus og trojanske heste** i ruden Scanningsresultater.

Bemærk! Hvis du vil arbejde med filer, som VirusScan har sat i karantæne, finder du flere oplysninger under Arbejde med filer i karantæne (side 39).

Arbejde med potentielt uønskede programmer

Hvis VirusScan registrerer et potentielt uønsket program på computeren, kan du fjerne programmet eller have tillid til det. Hvis du ikke kender programmet, anbefaler vi, at du overvejer at fjerne det. Fjernelse af et potentielt uønsket program sletter det ikke fra systemet. I stedet sættes det i karantæne, så det ikke kan beskadige computeren eller dine filer.

1 Åbn ruden Scanningsresultater.

   Hvordan?

   1. Dobbeltklik på ikonet **Scanning fuldført** i meddelelsesområdet længst til højre på proceslinjen.
   2. I ruden Status for scanning: Manuel scanning skal du klikke på **Vis resultater**.

2 Klik på **Potentielt uønskede programmer** i ruden Scanningsresultater.

3 Vælg et potentielt uønsket program.

4 Under **Jeg ønsker at**, skal du klikke på **Fjern** eller **Hav tillid til**.

5 Bekræft den valgte indstilling.

Arbejde med filer i karantæne

Når VirusScan sætter inficerede filer i karantæne, krypteres og isoleres de i en mappe for at forhindre disse filer i at beskadige computeren. Du kan derefter gendanne eller fjerne filerne i karantæne.

1 Åbn ruden Filer i karantæne.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Gendan**.
3. Klik på **Filer**.

2 Vælg en fil, der er sat i karantæne.

3 Nu kan du gøre følgende:

- Hvis du vil reparere den inficerede fil og flytte den tilbage til dens oprindelige placering på computeren, skal du klikke på **Gendan**.
- Hvis du vil fjerne den inficerede fil fra computeren, skal du klikke på **Fjern**.

4 Klik på **Ja** for at bekræfte den valgte indstilling.

Tip! Du kan gendanne eller fjerne flere filer på én gang.

Arbejde med programmer og cookies i karantæne

Når VirusScan sætter potentielt uønskede programmer eller sporingscookies i karantæne, krypteres de og flyttes derefter til en beskyttet mappe for at forhindre disse programmer eller cookies i at beskadige computeren. Du kan derefter gendanne eller fjerne elementerne i karantæne. I de fleste tilfælde kan du slette et element i karantæne, uden at det påvirker systemet.

1 Åbn ruden Programmer og sporingscookies i karantæne.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Gendan**.
3. Klik på **Programmer og Cookies**.

2 Vælg et program eller en cookie, der er sat i karantæne.

3 Nu kan du gøre følgende:

- Hvis du vil reparere den inficerede fil og flytte den tilbage til dens oprindelige placering på computeren, skal du klikke på **Gendan**.
- Hvis du vil fjerne den inficerede fil fra computeren, skal du klikke på **Fjern**.

4 Klik på **Ja** for at bekræfte handlingen.

Tip! Du kan gendanne eller fjerne flere programmer og cookies på én gang.

Scanningstyper

VirusScan byder på et komplet sæt scanningsindstillinger for virusbeskyttelse, herunder scanning i realtid (som konstant overvåger din pc for trusselsaktivitet), manuel scanning fra Windows Stifinder samt muligheden for at køre komplette, hurtige og brugertilpassede scanninger fra SecurityCenter eller tilpasse, hvornår planlagte scanninger finder sted. Ved scanning i SecurityCenter kan du skifte scanningsindstillinger undervejs.

Scanning i realtid:

Virusbeskyttelse i realtid overvåger konstant computeren for virusaktivitet og scanner filer, hver gang du eller din computer forsøger at åbne dem. Hvis du vil sikre, at computeren altid er beskyttet mod de seneste sikkerhedstrusler, skal du lade virusbeskyttelse i realtid være aktiveret og oprette en plan for regelmæssige og mere omfattende manuelle scanninger.

Du kan angive standardindstillinger for scanning i realtid, som omfatter scanning for ukendte virus og kontrol af trusler i sporingscookies og på netværksdrev. Du kan også drage nytte af beskyttelse for bufferoverløb, som er aktiveret som standard (undtagen hvis du bruger et Windows Vista 64-bit-operativsystem). Du kan få mere at vide under Vælge indstillinger for realtidsscanning (side 48).

Hurtig scanning

Med en hurtig scanning kan du kontrollere for trusselsaktivitet i processer, vigtige Windows-filer og andre sårbare områder på computeren.

Komplet scanning

Med en komplet scanning kan du kontrollere hele computeren grundigt for virus, spyware og andre sikkerhedstrusler, der kan forekomme hvor som helst på din pc.

Brugertilpasset scanning

Med en brugertilpasset scanning kan du vælge dine egne scanningsindstillinger for at kontrollere for trusselsaktivitet på din pc. Brugertilpassede scanningsindstillinger omfatter kontrol af trusler i alle filer, arkivfiler og cookies samt scanning for ukendte virus, spyware og skjulte programmer.

Du kan angive standardindstillinger for brugertilpassede scanninger, som omfatter scanning for ukendte virus, arkivfiler, spyware og potentielle trusler, sporingscookies og skjulte programmer. Du kan også scanne ved brug af færrest mulige computerressourcer. Du kan få mere at vide under Vælge indstillinger for brugertilpasset scanning (side 50).

Manuel scanning

Med en manuel scanning kan du hurtigt kontrollere for trusler i filer, mapper og på drev, mens du arbejder, i Windows Stifinder.

Planlagte scanninger

Planlagte scanninger kontrollerer din computer grundigt for virus og andre trusler på enhver dag og ethvert tidspunkt i løbet af ugen. Planlagte scanninger kontrollerer altid hele computeren ved hjælp af standardindstillingerne for scanning. Som standard gennemfører VirusScan en planlagt scanning en gang om ugen. Hvis du oplever langsom scanningshastighed, kan du deaktivere indstillingen for brug af færrest mulige computerressourcer. Du skal dog være opmærksom på, at virusbeskyttelse prioriteres højere end andre opgaver. Du kan få mere at vide under Planlægge en scanning (side 53)

Bemærk! Du kan få mere at vide om, hvilke scanningsindstillinger der er bedst til dig under Scanne pc'en (side 32)

KAPITEL 11

Bruge ekstra beskyttelse

Ud over virusbeskyttelse i realtid giver VirusScan avanceret beskyttelse mod scripts, spyware og potentielt skadelige vedhæftede filer i e-mail og onlinemeddelelser. Som standard er scriptscanning samt spyware-, e-mail- og onlinemeddelelsesbeskyttelse aktiveret og beskytter computeren.

Scriptscanning

Scriptscanning registrerer potentielt skadelige scripts og forhindrer dem i at køre på din computer eller i din internetbrowser. Funktionen overvåger computeren for mistænkelig scriptaktivitet, f.eks. et script, der opretter, kopierer eller sletter filer, eller som åbner din Windows-registreringsdatabase, og giver dig besked, inden der opstår skade.

Spywarebeskyttelse

Spywarebeskyttelse registrerer spyware, adware og andre potentielt uønskede programmer. Spyware er software, der hemmeligt kan installeres på din computer for at overvåge dine aktiviteter, indsamle personlige oplysninger og endda gribe ind i din kontrol over computeren ved at installere yderligere software eller omdirigere browseraktivitet.

E-mail-beskyttelse

E-mail-beskyttelse registrerer mistænkelig aktivitet i de e-mail-beskeder og vedhæftede filer, du afsender.

Beskyttelse af onlinemeddelelser

Beskyttelse af onlinemeddelelser registrerer potentielle sikkerhedstrusler i vedhæftede filer i onlinemeddelelser, som du modtager. Funktionen forhindrer også IM-programmer i at dele personlige oplysninger.

I dette kapitel

Starte scriptscanning

Slå scriptscanning til for at registrere potentielt skadelige scripts og forhindre dem i at køre på din computer. Scriptscanning giver dig besked, når et script forsøger at oprette, kopiere eller slette filer på computeren eller foretage ændringer i Windows-registreringsdatabasen.

1 Åbn konfigurationsruden Computer & filer.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **Computer & filer** i ruden Konfigurer.

2 Under **Scriptscanning** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå scriptscanning fra, men computeren bliver så sårbar over for skadelige scripts.

Starte spywarebeskyttelse

Slå spywarebeskyttelse til for at registrere og fjerne spyware, adware og andre potentielt uønskede programmer, som samler og sender data uden din viden eller tilladelse.

1 Åbn konfigurationsruden Computer & filer.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **Computer & filer** i ruden Konfigurer.

2 Under **Scriptscanning** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå spywarebeskyttelse fra, men computeren bliver så sårbar over for potentielt uønskede programmer.

Starte e-mail-beskyttelse

Slå e-mail-beskyttelse til for at registrere orm og potentielle trusler i indgående (POP3) og udgående (SMTP) e-mail-beskeder og vedhæftede filer.

1 Åbn konfigurationsruden E-mail & IM.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **E-mail & IM** i ruden Konfigurer.

2 Under **E-mail-beskyttelse** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå e-mail-beskyttelse fra, men computeren bliver så sårbar over for e-mail-trusler.

Starte beskyttelse af onlinemeddelelser

Slå beskyttelse af onlinemeddelelser til for at registrere sikkerhedstrusler i vedhæftede filer i indgående onlinemeddelelser.

1 Åbn konfigurationsruden E-mail & IM.

Hvordan?

1. Klik på menuen **Avanceret** i den venstre rude.
2. Klik på **Konfigurer**.
3. Klik derefter på **E-mail & IM** i ruden Konfigurer.

2 Under **Beskyttelse af onlinemeddelelser** skal du klikke på **Til**.

Bemærk! Du kan til enhver tid slå beskyttelse af onlinemeddelelser fra, men computeren bliver så sårbar over for skadelige vedhæftede filer i onlinemeddelelser.

KAPITEL 12

Konfigurere virusbeskyttelse

Du kan angive forskellige indstillinger for planlagte, brugertilpassede og realtidsscanninger. Da realtidsbeskyttelse konstant overvåger computeren, kan du f.eks. vælge et bestemt sæt grundlæggende scanningsindstillinger og reservere et mere omfattende sæt scanningsindstillinger til manuel, on-demand-beskyttelse.

Du kan også beslutte, hvordan VirusScan skal overvåge og håndtere potentielt uautoriserede eller uønskede ændringer på din pc vha. SystemGuards og lister med elementer, der er tillid til. SystemGuards overvåger, logfører, rapporterer og administrerer potentielt uautoriserede ændringer i Windows-databasen eller vigtige systemfiler på computeren. Uautoriserede ændringer i registreringsdatabasen kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler. Du kan bruge lister med elementer, der er tillid til, for at afgøre, om du har tillid til eller ønsker at fjerne regler, der registrerer fil- eller databaseændringer (SystemGuards) samt program- eller bufferoverløb. Hvis du har tillid til elementet og angiver, at du ikke ønsker at modtage besked om dets aktivitet i fremtiden, føjes elementet til en liste over elementer, der er tillid til. Derefter registrerer VirusScan det ikke længere og giver dig ikke besked om dets aktivitet.

I dette kapitel

Vælge indstillinger for realtidsscanning

Når du starter virusbeskyttelse i realtid, bruger VirusScan et standardsæt indstillinger til at scanne filer. Du kan dog ændre standardinstillingerne, så de opfylder dine behov.

Hvis du vil ændre indstillingerne for realtidsscanning, skal du vælge, hvad VirusScan skal kontrollere for under en scanning, og de placeringer og filtyper, der skal scannes. Du kan f.eks. vælge, om VirusScan skal kontrollere for ukendte virus eller cookies, som websteder kan bruge til at registrere dine aktiviteter, og om programmet skal scanne netværksdrev, der er tilknyttet computeren, eller kun lokale drev. Du kan også vælge, hvilke typer filer der skal scannes (alle filer eller kun programfiler og dokumenter, da de fleste virus registreres i disse filer).

Når du ændrer indstillingerne for realtidsscanning, skal du også afgøre, om det er vigtigt for computeren, at beskyttelse for bufferoverløb er aktiveret. En buffer er en del af hukommelsen, som midlertidigt lagrer computerinformation. Bufferoverløb kan forekomme, når den mængde oplysninger, som mistænkelig programmer eller processer lagrer i en buffer, overstiger bufferens kapacitet. Hvis det sker, bliver computeren sårbar over for sikkerhedsangreb.

Vælge indstillinger for realtidsscanning

Du kan angive indstillinger for realtidsscanning for at tilpasse, hvad VirusScan skal kontrollere for under en scanning, og de placeringer og filtyper, der skal scannes. Indstillingerne omfatter scanning for ukendte virus og sporingscookies samt beskyttelse mod bufferoverløb. Du kan også konfigurere realtidsscanning til at kontrollere netværksdrev, der er tilknyttet på computeren.

1 Åbn ruden Scanning i realtid.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.

2 Angiv de ønskede indstillinger for realtidsscanning, og klik derefter på **OK**.

For at...	Skal du...
Registrere ukendte virus og nye varianter af kendte virus	Vælge **Scan for ukendte virus**.
Registrere cookies	Vælge **Scan og fjern sporingscookies**.
Registrere virus og andre potentielle trusler på drev, der er tilsluttet netværket	Vælge **Scan netværksdrev**.
Beskytte computeren mod bufferoverløb	Vælge **Aktiver beskyttelse for bufferoverløb**.
Angive de filtyper, der skal scannes	Klikke på **Alle filer (anbefales)** eller **Kun programfiler og dokumenter**.

Standse virusbeskyttelse i realtid

Selvom det er sjældent, kan der forekomme tilfælde, hvor du midlertidigt vil standse realtidsscanningen (f.eks. for at ændre scanningsindstillinger eller fejlfinde et effektivitetsproblem). Når virusbeskyttelse i realtid er deaktiveret, er din computer ikke beskyttet, og beskyttelsesstatus i SecurityCenter er rød. Flere oplysninger om beskyttelsesstatus finder du under "Forklaring af beskyttelsesstatus" i SecurityCenter Hjælp.

Du kan slå virusbeskyttelse i realtid fra midlertidigt og derefter angive, hvornår den skal genstartes. Du kan automatisk genstarte beskyttelse efter 15, 30, 45 eller 60 minutter, når computeren genstartes, eller aldrig.

1 Åbn konfigurationsruden Computer & filer.

   Hvordan?

   1. Klik på menuen **Avanceret** i den venstre rude.
   2. Klik på **Konfigurer**.
   3. Klik derefter på **Computer & filer** i ruden Konfigurer.

2 Under **Virusbeskyttelse** skal du klikke på **Fra**.

3 Vælg, hvornår realtidsscanning skal genstartes, i dialogboksen.

4 Klik på **OK**.

Vælge indstillinger for brugertilpasset scanning

Brugertilpasset virusbeskyttelse giver dig mulighed for at scanne filer, når du ønsker det. Når du starter en brugertilpasset scanning, kontrollerer VirusScan computeren for virus og andre potentielt skadelige elementer ved hjælp af et mere omfattende sæt scanningsindstillinger. Hvis du vil ændre indstillingerne for brugertilpasset scanning, skal du vælge, hvad VirusScan skal kontrollere for under en scanning. Du kan f.eks. bestemme, om VirusScan skal søge efter ukendte virus, potentielt uønskede programmer, f.eks. spyware eller adware, skjulte programmer og rootkits (der kan give uautoriseret adgang til computeren) samt cookies, som websteder kan bruge til at spore dine aktiviteter. Du skal også vælge, hvilke filtyper der skal kontrolleres. Du kan f.eks. vælge, om VirusScan skal kontrollere alle filer eller kun programfiler og dokumenter (da de fleste virus registreres i disse filer). Du kan også vælge, om komprimerede filer (f.eks. .zip-filer) skal medtages i scanningen.

Som standard kontrollerer VirusScan alle drev og mapper på computeren samt alle netværksdrev, hver gang programmet kører en manuel scanning. Du kan dog ændre standardplaceringerne, så de opfylder dine behov. Du kan f.eks. vælge kun at scanne vigtige pc-filer, elementer på skrivebordet eller elementer i mappen Programmer. Medmindre du selv vil starte alle brugertilpassede scanninger, kan du definere en tidsplan for scanningerne. Planlagte scanninger kontrollerer altid hele computeren ved hjælp af standardindstillingerne for scanning. Som standard gennemfører VirusScan en planlagt scanning en gang om ugen.

Hvis du oplever langsom scanningshastighed, kan du deaktivere indstillingen for brug af færrest mulige computerressourcer. Du skal dog være opmærksom på, at virusbeskyttelse prioriteres højere end andre opgaver.

Bemærk! Når du f.eks. ser film, spiller spil eller udfører andre aktiviteter på computeren, som fylder hele skærmen, standser VirusScan en række opgaver midlertidigt, herunder automatiske opdateringer og brugertilpassede scanninger.

Vælge indstillinger for brugertilpasset scanning

Du kan angive indstillinger for brugertilpasset scanning for at tilpasse, hvad VirusScan skal kontrollere for under en brugertilpasset scanning, og de placeringer og filtyper, der skal scannes. Indstillinger omfatter scanning for ukendte virus, filarkiver, spyware og potentielt uønskede programmer, sporingscookies, rootkits og skjulte programmer. Du angiver placeringer til brugertilpasset scanning for at bestemme, hvor VirusScan skal søge efter virus og andre skadelige elementer under en brugertilpasset scanning. Du kan scanne alle filer, mapper og drev på computeren, eller du kan begrænse scanningen til bestemte mapper og drev.

1 Åbn ruden Brugertilpasset scanning.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.
5. Klik på **Manuel scanning** i ruden Virusbeskyttelse.

2 Angiv de ønskede indstillinger for brugertilpasset scanning, og klik derefter på **OK**.

For at...	Skal du...
Registrere ukendte virus og nye varianter af kendte virus	Vælge **Scan for ukendte virus**.
Registrere og fjerne virus i .zip-filer og andre komprimerede filer	Vælge **Scan arkivfiler.**
Registrere spyware, adware og andre potentielt uønskede programmer	Vælge **Scan for spyware og mulige trusler.**
Registrere cookies	Vælge **Scan og fjern sporingscookies**.
Registrere rootkits og skjulte programmer, der kan ændre og udnytte eksisterende Windows-systemfiler	Vælge **Scan for skjulte programmer.**

For at...	Skal du...
Bruge mindre processorkraft til scanninger, hvilket giver højere prioritet til andre opgaver (f.eks. surfing på internettet eller åbning af dokumenter)	Vælge **Scan ved brug af færrest mulige computerressourcer**.
Angive de filtyper, der skal scannes	Klikke på **Alle filer (anbefales)** eller **Kun programfiler og dokumenter**.

3 Klik på **Standardplacering, der skal scannes**, og marker eller fjern markeringen ud for de steder, der skal scannes eller springes over, og klik derefter på **OK**:

For at...	Skal du...
Scanne alle filer og mapper på computeren	Vælge **(Min) computer**.
Scanne bestemte filer, mapper og drev på computeren	Fjerne markeringen i afkrydsningsfeltet **(Min) computer** og markere en eller flere mapper eller et eller flere drev.
Scanne vigtige systemfiler	Fjerne markeringen i afkrydsningsfeltet **(Min) computer** og derefter markere afkrydsningsfeltet **Vigtige systemfiler**.

Planlægge en scanning

Planlæg scanninger for at tjekke din computer grundigt for virus og andre trusler på enhver dag og ethvert tidspunkt i løbet af ugen. Planlagte scanninger kontrollerer altid hele computeren ved hjælp af standardindstillingerne for scanning. Som standard gennemfører VirusScan en planlagt scanning en gang om ugen. Hvis du oplever langsom scanningshastighed, kan du deaktivere indstillingen for brug af færrest mulige computerressourcer. Du skal dog være opmærksom på, at virusbeskyttelse prioriteres højere end andre opgaver.

Planlæg scanninger, der kontrollerer hele computeren grundigt for virus og andre trusler vha. standardscanningsindstillingerne. Som standard gennemfører VirusScan en planlagt scanning en gang om ugen.

1 Åbn ruden Planlagt scanning.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Computer & filer** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i området Computer & filer.
   4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.
   5. Klik på **Planlagt scanning** i ruden Virusbeskyttelse.

2 Vælg **Aktiver planlagt scanning**.

3 Hvis du vil reducere den mængde processorkraft, der normalt bruges til scanning, skal du vælge **Scan ved brug af færrest mulige computerressourcer**.

4 Vælg en eller flere dage.

5 Angiv et starttidspunkt.

6 Klik på **OK**.

Tip! Du kan gendanne standardplanen ved at klikke på **Nulstil**.

Brug af indstillinger for systembeskyttelse

Systembeskyttelse overvåger, logger, rapporterer og administrerer potentielt uautoriserede ændringer i Windows-databasen eller vigtige systemfiler på computeren. Uautoriserede ændringer i registreringsdatabasen kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.

Ændringer i registreringsdatabase og filer er almindelige og kan forekomme regelmæssigt på computeren. Da mange af ændringerne er uskadelige, er standardindstillingerne for systembeskyttelse konfigureret til at sikre pålidelig, intelligent og virkelig beskyttelse mod uautoriserede ændringer, der potentielt kan medføre betydelig skade. Når systembeskyttelse f.eks. registrerer ændringer, der er ualmindelige og repræsenterer en potentielt væsentlig trussel, rapporteres og logges aktiviteten omgående. Ændringer, der er mere almindelige, men som stadig repræsenterer en potentiel skade, registreres kun i logfilen. Overvågning for standardændringer med lav risiko er dog som standard slået fra. Systembeskyttelsesteknologien kan konfigureres, så dens beskyttelse udvides til ethvert miljø, du ønsker.

Der findes tre typer systembeskyttelser: Program-systembeskyttelse, Windows-systembeskyttelse og Browser-systembeskyttelse.

Program-systembeskyttelse

Program-systembeskyttelse registrerer potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Disse vigtige registreringsdatabaseelementer og filer omfatter ActiveX-installationer, opstartselementer, Windows Shell Execute Hooks og Shell Service Object Delay Loads. Ved at overvåge disse standser Program-systembeskyttelse mistænkelige ActiveX-programmer (downloadet fra internettet) samt spyware og potentielt uønskede programmer, som automatisk kan startes, når Windows startes.

Windows-systembeskyttelse

Windows-systembeskyttelse registrerer også potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Disse vigtige registreringsdatabaseelementer og filer omfatter håndtering af genvejsmenuer, appInit DLL-filer og Windows-værtsfilen. Ved at overvåge disse hjælper Windows-systembeskyttelse med at forhindre computeren i at sende og modtage uautoriserede eller personlige oplysninger over internettet. Den hjælper også med at stoppe mistænkelige programmer, der kan forårsage uønskede ændringer i udseendet og funktionaliteten af de programmer, som er vigtige for dig og din familie.

Browser-systembeskyttelse

Ligesom Program- og Windows-systembeskyttelse registrerer Browser-systembeskyttelse også potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Browser-systembeskyttelse overvåger dog ændringer i vigtige registreringsdatabaseelementer og filer, som f.eks. Internet Explorer-tilføjelsesprogrammer, Internet Explorer-webadresser og Internet Explorer-sikkerhedszoner. Ved at overvåge disse hjælper Browser-systembeskyttelse med at forhindre uautoriseret browseraktivitet, som f.eks. omdirigering til mistænkelige websteder, ændringer i browserindstillinger uden din viden og uønsket tillid til mistænkelige websteder.

Aktivere systembeskyttelse

Aktiver systembeskyttelse for at registrere og få besked om potentielt uautoriserede ændringer i Windows-registreringsdatabasen og filer på computeren. Uautoriserede ændringer i registreringsdatabasen kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.

1 Åbn konfigurationsruden Computer & filer.

   Hvordan?

   1. Klik på menuen **Avanceret** i den venstre rude.
   2. Klik på **Konfigurer**.
   3. Klik derefter på **Computer & filer** i ruden Konfigurer.

2 Under **Systembeskyttelse** skal du klikke på **Til**.

Bemærk! Du kan deaktivere systembeskyttelse ved at klikke på **Fra**.

Konfigurere indstillinger for systembeskyttelse

Brug ruden Systembeskyttelse til at konfigurere indstillinger for beskyttelse, logføring og alarmer vedrørende uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Windows-filer, programmer og Internet Explorer. Uautoriserede ændringer i registreringsdatabasen kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.

1 Åbn ruden Systembeskyttelse.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at systembeskyttelse er aktiveret i konfigurationsruden Computer & Filer, og klik derefter på **Avanceret**.

2 Vælg en type systembeskyttelse på listen.

- **Program-systembeskyttelse**
- **Windows-systembeskyttelse**
- **Browser-systembeskyttelse**

3 Under **Jeg ønsker at** skal du udføre en af følgende handlinger:

- Hvis du vil registrere, logføre og rapportere uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Program-, Windows- og Browser-systembeskyttelser, skal du klikke på **Vis alarmer**.
- Hvis du vil registrere og logføre uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Program-, Windows- og Browser-systembeskyttelser, skal du klikke på **Logfør kun ændringer**.
- Hvis du vil deaktivere registrering af uautoriserede ændringer i registreringsdatabasen og filer i forbindelse med Program-, Windows- og Browser-systembeskyttelser, skal du klikke på **Deaktiver systembeskyttelse**.

Bemærk! Flere oplysninger om systembeskyttelsestyper finder du under Om systembeskyttelsestyper (side 57).

Om systembeskyttelsestyper

Systembeskyttelse registrerer potentielt uautoriserede ændringer i computerens registreringsdatabase og andre vigtige filer, der er kritiske for Windows. Der findes tre typer systembeskyttelser: Program-systembeskyttelse, Windows-systembeskyttelse og Browser-systembeskyttelse.

Program-systembeskyttelse

Program-systembeskyttelse standser mistænkelige ActiveX-programmer (downloadet fra internettet) samt spyware og potentielt uønskede programmer, som automatisk kan startes, når Windows startes.

System-beskyttelse	Registrerer...
ActiveX-installationer	Uautoriserede ændringer i ActiveX-installationer, der kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.
Opstartselementer	Spyware, adware og andre potentielt uønskede programmer, der kan kan installere fil- eller registreringsdatabaseændringer til startelementer, så mistænkelige programmer kan køres, når du starter din computer.
Windows Shell Execute Hooks	Spyware, adware og andre potentielt uønskede programmer, der kan installere Windows Shell Execute Hooks for at forhindre sikkerhedsprogrammer i at køre korrekt.
Shell Service Object Delay Load	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Shell Service Object Delay Load, så skadelige filer kan afvikles, når du starter din computer.

Windows-systembeskyttelse

Windows-systembeskyttelse hjælper med at forhindre computeren i at sende og modtage uautoriserede eller personlige oplysninger over internettet. Den hjælper også med at stoppe mistænkelige programmer, der kan forårsage uønskede ændringer i udseendet og funktionaliteten af de programmer, som er vigtige for dig og din familie.

System-beskyttelse	Registrerer...
Håndtering af genvejsmenu	Uautoriserede ændringer i registreringsdatabasen i forbindelse med håndtering af genvejsmenuer i Windows, der kan påvirke udseendet og funktionen af Windows-menuerne. Med genvejsmenuer kan du udføre handlinger på din computer, f.eks. højreklikke på filer.
AppInit DLL-filer	Uautoriserede ændringer i registreringsdatabasen i forbindelse med Windows AppInit_DLL-filer, der kan medføre, at potentielt skadelige filer kan afvikles, når du starter din computer.
Windows værtsfiler	Spyware, adware og potentielt uønskede programmer, der kan foretage uautoriserede ændringer i din Windows-værtsfil, hvilket gør det muligt, at din browser kan omdirigere dig til mistænkelige websteder og blokere softwareopdateringer.
Winlogon Shell	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Winlogon Shell, så andre programmer kan erstatte Windows Stifinder.
Winlogon Userinit	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Winlogon User Init, så mistænkelige programmer kan køre, når du logger på Windows.
Windows-protokoller	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Windows-protokoller, så den måde, hvorpå din computer sender og modtager oplysninger via internettet, påvirkes.

System-beskyttelse	Registrerer...
Winsock Layered Service Providers	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Winsock Layered Service Providers (LSP'er) for på den måde at opfange og ændre de oplysninger, som du sender og modtager via internettet.
Windows Shell -åbningskommandoer	Uautoriserede ændringer i Windows Shell-åbningskommandoer, der kan give mulighed for, at orme og andre skadelige programmer kan køre på din computer.
SharedTaskScheduler	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Shared Task Scheduler, så skadelige filer kan afvikles, når du starter din computer.
Windows Messenger Service	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Windows Messenger Service, så uopfordrede reklamer og eksternt afviklede programmer kan køre på din computer.
Windows-filen win.ini	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i Win.ini-filen, så mistænkelige programmer kan køres, når du starter din computer.

Browser-systembeskyttelse

Browser-systembeskyttelse hjælper med at forhindre uautoriseret browseraktivitet, som f.eks. omdirigering til mistænkelige websteder, ændringer i browserindstillinger uden din viden og uønsket tillid til mistænkelige websteder.

System-beskyttelse	Registrerer...
Browserhjælpeobjekter	Spyware, adware og andre potentielt uønskede programmer, der kan bruge browserhjælpeobjekter til at spore surfing på internettet og vise uopfordrede reklamer.
Værktøjslinjer i Internet Explorer	Uautoriserede ændringer i registreringsdatabasen i forbindelse med programmer på Internet Explorer-værktøjslinjen, f.eks. Søg og Foretrukne, der kan påvirke udseendet og funktionen af Internet Explorer.

System-beskyttelse	Registrerer...
Internet Explorer -tilføjelsesprogrammer	Spyware, adware og andre potentielt uønskede programmer, der kan installere Internet Explorer-tilføjelsesprogrammer til at spore surfing på internettet og vise uopfordrede reklamer.
Internet Explorer ShellBrowser	Uautoriserede ændringer i registreringsdatabasen i forbindelse med Internet Explorer ShellBrowser, der kan påvirke udseendet og funktionen af din webbrowser.
Internet Explorer WebBrowser	Uautoriserede ændringer i registreringsdatabasen i forbindelse med Internet Explorer-webbrowseren, der kan påvirke udseendet og funktionen af din webbrowser.
Internet Explorer URL Search Hooks	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Internet Explorer URL Search Hook, så din browser kan omdirigeres til mistænkelige websteder, når du søger på internettet.
Internet Explorer URLer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Internet Explorer URLer, som påvirker browserindstillingerne.
Begrænsninger af Internet Explorer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med begrænsninger af Internet Explorer, som påvirker browserindstillingerne og -muligheder.
Sikkerhedszoner i Internet Explorer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Sikkerhedszoner i Internet Explorer, så potentielt skadelige filer kan afvikles, når du starter din computer.
Websteder, der har tillid til i Internet Explorer	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med Websteder, du har tillid til i Internet Explorer, så din browser har tillid til mistænkelige websteder.
Internet Explorer-regler	Spyware, adware og andre potentielt uønskede programmer, der kan foretage ændringer i registreringsdatabasen i forbindelse med politikker i Internet Explorer, som browserens udseende og funktion.

Brug af lister, der er tillid til

Hvis VirusScan registrerer en fil- eller registreringsdatabaseændring (systembeskyttelse), program eller bufferoverløb, bliver du spurgt, om du har tillid til elementet eller vil fjerne det. Hvis du har tillid til elementet og angiver, at du ikke ønsker at modtage besked om dets aktivitet i fremtiden, føjes elementet til en liste over elementer, der er tillid til. Derefter registrerer VirusScan det ikke længere og giver dig ikke besked om dets aktivitet. Hvis et element er føjet til en liste, du har tillid til, men du ønsker at blokere dets aktivitet, kan du gøre det. Blokering forhindrer elementet i at køre eller foretage ændringer i computeren, uden at du får besked, hver gang der gøres et forsøg. Du kan også fjerne et element fra en liste over elementer, der er tillid til. Når du fjerner et element, kan VirusScan registrere dets aktiviteter igen.

Administrere lister over elementer, der er tillid til

Brug ruden Lister, der er tillid til, til at tillade eller blokere elementer, der tidligere er registreret og tilladt. Du kan også fjerne et element fra en liste over elementer, der er tillid til, så VirusScan registrerer det igen.

1 Åbn ruden Lister, der er tillid til.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Computer & filer** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i området Computer & filer.
4. Kontroller, at virusbeskyttelse er aktiveret i konfigurationsruden Computer & filer, og klik derefter på **Avanceret**.
5. Klik på **Lister, der er tillid til** i ruden Virusbeskyttelse.

2 Marker en af følgende typer af lister, der er tillid til:

- **Program-systembeskyttelse**
- **Windows-systembeskyttelse**
- **Browser-systembeskyttelse**
- **Programmer, der er tillid til**
- **Bufferoverløb, der er tillid til**

3 Under **Jeg ønsker at** skal du udføre en af følgende handlinger:

- Hvis du vil tillade, at det registrerede element foretager ændringer i Windows-registreringsdatabasen eller vigtige systemfiler på computeren uden at give dig besked, skal du klikke på **Hav tillid til**.
- Hvis du vil forhindre, at det registrerede element foretager ændringer i Windows-registreringsdatabasen eller vigtige systemfiler på computeren uden at give dig besked, skal du klikke på **Bloker**.
- Hvis du vil fjerne det registrerede element fra listen over elementer, der er tillid til, skal du klikke på **Fjern**:

4 Klik på **OK**.

Bemærk! Flere oplysninger om typer af lister, der er tillid til, finder du under Om typer af lister, der er tillid til (side 62).

Om typer af lister, der er tillid til

Systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater. Der findes fem typer af lister, der er tillid til, som du kan administrere i ruden Lister, der er tillid til: Program-systembeskyttelse, Windows-systembeskyttelse, Browser-systembeskyttelse, Programmer, der er tillid til, og Bufferoverløb, der er tillid til.

Indstilling	Beskrivelse
Program -systembeskyttelse	Program-systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater. Program-systembeskyttelse registrerer uautoriserede registreringsdatabase- og filændringer i forbindelse med ActiveX-installationer, opstartselementer, Windows Shell Execute Hooks og Shell Service Object Delay Loads. Disse typer uautoriserede registreringsdatabase- og filændringer kan beskadige din computer, ødelægge sikkerheden og beskadige værdifulde systemfiler.

Indstilling	Beskrivelse
Windows -systembeskyttelse	Windows-systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater. Windows-systembeskyttelse registrerer uautoriserede registreringsdatabase- og filændringer i forbindelse med håndtering af genvejsmenuer i Windows, appInit DLL-filer, Windows-værtsfilen, Winlogon Shell, Winsock Layered Service Providers (LSP'er) osv. Disse typer uautoriserede registreringsdatabase- og filændringer kan påvirke den måde, computeren sender og modtager information via internettet på, ændre programmers udseende og funktion og tillade, at mistænkelige programmer køres på computeren.
Browser -systembeskyttelse	Browser-systembeskyttelse i ruden Lister, der er tillid til, viser tidligere uautoriserede registreringsdatabase- og filændringer, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater. Browser-systembeskyttelse overvåger uautoriserede registreringsdatabaseændringer og andre uønskede aktiviteter i forbindelse med browserhjælpeobjekter, Internet Explorer-tilføjelsesprogrammer, Internet Explorer URLer, Internet Explorer-sikkerhedszoner osv. Disse typer uautoriserede registreringsdatabaseændringer kan resultere i uønsket browseraktivitet, som f.eks. omdirigering til mistænkelige websteder, ændringer i browserindstillinger uden din viden og uønsket tillid til mistænkelige websteder.
Programmer, der er tillid til	Programmer, der er tillid til, er potentielt uønskede programmer, som VirusScan tidligere har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater.
Bufferoverløb, der er tillid til	Bufferoverløb, der er tillid til, er tidligere uønsket aktivitet, som VirusScan har registreret, men som du har valgt at tillade fra en alarm eller fra ruden Scanningsresultater. Bufferoverløb kan skade din computer og beskadige filer. Bufferoverløb sker, når den mængde oplysninger, som mistænkelig programmer eller processer lagrer i en buffer, overstiger bufferens kapacitet.

KAPITEL 13

McAfee Personal Firewall

Personal Firewall giver dig avanceret beskyttelse af din computer og dine personlige data. Personal Firewall opstiller en barriere mellem computeren og internettet og ligger i baggrunden og overvåger, om der foregår mistænkelige aktiviteter i internettrafikken.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Personal Firewall

Standard- og tilpassede beskyttelsesniveauer	Beskyt dig imod indtrængen og mistænkelig aktivitet med Firewalls standardbeskyttelsesindstillinger, eller tilpas Firewall efter dine egne sikkerhedsbehov.
Anbefalinger i realtid	Modtag anbefalinger dynamisk for at hjælpe dig med at afgøre, hvilke programmer der skal tildeles internetadgang, eller om du kan have tillid til netværkstrafik.
Intelligent administration af adgang for programmer	Administrer internetadgang for programmer ved hjælp af alarmer og hændelseslogfiler, og konfigurer adgangstilladelser for bestemte programmer.
Beskyttelse ved spil	Forhindrer, at alarmer om forsøg på indtrængen og mistænkelig aktivitet forstyrrer dig, når du spiller i fuldskærmstilstand.
Beskyttelse ved start af computeren	Beskyt computeren mod forsøg på indtrængen, uønskede programmer og netværkstrafik, så snart Windows® startes.
Kontrol af systemtjenesteport	Administrer åbne og lukkede systemtjenesteporte, der kræves af nogle programmer.
Administrer computerforbindelser	Tillad og bloker eksterne forbindelser mellem andre computere og din computer.
Integration af HackerWatch-oplysninger	Spor globale hacking- og indtrængningsmønstre gennem HackerWatchs websted, som også tilbyder de seneste sikkerhedsoplysninger om programmer på computeren samt statistikker over globale sikkerhedshændelser og internetporte.
Lås firewall	Blokerer øjeblikkeligt al ind- og udgående trafik imellem computeren og internettet.
Gendan Firewall	Gendanner øjeblikkeligt de oprindelige beskyttelsesindstillinger for Firewall.
Avanceret registrering af trojanske heste	Registrer og bloker potentielt skadelige programmer som f.eks. trojanske heste fra at oprette forbindelse til internettet og sende dine personlige oplysninger.
Logføring af hændelser	Viser seneste indgående og udgående hændelser samt forsøg på indtrængen.
Overvågning af internettrafik	Se globale kort, der viser kilden til fjendtlige angreb og trafik verden over. Desuden kan du finde detaljerede ejeroplysninger og geografiske data for de afsendende IP-adresser. Du kan også analysere ind- og udgående trafik og overvåge programbåndbredde og programaktivitet.
Forhindring af indtrængen	Beskyt dine personlige oplysninger mod mulige internettrusler. McAfee byder på et tredje beskyttelseslag i form af en heuristisk funktion, der blokerer elementer, der viser tegn på at være under angreb eller være forsøgt hacket.
Sofistikeret trafikanalyse	Se både ind- og udgående internettrafik og programforbindelser, herunder dem der aktivt lytter efter åbne forbindelser. Dette gør det muligt for dig at se og reagere over for programmer, der kan være sårbare over for indtrængen.

KAPITEL 14

Starte Firewall

Når du har installeret Firewall, er computeren beskyttet mod indtrængen og uønsket netværkstrafik. Desuden er du klar til at håndtere alarmer og styre indgående og udgående internetadgang for kendte og ukendte programmer. Smarte anbefalinger og det automatiske sikkerhedsniveau (hvor kun udgående internetadgang er tilladt for programmer) aktiveres automatisk.

Selvom du kan deaktivere Firewall fra ruden Konfiguration af Internet & netværk, vil computeren ikke længere være beskyttet mod indtrængen og uønsket netværkstrafik, og du vil ikke kunne styre indgående og udgående internetforbindelser. Hvis det er nødvendigt at deaktivere firewall-beskyttelsen, skal det kun gøres midlertidigt, og kun når det er nødvendigt. Du kan også deaktivere Firewall fra panelet Konfiguration af Internet & netværk.

Firewall deaktiverer automatisk Windows®-firewall'en og angiver sig selv som standard-firewall.

Bemærk! Åbn ruden Konfiguration af Internet & netværk for at konfigurere Firewall.

I dette kapitel

Starte firewall-beskyttelse

Du kan aktivere Firewall for at beskytte din computer mod indtrængen og uønsket netværkstrafik og for at styre indgående og udgående internetforbindelser.

1. Klik på **Internet & netværk** i startruden for McAfee SecurityCenter, og klik derefter på **Konfigurer**.
2. Klik på **Til** under **Firewall-beskyttelse er deaktiveret** i ruden Konfiguration af Internet & netværk.

Stoppe firewall-beskyttelse

Du kan deaktivere Firewall, hvis du ikke vil beskytte din computer mod indtrængen og uønsket netværkstrafik. Når Firewall er deaktiveret, kan du ikke styre indgående og udgående internetforbindelser.

1. Klik på **Internet & netværk** i startruden for McAfee SecurityCenter, og klik derefter på **Konfigurer**.
2. Klik på **Fra** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.

KAPITEL 15

Arbejde med alarmer

Firewall benytter lang række alarmer til at hjælpe dig med at administrere din sikkerhed. Disse alarmer kan deles op i tre grundlæggende typer:

- Røde alarmer
- Gule alarmer
- Grønne alarmer

Alarmer kan også indeholde oplysninger, der kan hjælpe dig med at beslutte, hvordan alarmerne skal håndteres, eller med at få oplysninger om programmer, der kører på computeren.

I dette kapitel

Om alarmer

Firewall har tre grundlæggende alarmtyper. Nogle alarmer omfatter oplysninger, som kan hjælpe dig til at få mere at vide eller få flere oplysninger om programmer, der kører på din computer.

Røde alarm

En rød alarm vises, når Firewall registrerer og derefter blokerer en trojansk hest på din computer samt anbefaler, at du scanner for yderligere trusler. En trojansk hest ser ud til at være et legitimt program, men kan forstyrre, beskadige eller give uautoriseret adgang til din computer. Denne alarm opstår på alle sikkerhedsniveauer.

Gul alarm

Den mest almindelige alarmtype er en gul alarm, som oplyser dig om en programaktivitet eller netværkshændelse, som Firewall har registreret. Når det sker, beskriver alarmen programaktiviteten eller netværkshændelsen og giver dig derefter en eller flere muligheder, der kræver svar fra dig. Alarmen **Ny netværksforbindelse blev registreret** vises f.eks., når en computer, som Firewall er installeret på, tilsluttes et nyt netværk. Du kan angive det tillidsniveau, du ønsker at tildele til dette nye netværk, hvorefter det vises på listen over netværk. Hvis funktionen Smarte anbefalinger er aktiveret, føjes kendte programmer automatisk til ruden Programtilladelser.

Grøn alarm

I de fleste tilfælde giver en grøn alarm grundlæggende information omkring en hændelse og kræver ingen reaktion fra dig. Grønne alarmer er som standard deaktiveret.

Hjælp

Mange Firewall-alarmer indeholder yderligere oplysninger, der kan hjælpe dig med at administrere din computers sikkerhed, som omfatter følgende:

- **Få flere oplysninger om dette program**: Start McAfees globale sikkerhedswebsted for at få oplysninger om et program, som Firewall har registreret på din computer.
- **Fortæl McAfee om dette program**: Send oplysninger til McAfee om en ukendt fil, som Firewall har registreret på din computer.
- **McAfee anbefaler**: Råd om håndtering af alarmer. En alarm kan for eksempel anbefale, at du giver et program adgang.

KAPITEL 16

Administrere oplysningsalarmer

Firewall gør det muligt for dig at få vist eller skjule oplysningsalarmer, når programmet registrerer indtrængningsforsøg eller mistænkelig aktivitet under bestemte hændelser, f.eks. under spil i fuldskærmstilstand.

I dette kapitel

Vise alarmer, mens der spilles

Du kan tillade, at Firewall-oplysningsalarmer vises, når Firewall registrerer forsøg på indtrængen eller mistænkelig aktivitet under spil i fuldskærmstilstand.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Konfigurer**.
3. Klik på **Avanceret** under **Alarmer** i ruden Konfiguration af SecurityCenter.
4. Vælg **Vis oplysningsalarmer, når spilletilstand registreres** i ruden Alarmindstillinger.
5. Klik på **OK**.

Skjule oplysningsalarmer

Du kan forhindre, at Firewall-oplysningsalarmer vises, når Firewall registrerer forsøg på indtrængen eller mistænkelig aktivitet.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Konfigurer**.
3. Klik på **Avanceret** under **Alarmer** i ruden Konfiguration af SecurityCenter.
4. Klik på **Oplysningsalarmer** i ruden Konfiguration af SecurityCenter.
5. I ruden Oplysningsalarmer skal du gøre et af følgende:
   - Vælg **Vis ikke oplysningsalarmer** for at skjule alle oplysningsalarmer.
   - Vælg en alarmtype, der skal skjules.
6. Klik på **OK**.

KAPITEL 17

Konfigurere Firewall-beskyttelse

Firewall indeholder en række metoder til at administrere din sikkerhed og til at skræddersy den måde, hvorpå du vil reagere over for sikkerhedshændelser og alarmer.

Når du har installeret Firewall første gang, er dit beskyttelsesniveau indstillet til Automatisk, og programmerne tillades kun udgående internetadgang. Firewall har dog andre niveauer, der går fra meget restriktivt til meget lavt.

Firewall gør det også muligt for dig at modtage anbefalinger om alarmer og internetadgang for programmer.

I dette kapitel

Administrere Firewall-sikkerhedsniveauer

Firewalls sikkerhedsniveauer styrer den grad, hvori du vil administrere og reagere over for alarmer. Disse alarmer vises, når Firewall registrerer uønsket netværkstrafik og indgående og udgående internetforbindelser. Som standard er Firewalls sikkerhedsniveau indstillet til Automatisk med kun udgående adgang.

Når sikkerhedsniveauet Automatisk er angivet, og smarte anbefalinger er aktiveret, giver gule alarmer mulighed for at tillade eller blokere adgang for ukendte programmer, der kræver indgående adgang. Selvom grønne alarmer som standard er deaktiveret, vises de, når kendte programmer registreres, og der gives automatisk adgang. Når der gives adgang, gives et program tilladelse til at oprette udgående forbindelser og lytte efter uopfordrede indgående forbindelser.

Generelt gælder det, at jo mere restriktivt sikkerhedsniveauet er (Skjult og Standard), jo højere er antallet af indstillinger og alarmer, der vises, og som du derfor skal håndtere.

I følgende tabel beskrives Firewalls tre sikkerhedsniveauer startende fra det mest restriktive til det mindst restriktive:

Niveau	Beskrivelse
Skjult	Blokerer for alle indgående netværksforbindelser med undtagelse af åbne porte og skjuler derved din computer på internettet. Firewall giver dig besked, når nye programmer forsøger at få udgående adgang til internettet eller modtager indgående forbindelsesanmodninger. Blokerede og tilføjede programmer vises i ruden Programtilladelser.
Standard	Overvåger indgående og udgående forbindelser og giver dig besked, når nye programmer forsøger at få adgang til internettet. Blokerede og tilføjede programmer vises i ruden Programtilladelser.
Automatisk	Giver dine programmer enten fuld internetadgang (indgående og udgående) eller kun adgang til udgående. Som standard er sikkerhedsniveauet indstillet til Automatisk med kun udgående adgang. Hvis et program tillades fuld adgang, har Firewall automatisk tillid til det og føjer det til listen over tilladte programmer i ruden Programtilladelser. Hvis et program kun tillades udgående adgang, har Firewall automatisk tillid til det, når det kun opretter en udgående internetforbindelse. Firewall har ikke automatisk tillid til en indgående internetforbindelse.

Firewall tillader også, at du straks nulstiller dit sikkerhedsniveau til Automatisk (og kun tillader udgående adgang) i ruden Gendan standardindstillinger for firewall-beskyttelse.

Indstille sikkerhedsniveau til Skjult

Du kan indstille Firewall-sikkerhedsniveauet til Skjult for at blokere alle indgående netværksforbindelser med undtagelse af åbne porte for derved at skjule din computer på internettet.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Bevæg skyderen i ruden Sikkerhedsniveau, så **Skjult** vises som det aktuelle niveau.
4. Klik på **OK**.

Bemærk! I tilstanden Skjult giver Firewall dig besked, når nye programmer forsøger at få udgående adgang til internettet eller modtager indgående forbindelsesanmodninger.

Indstille sikkerhedsniveau til Standard

Du kan indstille sikkerhedsniveauet til Standard for at overvåge indgående og udgående forbindelser og få besked, når nye programmer forsøger at få internetadgang.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Bevæg skyderen i ruden Sikkerhedsniveau, så **Standard** vises som det aktuelle niveau.
4. Klik på **OK**.

Indstille sikkerhedsniveau til Automatisk

Du kan indstille Firewall-sikkerhedsniveauet til Automatisk for at tillade fuld adgang eller kun udgående adgang.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Bevæg skyderen i ruden Sikkerhedsniveau, så **Automatisk** vises som det aktuelle niveau.

4 Nu kan du gøre følgende:
   - Vælg **Tillad fuld adgang**, hvis du vil tillade fuld indgående og udgående netværksadgang.
   - Vælg **Tillad kun udgående adgang**, hvis du kun vil tillade udgående netværksadgang.

5 Klik på **OK**.

Bemærk!Tillad kun udgående adgang er standardindstillingen.

Konfigurere smarte anbefalinger til alarmer

Du kan konfigurere Firewall, så den inkluderer, udelukker eller viser anbefalinger ved alarmer om programmer, der forsøger at få adgang til internettet. Når smarte anbefalinger er aktiveret, får du hjælp til at bestemme, hvordan du skal håndtere alarmer.

Når smarte anbefalinger anvendes (og sikkerhedsniveauet er angivet til Automatisk med kun undgående adgang), tillader Firewall automatisk kendte programmer og blokerer potentielt skadelige programmer.

Når smarte anbefalinger er deaktiveret, hverken tillader eller blokerer Firewall internetadgang, og den anbefaler heller ikke en anbefaling i alarmen.

Når smarte anbefalinger er indstillet til Vis, giver en alarm dig besked på at tillade eller blokere adgang, og Firewall anbefaler en fremgangsmåde i alarmen.

Aktivere smarte anbefalinger

Hvis du aktiverer smarte anbefalinger, tillader eller blokerer Firewall automatisk programmer og advarer dig om ikke-genkendte og potentielt farlige programmer.

1 Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.

2 Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.

3 Vælg **Anvend smarte anbefalinger** i ruden Sikkerhedsniveau under **Smarte anbefalinger**.

4 Klik på **OK**.

Deaktivere smarte anbefalinger

Hvis du deaktiverer smarte anbefalinger, tillader eller blokerer Firewall programmer og advarer dig om ikke-genkendte og potentielt farlige programmer. Alarmerne indeholder dog ikke anbefalinger om at håndtere adgangen for programmer. Hvis Firewall registrerer et nyt program, der forekommer mistænkeligt eller er kendt som en mulig trussel, blokerer Firewall automatisk programmet, så det ikke kan få adgang til internettet.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Vælg **Anvend ikke smarte anbefalinger** i ruden Sikkerhedsniveau under **Smarte anbefalinger**.
4. Klik på **OK**.

Vise smarte anbefalinger

Du kan få smarte anbefalinger til kun at vise en anbefaling i alarmerne, så du kan beslutte, om du vil tillade eller blokere ikke-genkendte og potentielt farlige programmer.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Vælg **Vis smarte anbefalinger** i ruden Sikkerhedsniveau under **Smarte anbefalinger**.
4. Klik på **OK**.

Optimere Firewall-sikkerhed

Din computers sikkerhed kan blive kompromitteret på mange måder. Nogle programmer kan f.eks. forsøge at oprette forbindelse til internettet, når Windows® starter. Avancerede computerbrugere kan desuden spore (eller pinge) din computer for at finde ud af, om den er tilsluttet et netværk. De kan også sende oplysninger til din computer vha. UDP-protokollen i form af meddelelsesenheder (datagrammer). Firewall beskytter din computer mod disse typer forsøg på indtrængen ved at give dig mulighed for at forhindre programmer i at få adgang til internettet, når Windows starter, så du kan blokere ping-anmodninger, der hjælper andre brugere med at registrere din computer på et netværk, og så du kan forhindre, at andre brugere sender oplysninger til din computer i form af meddelelsesenheder (datagrammer).

Standardinstallationsindstillingerne inkluderer automatisk registrering af de mest almindelige forsøg på indtrængen, som f.eks. DoS-angreb (Denial of Service) eller udnyttelse. Vha. standardinstallationsindstillingerne kan du sikre, at du er beskyttet mod disse angreb og scanninger. Du kan dog deaktivere automatisk registrering for et eller flere angreb eller scanninger i ruden til registrering af indtrængen.

Beskytte computeren under opstart

Du kan beskytte computeren, når Windows starter, for at blokere nye programmer, der ikke har, og som nu har brug for, internetadgang under start. Firewall viser de relevante alarmer for programmer, der har anmodet om internetadgang, og du kan give tilladelse eller blokere.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Vælg **Aktiver beskyttelse ved opstart af Windows** i ruden Sikkerhedsniveau under **Sikkerhedsindstillinger**.
4. Klik på **OK**.

Bemærk! Blokerede forbindelser og indtrængen er ikke logført, når beskyttelsen ved start er aktiveret.

Konfigurere indstillinger for ping-anmodninger

Du kan tillade eller forhindre registrering af computeren på netværket af andre computerbrugere.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. I ruden Sikkerhedsniveau under **Sikkerhedsindstillinger** skal du gøre et af følgende:
   - Vælg **Tillad ICMP-ping-anmodninger** for at tillade registrering af din computer på netværket ved hjælp af ping-anmodninger.
   - Fjern markeringen i afkrydsningsfeltet **Tillad ICMP-ping-anmodninger** for at tillade registrering af din computer på netværket ved hjælp af ping-anmodninger.
4. Klik på **OK**.

Konfigurere UDP-indstillinger

Du kan tillade, at computerbrugere på andre netværk sender meddelelsesenheder (datagrammer) til din computer vha. UDP-protokollen. Du kan dog kun gøre dette, hvis du også har lukket en systemtjenesteport for at blokere denne protokol.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. I ruden Sikkerhedsniveau under **Sikkerhedsindstillinger** skal du gøre et af følgende:
   - Marker feltet **Aktiver UDP-sporing** for at tillade, at andre computerbrugere sender meddelelsesenheder (datagrammer) til din computer.
   - Fjern markeringen i feltet **Aktiver UDP-sporing** for at forhindre, at andre computerbrugere sender meddelelsesenheder (datagrammer) til din computer.
4. Klik på **OK**.

Konfigurere registrering af indtrængen

Du kan registrere forsøg på indtrængen for at beskytte computeren mod angreb og uautoriserede scanninger. Standardindstillingen i Firewall inkluderer automatisk registrering af de mest almindelige forsøg på indtrængen, som f.eks. DoS-angreb (Denial of Service) eller udnyttelse. Du kan dog deaktivere automatisk registrering for et eller flere angreb eller en eller flere scanninger.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Registrering af indtrængen** i fanen Firewall.
4. Under **Registrer forsøg på indtrængen** skal du gøre et af følgende:
   - Vælg et navn, der automatisk skal registrere angrebet eller scanningen.
   - Ryd et navn for at deaktivere automatisk registrering af angrebet eller scanningen.
5. Klik på **OK.**

Konfigurere Firewall-indstillingerne for beskyttelsesstatus

Du kan konfigurere Firewall til at ignorere, at bestemte problemer på din computer ikke rapporteres til SecurityCenter.

1. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i McAfee SecurityCenter-ruden.
2. Klik på **Avanceret** under **Beskyttelsesstatus** i ruden Konfiguration af SecurityCenter.
3. Vælg en eller flere af følgende muligheder i ruden Ignorerede problemer:
   - **Firewall-beskyttelsen er deaktiveret.**
   - **Firewall-tjenesten kører ikke.**
   - **Firewall-beskyttelse er ikke installeret på computeren.**
   - **Din Windows-firewall er deaktiveret.**
   - **Der er ikke installeret en udgående firewall på computeren.**
4. Klik på **OK**.

Låse og gendanne Firewall

Låsning af firewallen blokerer for alle indgående og udgående netværksforbindelser, herunder adgang til websteder, e-mail og sikkerhedsopdateringer. Lås firewall fungerer på samme måde, som når du trækker netværkskablerne ud af din computer. Du kan bruge denne indstilling til at blokere åbne porte i ruden Systemtjenester og som en hjælp til at isolere og løse et problem på din computer.

Låse Firewall øjeblikkeligt

Du kan låse Firewall øjeblikkeligt for at blokere al netværkstrafik mellem din computer og et hvilket som helst netværk, herunder internettet.

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Lås firewall**.
2. Klik på **Aktiver Lås firewall** i ruden Lås firewall.
3. Klik på **Ja** for at bekræfte.

Tip! Du kan også låse Firewall ved at højreklikke på SecurityCenter-ikonet i meddelelsesområdet længst til højre på proceslinjen. Klik derefter på **Direkte links**, og klik på **Lås firewall**.

Deaktivere låsning af Firewall øjeblikkeligt

Du kan låse Firewall op for øjeblikkeligt at tillade al netværkstrafik mellem din computer og et hvilket som helst netværk, herunder internettet.

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Lås firewall**.
2. Klik på **Deaktiver Lås firewall** i ruden Lås firewall.
3. Klik på **Ja** for at bekræfte.

Gendanne Firewall-indstillinger

Du kan hurtigt gendanne Firewalls oprindelige beskyttelsesindstillinger. Denne gendannelse nulstiller sikkerhedsniveauet til Automatisk og tillader kun udgående netværksadgang, aktiverer smarte anbefalinger, gendanner listen over standardprogrammer og deres tilladelser i ruden Programtilladelser, fjerner IP-adresser, der er tillid til, og forbudte IP-adresser og gendanner systemtjenester, indstillinger for hændelseslogfil og registrering af indtrængen.

1. Klik på **Gendan standardindstillinger for firewall** i McAfee SecurityCenter-ruden.
2. Klik på **Gendan standarder** i ruden Gendan standardindstillinger for firewall-beskyttelse.
3. Klik på **Ja** for at bekræfte.
4. Klik på **OK**.

KAPITEL 18

Administrere programmer og tilladelser

Firewall giver dig mulighed for at administrere og oprette adgangstilladelser til eksisterende og nye programmer, der kræver indgående og udgående internetadgang. Firewall giver dig mulighed for at tildele fuld eller kun udgående adgang til programmer. Du kan også blokere adgang for programmer.

I dette kapitel

Tillade internetadgang for programmer

For nogle programmer, såsom internetbrowsere, er det nødvendigt at have adgang til internettet, for at de kan fungere korrekt.

Firewall giver dig mulighed for at bruge siden Programtilladelser til at:

- tildele adgang for programmer
- tildele kun udgående adgang for programmer
- blokere adgang for programmer

Du kan også tillade, at et program har fuld og kun udgående internetadgang fra logfilen Udgående hændelser og Seneste hændelser.

Tillade fuld adgang for et program

Du kan tillade, at et eksisterende blokeret program på computeren får fuld indgående og udgående internetadgang.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Programtilladelser** i ruden Firewall.
4. Vælg et program med **Blokeret** eller **Kun udgående adgang** under **Programtilladelser**.
5. Klik på **Tillad adgang** under **Handling**.
6. Klik på **OK**.

Tillade fuld adgang for et nyt program

Du kan tillade, at et nyt program på computeren får fuld indgående og udgående internetadgang.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på**Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Programtilladelser** i ruden Firewall.
4. Klik på **Tilføj tilladt program** under **Programtilladelser**.
5. Søg efter og vælg de programmer, du vil tilføje, i dialogboksen **Tilføj program**, og klik derefter på **Åbn**.

Bemærk! Du kan ændre tilladelserne for et nyligt tilføjet program på samme måde som for et eksisterende program ved at vælge programmet og derefter klikke på **Tillad kun udgående adgang** eller **Bloker adgang** under **Handling**.

Tillade fuld adgang fra logfilen over seneste hændelser

Du kan tillade, at et eksisterende blokeret program, der vises i logfilen over seneste hændelser, får fuld indgående og udgående internetadgang.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Rapporter og logfiler**.
3. Vælg hændelsesbeskrivelsen under **Seneste hændelser**, og klik derefter på **Tillad adgang**.
4. Klik på **Ja** for at bekræfte i dialogboksen Programtilladelser.

Relaterede emner

- Visne udgående hændelser (side 107)

Tillade fuld adgang fra logfilen over udgående hændelser

Du kan tillade, at et eksisterende blokeret program, der vises i logfilen over udgående hændelser, får fuld indgående og udgående internetadgang.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Rapporter og logfiler**.
3. Klik på **Vis logfil** under **Seneste hændelser**.
4. Klik på **Internet & netværk**, og klik derefter på **Udgående hændelser**.
5. Vælg et program, og klik på **Tillad adgang** under **Jeg ønsker at**.
6. Klik på **Ja** for at bekræfte i dialogboksen Programtilladelser.

Tillade kun udgående adgang for programmer

Nogle programmer på din computer kræver udgående adgang til internettet. Firewall giver dig mulighed for at konfigurere programtilladelser til at tillade kun udgående adgang til internettet.

Tillade kun af udgående adgang for et program

Du kan tillade, at et program har kun udgående adgang til internettet.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Programtilladelser** i ruden Firewall.
4. Vælg et program med **Blokeret** eller **Fuld adgang** under **Programtilladelser**.
5. Klik på **Tillad kun udgående adgang** under **Handling**.
6. Klik på **OK**.

Tillade kun udgående adgang fra logfilen over seneste hændelser

Du kan tillade, at et eksisterende blokeret program, der vises i logfilen over seneste hændelser, får kun udgående internetadgang.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Rapporter og logfiler**.
3. Vælg hændelsesbeskrivelsen under **Seneste hændelser**, og klik derefter på **Tillad kun udgående adgang**.
4. Klik på **Ja** for at bekræfte i dialogboksen Programtilladelser.

Tillade kun udgående adgang fra logfilen over udgående hændelser

Du kan tillade, at et eksisterende blokeret program, der vises i logfilen over udgående hændelser, får kun udgående internetadgang.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Rapporter og logfiler**.
3. Klik på **Vis logfil** under **Seneste hændelser**.
4. Klik på **Internet & netværk**, og klik derefter på **Udgående hændelser**.
5. Vælg et program, og klik på **Tillad kun udgående adgang** under **Jeg ønsker at**.
6. Klik på **Ja** for at bekræfte i dialogboksen Programtilladelser.

Blokere internetadgang for programmer

Firewall giver dig mulighed for at blokere programmer fra at få adgang til internettet. Kontroller, at blokeringen af et program ikke forstyrrer din netværksforbindelse eller et andet program, der kræver adgang til internettet for at fungere korrekt.

Blokere adgang for program

Du kan blokere et program fra at have indgående og udgående adgang til internettet.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Programtilladelser** i ruden Firewall.
4. Vælg et program med **Fuld adgang** eller **Kun udgående adgang** under **Programtilladelser**.
5. Klik på **Bloker adgang** under **Handling**.
6. Klik på **OK**.

Blokere adgang for et nyt program

Du kan blokere et nyt program fra at have indgående og udgående adgang til internettet.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Programtilladelser** i ruden Firewall.
4. Klik på **Tilføj blokeret program** under **Programtilladelser**.
5. Søg efter og vælg et program, du vil tilføje, i dialogboksen Tilføj program, og klik derefter på **Åbn**.

Bemærk! Du kan ændre tilladelserne for et nyligt tilføjet program på samme måde som for et eksisterende program ved at vælge programmet og derefter klikke på **Tillad kun udgående adgang** eller **Tillad adgang** under **Handling**.

Blokere af adgang fra logfilen over seneste hændelser

Du kan blokere et program, der vises i logfilen over seneste hændelser, fra at få fuld indgående og udgående internetadgang.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Rapporter og logfiler**.
3. Vælg hændelsesbeskrivelsen under **Seneste hændelser**, og klik derefter på **Bloker adgang**.
4. Klik på **Ja** for at bekræfte i dialogboksen Programtilladelser.

Fjerne adgangstilladelser for programmer

Før du fjerner et programs tilladelse, skal du kontrollere, at det ikke vil påvirke computerens funktionalitet eller netværksforbindelsen.

Fjerne programtilladelse

Du kan blokere et program fra at have indgående og udgående adgang til internettet.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Programtilladelser** i ruden Firewall.
4. Vælg et program under **Programtilladelser**.
5. Klik på **Fjern programtilladelse** under **Handling**.
6. Klik på **OK**.

Bemærk! I nogle programmer forhindrer Firewall, at du foretager ændringer, ved at nedtone og deaktivere handlinger.

Om programmer

Hvis du ikke er sikker på, hvilke programtilladelser du skal anvende, kan du få oplysninger om programmet på McAfee-webstedet HackerWatch.

Indhente oplysninger om programmer

Du kan hente programoplysninger fra McAfees HackerWatch-websted, så du kan beslutte, om indgående og udgående adgang til internettet skal tillades eller blokeres.

Bemærk! Sørg for, at computeren har forbindelse til internettet, så browseren starter McAfees HackerWatch-websted, som indeholder opdaterede oplysninger om programmer, krav til internetadgang og sikkerhedstrusler.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Programtilladelser** i ruden Firewall.
4. Vælg et program under **Programtilladelser**.
5. Klik på **Flere oplysninger** under **Handling**.

Få programoplysninger fra logfilen over udgående hændelser

Fra logfilen over udgående hændelser kan du hente programoplysninger fra McAfees HackerWatch-websted, så du kan beslutte, om indgående og udgående adgang til internettet skal tillades eller blokeres.

Bemærk! Sørg for, at computeren har forbindelse til internettet, så browseren starter McAfees HackerWatch-websted, som indeholder opdaterede oplysninger om programmer, krav til internetadgang og sikkerhedstrusler.

1. Klik på menuen **Avanceret** i McAfee SecurityCenter-ruden.
2. Klik på **Rapporter og logfiler**.
3. Vælg en hændelse under Seneste hændelser, og klik på **Vis logfil**.
4. Klik på **Internet & netværk**, og klik derefter på **Udgående hændelser**.
5. Vælg en IP-adresse, og klik på **Flere oplysninger**.

KAPITEL 19

Administrere computerforbindelser

Du kan konfigurere Firewall til at administrere specifikke fjernforbindelser til din computer ved at oprette regler, der er baseret på Internet Protocol-adresser (IP-adresser), der er tilknyttet fjerncomputere. Computere med IP-adresser, der er tillid til, kan forbindes til din computer, og de IP-adresser, der er ukendte, mistænkelige, eller som du ikke har tillid til, kan forbydes forbindelse til din computer.

Når du tillader en forbindelse, bør du kontrollere, at den computer, du har tillid til, er sikker. Hvis en computer, som du har tillid til, inficeres via en orm eller en anden mekanisme, kan din computer være sårbar over for infektion. Desuden anbefaler McAfee, at den computer, du har tillid til, beskyttes af en firewall og et opdateret antivirusprogram. Firewall logfører ikke trafik eller genererer hændelsesalarmer fra IP-adresser, der er tillid til, på **Netværkslisten**.

Computere, der er tilknyttet ukendte eller mistænkelige IP-adresser eller IP-adresser, der ikke er tillid til, kan udelukkes, så de ikke kan oprette forbindelse til din computer.

Da Firewall blokerer al uønsket trafik, er det normalt ikke nødvendigt at forbyde en IP-adresse. Du bør kun forbyde en IP-adresse, når du er sikker på, at en internetforbindelse udgør en trussel. Kontroller, at du ikke blokerer vigtige IP-adresser, som f.eks. DNS- eller DHCP-serveren eller andre internetudbyderrelaterede servere.

I dette kapitel

Om computerforbindelser

Computerforbindelser er de forbindelser, som du opretter mellem andre computere på andre netværk end dit eget. Du kan tilføje, redigere eller fjerne IP-adresser på **netværkslisten**. Disse IP-adresser er tilknyttet netværk, som du skal tildele et tillidsniveau, når de opretter forbindelse til din computer: Tillid til, Standard og Offentlig.

Niveau	Beskrivelse
Tillid til	Firewall tillader trafik fra en IP-adresse til din computer gennem en hvilken som helst port. Aktivitet mellem den computer, der er tilknyttet en IP-adresse, der er tillid til, og din computer filtreres eller analyseres ikke af Firewall. Det første private netværk, Firewall finder, vises som standard som Tillid til på **netværkslisten**. Et netværk, der er tillid til, kunne f.eks. være en computer eller computere på dit lokale netværk eller på hjemmenetværket.
Standard	Firewall kontrollerer trafik fra en IP-adresse (men ikke fra andre computere på det pågældende netværk), når den opretter forbindelse til din computer, og tillader adgang eller blokerer for den, afhængigt af reglerne på listen **Systemtjenester**. Firewall logfører trafik og genererer hændelsesalarmer fra Standard-IP-adresser. Et standardnetværk er f.eks. en computer eller computere på et virksomhedsnetværk.
Offentlig	Firewall kontrollerer trafik fra et offentligt netværk, afhængigt af reglerne på listen **Systemtjenester**. Et offentligt netværk er f.eks. et internetnetværk på en cafe, et hotel eller i en lufthavn.

Når du tillader en forbindelse, bør du kontrollere, at den computer, du har tillid til, er sikker. Hvis en computer, som du har tillid til, inficeres via en orm eller en anden mekanisme, kan din computer være sårbar over for infektion. Desuden anbefaler McAfee, at den computer, du har tillid til, beskyttes af en firewall og et opdateret antivirusprogram.

Tilføje en computerforbindelse

Du kan tilføje en computerforbindelse, der er tillid til, en standard- eller en offentlig computerforbindelse og dens tilhørende IP-adresse.

1 Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.

2 Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.

3 Klik på **Netværk** i ruden Firewall.

4 Klik på **Tilføj** i ruden Netværk.

5 Hvis computerforbindelsen er på et IPv6-netværk, skal du markere afkrydsningsfeltet **IPv6**.

6 Under **Tilføj regel** skal du gøre et af følgende:

- Vælg **Enkelt**, og indtast derefter IP-adressen i feltet **IP-adresse**.
- Vælg **Område**, og indtast derefter de første og sidste IP-adresser i felterne **Fra IP-adresse** og **Til IP-adresse**. Hvis din computerforbindelse er på et IPv6-netværk, skal du angive start-IP-adressen og præfikslængden i boksene **Fra IP-adresse** og **Præfikslængde**.

7 Under **Type** skal du gøre et af følgende:

- Vælg **Tillid til** for at angive, at der er tillid til denne computerforbindelse (f.eks. en computer på et hjemmenetværk).
- Vælg **Standard** for at angive, at der er tillid til denne computerforbindelse (f.eks. en computer på et virksomhedsnetværk) og ikke til de andre computere på netværket.
- Vælg **Offentlig** for at angive, at denne computerforbindelse er offentlig (f.eks. en computer på en internetcafé, et hotel eller i en lufthavn).

8 Hvis en systemtjeneste bruger Deling af internetforbindelse, kan du tilføje følgende IP-adresseområde: 192.168.0.1 til 192.168.0.255.

9 Du kan også vælge **Regel udløber om** og derefter indtaste det antal dage, reglen skal løbe.

10 Du kan også indtaste en beskrivelse af reglen.

11 Klik på **OK**.

Bemærk! Du kan finde flere oplysningr om Deling af internetforbindelse under Konfigurere en ny systemtjeneste.

Tilføje en computer fra logfilen over indgående hændelser

Du kan tilføje en computerforbindelse, der er tillid til, eller en standardcomputerforbindelse og dens tilknyttede IP-adresse fra logfilen over indgående hændelser.

1. I ruden McAfee SecurityCenter under Almindelige opgaver skal du klikke på menuen **Avanceret**.
2. Klik på **Rapporter og logfiler**.
3. Klik på **Vis logfil** under **Seneste hændelser**.
4. Klik på **Internet & netværk**, og klik derefter på **Indgående hændelser**.
5. Vælg en kilde-IP-adresse, og gør et af følgende under **Jeg ønsker at**:
   - Klik på **Tilføj denne IP-adresse som Tillid til** for at tilføje denne computer til listen **Netværk** som en computer, der er tillid til.
   - Klik på **Tilføj denne IP-adresse som Standard** for at tilføje denne computer til listen **Netværk** som en standardcomputer.
6. Klik på **Ja** for at bekræfte.

Redigere en computerforbindelse

Du kan redigere en computerforbindelse, der er tillid til, en standard- eller en offentlig computerforbindelse og dens tilhørende IP-adresse.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Netværk** i ruden Firewall.
4. Vælg en IP-adresse i netværksruden, og klik på **Rediger**.
5. Hvis computerforbindelsen er på et IPv6-netværk, skal du markere afkrydsningsfeltet **IPv6**.
6. Under **Rediger regel** skal du gøre et af følgende:
   - Vælg **Enkelt**, og indtast derefter IP-adressen i feltet **IP-adresse**.
   - Vælg **Område**, og indtast derefter de første og sidste IP-adresser i felterne **Fra IP-adresse** og **Til IP-adresse**. Hvis din computerforbindelse er på et IPv6-netværk, skal du angive start-IP-adressen og præfikslængden i boksene **Fra IP-adresse** og **Præfikslængde**.

7 Under **Type** skal du gøre et af følgende:

- Vælg **Tillid til** for at angive, at der er tillid til denne computerforbindelse (f.eks. en computer på et hjemmenetværk).
- Vælg **Standard** for at angive, at der er tillid til denne computerforbindelse (f.eks. en computer på et virksomhedsnetværk) og ikke til de andre computere på netværket.
- Vælg **Offentlig** for at angive, at denne computerforbindelse er offentlig (f.eks. en computer på en internetcafé, et hotel eller i en lufthavn).

8 Du kan også kontrollere **Regel udløber om** og derefter indtaste det antal dage, reglen skal løbe.

9 Du kan også indtaste en beskrivelse af reglen.

10 Klik på **OK**.

Bemærk! Du kan ikke redigere de standardcomputerforbindelser, som Firewall automatisk har tilføjet fra et privat netværk, der er tillid til.

Fjerne en computerforbindelse

Du kan fjerne en computerforbindelse, der er tillid til, en standard- eller en offentlig computerforbindelse og dens tilhørende IP-adresse.

1 Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.

2 Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.

3 Klik på **Netværk** i ruden Firewall.

4 Vælg en IP-adresse i netværksruden, og klik på **Fjern**.

5 Klik på **Ja** for at bekræfte.

Forbyde computerforbindelser

Du kan tilføje, redigere og fjerne forbudte IP-adresser i ruden Forbudte IP-adresser.

Computere, der er tilknyttet ukendte eller mistænkelige IP-adresser eller IP-adresser, der ikke er tillid til, kan udelukkes, så de ikke kan oprette forbindelse til din computer.

Da Firewall blokerer al uønsket trafik, er det normalt ikke nødvendigt at forbyde en IP-adresse. Du bør kun forbyde en IP-adresse, når du er sikker på, at en internetforbindelse udgør en trussel. Kontroller, at du ikke blokerer vigtige IP-adresser, som f.eks. DNS- eller DHCP-serveren eller andre internetudbyderrelaterede servere.

Tilføje en forbudt computerforbindelse

Du kan tilføje en forbudt computerforbindelse og dens tilhørende IP-adresse.

Bemærk! Kontroller, at du ikke blokerer vigtige IP-adresser, som f.eks. DNS- eller DHCP-serveren eller andre internetudbyderrelaterede servere.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Forbudte IP-adresser** i ruden Firewall.
4. Klik på **Tilføj** i ruden Forbudte IP-adresser.
5. Hvis computerforbindelsen er på et IPv6-netværk, skal du markere afkrydsningsfeltet **IPv6**.
6. Under **Tilføj regel** skal du gøre et af følgende:
   - Vælg **Enkelt**, og indtast derefter IP-adressen i feltet **IP-adresse**.
   - Vælg **Område**, og indtast derefter de første og sidste IP-adresser i felterne **Fra IP-adresse** og **Til IP-adresse**. Hvis din computerforbindelse er på et IPv6-netværk, skal du angive start-IP-adressen og præfikslængden i boksene **Fra IP-adresse** og **Præfikslængde**.
7. Du kan også vælge **Regel udløber om** og derefter indtaste det antal dage, reglen skal løbe.
8. Du kan også indtaste en beskrivelse af reglen.
9. Klik på **OK**.
10. Klik på **Ja** for at bekræfte.

Redigere en forbudt computerforbindelse

Du kan redigere en forbudt computerforbindelse og dens tilhørende IP-adresse.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Forbudte IP-adresser** i ruden Firewall.
4. Klik på **Rediger** i ruden Forbudte IP-adresser.
5. Hvis computerforbindelsen er på et IPv6-netværk, skal du markere afkrydsningsfeltet **IPv6**.
6. Under **Rediger regel** skal du gøre et af følgende:
   - Vælg **Enkelt**, og indtast derefter IP-adressen i feltet **IP-adresse**.
   - Vælg **Område**, og indtast derefter de første og sidste IP-adresser i felterne **Fra IP-adresse** og **Til IP-adresse**. Hvis din computerforbindelse er på et IPv6-netværk, skal du angive start-IP-adressen og præfikslængden i boksene **Fra IP-adresse** og **Præfikslængde**.
7. Du kan også vælge **Regel udløber om** og derefter indtaste det antal dage, reglen skal løbe.
8. Du kan også indtaste en beskrivelse af reglen.
9. Klik på **OK**.

Fjerne en forbudt computerforbindelse

Du kan fjerne en forbudt computerforbindelse og dens tilhørende IP-adresse.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Forbudte IP-adresser** i ruden Firewall.
4. Vælg en IP-addresse i ruden Forbudte IP-adresser, og klik derefter på **Fjern**.
5. Klik på **Ja** for at bekræfte.

Forbyde en computer fra logfilen over indgående hændelser

Du kan forbyde en computerforbindelse og dens tilknyttede IP-adresse fra logfilen over indgående hændelser. Brug denne log, der indeholder IP-adresserne til al indgående internettrafik, til at forbyde en IP-adresse, som, du mener, er kilden til mistænkelig eller uønsket internetaktivitet.

Tilføj en IP-adresse til listen **Forbudte IP-adresser**, hvis du ønsker at blokere al indgående internettrafik fra den pågældende IP-adresse, uafhængigt af om systemtjenesteportene er åbne eller lukkede.

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på menuen **Avanceret**.
2. Klik på **Rapporter og logfiler**.
3. Klik på **Vis logfil** under **Seneste hændelser**.
4. Klik på **Internet & netværk**, og klik derefter på **Indgående hændelser**.
5. Vælg en kilde-IP-adresse, og klik på **Forbyd denne IP-adresse** under **Jeg ønsker at**.
6. Klik på **Ja** for at bekræfte.

Forbyde en computer fra logfilen til hændelser for registrering af indtrængen

Du kan forbyde en computerforbindelse og dens tilknyttede IP-adresse fra logfilen til hændelser for registrering af indtrængen.

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på menuen **Avanceret**.
2. Klik på **Rapporter og logfiler**.
3. Klik på **Vis logfil** under **Seneste hændelser**.
4. Klik på **Internet & netværk**, og klik derefter på **Hændelser for registrering af indtrængen**.
5. Vælg en kilde-IP-adresse, og klik på **Forbyd denne adresse** under **Jeg ønsker at**.
6. Klik på **Ja** for at bekræfte.

KAPITEL 20

Administrere systemtjenester

For at visse programmer (herunder webserver- og fildelingsserverprogrammer) kan fungere korrekt, skal de acceptere uopfordrede forbindelser fra andre computere via særlige systemtjenesteporte. Firewall lukker typisk disse systemtjenesteporte, fordi de repræsenterer den mest sandsynlige kilde til usikkerheder i dit system. For at kunne acceptere forbindelser fra fjerncomputere skal systemtjenesteportene dog være åbne.

I dette kapitel

Konfigurere systemtjenesteporte

Systemtjenesteporte kan konfigureres til at tillade eller blokere ekstern netværksadgang til en tjeneste på din computer. Disse systemtjenesteporte kan åbnes eller lukkes for computere, der er opført på **netværkslisten** som computere, der er tillid til, standardcomputere eller offentlige computere.

På listen nedenfor vises de almindelige systemtjenester og de tilknyttede porte:

- Almindelig operativsystemport 5357
- FTP-porte (File Transfer Protocol) 20-21
- Mail-serverport (IMAP) 143
- Mail-serverport (POP3) 110
- Mail-serverport (SMTP) port 25
- Microsoft Directory Server (MSFT DS) Port 445
- Microsoft SQL Server-port (MSFT SQL) 1433
- Protokolport for netværksklokkeslæt 123
- Fjernskrivebord-/ Fjernsupport-/Terminal Server-port (RDP) 3389
- RPC-porte (Remote Procedure Calls) 135
- Secure Web Server-port (HTTPS) 443
- Universal Plug and Play-port (UPNP) 5000
- Web-server (HTTP) port 80
- Windows-fildelingsporte (NETBIOS) 137-139

Systemtjenesteporte kan også konfigureres til at tillade, at en computer deler internetforbindelse med andre computere, der er forbundet med den via det samme netværk. Denne forbindelse, kaldet Deling af internetforbindelse (ICS), tillader, at den computer, der deler forbindelsen, fungerer som gateway til internettet for den anden computer på netværket.

Bemærk! Hvis din computer har et program, der accepterer Web- eller FTP-serverforbindelser, skal den computer, der deler forbindelsen, muligvis åbne den tilknyttede systemtjenesteport og tilladelse videresendelse af indgående forbindelser til disse porte.

Tillade adgang til en eksisterende systemtjenesteport

Du kan åbne en eksisterende port for at tillade ekstern adgang til en systemtjeneste på din computer.

Bemærk! En åben systemtjenesteport kan gøre computeren sårbar over for internetsikkerhedstrusler. Derfor bør du kun åbne en port, hvis det er nødvendigt.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Systemtjenester** i ruden Firewall.
4. Vælg en systemtjeneste under **Åbn systemtjenesteport** for at åbne dens port.
5. Klik på **Rediger**.
6. Nu kan du gøre følgende:
   - Du åbner en port til en computer på et netværk, der er tillid til, eller et standard- eller offentligt netværk (f.eks. et hjemmenetværk, et virksomhedsnetværk eller et internetnetværk) ved at vælge **Tillid til, Standard og Offentlig**.
   - Du åbner porten til en computer på et standardnetværk (f.eks. et virksomhedsnetværk) ved at vælge **Standard (omfatter Tillid til)**.
7. Klik på **OK**.

Blokere adgang til en eksisterende systemtjenesteport

Du kan lukke en eksisterende port for at blokere ekstern adgang til en systemtjeneste på din computer.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Systemtjenester** i ruden Firewall.
4. Fjern markeringen i afkrydsningsfeltet ud for den systemtjenesteport, du vil lukke, under **Åbn systemtjenesteport**.
5. Klik på **OK**.

Konfigurere en ny systemtjenesteport

Du kan konfigurere en ny netværkstjenesteport på din computer, som du kan åbne eller lukke for at tillade eller blokere ekstern adgang på din computer.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Systemtjenester** i ruden Firewall.
4. Klik på **Tilføj**.
5. Angiv følgende under **Tilføj regel for systemtjeneste** i ruden Systemtjenester:
   - Navn på systemtjeneste
   - Systemtjenestekategori
   - Lokale TCP/IP-porte
   - Lokale UDP-porte
6. Nu kan du gøre følgende:
   - Du åbner en port til en computer på et netværk, der er tillid til, eller et standard- eller offentligt netværk (f.eks. et hjemmenetværk, et virksomhedsnetværk eller et internetnetværk) ved at vælge **Tillid til, Standard og Offentlig**.
   - Du åbner porten til en computer på et standardnetværk (f.eks. et virksomhedsnetværk) ved at vælge **Standard (omfatter Tillid til)**.
7. Hvis du vil sende denne ports aktivitetsoplysninger til en anden Windows-computer, der deler din internetforbindelse, skal du vælge **Videresend netværksaktivitet på denne port til netværkscomputere, som anvender Deling af internetforbindelse**.
8. Du kan også beskrive den nye konfiguration.
9. Klik på **OK**.

Bemærk! Hvis din computer har et program, der accepterer Web- eller FTP-serverforbindelser, skal den computer, der deler forbindelsen, muligvis åbne den tilknyttede systemtjenesteport og tillade videresendelse af indgående forbindelser til disse porte. Hvis du bruger Deling af internetforbindelse, skal du også føje en computerforbindelse, der er tillid til, til **netværkslisten**. Flere oplysninger finder du under Tilføje en computerforbindelse.

Ændre en systemtjenesteport

Du kan ændre de indgående og udgående netværksadgangsoplysninger for en eksisterende systemtjenesteport.

Bemærk! Hvis portoplysningerne er indtastet forkert, mislykkes systemtjenesten.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Systemtjenester** i ruden Firewall.
4. Marker afkrydsningsfeltet ud for en systemtjeneste, og klik på **Rediger**.
5. Rediger følgende under **Tilføj regel for systemtjeneste** i ruden Systemtjenester:
   - Navn på systemtjeneste
   - Lokale TCP/IP-porte
   - Lokale UDP-porte
6. Nu kan du gøre følgende:
   - Du åbner en port til en computer på et netværk, der er tillid til, eller et standard- eller offentligt netværk (f.eks. et hjemmenetværk, et virksomhedsnetværk eller et internetnetværk) ved at vælge **Tillid til, Standard og Offentlig**.
   - Du åbner porten til en computer på et standardnetværk (f.eks. et virksomhedsnetværk) ved at vælge **Standard (omfatter Tillid til)**.
7. Hvis du vil sende denne ports aktivitetsoplysninger til en anden Windows-computer, der deler din internetforbindelse, skal du vælge **Videresend netværksaktivitet på denne port til netværkscomputere, som anvender Deling af internetforbindelse**.
8. Du kan også beskrive den ændrede konfiguration.
9. Klik på **OK**.

Fjerne en systemtjenesteport

Du kan fjerne en eksisterende systemtjenesteport fra computeren. Efter fjernelse kan eksterne computere ikke længere få adgang til netværkstjenesten på din computer.

1. Klik på **Internet & netværk** i McAfee SecurityCenter-ruden, og klik derefter på **Konfigurer**.
2. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
3. Klik på **Systemtjenester** i ruden Firewall.
4. Vælg en systemtjeneste, og klik på **Fjern**.
5. Klik på **Ja** for at bekræfte.

KAPITEL 21

Logføring, overvågning og analyse

Firewall har omfattende og letlæselig logføring, overvågning og analyse af internethændelser og -trafik. Det er nemmere at administrere dine internetforbindelser, hvis du forstår internettrafik og -hændelser.

I dette kapitel

Logføre hændelser

Firewall lader dig aktivere eller deaktivere logføring og vælge, hvilke hændelsestyper der skal logføres, hvis funktionen er aktiveret. Logføring af hændelser gør det muligt for dig at få vist de seneste ind- og udgående hændelser vedrørende indtrængen.

Konfigurere indstillinger for hændelseslogfil

Du kan vælge og konfigurere de typer Firewall-hændelser, der skal logges. Som standard er hændelseslogføring aktiveret for alle hændelser og aktiviteter.

1. Klik på **Avanceret** under **Firewall-beskyttelse er aktiveret** i ruden Konfiguration af Internet & netværk.
2. Klik på **Indstillinger for hændelseslogfil** i ruden Firewall.
3. Vælg **Aktiver Logføring af hændelser**, hvis funktionen ikke allerede er valgt.
4. Under **Aktiver Logføring af hændelser** skal du markere de hændelsestyper, du ønsker at logføre, og fjerne markeringen af de hændelsestyper, du ikke ønsker at logføre. Hændelsestyper omfatter følgende:
   - Blokerede programmer
   - ICMP-pings
   - Trafik fra forbudte IP-adresser
   - Hændelser på systemtjenesteporte
   - Hændelser på ukendte porte
   - Hændelser for registrering af indtrængen (IDS)
5. Hvis du vil forhindre logføring af bestemte porte, skal du vælge **Logfør ikke hændelser på følgende port(e)**, hvorefter du skal indtaste de enkelte portnumre adskilt med kommaer eller portområder adskilt med bindestreger. F.eks. `137-139, 445, 400-5000`.
6. Klik på **OK**.

Vise de seneste hændelser

Hvis logføring er aktiveret, kan du få vist de seneste hændelser. Ruden Seneste hændelser viser datoen for og beskrivelsen af hændelsen. Den viser aktiviteten for programmer, der er blevet udtrykkeligt blokeret, så de ikke kan få adgang til internettet.

- Klik på **Rapporter & logfiler** eller **Vis seneste hændelser** i ruden Almindelige opgaver i **Avanceret menu**. Du kan også klikke på **Vis seneste hændelser** i ruden Almindelige opgaver i den grundlæggende menu.

Visning af indgående hændelser

Hvis logføring er aktiveret, kan du få vist indgående hændelser. Indgående hændelser omfatter dato og tidspunkt, kilde-IP-adresse, værtsnavn samt oplysninger og hændelsestype.

1. Kontroller, at menuen Avanceret er aktiveret. Klik på **Rapporter & logfiler** i ruden Opgaver.
2. Klik på **Vis logfil** under **Seneste hændelser**.
3. Klik på **Internet & netværk**, og klik derefter på **Indgående hændelser**.

Bemærk! Du kan have tillid til, forbyde og spore en IP-adresse fra logfilen over indgående hændelser.

Vise udgående hændelser

Hvis logføring er aktiveret, kan du få vist og sortere udgående hændelser. Udgående hændelser omfatter navnet på det program, der forsøger at få udgående adgang, datoen og tidspunktet for hændelsen samt programmets placering på computeren.

1. Klik på **Rapporter & logfiler** i ruden Opgaver.
2. Klik på **Vis logfil** under **Seneste hændelser**.
3. Klik på **Internet & netværk**, og klik derefter på **Udgående hændelser**.

Bemærk! Du kan tildele fuld og kun udgående adgang til et program fra logfilen over udgående hændelser. Du kan også finde yderligere oplysninger om programmet.

Vise hændelser for registrering af indtrængen

Hvis logføring er aktiveret, kan du få vist indgående hændelser vedrørende indtrængen. Hændelser for registrering af indtrængen viser datoen og tidspunktet, kilde-IP-adressen, værtsnavnet for hændelsen og hændelsestypen.

1. Klik på **Rapporter & logfiler** i ruden Opgaver.
2. Klik på **Vis logfil** under **Seneste hændelser**.
3. Klik på **Internet & netværk**, og klik derefter på **Hændelser for registrering af indtrængen**.

Bemærk! Du kan forbyde og spore en IP-adresse fra logfilen til hændelser for registrering af indtrængen.

Arbejde med statistikker

Firewall benytter sig af McAfees HackerWatch-sikkerhedswebsted for at give dig statistikker over globale internetsikkerhedshændelser og portaktivitet.

Vise af statistik over globale sikkerhedshændelser

HackerWatch sporer sikkerhedshændelser på internettet over hele verden, som du kan få vist i SecurityCenter. Sporede oplysninger viser hændelser, der er rapporteret til HackerWatch inden for de seneste 24 timer, 7 dage og 30 dage.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **HackerWatch** i ruden Funktioner.
3. Få vist statistikker over sikkerhedshændelser under Hændelsessporing.

Vise global internetportaktivitet

HackerWatch sporer sikkerhedshændelser på internettet over hele verden, som du kan få vist i SecurityCenter. De viste oplysninger omfatter de vigtigste hændelser på porte, der er blevet rapporteret til HackerWatch inden for de seneste syv dage. Typisk vises oplysninger om HTTP-, TCP- og UDP-porte.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **HackerWatch** i ruden Funktioner.
3. Få vist de vigtigste porthændelser under **Recent Port Activity**.

Spore internettrafik

Firewall giver dig en række funktioner til sporing af internettrafik. Disse funktioner gør det muligt for dig geografisk at spore en netværkscomputer, få oplysninger om domæne og netværk samt at spore computere fra logfilerne over indgående hændelser og hændelser for registrering af indtrængen.

Spore en netværkscomputer geografisk

Du kan bruge den visuelle sporing til geografisk at finde en computer, der opretter forbindelse eller forsøger at oprette forbindelse til din computer, ved hjælp af dens navn eller IP-adresse. Du kan også få adgang til netværks- og registreringsoplysninger ved hjælp af den visuelle sporing. Når den visuelle sporing køres, viser den et verdenskort, som viser den mest sandsynlige datarute mellem kildecomputeren og din computer.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **Visuel sporing** i ruden Funktioner.
3. Indtast computerens IP-adresse, og klik på **Spor**.
4. Vælg **Kortvisning** under **Visuel sporing**.

Bemærk! Du kan ikke spore gentagne, private eller ugyldige IP-adressehændelser.

Indhente en computers registreringsoplysninger

Du kan få en computers registreringsoplysninger fra SecurityCenter ved hjælp af visuel sporing. Oplysningerne omfatter domænenavnet, den registreredes navn og adresse samt den administrative kontaktperson.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **Visuel sporing** i ruden Funktioner.
3. Indtast computerens IP-adresse, og klik derefter på **Spor**.
4. Vælg **Registreringsvisning** under **Visuel sporing**.

Indhente en computers netværksoplysninger

Du kan få en computers netværksoplysninger fra SecurityCenter ved hjælp af visuel sporing. Netværksoplysningerne omfatter oplysninger om det netværk, hvor domænet hører hjemme.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **Visuel sporing** i ruden Funktioner.
3. Indtast computerens IP-adresse, og klik derefter på **Spor**.
4. Vælg **Netværksvisning** under **Visuel sporing**.

Spore en computer fra logfilen over indgående hændelser

Du kan spore en IP-adresse, der vises i logfilen over indgående hændelser, fra ruden Indgående hændelser.

1. Kontroller, at menuen Avanceret er aktiveret. Klik på **Rapporter & logfiler** i ruden Opgaver.
2. Klik på **Vis logfil** under **Seneste hændelser**.
3. Klik på **Internet & netværk**, og klik derefter på **Indgående hændelser**.
4. Vælg en kilde-IP-adresse i ruden over indgående hændelser, og klik derefter på **Spor denne IP-adresse**.
5. I ruden Visuel sporing skal du gøre et af følgende:
   - **Kortvisning**: Find en computer, der bruger den valgte IP-adresse, geografisk.
   - **Registreringsvisning**: Find domæneoplysninger ved hjælp af den valgte IP-adresse.
   - **Netværksvisning**: Find netværksoplysninger ved hjælp af den valgte IP-adresse.
6. Klik på **Udført**.

Spor en computer fra logfilen til hændelser for registrering af indtrængen

Du kan spore en IP-adresse, der vises i logfilen til hændelser for registrering af indtrængen, i ruden Hændelser for registrering af indtrængen.

1. Klik på **Rapporter & logfiler** i ruden Opgaver.
2. Klik på **Vis logfil** under **Seneste hændelser**.
3. Klik på **Internet & netværk**, og klik derefter på **Hændelser for registrering af indtrængen**. Vælg en kilde-IP-adresse i ruden Hændelser for registrering af indtrængen, og klik derefter på **Spor denne IP-adresse**.

4 I ruden Visuel sporing skal du gøre et af følgende:

- **Kortvisning**: Find en computer, der bruger den valgte IP-adresse, geografisk.
- **Registreringsvisning**: Find domæneoplysninger ved hjælp af den valgte IP-adresse.
- **Netværksvisning**: Find netværksoplysninger ved hjælp af den valgte IP-adresse.

5 Klik på **Udført**.

Spor en overvåget IP-adresse

Du kan spore en overvåget IP-adresse for at få en geografisk visning, som viser den mest sandsynlige datarute fra kildecomputeren til din computer. Derudover kan du få registrerings- og netværksoplysninger om IP-adressen.

1 Sørg for, at menuen Avanceret er aktiveret, og klik på **Funktioner**.

2 Klik på **Trafikovervågning** i ruden Funktioner.

3 Klik på **Aktive programmer** under **Trafikovervågning**.

4 Vælg et program, og vælg derefter den IP-adresse, der vises under programnavnet.

5 Klik på **Spor denne IP-adresse** under **Programaktivitet**.

6 Under **Visuel sporing** kan du få vist et kort, som viser den mest sandsynlige datarute fra kildecomputeren til din computer. Derudover kan du få registrerings- og netværksoplysninger om IP-adressen.

Bemærk! Hvis du vil have vist de mest opdaterede statistikker, skal du klikke på **Opdater** under **Visuel sporing**.

Overvåge internettrafik

Firewall indeholder en række metoder til overvågning af din internettrafik. Dette gælder følgende programmer:

- **Grafen Trafikanalyse**: Viser seneste indgående og udgående internettrafik.
- **Grafen Trafikanvendelse**: Viser den forholdsmæssige procentdel af båndbredde, der er anvendt af de mest aktive programmer i løbet af den forgangne 24 timers periode.
- **Aktive programmer**: Viser de programmer, der aktuelt bruger flest netværksforbindelser på computeren, og de IP-adresser, som programmerne får adgang til.

Om grafen Trafikanalyse

Trafikanalysegrafen er en numerisk og grafisk gengivelse af ind- og udgående internettrafik. Trafikovervågningen viser også de programmer, der aktuelt bruger flest netværksforbindelser på computeren, og de IP-adresser, som programmerne får adgang til.

I ruden Trafikanalyse kan du få vist den seneste indgående og udgående internettrafik, aktuelle, gennemsnitlige og maksimale overførselshastigheder. Du kan også få vist trafikomfang, herunder mængden af trafik, efter at du startede Firewall, og den samlede trafik for den aktuelle og de foregående måneder.

Ruden til trafikanalyse viser internetaktivitet på din computer i realtid, herunder mængden og hastigheden af den seneste indgående og udgående internettrafik på din computer, hastigheden på internetforbindelsen samt de samlede byte, der overføres via internettet.

Den udfyldte grønne linje repræsenterer den aktuelle overførselshastighed for indgående trafik. Den prikkede grønne linje repræsenterer den gennemsnitlige overførselshastighed for indgående trafik. Hvis den aktuelle overførselshastighed og den gennemsnitlige overførselshastighed er den samme, vises den prikkede linje ikke på grafen. Den udfyldte linje repræsenterer både den gennemsnitlige og den aktuelle overførselshastighed.

Den udfyldte røde linje repræsenterer den aktuelle overførselshastighed for udgående trafik. Den røde prikkede linje repræsenterer den gennemsnitlige overførselshastighed for udgående trafik. Hvis den aktuelle overførselshastighed og den gennemsnitlige overførselshastighed er den samme, vises den prikkede linje ikke på grafen. Den udfyldte linje repræsenterer både den gennemsnitlige og den aktuelle overførselshastighed.

Analyse af indgående og udgående trafik

Trafikanalysegrafen er en numerisk og grafisk gengivelse af ind- og udgående internettrafik. Trafikovervågningen viser også de programmer, der aktuelt bruger flest netværksforbindelser på computeren, og de IP-adresser, som programmerne får adgang til.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **Trafikovervågning** i ruden Funktioner.
3. Klik på **Trafikanalyse** under **Trafikovervågning**.

Tip: Hvis du vil have vist de mest opdaterede statistikker, skal du klikke på **Opdater** under **Trafikanalyse**.

Overvågning af programmers båndbredde

Du kan få vist cirkeldiagrammet, som viser den omtrentlige procentdel af båndbredde, der er anvendt af de mest aktive programmer på computeren inden for de sidste fireogtyve timer. Cirkeldiagrammet viser en visuel gengivelse af de forholdsmæssige mængder båndbredde, som programmerne anvender.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **Trafikovervågning** i ruden Funktioner.
3. Klik på **Trafikanvendelse** under **Trafikovervågning**.

Tip: Hvis du vil have vist de mest opdaterede statistikker, skal du klikke på **Opdater** under **Trafikanvendelse**.

Overvågning af programaktivitet

Du kan få vist indgående og udgående programaktivitet, som viser en computers fjernforbindelser og -porte.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **Trafikovervågning** i ruden Funktioner.
3. Klik på **Aktive programmer** under **Trafikovervågning**.

4 Du kan få vist følgende oplysninger:

- Grafen Programaktivitet: Vælg et program, der skal vise en graf over dets aktivitet.
- Lytteforbindelse: Vælg et lytteelement under programnavnet.
- Computerforbindelse: Vælg en IP-adresse under programnavnet, systemprocessen eller tjenesten.

Bemærk! Hvis du vil have vist de mest opdaterede statistikker, skal du klikke på **Opdater** under **Aktive programmer**.

KAPITEL 22

Få mere at vide om internetsikkerhed

Firewall benytter sig af McAfees sikkerhedswebsted HackerWatch til at levere opdaterede oplysninger om programmer og global internetaktivitet. HackerWatch indeholder også en HTML-vejledning om Firewall.

I dette kapitel

Start vejledningen til HackerWatch

Hvis du vil vide mere om Firewall, kan du få adgang til vejledningen HackerWatch fra SecurityCenter.

1. Sørg for, at menuen Avanceret er aktiveret, og klik derefter på **Funktioner**.
2. Klik på **HackerWatch** i ruden Funktioner.
3. Klik på **Vis vejledning** under **HackerWatch-ressourcer**.

KAPITEL 23

McAfee Anti-Spam

Anti-Spam (tidligere kaldet SpamKiller) forhindrer, at du modtager uønskede e-mail-meddelelser i indbakken, ved at undersøge din indgående e-mail og derefter markere den som spam (e-mail, der opfordrer dig til at købe) eller phishing (e-mail, der opfordrer dig til at angive personlige oplysninger til et potentielt bedragerisk websted). Anti-Spam filtrerer derefter spam-e-mailen og flytter den til McAfee Anti-Spam-mappen.

Hvis dine venner nogle gange sender dig legitime e-mails, der ligner spam, kan du sikre, at de ikke filtreres, ved at føje deres e-mail-adresser til vennelisten i Anti-Spam. Du kan også tilpasse den måde, spam registreres på. Du kan f.eks. filtrere meddelelser mere aggressivt, angive, hvad programmet skal søge efter i meddelelserne, og oprette dine egne filtre.

Anti-Spam beskytter dig også, hvis du forsøger at få adgang til et potentielt bedragerisk websted gennem et link i en e-mail-meddelelse. Når du klikker på et link til et potentielt bedragerisk websted, omdirigeres du til den sikre phishing-filterside. Hvis der er websteder, du ikke ønsker filtreret, kan du føje dem til positivlisten (websteder på denne liste filtreres ikke).

Anti-Spam fungerer sammen med forskellige e-mail-programmer som f.eks. Yahoo®, MSN®/Hotmail®, Windows® Mail og Live™ Mail, Microsoft® Outlook® og Outlook Express og Mozilla Thunderbird™ samt forskellige e-mail-konti som f.eks. POP3, POP3 Webmail og MAPI (Microsoft Exchange Server). Hvis du bruger en browser til at læse e-mail, skal du føje din webmail-konto til Anti-Spam. Alle andre konti konfigureres automatisk, og du behøver ikke føje dem til Anti-Spam.

Det er ikke nødvendigt at konfigurere Anti-Spam, når du har installeret det, men hvis du er en avanceret bruger, vil du muligvis tilpasse de avancerede spam- og phishingbeskyttelsesfunktioner efter behov.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Anti-Spam

Spamfiltrering
Undgå, at uopfordrede e-mail-meddelelser kommer i din Indbakke. Anti-Spams avancerede filtre opdateres automatisk for alle dine e-mail-konti. Du kan også oprette tilpassede filtre for at sikre, at al spam filtreres, og rapportere spam til McAfee til analyse.

Phishing-filtrering
Identificer potentielle phishing- (bedrageriske) websteder, der beder dig opgive personlige oplysninger.

Tilpasset behandling af spam
Marker uønsket e-mail som spam, og flyt den til din McAfee Anti-Spam-mappe, eller marker legitim e-mail som ikke-spam, og flyt den til indbakken.

Venner
Importer dine venners e-mail-adresser til vennelisten, så deres e-mails ikke filtreres.

KAPITEL 24

Konfigurere spamregistrering

Anti-Spam giver dig mulighed for at tilpasse den måde, spam registreres på. Du kan filtrere meddelelser mere aggressivt, angive, hvad programmet skal søge efter i meddelelserne, og søge efter bestemte tegn, når der analyseres for spam. Du kan også oprette personlige filtre for at finjustere, hvilke meddelelser Anti-Spam identificerer som spam. Hvis uønsket e-mail, der indeholder ordet "mortgage", ikke filtreres, kan du tilføje et filter, der indeholder ordet mortgage.

Hvis du har problemer med din e-mail, kan du deaktivere spambeskyttelse som en del af fejlfindingsstrategien.

I dette kapitel

Konfigurere filtreringsindstillinger

Juster filtreringsindstillingerne i Anti-Spam, hvis du vil filtrere meddelelser mere aggressivt, angive, hvordan du ønsker at behandle spam og søge efter bestemte tegn, når der analyseres for spam.

Filtreringsniveau

Filtreringsniveauet angiver, hvor aggressivt din e-mail filtreres. Hvis spam f.eks. ikke filtreres, og dit filtreringsniveau er indstillet til Mellem, kan du ændre det til Mellem-Højt eller Højt. Hvis filtreringsniveauet er indstillet til Højt, accepteres kun e-mail-meddelelser fra afsendere på din venneliste: alle andre filtreres.

Spambehandling

Anti-Spam giver dig mulighed for at tilpasse den måde, spam behandles på. Du kan f.eks. placere spam- og phishing-meddelelser i bestemte mapper, ændre navnet på det mærke, der vises i emnelinjen for spam- og phishing-meddelelsen, angive en maksimal størrelse for filtreringen samt angive, hvor ofte spam-reglerne skal opdateres.

Tegnsæt

Anti-Spam kan søge efter bestemte tegnsæt, når der analyseres for spam. Tegnsæt bruges til at vise et sprog, herunder sprogets alfabet, tal og andre symboler. Hvis du modtager spam på græsk, kan du filtrere alle meddelelser, der indeholder det græske tegnsæt.

Bloker dog ikke tegnsæt for sprog, du modtager legitim e-mail på. Hvis du f.eks. kun vil filtrere meddelelser på italiensk, vælger du måske Vesteuropæisk, fordi Italien er beliggende i Vesteuropa. Hvis du modtager legitim e-mail på f.eks. engelsk, filtreres meddelelser på engelsk og andre sprog i det vesteuropæiske tegnsæt også, hvis du vælger Vesteuropæisk. I det tilfælde kan du ikke filtrere meddelelser på kun italiensk.

Bemærk! Angivelse af et tegnsætfilter er for avancerede brugere.

Ændre filtreringsniveauet

Du kan ændre, hvor aggressivt meddelelserne skal filtreres. Hvis legitime e-mail-meddelelser for eksempel filtreres, kan du sænke filtreringsniveauet.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Filtreringsindstillinger** i ruden Spambeskyttelse.

3 Vælg det passende niveau på listen **Angiv et spamfilter-niveau**, og klik på **OK**.

Niveau	Beskrivelse
Lavt	De fleste e-mail-meddelelser accepteres.
Mellem-lavt	Kun åbenlyse spammeddelelser filtreres.
Medium (Anbefalet)	E-mail filtreres på det anbefalede niveau.
Mellem-højt	Alle e-mail-meddelelser, der minder om spam, filtreres.
Højt	Kun meddelelser fra afsendere på din venneliste accepteres.

Tilpasse, hvordan spam behandles og markeres

Du kan angive en mappe, som spam- og phishing-meddelelser skal placeres i, ændre det [SPAM]- eller [PHISH]-mærke, der vises i meddelelsens emnelinje, angive en maksimal størrelse for filtreringen samt, hvor ofte dine spam-regler skal opdateres.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Filtreringsindstillinger** i ruden Spambeskyttelse.

3 Rediger eller vælg de relevante indstillinger nedenfor, og klik derefter på **OK**.

For at...	Skal du...
Angive den placering, hvor spam- og phishing-meddelelser skal placeres	Vælge en mappe på listen **Anbring spam-mail i denne mappe**. Standardmappen er McAfee Anti-Spam.
Ændre emnelinjen for spam-meddelelsen	Angive et mærke, der skal føjes til emnelinjen i en spam-meddelelse i **Marker emnet på spam-mailen med**. Standardmærket er [SPAM].
Ændre emnelinjen for phising-meddelelsen	Angive et mærke, der skal føjes til emnelinjen i en phishing-meddelelse i **Marker emnet på phish-e-mailen med**. Standardmærket er [PHISH].
Angive maksimumstørrelse for meddelelser, der skal filtreres	Angive maksimumstørrelsen for de meddelelser, du vil filtrere, i **Angiv den maksimale e-mail-størrelse til (størrelse i KB)**.
Opdatere spam-reglerne	Vælge **Opdater spam-regler (i minutter)** og derefter angive hyppigheden for opdatering af spam-reglerne. Den anbefalede hyppighed er 30 minutter. Hvis du har en hurtig netværksforbindelse, kan du angive en høj værdi, f.eks. 5 minutter, for at få et bedre resultat.
Undgå at opdatere spam-reglerne	Vælge **Opdater ikke spam-regler**.

Anvende tegnsætfiltre

Bemærk! Filtrering af meddelelser, der indeholder tegn fra et bestemt tegnsæt, er for avancerede brugere.

Du kan filtrere tegnsæt for bestemte sprog. Bloker dog ikke tegnsæt for sprog, du modtager legitim e-mail på.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Tegnsæt** i ruden Spambeskyttelse.

3 Marker afkrydsningsfelterne ved siden af de tegnsæt, som du ønsker at filtrere.

4 Klik på **OK**.

Bruge personlige filtre

Et personligt filter angiver, hvorvidt e-mail-meddelelser skal tillades eller blokeres på baggrund af bestemte ord eller sætninger. Hvis en e-mail-meddelelse indeholder et ord eller en sætning, som filteret er angivet til at blokere, markeres meddelelsen som spam og forbliver i din Indbakke eller flyttes til mappen McAfee Anti-Spam. Du kan finde flere oplysninger om, hvordan spam håndteres, under Tilpasse, hvordan en meddelelse behandles og markeres (side 121).

Anti-Spam er udstyret med et avanceret filter for at forhindre, at uopfordrede e-mail-meddelelser får adgang til din Indbakke. Du kan dog oprette et personligt filter, hvis du ønsker at finjustere, hvilke meddelelser Anti-Spam identificerer som spam. Hvis du f.eks. tilføjer et filter, der indeholder ordet "mortgage", filtreres meddelelser med ordet mortgage. Opret ikke filtre for almindelige ord, der vises i legitime e-mail-meddelelser, fordi ikke-spam også filtreres derved. Når du har oprettet et filter, kan du redigere det, hvis filtret stadig ikke registrerer bestemt spam. Hvis du f.eks. har oprettet et filter, der skal søge efter ordet viagra i meddelelsens emne, men du stadig modtager meddelelser, der indeholder ordet viagra, fordi det vises i selve teksten, skal du ændre filtret, så det søger efter viagra i meddelelsesteksten i stedet for meddelelsesemnet.

Regulære udtryk (RegEx) er særlige tegn og sekvenser, der også kan bruges i personlige filtre. McAfee anbefaler dog kun, at du bruger regulære udtryk, hvis du er avanceret bruger. Hvis du ikke har kendskab til regulære udtryk, eller du ønsker flere oplysninger om, hvordan de bruges, kan du søge oplysninger om regulære udtryk på internettet (gå f.eks. til http://en.wikipedia.org/wiki/Regular_expression).

Tilføje et personligt filter

Du kan tilføje personlige filtre for at finjustere, hvilke meddelelser Anti-Spam identificerer som spam.

1 Åbn ruden Spambeskyttelse.

Hvordan?

1. Klik på **E-mail & IM** i startruden for SecurityCenter.
2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Personlige filtre** i ruden Spambeskyttelse.

3 Klik på **Tilføj**.

4 Angiv, hvad det personlige filter skal søge efter (side 125) i en e-mail-meddelelse.

5 Klik på **OK**.

Redigere et personligt filter

Rediger eksisterende personlige filtre for at finjustere, hvilke meddelelser Anti-Spam identificerer som spam.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Personlige filtre** i ruden Spambeskyttelse.

3 Marker det filter, som du vil redigere, og klik på **Rediger**.

4 Angiv, hvad det personlige filter skal søge efter (side 125) i en e-mail-meddelelse.

5 Klik på **OK**.

Fjerne et personligt filter

Du kan permanent fjerne de filtre, som du ikke længere vil bruge.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Personlige filtre** i ruden Spambeskyttelse.

3 Marker det filter, som du vil fjerne, og klik på **Fjern**.

4 Klik på **OK**.

Angive et personligt filter

Denne tabel beskriver, hvad et personligt filter søger efter i en e-mail-meddelelse.

For at...	Skal du...
Angive den e-mail-del, der skal filtreres	Klikke på en post på listen **E-mail-del** for at fastslå, om filtret leder efter ord eller sætninger i meddelelsens emnelinje, meddelelsestekst, afsender, overskrift eller meddelelsens modtager. Klikke på en post på listen **E-mail-del** for at fastslå, om filtret leder efter en meddelelse, der indeholder eller ikke indeholder de ord eller sætninger, som du angiver.
Angive ordene eller sætningerne i dit filter	Skrive det, der skal søges efter i en e-mail, i **Ord eller sætninger**. Hvis du for eksempel angiver *mortgage*, filtreres alle meddelelser, der indeholder dette ord.
Angive, at filteret skal benytte regulære udtryk	Vælge **Dette filter anvender regulære udtryk**.
Vælge, hvorvidt e-mail-meddelelser skal blokeres eller tillades, afhængigt af ordene eller sætningerne i dit filter.	I **Udfør denne handling** enten vælge **Bloker** eller **Tillad** for at blokere eller tillade e-mail-meddelelser, der indeholder ordene eller sætningerne i dit filter.

Deaktivere spambeskyttelse

Du kan deaktivere spambeskyttelse for at forhindre, at Anti-Spam filtrerer e-mail-meddelelserne.

1. Klik på **Konfigurer** i menuen Avanceret.
2. Klik derefter på **E-mail & IM** i ruden Konfigurer.
3. Under **Spambeskyttelse er aktiveret** skal du klikke på **Fra**.

Tip! Husk at klikke på **Til** under **Spambeskyttelse er deaktiveret**, så computeren er beskyttet mod spam.

KAPITEL 25

Filtrere e-mail

Anti-Spam undersøger indgående e-mail og kategoriserer den som spam (e-mails, der opfordrer dig til at købe) eller phishing (e-mails, der opfordrer dig til at angive personlige oplysninger til et kendt eller muligt bedragerisk websted). Som standard markerer Anti-Spam derefter hver uønsket e-mail som spam eller phishing (mærket [SPAM] eller [PHISH] vises i meddelelsens emnelinje) og flytter meddelelsen til McAfee Anti-Spam-mappen.

Du kan markere e-mail-meddelelser som spam eller ikke-spam fra Anti-Spam-værktøjslinjen, ændre den placering, hvortil spam-meddelelser flyttes eller ændre det mærke, der vises i emnelinjen.

Du kan også deaktivere Anti-Spam-værktøjslinjer som en del af din fejlfindingsstrategi, hvis du har problemer med dit e-mail-program.

I dette kapitel

Markere en meddelelse fra Anti-Spam-værktøjslinjen

Når du markerer en meddelelse som spam, markeres meddelelsens emne med [SPAM] eller et mærke efter eget valg og efterlades i indbakken, McAfee Anti-Spam-mappen (Outlook, Outlook Express, Windows Mail, Thunderbird) eller i mappen med uønsket post (Eudora®). Når du markerer en meddelelse som ikke-spam, fjernes meddelelsens mærke, og meddelelsen flyttes til indbakken.

Sådan markerer du en meddelelse i ...	Marker en meddelelse, og ...
Outlook, Outlook Express, Windows Mail	Klik på **Marker som spam** eller **Marker som ikke spam**.
Eudora	Klik på **Marker som spam** eller **Marker som ikke spam** i menuen **Anti-Spam**.
Thunderbird	Peg på **M**, og peg på **Marker som** på værktøjslinjen **Anti-Spam**, og klik derefter på **Spam** eller **Ikke spam**.

Deaktivere Anti-Spam-værktøjslinjen

Hvis du bruger Outlook, Outlook Express, Windows Mail Eudora eller Thunderbird, kan du deaktivere Anti-Spam-værktøjslinjen.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **E-mail-værktøjslinjer** i ruden Spambeskyttelse.

3 Fjern markeringen i afkrydsningsfeltet ved siden af den værktøjslinje, som du vil deaktivere.

4 Klik på **OK**.

Tip! Du kan til enhver tid aktivere dine Anti-Spam-værktøjslinjer igen ved at markere deres afkrydsningsfelter.

KAPITEL 26

Konfigurere venner

Eftersom Anti-Spams filter er blevet forbedret og genkender samt tillader legitime e-mail-meddelelser, er det sjældent, at du behøver at føje dine venners e-mail-adresser til din venneliste, uanset om du tilføjer dem manuelt eller importerer dem fra adressebogen. Hvis du alligevel tilføjer en vens e-mail-adresse, og nogen laver fup med den, vil Anti-Spam tillade meddelelser fra den pågældende e-mail-adresse i din Indbakke.

Hvis du stadigvæk ønsker at importere dine adressebøger, og de ændres, skal du importere dem igen, fordi Anti-Spam ikke automatisk opdaterer din venneliste.

Du kan også opdatere vennelisten i Anti-Spam manuelt eller tilføje et helt domæne, hvis du ønsker, at alle brugere i domænet skal føjes til din venneliste. Hvis du f.eks. tilføjer domænet virksomhed.dk, filtreres ingen e-mail fra denne organisation.

I dette kapitel

Importere en adressebog

Importer dine adressebøger, hvis du ønsker, at Anti-Spam skal føje e-mail-adresserne i bøgerne til din venneliste.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Venner** i ruden Spambeskyttelse.

3 Klik på **Importer** i ruden Venner.

4 Klik på den type adressebog, som du vil importere, på listen **Vælg en adressebog, der skal importeres**.

5 Klik på **Importer nu**.

Konfigurere venner manuelt

Du kan opdatere din venneliste ved at redigere posterne en for en. Hvis du f.eks. modtager en e-mail fra en ven, hvis adresse ikke findes i din adressebog, kan du manuelt tilføje deres e-mail-adresse med det samme. Det er nemmest at gøre ved hjælp af værktøjslinjen i Anti-Spam. Hvis du ikke bruger værktøjslinjen i Anti-Spam, skal du angive oplysningerne om vennen.

Tilføje en ven fra Anti-Spam-værktøjslinjen

Hvis du bruger e-mail-programmerne Outlook, Outlook Express, Windows Mail, Eudora™ eller Thunderbird, kan du tilføje venner direkte fra Anti-Spam-værktøjslinjen.

Sådan tilføjer du en ven fra...	Marker en meddelelse, og ...
Outlook, Outlook Express, Windows Mail	Klik på **Tilføj en ven**.
Eudora	Klik på **Tilføj en ven** i menuen **Anti-Spam**.
Thunderbird	Peg på **M**, og peg på **Marker som** på værktøjslinjen **Anti-Spam**, og klik derefter på **Ven**.

Tilføje en ven manuelt

Hvis du ikke ønsker at tilføje en ven direkte fra værktøjslinjen, eller du glemte at gøre det, da du modtog e-mail-meddelelsen, kan du stadigvæk tilføje en ven til din venneliste.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Venner** i ruden Spambeskyttelse.

3 Klik på **Tilføj** i ruden Venner.

4 Skriv navnet på din ven i boksen **Navn**.

5 Vælg **Enkelt e-mail-adresse** på listen **Type**.

6 Skriv din vens e-mail-adresse i feltet **E-mail-adresse**.

7 Klik på **OK**.

Tilføje et domæne

Tilføj et helt domæne, hvis du ønsker at føje alle brugere i det pågældende domæne til din venneliste. Hvis du f.eks. tilføjer domænet virksomhed.dk, filtreres ingen e-mail fra denne organisation.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Venner** i ruden Spambeskyttelse.

3 Klik på **Tilføj** i ruden Venner.

4 Skriv navnet på organisationen eller gruppen i feltet **Navn**.

5 Vælg **Helt domæne** på listen **Type**.

6 Skriv domænenavnet i feltet **E-mail-adresse**.

7 Klik på **OK**.

Redigere en ven

Hvis oplysningerne om en ven ændres, kan du opdatere vennelisten for at sikre, at Anti-Spam ikke markerer meddelelser fra den pågældende person som spam.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Venner** i ruden Spambeskyttelse.

3 Marker den ven, som du vil redigere, og klik på **Rediger**.

4 Rediger navnet på din ven i feltet **Navn**.

5 Skriv din vens e-mail-adresse i feltet **E-mail-adresse**.

6 Klik på **OK**.

Redigere et domæne

Hvis oplysningerne om et domæne ændres, kan du opdatere vennelisten for at sikre, at Anti-Spam ikke markerer meddelelser fra dette domæne som spam.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Venner** i ruden Spambeskyttelse.

3 Klik på **Tilføj** i ruden Venner.

4 Rediger navnet på organisationen eller gruppen i feltet **Navn**.

5 Vælg **Helt domæne** på listen **Type**.

6 Skriv domænenavnet i feltet **E-mail-adresse**.

7 Klik på **OK**.

Fjerne en ven

Hvis en person eller et domæne på vennelisten sender dig spam, skal du fjerne den pågældende fra vennelisten i Anti-Spam, så hans/hendes meddelelser filtreres igen.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Venner** i ruden Spambeskyttelse.

3 Marker den ven, som du vil fjerne, og klik på **Fjern**.

KAPITEL 27

Konfigurere webmail-konti

Hvis du bruger en browser til at læse e-mail, skal du konfigurere Anti-Spam til at oprette forbindelse til kontoen og filtrere dine meddelelser. Hvis du vil føje din webmail-konto til Anti-Spam, skal du blot tilføje de kontooplysninger, du har modtaget fra e-mail-udbyderen.

Når du har tilføjet en webmail-konto, kan du redigere dine kontooplysninger og hente flere oplysninger om filtreret webmail. Hvis du ikke længere bruger en webmail-konto, eller du ikke ønsker den filtreret, kan du fjerne den.

Anti-Spam fungerer sammen med forskellige e-mail-programmer som f.eks. Yahoo®, MSN®/Hotmail®, Windows® Mail og Live™ Mail, Microsoft® Outlook® og Outlook Express og Mozilla Thunderbird™ samt forskellige e-mail-konti som f.eks. POP3, POP3 Webmail og MAPI (Microsoft Exchange Server). POP3 er den mest almindelige kontotype og er standarden for internet-e-mail. Hvis du har en POP3-konto, etablerer Anti-Spam direkte forbindelse til e-mail-serveren og filtrerer meddelelserne, inden de hentes af din webmail-konto. POP3-webmail-, Yahoo!-, MSN/Hotmail- og Windows Mail-konti er webbaserede. Filtrering af POP3-webmail-konti svarer til filtrering af POP3-konti.

I dette kapitel

Tilføje en webmail-konto

Tilføj en POP3-konto (f.eks. Yahoo), MSN/Hotmail-konto eller Windows Mail-webmail-konto (kun betalte versioner understøttes fuldt ud), hvis du vil filtrere meddelelserne på kontoen for spam.

1 Åbn ruden Spambeskyttelse.

Hvordan?

1. Klik på **E-mail & IM** i startruden for SecurityCenter.
2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Webmail-konti** i ruden Spambeskyttelse.

3 Klik på **Tilføj** i ruden Webmail-konti.

4 Angiv kontooplysningerne (side 135), og klik derefter på **Næste**.

5 Under **Kontrollerer indstillinger** skal du angive, hvornår Anti-Spam kontrollerer din konto for spam (side 135).

6 Hvis du bruger en opkaldsforbindelse, skal du angive, hvordan Anti-Spam opretter forbindelse til internettet (side 135).

7 Klik på **Udfør**.

Redigere en webmail-konto

Du skal redigere dine webmail-kontooplysninger, hvis der forekommer ændringer i din konto. Du skal f.eks. redigere din webmail-konto, hvis du ændrer din adgangskode, eller du ønsker, at Anti-Spam skal søge efter spam oftere.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Webmail-konti** i ruden Spambeskyttelse.

3 Marker den konto, du vil ændre, og klik på **Rediger**.

4 Angiv kontooplysningerne (side 135), og klik derefter på **Næste**.

5 Under **Kontrollerer indstillinger** skal du angive, hvornår Anti-Spam kontrollerer din konto for spam (side 135).

6 Hvis du bruger en opkaldsforbindelse, skal du angive, hvordan Anti-Spam opretter forbindelse til internettet (side 135).

7 Klik på **Udfør**.

Fjerne en webmail-konto

Fjern en webmail-konto, hvis du ikke længere ønsker at filtrere den for spam. Hvis din konto f.eks. ikke er aktiv længere, eller du oplever problemer, kan du fjerne kontoen, mens du foretager fejlfinding af problemet.

1 Åbn ruden Spambeskyttelse.

Hvordan?

1. Klik på **E-mail & IM** i startruden for SecurityCenter.
2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **Webmail-konti** i ruden Spambeskyttelse.

3 Marker den konto, som du vil fjerne, og klik på **Fjern**.

Forklaring af webmail-kontooplysninger

I følgende tabeller beskrives de oplysninger, du skal angive, når du tilføjer eller redigerer webmail-konti.

Kontooplysninger

Oplysninger	Beskrivelse
Beskrivelse	Beskriv kontoen, så du selv kan finde den. I dette felt kan du indtaste din egen beskrivelse.
E-mail-adresse	Angiv den e-mail-adresse, der er knyttet til denne e-mail-konto.
Kontotype	Vælg den e-mail-kontotype, du vil tilføje (f.eks. POP3-webmail eller MSN/Hotmail.
Server	Angiv navnet på mail-serveren for denne konto. Hvis du ikke kender servernavnet, kan du se oplysningerne fra din internetudbyder.
Brugernavn	Angiv brugernavnet for denne e-mail-konto Hvis din e-mail-adresse f.eks. er *brugernavn*@hotmail.com, er brugernavnet sandsynligvis *brugernavn*.
Adgangskode	Angiv adgangskoden til denne e-mail-konto
Bekræft adgangskode	Bekræft adgangskoden til denne e-mail-konto

Kontrollerer indstillinger

Indstilling	Beskrivelse
Kontroller hver	Anti-Spam kontrollerer denne konto med det interval (antal minutter), du angiver. Intervallet skal være mellem 5 og 3600 minutter.
Kontroller ved start	Anti-Spam kontrollerer kontoen, hver gang du genstarter computeren.

Forbindelsesindstillinger

Indstilling	Beskrivelse
Ring aldrig op	Anti-Spam ringer ikke automatisk op for dig. Du skal starte din opkaldsforbindelse manuelt.
Ring op, når der ikke er en tilgængelig forbindelse	Når der ikke er en tilgængelig internetforbindelse, forsøger Anti-Spam at oprette forbindelse til internettet ved hjælp af den opkaldsforbindelse, du angav.
Ring altid op til den angivne forbindelse	Anti-Spam forsøger at oprette forbindelse til den opkaldsforbindelse, du angav. Hvis du har oprettet forbindelse gennem en anden opkaldsforbindelse end den, du angiver, afbrydes forbindelsen.
Ring denne forbindelse op	Angiv den opkaldsforbindelse, Anti-Spam bruger til at oprette forbindelse til internettet.
Opretholdforbindelse efter filtrering er udført	Computeren opretholder forbindelse til internettet efter udført filtrering.

KAPITEL 28

Arbejde med filtreret e-mail

Noget spam registreres i nogle tilfælde ikke. Hvis det sker, kan du rapportere spam til McAfee, der vil analysere det og oprette filteropdateringer.

Hvis du bruger en webmail-konto, kan du få vist, eksportere og slette dine filtrerede e-mail-meddelelser. Dette er nyttigt, hvis du ikke er sikker på, om en legitim meddelelse er blevet filtreret, eller du ønsker at vide, hvornår meddelelsen blev filtreret.

I dette kapitel

Rapportere e-mail-meddelelser til McAfee

Du kan rapportere e-mail-meddelelser til McAfee, når du markerer dem som spam eller som ikke-spam, som vi analyserer med det formål at oprette filteropdateringer.

1 Åbn ruden Spambeskyttelse.

   Hvordan?

   1. Klik på **E-mail & IM** i startruden for SecurityCenter.
   2. I området med oplysninger om e-mail & IM information skal du klikke på **Konfigurer**.
   3. Klik på **Avanceret** under **Spambeskyttelse** i konfigurationsruden E-mail & IM.

2 Klik på **E-mail-værktøjslinjer** i ruden Spambeskyttelse.

3 Marker de relevante afkrydsningsfelter under **Hjælp med at forbedre Anti-Spam**, og klik derefter på **OK**.

For at...	Skal du...
Rapportere en e-mail til McAfee, hver gang du markerer en som spam	Vælge **Du markerer e-mail som spam**.
Rapportere en e-mail til McAfee, hver gang du markerer en som ikke spam	Vælge **Du markerer e-mail som ikke spam**.

For at...	Skal du...
Sende hele e-mail-meddelelsen, ikke kun overskriften, til McAfee, når du rapporterer en e-mail som ikke spam	Vælge **Send hele e-mailen (ikke kun overskrift).**

Bemærk! Når du rapporterer en e-mail-meddelelse som ikke spam og sender hele meddelelsen til McAfee, krypteres e-mail-meddelelsen ikke.

Få vist, eksportere eller slette filtreret webmail

Du kan få vist, eksportere eller slette meddelelser, der er filtreret i din webmail-konto.

1. Under **Almindelige opgaver** skal du klikke på **Rapporter & Logfiler**.
2. I ruden Rapporter & logfiler skal du klikke på **Filtreret webmail**.
3. Marker en meddelelse.
4. Under **Jeg ønsker at** skal du udføre en af følgende handlinger:
   - Klik på **Vis** for at se meddelelsen i dit standard-e-mail-program.
   - Klik på **Eksporter** for at kopiere meddelelsen til din computer.
   - Klik på **Slet** for at slette meddelelsen.

Vise en hændelse for filtreret webmail

Du kan få vist, hvornår e-mail-meddelelsen blev filtreret, og den konto, der modtog den.

1. Klik på **Vis seneste hændelser** under **Almindelige opgaver**.
2. Klik på **Vis logfil** i ruden Seneste hændelser.
3. Udvid listen **E-mail & IM**, og klik på **Hændelser for filtrering af webmail** i den venstre rude.
4. Vælg den logfil, du ønsker at se.

KAPITEL 29

Konfigurere phishing-beskyttelse

Anti-Spam kategoriserer uønsket e-mail som spam (e-mails, der opfordrer dig til at købe) eller phishing (e-mails, der opfordrer dig til at angive personlige oplysninger til et kendt eller muligt bedragerisk websted). Phishing-beskyttelse hjælper med at beskytte dig mod bedrageriske websteder. Når du klikker på et link i en e-mail til et potentielt bedragerisk websted, omdirigeres du til den sikre phishing-filterside.

Hvis der er websteder, du ikke vil filtrere, skal du føje dem til phishing-positivlisten. Du kan også redigere eller fjerne websteder fra positivlisten. Du behøver ikke tilføje websteder, som f.eks. Google®, Yahoo eller McAfee, da disse websteder ikke betragtes som bedrageriske.

Bemærk! Hvis du har installeret SiteAdvisor, modtager du ikke phishing-beskyttelse i Anti-Spam, fordi SiteAdvisor allerede omfatter phishing-beskyttelse svarende til beskyttelsen i Anti-Spam.

I dette kapitel

Tilføje et websted til positivlisten

Hvis der er websteder, du ikke vil filtrere, skal du føje dem til phishing-positivlisten.

1. Åbn ruden Phishing-beskyttelse.

   Hvordan?

   1. Klik på **Internet & netværk** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i området Internet- & netværksoplysninger.

2. Klik på **Avanceret** i ruden Phishing-beskyttelse.
3. Klik på **Tilføj** under **Positivliste**.
4. Skriv webstedets adresse, og klik på **OK**.

Redigere websteder på positivlisten

Hvis du har føjet et websted til positivlisten, og webstedets adresse ændres, kan du altid opdatere den.

1. Åbn ruden Phishing-beskyttelse.

   Hvordan?

   1. Klik på **Internet & netværk** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i området Internet- & netværksoplysninger.

2. Klik på **Avanceret** i ruden Phishing-beskyttelse.
3. Vælg det websted, du vil opdatere, under **Positivliste**, og klik derefter på **Rediger**.
4. Rediger webstedets adresse, og klik på **OK**.

Fjerne et websted fra positivlisten

Hvis du har føjet et websted til positivlisten, fordi du ønskede adgang til det, men du nu ønsker at filtrere det, skal du fjerne det fra positivlisten.

1. Åbn ruden Phishing-beskyttelse.

   Hvordan?

   1. Klik på **Internet & netværk** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i området Internet- & netværksoplysninger.

2. Klik på **Avanceret** i ruden Phishing-beskyttelse.
3. Vælg det websted, du vil fjerne, under **Positivliste**, og klik derefter på **Fjern**.

Deaktivere phishing-beskyttelse

Hvis du allerede har phishing-software, som ikke er fra McAfee, og der er en konflikt, kan du deaktivere phishing-beskyttelse i Anti-Spam.

1. Klik på **Internet & netværk** i startruden for SecurityCenter.
2. Klik på **Konfigurer** i området Internet- & netværksoplysninger.
3. Klik på **Fra** under **Phishing-beskyttelse er aktiveret**.

Tip! Når du er færdig, skal du huske at klikke på **Til** under **Phishing-beskyttelse er deaktiveret**, så du er beskyttet mod bedrageriske websteder.

KAPITEL 30

McAfee Parental Controls

Forældrestyring giver dig avanceret beskyttelse af dig selv, din familie, dine personlige filer og din computer. Det hjælper dig med at beskytte imod identitetstyveri på internettet, blokere for overførsel af personlige oplysninger og filtrere onlineindhold, der kan være anstødeligt (herunder billeder). Det giver dig også mulighed for at overvåge, administrere og registrere uautoriseret internetsurfing samt byder på et sikkert opbevaringsområde til personlige adgangskoder.

Før du begynder at bruge Forældrestyring, kan du gøre dig bekendt med nogle af de mest populære funktioner. Oplysninger om, hvordan du konfigurerer og bruger disse funktioner, finder du i Hjælp til Forældrestyring.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Forældrestyring

Forældrestyring	Filtrér potentielt upassende billeder, aktivér alderssvarende søgning, konfigurér indholdsbedømmelsesgrupper (aldersgrupper, der bruges til at begrænse de websteder og det indhold, som en bruger kan se), og angiv tidsbegrænsning på surfing på internettet (den periode og varighed, en bruger har adgang til nettet) for brugere af SecurityCenter. Med Forældrestyring kan du også begrænse adgangen til bestemte websteder og tildele og blokere adgang på grundlag af nøgleord.
Beskyttelse af personlige oplysninger	Blokér overførslen af følsomme eller fortrolige oplysninger (f.eks. kreditkortnumre, kontonumre, adresser osv.) på nettet.
Adgangskodeboks	Opbevar dine personlige adgangskoder sikkert, så ingen andre brugere (ikke engang en administrator) kan få adgang til dem.

KAPITEL 31

Beskytte dine børn

Hvis dine børn bruger computeren, kan du bruge Forældrestyring til at regulere, hvad det enkelte barn kan se og gøre, når han/hun surfer på internettet. Du kan f.eks. aktivere eller deaktivere aldersbaseret søgning og billedfiltrering, vælge en indholdsbedømmelsesgruppe og angive tidsgrænser for surfing på internettet.

Aldersbaseret søgning sørger for, at sikkerhedsfiltrene i nogle populære søgemaskiner aktiveres, så potentielt upassende elementer automatisk udelades fra dit barns søgeresultater. Billedfiltrering blokerer potentielt upassende billeder i at blive vist, når et barn surfer på internettet. Indholdsbedømmelsesgruppen afgør, hvilket internetindhold der er tilgængeligt for et barn, afhængigt af barnets aldersgruppe. Tidsgrænser for internetsurfing definerer, hvilke dage og tidspunkter barnet har adgang til internettet. Du kan også filtrere (blokere eller tillade) bestemte websteder for alle børn.

Bemærk! Du konfigurerer Forældrestyring til beskyttelse af dine børn ved at logge på computeren som en Windows-administrator. Hvis du har opgraderet fra en tidligere version af dette McAfee-produkt og stadigvæk benytter McAfee-brugere, skal du også sørge for, at du er logget på som en McAfee-administrator.

I dette kapitel

Filtrere websteder ved hjælp af nøgleord

Nøgleordsfiltrering giver dig mulighed for at forhindre, at ikke-voksne brugere besøger websteder, som indeholder potentielt upassende ord. Når nøgleordsfiltrering er aktiveret, bruges standardlisten over nøgleord til at bedømme indholdet for brugere i henhold til deres indholdsbedømmelsesgruppe. Brugere skal tilhøre bestemte aldersgrupper for at få adgang til websteder, som indeholder bestemte nøgleord. Kun medlemmer af gruppen Voksen kan få adgang til websteder, der indeholder ordet *porno*, og kun medlemmer af gruppen Barn (og ældre) kan få adgang til websteder, der indeholder ordet *narko*.

Du kan også føje dine egnen nøgleord til standardlisten og knytte disse til bestemte indholdsbedømmelsesgrupper. Nøgleordsregler, som du selv tilføjer, tilsidesætter de regler, der eventuelt er oprettet for det tilsvarende nøgleord på standardlisten.

Blokere websteder baseret på nøgleord

Hvis du vil blokere websteder på grund af upassende indhold, men ikke kender de specifikke adresser på webstederne, kan du blokere dem baseret på deres nøgleord. Indtast et nøgleord, og angiv derefter, hvilke indholdsbedømmelsesgrupper der kan åbne websteder, som indeholder dette nøgleord.

1 Åbn ruden Forældrestyring.

Hvordan?

1. Klik på **Forældrestyring** i startruden for SecurityCenter.
2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
3. Kontroller, at Forældrestyring er aktiveret i ruden Konfiguration af forældrestyring, og klik derefter på **Avanceret**.

2 Klik på **Nøgleord** i ruden Forældrestyring, og kontroller, at funktionen er aktiveret.

3 Skriv et nøgleord i feltet **Søg efter** under **Nøgleordsliste**.

4 Flyt skyderen **Minimumsalder** for at angive den laveste aldersgruppe.
Brugere i og over denne aldersgruppe kan åbne websteder, der indeholder nøgleordet.

5 Klik på **OK**.

Deaktivere nøgleordsfiltrering

Som standard er nøgleordsfiltrering. Det betyder, at en standardliste over nøgleord bruges til at bedømme indholdet for brugere i henhold til deres indholdsbedømmelsesgruppe. Selvom det ikke anbefales af McAfee, er det til enhver tid muligt at deaktivere nøgleordsfiltrering.

1 Åbn ruden Forældrestyring.

   Hvordan?

   1. Klik på **Forældrestyring** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   3. Kontroller, at Forældrestyring er aktiveret i ruden Konfiguration af forældrestyring, og klik derefter på **Avanceret**.

2 Klik på **Nøgleord** i ruden Forældrestyring.

3 Klik på **Fra** i ruden Nøgleord.

4 Klik på **OK**.

Filtrere websteder

Du kan filtrere (blokere eller tillade) websteder for alle brugere med undtagelse af brugerne i gruppen Voksen. Du kan blokere et websted for at forhindre dine børn i at besøge det, når de søger på internettet. Hvis et barn forsøger at åbne et blokeret websted, vises en meddelelse, der fortæller, at webstedet ikke kan åbnes, fordi det er blokeret af McAfee.

Du kan tillade et websted, hvis McAfee har blokeret det som standard, men du vil give dine børn adgang til det. Flere oplysninger om websteder, som McAfee-blokerer som standard, finder du under Filtrere websteder ved hjælp af nøgleord (side 146). Du kan til enhver tid opdatere eller fjerne et filtreret websted.

Bemærk! Brugere (herunder administratorer), der tilhører gruppen Voksen, har adgang til alle websteder, selvom webstederne er blevet blokeret. Hvis du vil teste blokerede websteder, skal du logge på som en ikke-voksen bruger, men huske at fjerne din browser-historik i internetbrowseren, når du er færdig med at teste.

Fjerne et filtreret websted

Du kan fjerne et filtreret websted, hvis du ikke længere vil blokere eller tillade det.

1 Åbn ruden Forældrestyring.

   Hvordan?

   1. Klik på **Forældrestyring** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   3. Kontroller, at Forældrestyring er aktiveret i ruden Konfiguration af forældrestyring, og klik derefter på **Avanceret**.

2 Klik på **Filtrerede websteder** i ruden Forældrestyring.

3 Klik på en post på listen **Filtrerede websteder** i ruden Filtrerede websteder, og klik derefter på **Fjern**.

4 Klik på **OK**.

Opdatere et filtreret websted

Hvis adressen på et websted ændres, eller du har angivet den forkert, da du blokerede eller tillod den, kan du opdatere den.

1 Åbn ruden Forældrestyring.

   Hvordan?

   1. Klik på **Forældrestyring** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   3. Kontroller, at Forældrestyring er aktiveret i ruden Konfiguration af forældrestyring, og klik derefter på **Avanceret**.

2 Klik på **Filtrerede websteder** i ruden Forældrestyring.

3 Klik på en post på listen **Filtrerede websteder** i ruden Filtrerede websteder, rediger webadresse i feltet **http://**, og klik derefter på **Opdater**.

4 Klik på **OK**.

Tillade et websted

Du kan tillade et websted for at sikre, at det ikke blokeres for nogen brugere. Hvis du tillader et websted, som McAfee har blokeret som standard, tilsidesætter du standardindstillingen.

1 Åbn ruden Forældrestyring.

Hvordan?

1. Klik på **Forældrestyring** i startruden for SecurityCenter.
2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
3. Kontroller, at Forældrestyring er aktiveret i ruden Konfiguration af forældrestyring, og klik derefter på **Avanceret**.

2 Klik på Filtrerede websteder i ruden Forældrestyring.

3 Indtast adressen på et websted i feltet **http://** i ruden Filtrerede websteder, og klik derefter på **Tillad**.

4 Klik på **OK**.

Tip! Du kan tillade et tidligere blokeret websted ved at klikke på webadressen på listen **Filtrerede websteder** og derefter klikke på **Tillad**.

Blokere et websted

Du kan blokere et websted for at forhindre dine børn i at besøge det, når de søger på internettet. Hvis et barn forsøger at åbne et blokeret websted, vises en meddelelse, der fortæller, at webstedet ikke kan åbnes, fordi det er blokeret af McAfee.

1 Åbn ruden Forældrestyring.

Hvordan?

1. Klik på **Forældrestyring** i startruden for SecurityCenter.
2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
3. Kontroller, at Forældrestyring er aktiveret i ruden Konfiguration af forældrestyring, og klik derefter på **Avanceret**.

2 Klik på Filtrerede websteder i ruden Forældrestyring.

3 Indtast adressen på et websted i feltet **http://** i ruden Filtrerede websteder, og klik derefter på **Bloker**.

4 Klik på **OK**.

Tip! Du kan blokere et tidligere tilladt websted ved at klikke på webadressen på listen **Filtrerede websteder** og derefter klikke på **Bloker**.

Indstille internettidsgrænser

Hvis du er bekymret for uansvarlig eller overdreven brug af internettet, kan du angive, hvor når børnene må søge på internettet. Når du begrænser internetsøgningen til bestemte tidspunkter for børnene, vil SecurityCenter håndhæve disse begrænsninger, også selvom du ikke er hjemme.

Som standard har et barn tilladelse til at søge på internettet døgnet rundt, alle ugens dage. Du kan begrænse internetsøgningen til bestemte tidspunkter eller data, eller du kan forbyde internetsøgning fuldstændigt. Hvis et barn forsøger at anvende internettet i en forbudt periode, giver McAfee barnet besked om, at det ikke er muligt. Hvis du fuldstændigt forbyder internetsøgning, kan barnet logge på og bruge computeren, herunder internetprogrammer, som f.eks. e-mail, chatprogrammer, ftp, spil osv., men barnet kan ikke søge på internettet.

Indstille internettidsgrænser

Du kan bruge gitteret til internettidsgrænser til at begrænse et barns søgning på internettet til bestemte dage og tidspunkter.

1 Åbn ruden Brugerindstillinger.

Hvordan?

1. Klik på **Forældrestyring** i startruden for SecurityCenter.
2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
3. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
4. Klik på **Bruger indstillinger** i ruden Forældrestyring.

2 Klik på et brugernavn i ruden Brugerindstillinger, og klik derefter på **Rediger**.

3 Under **Tidsbegrænsning på surfing på internettet** i vinduet Rediger brugerkonto skal du trække musen for at angive, hvilke dage og tidspunkter denne bruger ikke kan få adgang til internettet.

4 Klik på **OK**.

Indstille indholdsbedømmelsesgruppe

En bruger kan tilhøre en af følgende indholdsbedømmelsesgrupper:

- Lille barn
- Barn
- Yngre teenager
- Ældre teenager
- Voksen

Forældrestyring bedømmer (blokerer eller tillader) webindhold ud fra den indholdsbedømmelsesgruppe, en bruger tilhører. Det giver dig mulighed for at blokere eller tillade visse websteder for visse brugere i dit hjem. Du kan f.eks. blokere internetindhold for brugere, der tilhører gruppen Lille barn, men tillade det for brugere, der tilhører gruppen Yngre teenager. Hvis du vil anvende en mere striks bedømmelse af indholdet for en bruger, kan du tillade, at brugeren kun åbner websteder, der er tilladte på listen **Filtrerede websteder**. Du kan finde flere oplysninger under Filtrere websteder (side 147).

Angive en brugers indholdsbedømmelsesgruppe

Som standard føjes en ny bruger til gruppen Voksen, som giver brugeren adgang til alt indhold på internettet. Du kan derefter justere brugerens indholdsbedømmelsesgruppe efter personens alder og modenhed.

1 Åbn ruden Brugerindstillinger.

   Hvordan?

   1. Klik på **Forældrestyring** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   3. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
   4. Klik på **Bruger indstillinger** i ruden Forældrestyring.

2 Klik på et brugernavn i ruden Brugerindstillinger, og klik derefter på **Rediger**.

3 Klik på den aldersgruppe, du vil knytte brugeren til, under **Indholdsbedømmelse** i vinduet Rediger brugerkonto.

   Hvis du vil forhindre brugeren i at få vist websteder, der er blokerede på listen **Filtrerede websteder**, skal du markere afkrydsningsfeltet **Denne bruger kan kun få adgang til websteder på listen Tilladte websteder**.

4 Klik på **OK**.

Filtrere potentielt upassende internetbilleder

Afhængigt af en brugers alder eller modenhed kan du filtrere (blokere eller tillade) potentielt upassende billeder, når brugeren søger på internettet. Du kan f.eks. blokere visningen af potentielt upassende billeder, når dine mindre børn er på internettet, men tillade visningen af dem for ældre teenagere og voksne i dit hjem. Som standard er billedfiltrering deaktiveret for alle medlemmer af gruppen Voksen. Det betyder, at potentielt upassende billeder evt. vises, når disse brugere søger på internettet. Flere oplysninger om angivelse af aldersgruppen for en bruger finder du under Indstille indholdsbedømmelsesgruppe (side 151).

Filtrere potentielt upassende internetbilleder

Som standard føjes nye brugere til gruppen Voksen, og billedfiltrering er slået fra. Hvis du vil blokere visningen af potentielt upassende billeder, når en bestemt bruger søger på internettet, kan du aktivere billedfiltrering. Hvert potentielt upassende internetbillede erstattes automatisk med et statisk McAfee-billede.

1 Åbn ruden Brugerindstillinger.

   Hvordan?

   1. Klik på **Forældrestyring** i startruden for SecurityCenter.
   2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   3. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
   4. Klik på **Bruger indstillinger** i ruden Forældrestyring.

2 Klik på et brugernavn i ruden Brugerindstillinger, og klik derefter på **Rediger**.

3 Klik på **Til** under **Billedfiltrering** i vinduet Rediger brugerkonto.

4 Klik på **OK**.

Aktivere alderssvarende søgning

Nogle populære søgemaskiner (f.eks. Yahoo! og Google) tilbyder "sikker søgning" – en søgningsindstilling, der forhindrer potentielt upassende søgeresultater i at blive vist på resultatlisten. Disse søgemaskiner lader dig som regel vælge, hvor restriktiv den sikre søgefiltrering skal være, men giver også dig eller en hvilken som helst anden bruger mulighed for at deaktivere filtreringen når som helst.

I Forældrestyring er alderssvarende søgning en praktisk måde at sørge for, at sikker søgning altid er aktiveret for en bruger, når en af følgende søgemaskiner anvendes:

- Google™
- MSN®
- Windows® Live Search
- Yahoo!®

Hvis du aktiverer alderssvarende søgning, sørger vi for, at søgemaskinernes sikre søgefiltrering er aktiveret for den pågældende bruger og angivet til den mest restriktive indstilling, og hvis en bruger forsøger at deaktivere den (i søgemaskinens egenskaber eller avancerede indstillinger), aktiveres den automatisk igen.

Alderssvarende søgning er som standard aktiveret for alle brugere, undtagen administratorer og brugerne i aldersgruppen Voksne. Flere oplysninger om angivelse af aldersgruppen for en bruger finder du under Indstille indholdsbedømmelsesgruppe (side 151).

Aktivere alderssvarende søgning

Som standard føjes nye brugere til gruppen Voksen, og alderssvarende søgning er deaktiveret. Hvis du vil være sikker på, at den sikre søgefiltrering, som nogle af de populære søgemaskiner tilbyder, er aktiveret for en voksen bruger, kan du aktivere alderssvarende søgning.

1 Åbn ruden Brugerindstillinger.

Hvordan?

1. Klik på **Forældrestyring** i startruden for SecurityCenter.
2. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
3. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
4. Klik på **Bruger indstillinger** i ruden Forældrestyring.

2 Klik på et brugernavn i ruden Brugerindstillinger, og klik derefter på **Rediger**.

3 Klik på **Til** under **Alderssvarende søgning**, i vinduet Rediger brugerkonto.

4 Klik på **OK**.

KAPITEL 32

Konfigurere brugere

Når du konfigurerer Forældrestyring til beskyttelse af dine børn, tildeler du bestemte tilladelser til dem i SecurityCenter. Disse tilladelser afgør, hvad hvert barn kan se og foretage sig på internettet.

Som standard svarer SecurityCenter-brugere til de Windows-brugere, der er konfigureret på computeren. Hvis du har opgraderet fra en tidligere version af SecurityCenter, der anvendte McAfee-brugere, bevares dine McAfee-brugere og deres tilladelser.

Bemærk! Du skal logge på computeren som en Windows-administrator for at konfigurere brugere. Hvis du har opgraderet fra en tidligere version af dette McAfee-produkt og stadigvæk benytter McAfee-brugere, skal du også sørge for, at du er logget på som en McAfee-administrator.

I dette kapitel

Arbejde med McAfee-brugere

Hvis du har opgraderet fra en tidligere version af SecurityCenter, der anvendte McAfee-brugere, bevares dine McAfee-brugere og deres tilladelser automatisk. Du kan fortsætte med at konfigurere og administrere McAfee-brugere. McAfee anbefaler dog, at du skifter til Windows-brugere. Når du har skiftet til Windows-brugere, kan du ikke gå tilbage til McAfee-brugere igen.

Hvis du fortsætter med at bruge McAfee-brugere, kan du tilføje, redigere eller fjerne brugere og ændre eller hente McAfee-administratorens adgangskode.

Hente McAfee-administratoradgangskoden

Hvis du har glemt administratoradgangskoden, kan du hente den.

1. Højreklik på SecurityCenter-ikonet, og klik derefter på **Skift bruger**.
2. Vælg **Administrator** på listen **Brugernavn**, og klik på **Glemt adgangskode?**.
3. Skriv svaret på dit hemmelige spørgsmål i feltet **Svar**.
4. Klik på **Send**.

Ændre McAfee-administratoradgangskoden

Hvis du har problemer med at huske McAfee-administratoradgangskoden eller har mistanke om, at den er blevet kompromitteret, kan du ændre den.

1. Log på SecurityCenter som administrator.
2. Åbn ruden Brugerindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Forældrestyring** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   4. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
3. Vælg **Administrator** under **McAfee-brugerkonti** i ruden Brugerindstillinger, og klik derefter på **Rediger**.
4. Skriv den nye adgangskode i feltet **Ny adgangskode** i dialogboksen Rediger brugerkonto, og skriv den igen i feltet **Bekræft ny adgangskode**.
5. Klik på **OK**.

Fjerne en McAfee-bruger

Du kan til enhver tid fjerne en McAfee-bruger.

Sådan fjerner du en McAfee-bruger:

1. Log på SecurityCenter som administrator.
2. Åbn ruden Brugerindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Forældrestyring** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   4. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
3. Klik på et brugernavn i ruden Brugerindstillinger under **McAfee-brugerkonti**, og klik derefter på **Fjern**.

Redigere kontooplysninger for en McAfee-bruger

Du kan ændre en McAfee-brugers adgangskode, kontotype eller mulighed for automatisk login.

1. Log på SecurityCenter som administrator.
2. Åbn ruden Brugerindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Forældrestyring** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   4. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
3. Klik på et brugernavn i ruden Brugerindstillinger, og klik derefter på **Rediger**.
4. Følg anvisningerne på skærmen for at redigere brugerens adgangskode, kontotype eller Forældrestyring-beskyttelse.
5. Klik på **OK**.

Tilføje en McAfee-bruger

Når du har oprettet en McAfee-bruger, kan du konfigurere Forældrestyring-beskyttelse for brugeren. Flere oplysninger findes i Forældrestyring Hjælp.

1. Log på SecurityCenter som administrator.
2. Åbn ruden Brugerindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Forældrestyring** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   4. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
3. Klik på **Tilføj** i ruden Brugerindstillinger.
4. Følg anvisningerne på skærmen for at konfigurere brugernavn, adgangskode og indstillinger for Forældrestyring.
5. Klik på **Opret**.

Skifte til Windows-brugere

McAfee anbefaler, at du skifter til Windows-brugere. Hvis du gør det, er det dog ikke muligt at skifte tilbage til McAfee-brugere.

1. Åbn ruden Brugerindstillinger.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Forældrestyring** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet med oplysninger om Forældrestyring.
   4. Klik på **Avanceret** i ruden Konfiguration af forældrestyring.
2. Klik på **Skift** i ruden Brugerindstillinger.
3. Bekræft handlingen.

Arbejde med Windows-brugere

Som standard svarer SecurityCenter-brugere til de Windows-brugere, der er konfigureret på computeren. Du tilføjer brugere, redigerer brugernes kontooplysninger og fjerner brugere under Computeradministration i Windows. Du kan derefter konfigurere Forældrestyring-beskyttelse for disse brugere i SecurityCenter.

Hvis du har opgraderet fra en tidligere version af SecurityCenter, der anvendte McAfee-brugere, kan du finde flere oplysninger under Arbejde med McAfee-brugere (side 156).

KAPITEL 33

Beskytte oplysninger på internettet

Du kan også forhindre, at dine personlige oplysninger (f.eks. navn, adresse, kreditkortnumre og bankkontonumre) bliver overført via internettet ved at tilføje dem til området med beskyttede oplysninger.

Bemærk! Forældrestyring blokerer ikke sikre websteders overførsel af personlige oplysninger, dvs. websteder, der bruger protokollen https://, som f.eks. bankwebsteder.

I dette kapitel

Beskytte personlige oplysninger

Du kan forhindre, at dine personlige oplysninger (f.eks. navn, adresse, kreditkortnumre og bankkontonumre) bliver overført via internettet, ved at blokere dem. Når McAfee registrerer personlige oplysninger i meddelelser, der er ved at blive sendt via internettet, sker der følgende:

- Hvis du er administrator, skal du bekræfte, om oplysningerne skal sendes.
- Hvis du ikke er administrator, erstattes de blokerede oplysninger med en stjerne (*). Hvis et ondsindet websted forsøger at sende dit kreditkortnummer til en anden computer, erstattes selve nummeret med stjerner.

Beskytte personlige oplysninger

Du kan blokere følgende typer personlige oplysninger: navn, adresse, postnummer, cpr-nummer, telefonnummer, kreditkortnumre, bankkonti, mæglerkonti og telefonkort. Hvis du vil blokere personlige oplysninger af en anden type, kan du angive typen som **andet**.

1 Åbn ruden Beskyttede oplysninger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Internet & netværk** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i afsnittet Internet- & netværksoplysninger.
4. Kontroller, at Beskyttelse af personlige oplysninger er aktiveret i ruden Konfiguration af Internet & netværk, og klik derefter på **Avanceret**.

2 Klik på **Tilføj** i ruden Beskyttede oplysninger.

3 Vælg den type oplysninger, du ønsker at blokere, på listen.

4 Angiv de personlige oplysninger, og klik derefter på **OK**.

KAPITEL 34

Beskytte adgangskoder

Adgangskodeboksen er et sikkert opbevaringsområde for dine personlige adgangskoder. Den giver dig mulighed for at opbevare dine adgangskoder med tillid til, at ingen andre brugere kan få adgang til dem (heller ikke en administrator).

I dette kapitel

Konfigurere adgangskodeboksen

Før du begynder at bruge adgangskodeboksen, skal du konfigurere en adgangskode til adgangskodeboksen. Kun brugere, der kender denne adgangskode, kan få adgang til din adgangskodeboks. Hvis du glemmer din adgangskode til adgangskodeboksen, kan du nulstille den, men alle de adgangskoder, du har gemt i adgangskodeboksen, vil da blive slettet.

Når du har konfigureret en adgangskode til adgangskodeboksen, kan du tilføje, redigere eller fjerne adgangskoder fra din boks. Du kan til enhver tid ændre din adgangskode til adgangskodeboksen.

Nulstille adgangskoden til adgangskodeboksen

Hvis du glemmer din adgangskode til adgangskodeboksen, kan du nulstille den, men alle de adgangskoder, du har gemt i adgangskodeboksen vil da blive slettet.

1 Åbn ruden Adgangskodeboks.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Internet & netværk** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i afsnittet Internet- & netværksoplysninger.
4. Klik på **Avanceret** under **Adgangskodeboks** i ruden Konfiguration af Internet & netværk.

2 Klik på **Har du glemt din adgangskode?**

3 Skriv den nye adgangskode i feltet **Adgangskode** i dialogboksen Nulstil adgangskodeboks, og skriv den igen i feltet **Bekræft ny adgangskode**.

4 Klik på **Nulstil**.

5 Klik på **Ja** i dialogboksen Bekræftelse af nulstilling af adgangskode.

Ændre adgangskode til adgangskodeboksen

Du kan til enhver tid ændre din adgangskode til adgangskodeboksen.

1 Åbn ruden Adgangskodeboks.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Internet & netværk** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet Internet- & netværksoplysninger.
   4. Klik på **Avanceret** under **Adgangskodeboks** i ruden Konfiguration af Internet & netværk.

2 Skriv din nuværende adgangskode i feltet **Adgangskode** i ruden Adgangskodeboks, og klik derefter på **Åbn**.

3 Klik på **Rediger adgangskode** i ruden Administrer adgangskodeboks.

4 Skriv en ny adgangskode i feltet **Vælg en adgangskode**, og indtast den derefter igen i feltet **Bekræft adgangskode**.

5 Klik på **OK**.

6 Klik på **OK** i dialogboksen Adgangskode til adgangskodeboks er ændret.

Fjerne en adgangskode

Du kan til enhver tid fjerne en adgangskode fra adgangskodeboksen. Det er ikke muligt at gendanne en adgangskode, der er fjernet fra adgangskodeboksen.

1 Åbn ruden Adgangskodeboks.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Internet & netværk** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet Internet- & netværksoplysninger.
   4. Klik på **Avanceret** under **Adgangskodeboks** i ruden Konfiguration af Internet & netværk.

2 Indtast din adgangskode til adgangskodeboksen i feltet **Adgangskode**.

3 Klik på **Åbn**.

4 Klik på en adgangskodepost i ruden Administrer adgangskodeboks, og klik derefter på **Fjern**.

5 Klik på **Ja** i bekræftelsesdialogboksen for fjernelsen.

Redigere en adgangskode

For at sikre, at oplysningerne i adgangskodeboksen altid er korrekte og troværdige, skal du opdatere dem, når adgangskoderne ændres.

1 Åbn ruden Adgangskodeboks.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Internet & netværk** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet Internet- & netværksoplysninger.
   4. Klik på **Avanceret** under **Adgangskodeboks** i ruden Konfiguration af Internet & netværk.

2 Indtast din adgangskode til adgangskodeboksen i feltet **Adgangskode**.

3 Klik på **Åbn**.

4 Klik på en adgangskodepost i ruden Administrer adgangskodeboks, og klik derefter på **Rediger**.

5 Rediger beskrivelsen af adgangskoden i feltet **Beskrivelse** (f.eks. hvad den bruges til), eller rediger adgangskoden i feltet **Adgangskode**.

6 Klik på **OK**.

Tilføje en adgangskode

Hvis du har svært ved at huske dine adgangskoder, kan du føje dem til adgangskodeboksen. Adgangskodeboksen er en sikker placering, som kun kan åbnes af brugere, der kender din adgangskode til adgangskodeboksen.

1 Åbn ruden Adgangskodeboks.

   Hvordan?

   1. Klik på **Start** under **Almindelige opgaver**.
   2. Klik på **Internet & netværk** i startruden for SecurityCenter.
   3. Klik på **Konfigurer** i afsnittet Internet- & netværksoplysninger.
   4. Klik på **Avanceret** under **Adgangskodeboks** i ruden Konfiguration af Internet & netværk.

2 Indtast din adgangskode til adgangskodeboksen i feltet **Adgangskode**.

3 Klik på **Åbn**.

4 Klik på **Tilføj** i ruden Administrer adgangskodeboks.

5 Angiv en beskrivelse af adgangskoden i feltet **Beskrivelse** (f.eks. hvad den bruges til), og indtast derefter adgangskoden i feltet **Adgangskode**.

6 Klik på **OK**.

KAPITEL 35

McAfee Sikkerhedskopiering og gendannelse

Brug McAfee® Sikkerhedskopiering og gendannelse til at undgå, at du mister data ved et uheld, ved at arkivere dine filer til cd, dvd, USB-drev, en ekstern harddisk eller et netværksdrev. Lokal arkivering giver dig mulighed for at arkivere (sikkerhedskopiere) dine personlige data på cd, dvd, USB-drev, en ekstern harddisk eller på et netværksdrev. Det giver dig en lokal kopi af dine poster, dokumenter og andet personligt materiale i tilfælde af datatab.

Før du begynder at bruge Sikkerhedskopiering og gendannelse, kan du se lidt på nogle af de mest anvendte funktioner. Hjælpen i Sikkerhedskopiering og gendannelse indeholder oplysninger om konfiguration og brug af disse funktioner. Når du har gennemset programmets funktioner, skal du kontrollere, at du har de nødvendige arkiveringsmedier til at udføre lokale arkiver.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Sikkerhedskopiering og gendannelse

Lokal planlagt arkivering

Beskyt dine data ved at arkivere filer og mapper på cd-, dvd-, USB-drev, ekstern harddisk eller netværksdrev. Når du har startet det første arkiv, oprettes der automatisk trinvise arkiver for dig.

Gendannelse med ét klik

Hvis filer eller mapper slettes ved en fejl eller bliver beskadiget på computeren, kan du hente de senest arkiverede versioner fra det anvendte arkiveringsmedie.

Komprimering og kryptering

De arkiverede filer komprimeres som standard, hvilket sparer plads på arkiveringsmediet. Som en yderligere sikkerhedsforanstaltning krypteres arkiverne som standard.

KAPITEL 36

Arkivere filer

Du kan bruge McAfee Sikkerhedskopiering og gendannelse til at arkivere en kopi af filerne på din computer på cd, dvd, USB-drev, en ekstern harddisk eller på et netværksdrev. Ved at arkivere dine filer på denne måde er det nemt at hente oplysninger, hvis data er blevet beskadigede eller er gået tabt.

Før du begynder at arkivere filer, skal du vælge en standardplacering (cd, dvd, USB-drev, ekstern harddisk eller et netværksdrev). Nogle indstillinger i McAfee er forudindstillede, f.eks. de mapper og filtyper, der skal arkiveres, men du kan ændre disse indstillinger.

Når du har angivet indstillingerne for lokal arkivering, kan du redigere standardindstillingerne for, hvor tit Sikkerhedskopiering og gendannelse kører fulde eller hurtige arkiveringer. Du kan køre manuel arkivering når som helst.

I dette kapitel

Aktivere og deaktivere lokal arkivering

Første gang du starter Sikkerhedskopiering og gendannelse, afgør du, om du vil aktivere eller deaktivere lokal arkivering, afhængigt af hvordan du ønsker at bruge Sikkerhedskopiering og gendannelse. Når du logger på og begynder at bruge Sikkerhedskopiering og gendannelse, kan du når som helst aktivere eller deaktivere lokal arkivering.

Hvis du ikke ønsker at arkivere en kopi af filerne på din computer på cd, dvd, USB-drev, en ekstern harddisk eller på et netværksdrev, kan du deaktivere lokal arkivering.

Aktivere lokal arkivering

Du kan aktivere lokal arkivering, hvis du ønsker at arkivere en kopi af filerne på din computer på cd, dvd, USB-drev, en ekstern harddisk eller på et netværksdrev.

1. Klik på **Konfigurer** i menuen **Avanceret** i SecurityCenter.
2. Klik derefter på **Computer & filer** i konfigurationsruden.
3. I konfigurationsruden Computer & filer skal du klikke på **Til** under **Lokal arkivering er deaktiveret**.

Deaktivere lokal arkivering

Du kan deaktivere lokal arkivering, hvis du ikke ønsker at arkivere en kopi af filerne på din computer på cd, dvd, USB-drev, en ekstern harddisk eller på et netværksdrev.

1. Klik på **Konfigurer** i menuen **Avanceret** i SecurityCenter.
2. Klik derefter på **Computer & filer** i konfigurationsruden.
3. I konfigurationsruden Computer & filer skal du klikke på **Fra** under **Lokal arkivering er aktiveret**.

Angive arkiveringsindstillinger

Før du begynder at arkivere dine filer, skal du angive nogle indstillinger for lokal arkivering. Du skal f.eks. angive overvågningsplaceringerne og overvågningsfiltyperne. Overvågningsplaceringer er mapper på din computer, som Sikkerhedskopiering og gendannelse kontrollerer for nye filer eller filændringer. Overvågningsfiltyper er de typer filer (f.eks. .doc, .xls osv.), som Sikkerhedskopiering og gendannelse arkiverer i overvågningsplaceringerne. Følgende filtyper arkiveres som standard, men du kan også arkivere andre filtyper:

- Microsoft® Word-dokumenter (.doc, .docx)
- Microsoft Excel®-regneark (.xls, .xlsx)
- Microsoft PowerPoint®-præsentationer (.ppt, .pptx)
- Microsoft Project®-filer (.mpp)
- Adobe® PDF-filer (.pdf)
- Almindelige tekstfiler (.txt)
- HTML-filer (.html)
- Joint Photographic Experts Group-filer (.jpg, .jpeg)
- Tagged-billedformatfiler (.tif)
- MPEG Audio Stream III-filer (.mp3)
- Videofiler (.vdo)

Bemærk! Du kan ikke arkivere følgende filtyper: .ost og .pst.

Du kan angive to typer overvågningsplaceringer: overordnede mapper og undermapper og kun overordnede mapper. Hvis du angiver en placering med overordnede mapper og undermapper, arkiverer Sikkerhedskopiering og gendannelse overvågningsfiltyperne i den pågældende mappe og i de tilknyttede undermapper. Hvis du angiver en overordnet mappeplacering, arkiverer Sikkerhedskopiering og gendannelse kun overvågningsfiltyperne i denne mappe (ikke undermapperne). Du kan også identificere placeringer, som du ønsker at udelade fra den lokale arkivering. Placeringerne Windows Skrivebord og Dokumenter angives som standard som overvågningsplaceringer bestående af overordnede mapper og undermapper.

Når du har angivet overvågningsfiltyperne og -placeringerne, skal du angive arkiveringsplaceringen (dvs. den cd, den dvd, den USB-placering, den eksterne harddisk eller det netværksdrev, hvor arkiverede data vil blive gemt). Du kan til enhver tid ændre arkiveringsplaceringen.

Af sikkerhedsmæssige årsager eller af hensyn til størrelsen er kryptering eller komprimering som standard aktiveret for dine arkiverede filer. Indholdet af de krypterede filer omformes fra tekst til kode, der skjuler oplysningerne for at gøre dem ulæselige for folk, der ikke ved, hvordan de skal dekrypteres. Komprimerede filer komprimeres i en form, der minimerer den plads, som er påkrævet for at gemme eller sende dem. Selvom McAfee ikke anbefaler det, kan du til enhver tid deaktivere kryptering eller komprimering.

Medtage en placering i arkivet

Du kan oprette to typer overvågede arkiveringsplaceringer: overordnede mapper og undermapper og kun overordnede mapper. Hvis du angiver en placering bestående af overordnede mapper og undermapper, overvåger Sikkerhedskopiering og gendannelse indholdet i den pågældende mappe og de tilknyttede undermapper for ændringer. Hvis du angiver en overordnet mappeplacering, overvåger Sikkerhedskopiering og gendannelse kun indholdet i mappen (ikke de tilknyttede undermapper).

1 Åbn dialogboksen Indstillinger for lokal arkivering.

   Hvordan?

   1. Klik på fanen **Lokalt arkiv**.
   2. Klik på **Indstillinger** i den venstre rude.

2 Klik på **Overvågningsplaceringer**.

3 Nu kan du gøre følgende:

   - Hvis du vil arkivere indholdet i en mappe inklusive indholdet i de tilknyttede undermapper, skal du klikke på **Tilføj mappe** under **Arkiver overordnede mapper og undermapper**.
   - Hvis du vil arkivere indholdet i en mappe, men ikke indholdet i de tilknyttede undermapper, skal du klikke på **Tilføj mappe** under **Arkiver overordnede mapper**.
   - Hvis du vil arkivere en hel fil, skal du klikke på **Tilføj fil** under **Arkiver overordnede mapper**.

4 Gå til den mappe, der skal overvåges, i dialogboksen Søg efter mappe (eller Åbn), gå til den mappe (eller fil), du vil overvåge, og klik derefter på **OK**.

5 Klik på **OK**.

Tip! Hvis McAfee Data Backup skal overvåge en mappe, der endnu ikke er oprettet, skal du klikke på **Opret ny mappe** i dialogboksen Søg efter mappe, for at tilføje en mappe og oprette den som overvågningsplacering på samme tid.

Angive arkivfiltyper

Du kan angive, hvilke typer filer i placeringerne overordnede mapper og undermapper eller overordnede mapper der arkiveres. Du kan vælge fra en eksisterende liste over filtyper eller tilføje en ny type på listen.

1 Åbn dialogboksen Indstillinger for lokal arkivering.

   Hvordan?

   1. Klik på fanen **Lokalt arkiv**.
   2. Klik på **Indstillinger** i den venstre rude.

2 Klik på **Filtyper**.

3 Udvid filtypelisten, og marker afkrydsningsfelterne ud for de filtyper, du vil arkivere.

4 Klik på **OK**.

Tip! Hvis du vil tilføje en ny filtype til listen **Valgte filtyper**, skal du indtaste filtypenavnet i boksen **Føj brugerdefineret filtype til "Andet"**, klikke på **Tilføj** og derefter klikke på **OK**. Den nye filtype bliver automatisk en overvågningsfiltype.

Udelade en placering fra arkivet

Du kan udelade en placering fra arkivet, hvis du vil forhindre, at denne placering (mappe) og dens indhold arkiveres.

1 Åbn dialogboksen Indstillinger for lokal arkivering.

   Hvordan?

   1. Klik på fanen **Lokalt arkiv**.
   2. Klik på **Indstillinger** i den venstre rude.

2 Klik på **Overvågningsplaceringer**.

3 Klik på **Tilføj mappe** under **Mapper, der er udeladte fra sikkerhedskopiering**.

4 Gå til den mappe, der skal udelades, i dialogboksen Søg efter mappe, marker den, og klik derefter på **OK**.

5 Klik på **OK**.

Tip! Hvis Sikkerhedskopiering og gendannelse skal udelade en mappe, der endnu ikke er oprettet, skal du klikke på **Opret ny mappe** i dialogboksen Søg efter mappe for at tilføje en mappe og udelade den på samme tid.

Skifte arkiveringsplacering

Når du ændrer arkiveringsplaceringen, vises de filer, der tidligere var arkiveret på en anden placering, som *Aldrig arkiveret*.

1. Åbn dialogboksen Indstillinger for lokal arkivering.

   Hvordan?

   1. Klik på fanen **Lokalt arkiv**.
   2. Klik på **Indstillinger** i den venstre rude.

2. Klik på **Skift arkiveringsplacering**.
3. Benyt en af følgende fremgangsmåder i dialogboksen Arkiveringsplacering:
   - Klik på **Vælg cd-/dvd-brænder**, klik på computerens cd- eller dvd-drev på listen **Brænder**, og klik derefter på **OK**.
   - Klik på **Vælg diskplacering**, gå til og marker et USB-drev, et lokalt drev eller en ekstern harddisk, og klik derefter på **OK**.
   - Klik på **Vælg netværksplacering**, gå til netværksmappen, marker den, og klik derefter på **OK**.
4. Bekræft den nye arkiveringsplacering under **Valgt arkiveringsplacering**, og klik derefter på **OK**.
5. Klik på **OK** i bekræftelsesdialogboksen.
6. Klik på **OK**.

Bemærk! Når du ændrer arkiveringsplaceringen, vises de filer, der tidligere blev arkiveret, som **Ikke arkiveret** i kolonnen **Status**.

Deaktivere kryptering og komprimering af arkiver

Kryptering af arkiverede filer beskytter dine data ved at sløre indholdet af filerne, så de ikke kan læses. Komprimering af arkiverede filer minimerer filstørrelsen. Som standard er både kryptering og komprimering aktiveret, men du kan deaktivere disse indstillinger efter behov.

1 Åbn dialogboksen Indstillinger for lokal arkivering.

   Hvordan?

   1. Klik på fanen **Lokalt arkiv**.
   2. Klik på **Indstillinger** i den venstre rude.

2 Klik på **Avancerede indstillinger**.

3 Fjern markeringen i afkrydsningsfeltet **Aktiver kryptering for at øge sikkerheden**.

4 Fjern markeringen i afkrydsningsfeltet **Aktiver komprimering for at spare plads**.

5 Klik på **OK**.

Bemærk! McAfee anbefaler, at du ikke deaktiverer kryptering og komprimering under arkivering af filer.

Køre fulde og hurtige arkiveringer

Du kan køre to typer arkiveringer: fulde eller hurtige. Når du kører en fuld arkivering, arkiverer du et komplet sæt data baseret på de overvågningsfiltyper og -placeringer, som du har angivet. Når du kører en hurtig arkivering, arkiverer du kun de overvågningsfiler, der har ændret sig siden den sidste fulde eller hurtige arkivering.

Sikkerhedskopiering og gendannelse er som standard indstillet til at køre en fuldstændig arkivering af overvågningsfiltyperne på dine overvågningsplaceringer hver mandag kl. 9:00 og en hurtig arkivering for hver 48. timer efter den sidste fulde eller hurtige arkivering. Denne tidsplan sikrer, at det aktuelle filarkiv hele tiden vedligeholdes. Hvis du imidlertid ikke ønsker at arkivere for hver 48. timer, kan du justere tidsplanen, så den passer til dine behov.

Hvis du ønsker at arkivere indholdet af dine overvågningsplaceringer efter behov, kan du til enhver tid gøre det. Hvis du f.eks. ændrer en fil og ønsker at arkivere den, men Sikkerhedskopiering og gendannelse ikke er indstillet til at køre en fuld eller hurtig arkivering i endnu et par timer, kan du arkivere filerne manuelt. Når du arkiverer filer manuelt, nulstilles det interval for automatiske arkiveringer, som du har angivet.

Du kan også afbryde en automatisk eller manuel arkivering, hvis den forekommer på et upassende tidspunkt. Du kan f.eks. stoppe den, hvis du er ved at udføre en opgave, der kræver mange ressourcer, og en automatisk arkivering starter. Når du stopper en automatisk arkivering, nulstilles det interval for automatiske arkiveringer, som du har angivet.

Planlægge automatiske arkiveringer

Du kan angive hyppigheden af fulde og hurtige arkiveringer for at sikre, at dine data altid er beskyttede.

1. Åbn dialogboksen Indstillinger for lokal arkivering.

   Hvordan?

   1. Klik på fanen **Lokalt arkiv**.
   2. Klik på **Indstillinger** i den venstre rude.

2. Klik på **Generelt**.
3. Hvis du vil køre en fuld arkivering hver dag, uge eller måned, skal du klikke på et af følgende under **Fuld arkivering hver**:
   - **dag**
   - **uge**
   - **måned**
4. Marker afkrydsningsfeltet ud for den dag, hvor du ønsker at køre den fulde arkivering.
5. Klik på en værdi på listen **Kl.** for at angive det tidspunkt, hvor du vil køre den fulde arkivering.
6. Hvis du vil køre en hurtig arkivering hver dag eller time, skal du klikke på et af følgende under **Hurtigarkivering**:
   - **timer**
   - **dage**
7. Indtast det tal, der repræsenterer hyppigheden, i boksen **Hurtigarkivering hver**.
8. Klik på **OK**.

Bemærk! Du kan deaktivere en planlagt arkivering ved at vælge **Manuel** under **Fuld arkivering hver**.

Afbryde en automatisk arkivering

Sikkerhedskopiering og gendannelse arkiverer automatisk filer og mapper i de overvågede placeringer i henhold til den definerede tidsplan. Du kan dog altid afbryde en automatisk arkivering.

1 Klik på **Stop arkivering** i den venstre rude.

2 Klik på **Ja** i dialogboksen til bekræftelse.

Bemærk! Linket **Stop arkivering** vises kun, når en arkivering er i gang.

Køre arkiveringer manuelt

Selvom automatiske arkiveringer kører efter en foruddefineret tidsplan, kan du til enhver tid køre en hurtig eller fuld arkivering manuelt. En hurtig arkivering arkiverer kun de filer, der har ændret sig siden den sidste fulde eller hurtige arkivering. En fuld arkivering arkiverer de overvågede filtyper på alle overvågede steder.

1 Klik på fanen **Lokalt arkiv**.

2 Nu kan du gøre følgende:

- Klik på **Hurtigarkivering** i venstre rude for at køre en hurtig arkivering.
- Klik på **Fuld arkivering** i venstre rude for at køre en fuld arkivering.

3 Kontroller lagerpladsen og indstillingerne i dialogboksen Start arkivering, og klik derefter på **Fortsæt**.

KAPITEL 37

Arbejde med arkiverede filer

Når du har arkiveret nogle filer, kan du bruge Sikkerhedskopiering og gendannelse til at arbejde med dem. Du præsenteres for dine arkiverede filer i en almindelig stifinder, hvilket gør dem lette at finde. Efterhånden som arkivet vokser, kan det være en god idé at sortere filerne eller søge efter dem. Du kan også åbne filer direkte i stifinderen for at undersøge indholdet uden at hente filerne.

Du henter filer fra et arkiv, hvis din lokale kopi af filen er forældet, mangler eller beskadiget. Sikkerhedskopiering og gendannelse giver dig også nyttige oplysninger, som du kan bruge til at håndtere dine lokale arkiver og lagermedier.

I dette kapitel

Bruge stifinderen for lokalt arkiv

Med stifinderen for det lokale arkiv kan du få vist og manipulere de filer, som du har arkiveret lokalt. Du kan få vist hver enkelt fils navn, type, placering, størrelse, tilstand (arkiveret, ikke arkiveret eller arkivering i gang) og den dato, hvor filen sidst blev arkiveret. Du kan også sortere filerne ud fra et af disse kriterier.

Hvis du har et stort arkiv, kan du hurtigt finde en fil ved at søge efter den. Du kan søge efter hele eller en del af filens navn eller sti, og du kan derefter begrænse søgningen ved at angive den omtrentlige filstørrelse og datoen, hvor den sidst blev arkiveret.

Når du har fundet en fil, kan du åbne den direkte i stifinderen for det lokale arkiv. Sikkerhedskopiering og gendannelse åbner filen i det program, hvor den er oprettet, hvilket gør det muligt for dig at foretage ændringer uden at forlade stifinderen for det lokale arkiv. Filen gemmes på den oprindelige overvågningsplacering på din computer og arkiveres automatisk i overensstemmelse med den arkiveringstidsplan, du har defineret.

Sorter arkiverede filer

Du kan sortere dine arkiverede filer og mapper med følgende kriterier: Navn, filtype, størrelse, tilstand (dvs. arkiveret, ikke arkiveret eller arkivering i gang), den dato hvor filerne sidst blev arkiveret eller placeringen af filerne på din computer (sti).

Sådan sorteres arkiverede filer:

1. Klik på fanen **Lokalt arkiv**.
2. Klik på et kolonnenavn i højre rude.

Søge efter en arkiveret fil

Hvis du har et stort lager af arkiverede filer, kan du hurtigt finde en fil ved at søge efter den. Du kan søge efter hele eller en del af filens navn eller sti, og du kan derefter begrænse søgningen ved at angive den omtrentlige filstørrelse og datoen, hvor den sidst blev arkiveret.

1. Indtast hele eller en del af filnavnet i boksen **Søg** øverst i skærmbilledet, og tryk derefter på ENTER.
2. Indtast hele eller en del af stien i boksen **Hele eller en del af stien**.
3. Angiv den omtrentlige størrelse på den fil, som du søger efter, ved at gøre følgende:
   - Klik på **Mindre end 100 KB**, **Mindre end 1 MB** eller **Mere end 1 MB**.
   - Klik på **Størrelse i KB**, og vælg derefter de pågældende størrelsesværdier på listerne.

4 Angiv den omtrentlige dato på filens sidste arkivering ved at gøre et af følgende:
   - Klik på **Denne uge**, **Denne måned** eller **Dette år**.
   - Klik på **Angiv datoer**, klik på **Arkiveret** på listen, og klik derefter på de relevante datoværdier på datolisterne.
5 Klik på **Søg**.

Bemærk! Hvis du ikke kender den omtrentlige størrelse eller dato for den sidste arkivering, skal du klikke på **Ukendt**.

Åbning af en arkiveret fil

Du kan undersøge indholdet af en arkiveret fil ved at åbne den direkte i stifinderen for det lokale arkiv.

Sådan åbnes arkiverede filer:

1 Klik på fanen **Lokalt arkiv**.
2 Klik på et filnavn i højre rude, og klik derefter på **Åbn**.

Tip: Du kan også åbne en arkiveret fil ved at dobbeltklikke på filnavnet.

Gendanne arkiverede filer

Hvis en overvågningsfil bliver beskadiget, mangler eller slettes ved et uheld, kan du gendanne en kopi af filen fra det lokale arkiv. Derfor er det vigtigt at sikre, at du arkiverer dine filer med jævne mellemrum. Du kan også gendanne ældre versioner af filer fra et lokalt arkiv. Hvis du f.eks. jævnligt arkiverer en fil, men gerne vil vende tilbage til en tidligere version af filen, kan du finde filen på arkiveringsplaceringen. Hvis arkiveringsplaceringen er et lokalt drev eller et netværksdrev, kan du søge efter filen. Hvis arkiveringsplaceringen er en ekstern harddisk eller et USB-drev, skal du tilslutte drevet til computeren og derefter søge efter filen. Hvis arkiveringsplaceringen er en cd eller en dvd, skal du indsætte cd'en eller dvd'en i computeren og derefter søge efter filen.

Du kan også gendanne filer, du har arkiveret på én computer, fra en anden computer. Hvis du f.eks. arkiverer et sæt filer på en ekstern harddisk på computer A, kan du gendanne disse filer på computer B. For at gøre det skal du installere Sikkerhedskopiering og gendannelse på computer B og tilslutte den eksterne harddisk. Derefter kan du søge efter filerne i Sikkerhedskopiering og gendannelse, og de tilføjes på listen **Manglende filer**, så de kan gendannes.

Yderligere oplysninger om arkivering af filer finder du under Arkivere filer. Hvis du sletter en overvåget fil fra arkivet, kan du også slette den fra listen **Manglende filer**.

Gendanne manglende filer fra et lokalt arkiv

Med det lokale arkiv i Sikkerhedskopiering og gendannelse kan du gendanne data, der mangler i en overvågningsmappe på din lokale computer. Hvis en fil f.eks. er blevet flyttet fra overvågningsmappen eller er blevet slettet og allerede er arkiveret, kan du gendanne den fra det lokale arkiv.

1. Klik på fanen **Lokalt arkiv**.
2. Marker afkrydsningsfeltet ud for navnet på den fil, du ønsker at gendanne, på fanen **Manglende filer** i bunden af skærmen.
3. Klik på **Gendan**.

Tip! Du kan gendanne alle filerne på listen **Manglende filer** ved at klikke på **Gendan alle**.

Gendannelse af en ældre version af en fil fra et lokalt arkiv

Hvis du vil gendanne en ældre version af en arkiveret fil, kan du finde den og tilføje den på listen **Manglende filer**. Derefter kan du gendanne filer på samme måde som med en fil på listen **Manglende filer**.

1. Klik på fanen **Lokalt arkiv**.
2. Klik på fanen **Gennemse** på fanen **Manglende filer** i bunden af skærmen, og naviger så til den placering, hvor arkivet er lagret.

   Arkivmappenavne har følgende format: `cre ddmmyy_hh-mm-ss_***`, hvor `ddmmyy` er den dato, hvor filerne blev arkiveret, `hh-mm-ss` er det tidspunkt, hvor filerne blev arkiveret, og `***` er enten `Fuld` eller `Inkl`, afhængigt af, om det drejer sig om en fuld arkivering eller en hurtig arkivering.
3. Vælg placering, og klik derefter på **OK**.

   Filer på den valgte placering vises på listen **Manglende filer** og er klar til at blive hentet. Yderligere oplysninger finder du under Gendanne manglende filer fra et lokalt arkiv (side 184).

Fjernelse af filer fra listen over manglende filer

Når en arkiveret fil flyttes fra den overvågede mappe eller slettes, bliver den automatisk vist på listen **Manglende filer**. Dette advarer dig om, at der er inkonsekvens mellem de filer, der er arkiveret og filerne i de overvågede mapper. Hvis filen blev flyttet fra overvågningsmappen eller blev slettet ved et uheld, kan du slette den fra listen **Manglende filer**.

Sådan fjernes en fil fra listen over manglende filer:

1. Klik på fanen **Lokalt arkiv**.
2. Marker afkrydsningsfeltet ud for navnet på den fil, du ønsker at fjerne, på fanen **Manglende filer** i bunden af skærmen.
3. Klik på **Slet**.

Tip: Du kan fjerne alle filerne på listen **Manglende filer** ved at klikke på **Slet alle**.

Administration af arkiver

Du kan når som helst få vist en oversigt over oplysninger om dine fulde og hurtige arkiveringer. Du kan f.eks. se oplysninger om mængden af data, der overvåges for øjeblikket, mængden af data, der er blevet arkiveret, og mængden af data, der overvåges for øjeblikket, men som ikke er arkiveret. Du kan også se oplysninger om din arkiveringsplan, f.eks. datoen for den sidste og den næste arkivering.

Få vist en oversigt over arkiveringsaktiviteten

Du kan til enhver tid få vist oplysninger om arkiveringsaktiviteten. Du kan f.eks. få vist den procent af filer, der er blevet arkiveret, størrelsen på de data der overvåges, størrelsen på de data der er blevet arkiveret og størrelsen på de data der overvåges, men endnu ikke er blevet arkiveret. Du kan også få vist de datoer, hvor den sidste eller næste arkivering finder sted.

1. Klik på fanen **Lokalt arkiv**.
2. Klik på **Kontooversigt** øverst i skærmbilledet.

KAPITEL 38

McAfee QuickClean

QuickClean forbedrer din computers ydeevne ved at slette filer, som kan skabe rod på din computer. Det tømmer din papirkurv og sletter midlertidige filer, genveje, mistede filfragmenter, registreringsdatabasefiler, cachelagrede filer, cookies, webstedshistorik, sendte og slettede e-mails, filer brugt for nylig, Active-X-filer og systemgendannelsespunktfiler. QuickClean beskytter desuden dit privatliv ved at bruge McAfee Shredder-komponenter til sikkert og permanent at slette elementer, der kan indeholde følsomme personlige oplysninger, som f.eks. dit navn og din adresse. Flere oplysninger om makulering af filer finder du under McAfee Shredder.

Disk Defragmenter arrangerer filer og mapper på din computer for at sikre, at de ikke bliver spredt (dvs. fragmenteret), når du gemmer på din computers harddisk. Ved at defragmentere din harddisk med jævne mellemrum sikrer du, at disse fragmenterede filer og mapper konsolideres, så de senere hurtigt kan hentes.

Hvis du ikke ønsker at vedligeholde din computer manuelt, kan du indstille både QuickClean og Disk Defragmenter til at køre automatisk som uafhængige opgaver med de mellemrum, som du vil have.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i QuickClean

Filrenser	Slet unødvendige filer hurtigt og sikkert vha. forskellige rensninger. Ved at slette disse filer kan du øge pladsen på din computers harddisk og forbedre dens ydeevne.

KAPITEL 39

Rense computeren

QuickClean sletter filer, der kan skabe rod på din computer. Det tømmer din Papirkurv og sletter midlertidige filer, genveje, mistede filfragmenter, registreringsdatabasefiler, cachelagrede filer, cookies, websted shistorik, sendte og slettede e-mails, filer brugt for nylig, Active-X-filer og systemgendannelsespunktfiler. QuickClean sletter disse filer, uden at det påvirker andre vigtige oplysninger.

Du kan anvende alle oprydningsfunktionerne i QuickClean til at slette unødvendige filer på din computer. Følgende tabel beskriver de forskellige oprydningsfunktioner i QuickClean:

Navn	Funktion
Rensning af Papirkurv	Sletter filer i Papirkurv.
Rensning af midlertidige filer	Sletter filer, som er gemt i midlertidige mapper.
Genvejsrensning	Sletter ødelagte genveje og genveje uden et associeret program.
Rensning af tabt filfragment	Sletter tabte filfragmenter på din computer.
Rensning af registreringsdatabase	Sletter Windows®-registreringsdatabaseoplysninger for programmer, der ikke længere eksisterer på computeren. Registreringsdatabasen er en database, hvori Windows gemmer sine konfigurationsoplysninger. Registreringsdatabasen indeholder profiler for hver bruger af computeren og oplysninger om systemhardware, installerede programmer og egenskabsindstillinger. Windows anvender konstant disse informationer.
Cacherensning	Sletter de cache-filer, som akkumuleres, når du besøger websider. Disse filer gemmes normalt som midlertidige filer i en cache-mappe. En cache-mappe er et midlertidigt opbevaringsområde på din computer. Hastigheden og effektiviteten på din internetsøgning kan øges ved, at din browser henter en webside fra sin cache-mappe (i stedet for fra en fjernserver), næste gang du vil have den vist.

Navn	Funktion
Cookie-rensning	Sletter cookies. Disse filer gemmes normalt som midlertidige filer. En cookie er en lille fil, der indeholder oplysninger om f.eks. brugernavn og den aktuelle dato og tid, som gemmes på computeren, når der søges på internettet. Cookies bruges hovedsagelig af websider til at identificere brugere, som tidligere har registreret sig på eller besøgt siden. De kan dog også fungere som en informationskilde for hackere.
Rensning af browser-historik	Sletter din browsers webhistorik.
Outlook Express- og Outlook E-mail Cleaner (sendte og slettede elementer)	Sletter sendte og slettede e-mails fra Outlook® og Outlook Express.
Seneste rensning	Sletter seneste filer, der er blevet oprettet med et hvilket som helst af disse programmer: ▪ Adobe Acrobat® ▪ Corel® WordPerfect® Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft® Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX Cleaner	Sletter ActiveX-objekter. ActiveX er en softwarekomponent, der bruges af programmer eller websider til at tilføje funktionalitet, som kan indgå og fremstå som en normal del af programmet eller websiden. De fleste ActiveX-objekter er harmløse, men der er dog nogle, som kan opsnappe oplysninger fra din computer.
Rensning af systemgendannelsespunkt	Sletter gamle systemgendannelsespunkter (på nær de seneste) fra computeren. Systemgendannelsespunkter oprettes ved hjælp af Windows for at markere eventuelle ændringer, der er foretaget på din computer, så du kan gå tilbage til en tidligere indstilling, hvis der opstår problemer.

I dette kapitel

Rensning af din computer

Du kan anvende alle oprydningsfunktionerne i QuickClean til at slette unødvendige filer på din computer. Når oprydningen er afsluttet, kan du under **Oversigt over QuickClean** se den mængde diskplads, der blev frigjort, antallet af filer som blev slettet og den dato og det tidspunkt, QuickClean sidst blev brugt på din computer.

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
2. Klik på **Start** under **McAfee QuickClean**.
3. Nu kan du gøre følgende:
   - Klik på **Næste** for at acceptere standardrensningstyperne på listen.
   - Vælg eller fravælg de relevante rensninger, og klik derefter på **Næste.** Hvis du vælger Seneste rensning, kan du klikke på **Egenskaber** for at vælge eller rense de filer, der senest er blevet oprettet med et af programmerne på listen. Klik derefter på **OK**.
   - Klik på **Gendan standarder** for at gendanne standardrensningstyperne, og klik derefter på **Næste.**
4. Når analysen er udført, skal du klikke på **Næste**.
5. Klik på **Næste** for at bekræfte sletningen af filen.
6. Nu kan du gøre følgende:
   - Klik på **Næste** for at acceptere standardindstillingen **Nej, jeg vil slette filer med standard Windows-sletning**.
   - Klik på **Ja, jeg vil slette mine filer sikkert med Shredder**, angiv antallet af sletningsgennemløb (op til 10) og klik derefter på **Næste**. Makuleringen af filer kan tage lang tid, hvis det er en stor mængde oplysninger, der skal slettes.

7 I tilfælde af at visse filer eller elementer var låst under rensningen, kan du blive bedt om at genstarte din computer. Klik på **OK** for at lukke dialogboksen.

8 Klik på **Udfør**.

Bemærk! Filer, der slettes med Shredder, kan ikke gendannes. Yderligere oplysninger om makulering af filer finder du under McAfee Shredder.

KAPITEL 40

Defragmentering af din computer

Disk Defragmenter arrangerer filer og mapper på din computer, så de ikke bliver spredt (dvs. fragmenteret), når du gemmer på din computers harddisk. Ved at defragmentere din harddisk med jævne mellemrum sikrer du, at disse fragmenterede filer og mapper konsolideres, så de senere hurtigt kan hentes.

Defragmentering af din computer

Du kan defragmentere din computer, hvis du vil forbedre din adgang til og søgning efter filer og mapper.

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
2. Klik på **Analyser** under **Diskdefragmentering**.
3. Følg vejledningen på skærmen.

Bemærk! Yderligere oplysninger om Disk Defragmenter finder du under Hjælp i Windows.

KAPITEL 41

Planlæg en opgave

Task Scheduler automatiserer den frekvens, som QuickClean eller Disk Defragmenter skal køre med på din computer. Du kan eksempelvis planlægge, at QuickClean skal tømme din papirkurv søndag kl. 21.00, eller at Disk Defragmenter skal defragmentere din computers harddisk sidste dag i hver måned. Du kan til enhver tid oprette, ændre eller stoppe en opgave. Du skal være logget på din computer, for at en planlagt opgave kan udføres. Hvis opgaven ikke udføres af en eller anden grund, vil den blive planlagt igen fem minutter efter, at du logger ind næste gang.

Planlæg en opgave i QuickClean

Du kan planlægge en opgave i QuickClean, så programmet automatisk renser din computer ved hjælp af en eller flere oprydningsfunktioner. Når rensningen er udført, kan du under **Oversigt over QuickClean** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

1. Åbn ruden Task Scheduler.

   Hvordan?

   1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
   2. Klik på **Start** under **Opgavestyring**.

2. Klik på **McAfee QuickClean** på listen **Vælg opgave, der skal planlægges**.
3. Angiv et navn på din opgave i boksen **Opgavenavn**, og klik derefter på **Opret**.
4. Nu kan du gøre følgende:
   - Klik på **Næste** for at acceptere oprydningsfunktionerne på listen.
   - Vælg eller fravælg de relevante oprydningsfunktioner, og klik derefter på **Næste**. Hvis du vælger Seneste rensning, kan du klikke på **Egenskaber** for at vælge eller rense de filer, der senest er blevet oprettet med et af programmerne på listen. Klik derefter på **OK**.
   - Klik på **Gendan standarder** for at gendanne standardrensningstyperne, og klik derefter på **Næste.**
5. Nu kan du gøre følgende:
   - Klik på **Planlæg** for at acceptere standardindstillingen **Nej, jeg vil slette filer med standard Windows-sletning**.

- Klik på **Ja, jeg vil slette mine filer sikkert med Shredder**, angiv antallet af sletningsgennemløb (op til 10) og klik derefter på **Planlæg**.

6 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.

7 Hvis du foretog ændringer i egenskaberne for Seneste rensning, kan du blive bedt om at genstarte computeren. Klik på **OK** for at lukke dialogboksen.

8 Klik på **Udfør**.

Bemærk! Filer, der slettes med Shredder, kan ikke gendannes. Yderligere oplysninger om makulering af filer finder du under McAfee Shredder.

Lav ændringer i en opgave i QuickClean

Du kan ændre en planlagt opgave i QuickClean, så oprydningsfunktionerne ændres, eller frekvensen, som programmet er indstillet til på din computer, laves om. Når rensningen er udført, kan du under **Oversigt over QuickClean** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

1 Åbn ruden Task Scheduler.

   Hvordan?

   1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
   2. Klik på **Start** under **Opgavestyring**.

2 Klik på **McAfee QuickClean** på listen **Vælg opgave, der skal planlægges**.

3 Marker opgaven på listen **Vælg en eksisterende opgave**, og klik derefter på **Rediger**.

4 Nu kan du gøre følgende:

- Klik på **Næste** for at acceptere rensningstyperne for opgaven.
- Vælg eller fravælg de relevante oprydningsfunktioner, og klik derefter på **Næste**. Hvis du vælger Seneste rensning, kan du klikke på **Egenskaber** for at vælge eller rense de filer, der senest er blevet oprettet med et af programmerne på listen. Klik derefter på **OK**.
- Klik på **Gendan standarder** for at gendanne standardrensningstyperne, og klik derefter på **Næste.**

5 Nu kan du gøre følgende:

- Klik på **Planlæg** for at acceptere standardindstillingen **Nej, jeg vil slette filer med standard Windows-sletning**.

- Klik på **Ja, jeg vil slette mine filer sikkert med Shredder**, angiv antallet af sletningsgennemløb (op til 10) og klik derefter på **Planlæg**.

6 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.

7 Hvis du foretog ændringer i egenskaberne for Seneste rensning, kan du blive bedt om at genstarte computeren. Klik på **OK** for at lukke dialogboksen.

8 Klik på **Udfør**.

Bemærk! Filer, der slettes med Shredder, kan ikke gendannes. Yderligere oplysninger om makulering af filer finder du under McAfee Shredder.

Slet en opgave i QuickClean

Du kan slette en planlagt opgave i QuickClean, hvis du ikke længere ønsker, at den skal køre automatisk.

1 Åbn ruden Task Scheduler.

Hvordan?

1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
2. Klik på **Start** under **Opgavestyring**.

2 Klik på **McAfee QuickClean** på listen **Vælg opgave, der skal planlægges**.

3 Marker opgaven på listen **Vælg en eksisterende opgave**.

4 Klik på **Slet**, og klik derefter på **Ja** for at bekræfte sletningen.

5 Klik på **Udfør**.

Planlæg en opgave i Disk Defragmenter

Du kan planlægge en opgave i Disk Defragmenter for at indstille frekvensen, som din computer automatisk defragmenterer harddisken med. Når rensningen er udført, kan du under **Disk Defragmenter** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

1 Åbn ruden Task Scheduler.

Hvordan?

1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
2. Klik på **Start** under **Opgavestyring**.

2 Klik på **Disk Defragmenter** på listen **Vælg opgave, der skal planlægges**.

3 Angiv et navn på din opgave i boksen **Opgavenavn**, og klik derefter på **Opret**.

4 Nu kan du gøre følgende:

- Klik på **Planlæg** for at acceptere standardindstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**.
- Fravælg indstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**, og klik derefter **Planlæg**.

5 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.

6 Klik på **Udfør**.

Lav ændring i en opgave i Disk Defragmenter

Du kan ændre en planlagt opgave i Disk Defragmenter, så frekvensen, som programmet er indstillet til at køre med på din computer, laves om. Når rensningen er udført, kan du under **Disk Defragmenter** se den dato og det tidspunkt, hvor din opgave er planlagt til at køre næste gang.

1 Åbn ruden Task Scheduler.

Hvordan?

1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
2. Klik på **Start** under **Opgavestyring**.

2 Klik på **Disk Defragmenter** på listen **Vælg opgave, der skal planlægges**.

3 Marker opgaven på listen **Vælg en eksisterende opgave**, og klik derefter på **Rediger**.

4 Nu kan du gøre følgende:

- Klik på **Planlæg** for at acceptere standardindstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**.
- Fravælg indstillingen **Foretag defragmentering, selvom den ledige plads er begrænset**, og klik derefter **Planlæg**.

5 Vælg den frekvens, som du vil have, at opgaven skal udføres med i dialogboksen **Planlæg**, og klik derefter på **OK**.

6 Klik på **Udfør**.

Slet en opgave i Disk Defragmenter

Du kan slette en planlagt opgave i Disk Defragmenter, hvis du ikke længere ønsker, at den skal køre automatisk.

1 Åbn ruden Task Scheduler.

   Hvordan?

   1. I McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på **Vedligehold computer**.
   2. Klik på **Start** under **Opgavestyring**.

2 Klik på **Disk Defragmenter** på listen **Vælg opgave, der skal planlægges**.

3 Marker opgaven på listen **Vælg en eksisterende opgave**.

4 Klik på **Slet**, og klik derefter på **Ja** for at bekræfte sletningen.

5 Klik på **Udfør**.

KAPITEL 42

McAfee Shredder

McAfee Shredder sletter (eller makulerer) filer permanent fra din computers harddisk. Selv når du sletter filer og mapper manuelt, tømmer din Papirkurv eller sletter mappen Midlertidige internetfiler, kan du stadig genfinde disse data ved hjælp af computerens sporingsværktøjer. Ligeledes kan slettede filer genfindes, idet nogle programmer laver midlertidige, gemte kopier af åbnede filer. Shredder beskytter dine private oplysninger ved at slette disse uønskede filer permanent og sikkert. Det er vigtigt at huske, at makulerede filer ikke kan gendannes.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Shredder

Slet filer og mapper permanent

Slet filer fra din computers harddisk, så deres tilknyttede oplysninger ikke kan gendannes. Det beskytter dit privatliv ved sikkert og permanent at slette filer og mapper, elementer i din Papirkurv og mappen Midlertidige internetfiler og hele indholdet på computerdiske, som f.eks. genskrivbare cd'er, eksterne harddiske og disketter.

Makulerer filer og indholdet af mapper og diske.

Shredder sørger for at de data, der findes i slettede filer og mapper i din Papirkurv og i mappen Midlertidige internetfiler, ikke kan genfindes selv med specialværktøjer. Med Shredder kan du angive, hvor mange gange (op til 10) du ønsker, at et element skal makuleres. Et højere antal makuleringsgennemløb øger sikkerhedsniveauet for sletningen af filen.

Makuler filer og mapper

Du kan makulere filer og mapper på din computers harddisk inklusive elementer i din Papirkurv og i mappen Midlertidige internetfiler.

1. Åbn **Shredder**.

   Hvordan?

   1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på menuen **Avanceret**.
   2. Klik på **Værktøjer** i den venstre rude.
   3. Klik på **Shredder**.

2. I ruden Makuler filer og mapper under **Jeg vil** skal du klikke på **Slet filer og mapper**.
3. Under **Makuleringsniveau** skal du klikke på et af følgende niveauer:
   - **Hurtig**: Makulerer det markerede element(er) en gang.
   - **Omfattende**: Makulerer det markerede element(er) 7 gange.
   - **Brugerdefineret**: Makulerer det markerede element(er) op til 10 gange.
4. Klik på **Næste**.
5. Nu kan du gøre følgende:
   - På listen **Marker de filer, der skal makuleres** skal du klikke enten på **Indhold i Papirkurv** eller **Midlertidige internetfiler**.
   - Klik på **Gennemse**, og find den fil, du ønsker at makulere. Vælg derefter **Åbn**.

6 Klik på **Næste**.

7 Klik på **Start**.

8 Når Shredder er færdig, skal du klikke på **Udført**.

Bemærk! Du bør ikke arbejde med nogen filer, før Shredder har fuldført denne opgave.

Makulere en hel disk

Du kan makulere alt indholdet på en disk på en gang. Det er kun flytbare diske som f.eks. eksterne harddiske, skrivbare cd'er og disketter, der kan makuleres.

1 Åbn **Shredder**.

Hvordan?

1. I ruden McAfee SecurityCenter under **Almindelige opgaver** skal du klikke på menuen **Avanceret**.
2. Klik på **Værktøjer** i den venstre rude.
3. Klik på **Shredder**.

2 I ruden Makuler filer og mapper under **Jeg vil** skal du klikke på **Slet en hel disk**.

3 Under **Makuleringsniveau** skal du klikke på et af følgende niveauer:

- **Hurtig**: Makulerer den markerede disk en gang.
- **Omfattende**: Makulerer den markerede disk 7 gange.
- **Brugerdefineret**: Makulerer den markerede disk op til 10 gange.

4 Klik på **Næste**.

5 På listen **Vælg disken** skal du klikke på det drev, du vil makulere.

6 Klik på **Næste**, og klik derefter på **Ja** for at bekræfte.

7 Klik på **Start**.

8 Når Shredder er færdig, skal du klikke på **Udført**.

Bemærk! Du bør ikke arbejde med nogen filer, før Shredder har fuldført denne opgave.

KAPITEL 43

McAfee Network Manager

Netværksadministration giver en grafisk oversigt over computere og andre enheder i hjemmenetværket. Du kan bruge Netværksadministration til at fjernadministrere beskyttelsesstatussen for hver af de administrerede computere i netværket og fjernreparere rapporterede sikkerhedsproblemer på disse computere. Hvis du har installeret McAfee Total Protection, kan Netværksadministration overvåge netværket for uautoriserede brugere (computere eller enheder, som du ikke genkender eller har tillid til), der forsøger at oprette forbindelse til netværket.

Før du bruger Netværksadministration, kan du sætte dig ind i nogle af funktionerne. Der findes detaljerede oplysninger om konfiguration og brug af disse funktioner i hjælpen til Netværksadministration.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i Network Manager

Grafisk netværkskort

Få vist en grafisk oversigt over beskyttelsesstatus for de computere og enheder, der udgør dit hjemmenetværk. Når du foretager ændringer i netværket (f.eks. tilføjer en computer), registrerer netværkskortet disse ændringer. Du kan opdatere netværkskortet, omdøbe netværket og vise eller skjule komponenter i netværkskortet for at tilpasse visningen. Du kan også få vist oplysninger vedrørende en af de enheder, der vises på netværkskortet.

Fjernstyring

Administrer beskyttelsesstatusen for de computere, der udgør dit hjemmenetværk. Du kan invitere en computer til at tilslutte til det administrerede netværk, overvåge en administreret computers beskyttelsesstatus og udbedre kendte sikkerhedsproblemer fra en fjerncomputer i netværket.

Netværksovervågning

Hvis Netværksadministration er tilgængelig, kan du lade den overvåge dine netværk og give dig besked, når venner eller uautoriserede brugere opretter forbindelse. Netværksovervågning er kun tilgængelig, hvis du har købt McAfee Total Protection.

Forklaring af ikoner i Network Manager

Følgende tabel beskriver de almindeligt brugte ikoner på netværkskortet i Network Manager.

Ikon	Beskrivelse
	Repræsenterer en administreret computer, der er online
	Repræsenterer en administreret computer, der er offline
	Repræsenterer en ikke-administreret computer, som har SecurityCenter installeret
	Repræsenterer en ikke-administreret computer, der er offline
	Repræsenterer en computer, der er online, og som ikke har SecurityCenter installeret, eller en ukendt netværksenhed
	Repræsenterer en computer, der er offline, og som ikke har SecurityCenter installeret, eller en ukendt netværksenhed
	Angiver, at det tilsvarende element er beskyttet og tilsluttet
	Angiver, at det tilsvarende element evt. kræver din opmærksomhed
	Angiver, at det tilsvarende element kræver din opmærksomhed omgående
	Repræsenterer en trådløs hjemmerouter
	Repræsenterer en standardhjemmerouter
	Repræsenterer internettet, når der er oprettet forbindelse
	Repræsenterer internettet, når forbindelsen er afbrudt

KAPITEL 44

Konfigurere et administreret netværk

Du konfigurerer et administreret netværk ved at godkende netværket (hvis du ikke allerede har gjort det) og tilføje medlemmer (computere) til netværket. Hvis en computer skal kunne fjernadministreres eller selv skal fjernadministrere andre computere på netværket, skal den være et netværksmedlem, der er tillid til. Nye computere gøres til medlemmer af netværket af eksisterende netværksmedlemmer (computere), der har administratorrettigheder.

Du kan få vist oplysninger vedrørende et af de elementer, der vises på netværkskortet, også efter at du har foretaget ændringer i netværket (f.eks. tilføjet en computer).

I dette kapitel

Arbejde med netværkskortet

Når du forbinder en computer til netværket, analyserer Netværksadministration netværkets status for at afgøre, om der er administrerede eller ikke-administrerede medlemmer, routerens attributter og internetstatussen. Hvis der ikke findes nogen medlemmer, vil Netværksadministration gå ud fra, at den computer, der er tilsluttet i øjeblikket, er den første computer i netværket, og gøre computeren til et administreret medlem med administratorrettigheder. Navnet på netværket indeholder som standard navnet på den første computer med SecurityCenter installeret, der sluttes til netværket. Netværket kan dog til enhver tid omdøbes.

Når du foretager ændringer i netværket (f.eks. tilføjer en computer), kan du brugertilpasse netværkskortet. Du kan f.eks. opdatere netværkskortet, omdøbe netværket og tilpasse visningen ved at vise eller skjule elementer på netværkskortet. Du kan også få vist oplysninger vedrørende et af de elementer, der vises på netværkskortet.

Åbne netværkskortet

Netværkskortet giver en grafisk gengivelse af computere og elementer på dit hjemmenetværk.

- Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.

Bemærk! Hvis du ikke allerede har godkendt netværket (vha. McAfee Personal Firewall), bliver du bedt om at gøre det, første gang du anvender netværkskortet.

Opdatere netværkskortet

Du kan til enhver tid opdatere netværkskortet, f.eks. når der er blevet sluttet en ny computer til netværket.

1. Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.
2. Klik på **Opdater netværkskortet** under **Jeg ønsker at**.

Bemærk! Linket **Opdater netværkskortet** er kun tilgængeligt, når ingen af elementerne på netværskortet er markeret. Hvis du vil fjerne markeringen fra et element, skal du klikke på det markerede element eller på et hvidt område på netværkskortet.

Omdøbe netværket

Navnet på netværket indeholder som standard navnet på den første computer med SecurityCenter installeret, der sluttes til netværket. Hvis du foretrækker et andet navn, kan du ændre det.

1. Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.
2. Klik på **Omdøb netværket** under **Jeg ønsker at**.
3. Skriv navnet på netværket i feltet **Netværksnavn**.
4. Klik på **OK**.

Bemærk! Linket **Opdater netværkskortet** er kun tilgængeligt, når ingen af elementerne på netværkskortet er markeret. Hvis du vil fjerne markeringen fra et element, skal du klikke på det markerede element eller på et hvidt område på netværkskortet.

Vise eller skjule elementer på netværkskortet

Som standard vises alle hjemmenetværkets computere og enheder på netværkskortet. Hvis der er skjulte elementer, kan du til enhver tid få dem vist igen. Kun ikke-administrerede elementer kan skjules. Administrerede computere kan ikke skjules.

For at...	Klik på Netværksadministration i menuen Grundlæggende eller Avanceret, og gør derefter følgende...
Skjule et element på netværkskortet	Klik på et element på netværkskortet, og klik derefter på **Skjul dette element** under **Jeg ønsker at**. Klik på **Ja** i dialogboksen til bekræftelse.
Vise skjulte elementer på netværkskortet	Klik på **Vis skjulte elementer** under **Jeg ønsker at**.

Få vist yderligere oplysninger om et element

Du kan få vist detaljerede oplysninger om hver enkelt element i netværket ved at markere komponenten på netværkskortet. Blandt de viste oplysninger er elementets navn og beskyttelsesstatus samt andre oplysninger, der skal bruges for at kunne administrere elementet.

1. Klik på ikonet for et element på netværkskortet.
2. Se oplysningerne om elementet under **Detaljer**.

Tilslutte computeren til det administrerede netværk

Hvis en computer skal kunne fjernadministreres eller selv skal fjernadministrere andre computere på netværket, skal den være et netværksmedlem, der er tillid til. Nye computere gøres til medlemmer af netværket af eksisterende netværksmedlemmer (computere), der har administratorrettigheder. For at sikre at kun computere, der er tillid til, deltager i netværket, skal brugerne på den adgangsgivende og den tilknyttende computer godkende hinanden.

Når en computer tilknyttes netværket, bliver den bedt om at vise sin beskyttelsesstatus i McAfee til de andre computere på netværket. Hvis en computer accepterer at vise sin beskyttelsesstatus, bliver den administreret medlem af netværket. Hvis en computer afviser at vise sin beskyttelsesstatus, bliver den ikke-administreret medlem af netværket. Ikke-administrerede medlemmer af netværket er sædvanligvis gæstecomputere, der ønsker adgang til andre netværksfunktioner (f.eks. fil- eller printerdeling).

Bemærk! Hvis computeren har andre McAfee-netværksprogrammer installeret (f.eks. EasyNetwork), vil computeren også blive anerkendt som administreret computer af disse programmer, når den er blevet medlem af netværket. Det tilladelsesniveau, som computeren tildeles i Network Manager, anvendes i alle McAfee-netværksprogrammer. Yderligere oplysninger om, hvad rettighedsniveauerne gæst, fuld og administrator betyder for andre McAfee-netværksprogrammer, finder du i den medfølgende dokumentation for det enkelte program.

Tilslutte computeren til et administreret netværk

Når du modtager en invitation til at slutte dig til et administreret netværk, kan du enten acceptere eller afvise den. Du kan også afgøre, om de andre computere på netværket skal administrere denne computers sikkerhedsindstillinger.

1. Kontroller, at afkrydsningsfeltet **Tillad alle computere på dette netværk at overvåge sikkerhedsindstillingerne** er markeret i dialogboksen Administreret netværk.
2. Klik på **Deltag**.
   Når du accepterer invitationen, vises to spillekort.
3. Bekræft, at spillekortene er de samme som dem, der vises på den computer, der har inviteret dig til at deltage i det administrerede netværk.
4. Klik på **OK**.

Bemærk! Hvis den computer, der inviterede dig til at deltage i det administrerede netværk, ikke viser de samme spillekort som i dialogboksen til bekræftelse af sikkerheden, er der sket et sikkerhedsbrud på det administrerede netværk. I sådanne tilfælde kan det være risikabelt at tilslutte computeren til netværket. Derfor skal du klikke på **Annuller** i dialogboksen til bekræftelse af sikkerheden.

Invitere en computer til at deltage i det administrerede netværk

Hvis en computer føjes til det administrerede netværk, eller hvis der findes en anden, ikke-administreret computer på netværket, kan du invitere denne computer til at deltage i det administrerede netværk. En computer kan kun invitere andre computere til at deltage i netværket, hvis den har administratorrettigheder på netværket. Når du sender invitationen, skal du også angive tilladelsesniveauet for den computer, der skal tilsluttes.

1. Klik på ikonet for en ikke-administreret computer på netværkskortet.
2. Klik på **Administrer denne computer** under **Jeg ønsker at**.
3. I dialogboksen Inviter en computer til at deltage i dette administrerede netværk skal du gøre et af følgende:
   - Klik på **Giv gæsteadgang til administrerede netværksprogrammer** for at give computeren adgang til netværket (du kan bruge denne indstilling for midlertidige brugere i dit hjem).
   - Klik på **Giv fuld adgang til administrerede netværksprogrammer** for at give computeren adgang til netværket.

- Klik på **Giv administratoradgang til administrerede netværksprogrammer** for at give computeren adgang til netværket med administratorrettigheder. Det giver også computeren adgang til at tildele adgangstilladelser til andre computere, der ønsker at deltage i det administrerede netværk.

4 Klik på **OK**.
Der sendes en invitation til at deltage i det administrerede netværk til computeren. Når computeren accepterer invitationen, vises to spillekort.

5 Bekræft, at spillekortene er de samme som dem, der vises på den computer, du har inviteret til at deltage i det administrerede netværk.

6 Klik på **Tildel adgang**.

Bemærk! Hvis den computer, du har inviteret til at deltage i det administrerede netværk, ikke viser de samme spillekort som i dialogboksen til bekræftelse af sikkerheden, er der sket et sikkerhedsbrud på det administrerede netværk. Hvis computeren gives adgang til at deltage i netværket, kan de andre computere muligvis udsættes for risiko, og du skal derfor klikke på **Afvis adgang** i dialogboksen til bekræftelse af sikkerheden.

Stoppe med at stole på andre computere på netværket

Hvis du ved en fejl har haft tillid til andre computere på netværket, kan du annullere dette.

- Klik på **Stop med at stole på andre computere på dette netværk** under **Jeg ønsker at**.

Bemærk! Linket **Stop med at stole på andre computere på dette netværk** er ikke tilgængeligt, hvis du har administratorrettigheder, og der er andre administrerede computere på netværket.

KAPITEL 45

Administrere netværket eksternt

Når du konfigurerer det administrerede netværk, kan du administrere netværkets computere og enheder eksternt. Du kan administrere computernes status og tilladelsesniveauer og afhjælpe de fleste sikkerhedssårbarheder eksternt.

I dette kapitel

Administrere status og tilladelser

I et administreret netværk findes der administrerede og ikke-administrerede medlemmer. Administrerede medlemmer tildeler andre computere adgang til netværket for at administrere deres beskyttelsesstatus i McAfee – det gør andre medlemmer ikke. Ikke-administrerede medlemmer er sædvanligvis gæstecomputere, der ønsker adgang til andre netværksfunktioner (f.eks. fil- eller printerdeling). En ikke-administreret computer kan til enhver tid inviteres til at blive administreret computer af en anden administreret computer med administrative tilladelser på netværket. På samme måde kan en administreret computer med administrative tilladelser når som helst fjerne administreringen af en anden administreret computer.

Administrerede computere er enten tildelt tilladelsesniveauet administrator, fuld eller gæst. En administreret computer med administratorrettigheder kan administrere beskyttelsesstatussen for alle andre administrerede computere på netværket og kan tildele andre computere medlemskab af netværket. En computer med tilladelsesniveauet fuld eller gæst har kun adgang til netværket. Du kan til enhver tid redigere en computers tilladelsesniveau.

Da et administreret netværk også kan bestå af enheder (f.eks. routere), kan Netværksadministration også bruges til at administrere disse. Du kan også konfigurere og redigere displayegenskaber for en enhed på netværkskortet.

Administrere en computers beskyttelsesstatus

Hvis en computers beskyttelsesstatus ikke administreres på netværket (computeren er ikke medlem af netværket, eller computeren er ikke-administreret medlem), kan du anmode om at administrere den.

1. Klik på ikonet for en ikke-administreret computer på netværkskortet.
2. Klik på **Administrer denne computer** under **Jeg ønsker at**.

Indstille administrering af en computers beskyttelsesstatus

Du kan standse administreringen af beskyttelsesstatussen for en administreret computer på netværket. Computeren bliver så ikke-administreret, og du kan ikke fjernovervåge dens beskyttelsesstatus.

1. Klik på ikonet for en administreret computer på netværkskortet.
2. Klik på **Stop administration af denne pc** under **Jeg ønsker at**.
3. Klik på **Ja** i dialogboksen til bekræftelse.

Redigere tilladelser for en administreret computer

Du kan til enhver tid redigere tilladelser for en administreret computer. Dette giver dig mulighed for at justere, hvilke computere der kan administrere beskyttelsesstatussen (sikkerhedsindstillingerne) for andre computere på netværket.

1. Klik på ikonet for en administreret computer på netværkskortet.
2. Klik på **Rediger tilladelser for denne computer** under **Jeg ønsker at**.
3. Marker afkrydsningsfeltet i dialogboksen Rediger tilladelser for at bestemme, om denne computer eller andre computere på det administrerede netværk kan administrere hinandens beskyttelsesstatus.
4. Klik på **OK**.

Administrere en enhed

Du kan administrere en enhed ved at åbne dens administrationswebside fra netværkskortet.

1. Klik på ikonet for en enhed på netværkskortet.
2. Klik på **Administrer denne enhed** under **Jeg ønsker at**. Der åbnes en webbrowser, der viser enhedens administrationswebside.
3. Angiv dine loginoplysninger i webbrowseren og konfigurer enhedens sikkerhedsindstillinger.

Bemærk! Hvis enheden er en trådløs router eller et trådløst adgangspunkt, der er beskyttet med Wireless Network Security, skal du bruge McAfee Wireless Network Security til at konfigurere enhedens sikkerhedsindstillinger.

Redigere en enheds displayegenskaber

Når du redigerer en enheds displayegenskaber, kan du ændre enhedens viste navn på netværkskortet og angive, om enheden er en trådløs router.

1. Klik på ikonet for en enhed på netværkskortet.
2. Klik på **Rediger enhedsegenskaber** under **Jeg ønsker at**.
3. Hvis du vil angive enhedens viste navn, skal du angive et navn i feltet **Navn**.
4. Hvis du vil angive enhedstypen, skal du klikke på **Standardrouter**, hvis det ikke er en trådløs router, eller **Trådløs router**, hvis den er trådløs.
5. Klik på **OK**.

Afhjælpe sikkerhedssårbarheder

Administrerede computere med administratorrettigheder kan administrere statussen for McAfee-beskyttelsen på andre administrerede computere på netværket og afhjælpe eventuelle rapporterede sikkerhedssårbarheder eksternt. Hvis f.eks. en administreret computers status for McAfee-beskyttelse viser, at VirusScan er deaktiveret, kan en anden administreret computer med administratorrettigheder fjernaktivere VirusScan.

Når du fjernafhjælper sikkerhedssårbarheder, reparerer Netværksadministration automatisk de fleste rapporterede problemer. Visse sikkerhedssårbarheder kan dog kræve manuel indgriben på den lokale computer. I dette tilfælde afhjælper Network Manager de problemer, der kan repareres eksternt, og viser en besked, der beder dig afhjælpe de resterende problemer ved at logge på SecurityCenter på den berørte computer og følge den angivne vejledning. I nogle tilfælde foreslås det at afhjælpe problemet ved at installere den seneste version af SecurityCenter på en eller flere fjerncomputere på netværket.

Afhjælpe sikkerhedssårbarheder

Du kan bruge Network Manager til automatisk at afhjælpe de fleste sikkerhedssårbarheder på administrerede fjerncomputere. Hvis f.eks. VirusScan er deaktiveret på en fjerncomputer, kan du aktivere programmet.

1. Klik på ikonet for et element på netværkskortet.
2. Få vist elementets beskyttelsesstatus under **Detaljer**.
3. Klik på **Afhjælp sikkerhedssårbarheder** under **Jeg ønsker at**.
4. Klik **OK**, når sikkerhedsproblemet er afhjulpet.

Bemærk! Selvom Network Manager kan afhjælpe de fleste sikkerhedssårbarheder automatisk, vil nogle reparationer muligvis kræve, at du starter SecurityCenter på den berørte computer og følger den angivne vejledning.

Installere McAfees sikkerhedssoftware på fjerncomputere

Hvis en eller flere computere på netværket ikke har den seneste version af SecurityCenter installeret, kan deres sikkerhedsstatus ikke fjernadministreres. Hvis du vil fjernadministrere disse computere, skal du installere den seneste version af SecurityCenter lokalt på hver enkelt computer.

1. Sørg for, at du følger denne vejledning på den computer, du ønsker at fjernadministrere.
2. Hav dine McAfee-loginoplysninger ved hånden. Dette er den e-mail-adresse og adgangskode, som du anvendte, da du aktiverede din McAfee-software for første gang.
3. Åbn en browser, gå til McAfees websted, log på, og klik på **Min konto**.
4. Find det produkt, du vil installere, klik på knappen **Download**, og følg derefter vejledningen på skærmen.

Tip! Du kan også få mere at vide om, hvordan du installerer McAfees sikkerhedssoftware på fjerncomputere ved at åbne netværkskortet og klikke på **Beskyt mine pc'er** under **Jeg ønsker at**.

KAPITEL 46

Overvåge dine netværk

Hvis McAfee Total Protection er installeret, overvåger Netværksadministration også dine netværk for uautoriserede brugere. Hver gang en ukendt computer eller enhed opretter forbindelse til dit netværk, får du besked herom, så du kan afgøre, om computeren eller enheden er en ven eller en uautoriseret bruger. En ven er en computer eller enhed, som du genkender og har tillid til, og en uautoriseret bruger er en computer eller enhed, du ikke genkender eller har tillid til. Hvis du markerer en computer eller enhed som en ven, kan du afgøre, om du vil have besked, hver gang den pågældende ven opretter forbindelse til netværket. Hvis du markerer en computer eller enhed som en uautoriseret bruger, får du automatisk en advarsel, hver gang den uautoriserede bruger opretter forbindelse.

Første gang, du opretter forbindelse til et netværk, når du har installeret eller opgraderet til denne version af Total Protection, markeres hver computer eller enhed automatisk som en ven, og du får ikke besked, når de opretter forbindelse til netværket fremover. Efter tre dage vil du modtage meddelelser om enhver ukendt computer eller enhed, der opretter forbindelse, så du selv kan markere dem.

Bemærk! Netværksovervågning er en funktion i Netværksadministration, som kun er tilgængelig med McAfee Total Protection. Besøg vores websted for flere oplysninger om Total Protection.

I dette kapitel

Stoppe overvågning af netværk

Hvis du deaktiverer overvågning af netværk, kan vi ikke længere advare dig, hvis uautoriserede brugere opretter forbindelse til dit hjemmenetværk eller til et andet netværk, du er tilsluttet.

1 Åbn konfigurationsruden Internet & Netværk.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.

2. Klik på **Internet & netværk** i startruden for SecurityCenter.
3. Klik på **Konfigurer** i afsnittet Internet- & netværksoplysninger.

2 Klik på **Fra** under **Netværksovervågning**.

Aktivere netværksovervågningsalarmer igen

Selvom du kan deaktivere netværksovervågningsalarmer, fraråder vi, at du gør det. Hvis du gør det, kan vi muligvis ikke længere meddele dig, når ukendte computere eller uautoriserede brugere opretter forbindelse til netværket. Hvis du ved en fejl deaktiverer disse advarsler (hvis du f.eks. markerer afkrydsningsfeltet **Vis ikke denne advarsel igen** i en advarsel), kan du når som helst aktivere dem igen.

1 Åbn ruden Alarmindstillinger.

Hvordan?

1. Klik på **Start** under **Almindelige opgaver**.
2. Klik på **Konfigurer** under **Oplysninger om SecurityCenter** i ruden til højre.
3. Under **Alarmer** skal du klikke på **Avanceret**.

2 Klik på **Oplysningsalarmer** i ruden Konfiguration af SecurityCenter.

3 Sørg for, at følgende afkrydsningsfelter ikke er markeret i ruden Oplysningsalarmer:

- **Vis ikke alarmer , når der er registreret ukendte pc'er eller enheder**
- **Vis ikke alarmer, når der registreres en uautoriseret bruger**
- **Vis ikke alarmer for venner, som jeg ønsker at blive informeret om**
- **Vis ikke alarmer, når overvågede pc'er eller enheder er registreret**
- **Vis ikke alarmer, når McAfee har afsluttet registreringen af nye venner**

4 Klik på **OK**.

Markere som uautoriseret bruger

Du skal kun markere en computer eller enhed på netværket som en uautoriseret bruger, hvis du ikke genkender den eller har tillid til den. Du får automatisk en advarsel, hver gang den uautoriserede bruger opretter forbindelse til netværket.

1. Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.
2. Klik på et element på netværkskortet.
3. Klik på **Marker som ven eller uautoriseret bruger** under **Jeg ønsker at**.
4. Klik på **En uautoriseret bruger** i dialogboksen.

Markere som ven

Du skal kun markere en computer eller enhed på netværket som en ven, hvis du genkender den eller har tillid til den. Når du markerer en computer eller enhed som en ven, kan du afgøre, om du vil have besked, hver gang den pågældende ven opretter forbindelse til netværket.

1. Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.
2. Klik på et element på netværkskortet.
3. Klik på **Marker som ven eller uautoriseret bruger** under **Jeg ønsker at**.
4. Klik på **En ven** i dialogboksen.
5. Hvis du vil have besked, hver gang denne ven opretter forbindelse til netværket, skal du markere afkrydsningsfeltet **Giv mig besked, når denne computer eller enhed opretter forbindelse til netværket**.

Indstille registrering af nye venner

I de første tre dage, efter du har oprettet forbindelse til et netværk og har denne version af Total Protection installeret, markerer vi automatisk hver computer eller enhed som en ven, du ikke ønsker at få besked om. Du kan indstille denne automatiske markering når som helst i løbet af de tre dage, men du kan ikke starte markeringen igen.

1. Klik på **Netværksadministration** i menuen Grundlæggende eller Avanceret.
2. Klik på **Stop registrering af nye venner** under **Jeg ønsker at**.

KAPITEL 47

McAfee EasyNetwork

EasyNetwork gør det muligt at foretage sikker fildeling, letter filoverførsler og automatiserer printerdeling mellem computere på hjemmenetværket. EasyNetwork skal dog være installeret på computerne på netværket, for at de kan få adgang til disse funktioner.

Før du bruger EasyNetwork, kan du sætte dig ind i nogle af funktionerne. Oplysninger om, hvordan du konfigurerer og bruger disse funktioner, finder du i EasyNetwork Hjælp.

Bemærk! SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician.

I dette kapitel

Funktioner i EasyNetwork

EasyNetwork indeholder følgende funktioner.

Fildeling

EasyNetwork gør det nemt at dele filer på computeren med andre computere på netværket. Når du deler filer, giver du andre computere læseadgang til disse filer. Kun computere, der har fuld eller administrativ adgang til det administrerede netværk (dvs. medlemmer) kan dele filer eller åbne filer, der deles af andre medlemmer.

Filoverførsel

Du kan sende filer til andre computere, der har fuld eller administrativ adgang til det administrerede netværk (dvs. medlemmer). Når du modtager en fil, vises den i EasyNetwork-indbakken. Indbakken er en midlertidig lagerplacering for alle filer, der sendes til dig af andre computere på netværket.

Automatisk printerdeling

Når du har tilsluttet computeren til et administreret netværk, kan du dele alle lokale printere, der er tilsluttet din computer, med andre medlemmer ved at bruge printerens aktuelle navn som navnet på den delte printer. EasyNetwork registrerer også printere, der deles af andre computere på netværket, og giver dig mulighed for at konfigurere og bruge disse printere.

KAPITEL 48

Konfigurere EasyNetwork

Før du kan bruge EasyNetwork, skal du starte programmet og tilslutte dig et administreret netværk. Når du har tilsluttet din computer et administreret netværk, kan du dele, søge efter og sende filer til andre computere på netværket. Du kan også dele printere. Du kan til enhver tid forlade netværket igen.

I dette kapitel

Åbne EasyNetwork

Du kan åbne EasyNetwork fra startmenuen i Windows eller ved at klikke på ikonet på skrivebordet.

- I menuen **Start** skal du gå til **Programmer** og **McAfee** og derefter klikke på **McAfee EasyNetwork**.

Tip! Du kan også åbne EasyNetwork ved at dobbeltklikke på McAfee EasyNetwork-ikonet på skrivebordet.

Tilslutte computeren til et administreret netværk

Hvis ingen computeren på det netværk, du i øjeblikket er tilsluttet til, har SecurityCenter, bliver du medlem af netværket og bliver bedt om at angive, om du har tillid til netværket. Hvis computeren er den første, der tilsluttes til netværket, inkluderes dens navn i netværksnavnet, men du kan til enhver tid omdøbe netværket.

Når en computer opretter forbindelse til netværket, sendes en anmodning om tilladelse til tilslutning til alle andre computere, der i øjeblikket er på netværket. Tilladelsen kan gives af alle computere på netværket, som har administratorrettigheder. Tildeleren kan også afgøre tilladelsesniveauet for den computer, der i øjeblikket tilslutter til netværket, f.eks. gæst (kun filoverførselsfunktion) eller fuld/administrator (filoverførsels- og fildelingsfunktion). I EasyNetwork kan computere med administratoradgang give adgang til andre computere og administrere rettigheder (dvs. forfremme eller degradere computere). Computere med fuld adgang kan ikke udføre disse administrative opgaver.

Bemærk! Hvis computeren har andre McAfee-netværksprogrammer installeret (f.eks. EasyNetwork), vil computeren også blive anerkendt som administreret computer af disse programmer, når den er blevet medlem af netværket. Det niveau af rettigheder, der tildeles til en computer i EasyNetwork, gælder for alle McAfee-netværksprogrammer. Yderligere oplysninger om, hvad rettighedsniveauerne gæst, fuld og administrator betyder for andre McAfee-netværksprogrammer, finder du i den medfølgende dokumentation for det enkelte program.

Tilslutte til netværket

Når en computer opretter forbindelse til et pålideligt netværk første gang efter installationen af EasyNetwork, vises en meddelelse, der spørger om du vil tilslutte din computer til det administrerede netværk. Når computeren siger ja til at tilslutte, sendes en anmodning til alle andre computere på netværket, som har administratoradgang. Denne anmodning skal imødekommes, før computeren kan dele printere eller filer eller sende og kopiere filer på netværket. Den første computer på netværket tildeles automatisk administratortilladelser.

1. Klik på **Tilslut til dette netværk** i vinduet Delte filer. Når en administratorcomputer i netværket giver tilladelse til tilslutning, vises en meddelelse, der spørger, om du vil tillade denne og andre computere på netværket at administrere hinandens sikkerhedsindstillinger.
2. Klik på **OK** for at give denne og andre computere på netværket tilladelse til at administrere hinandens sikkerhedsindstillinger. Ellers klik på **Annuller**.
3. Bekræft, at den computer, der giver tilladelsen, viser de spillekort, der i øjeblikket vises i dialogboksen til sikkerhedsbekræftelse, og klik derefter på **OK**.

Bemærk! Hvis den computer, der inviterede dig til at deltage i det administrerede netværk, ikke viser de samme spillekort som i dialogboksen til bekræftelse af sikkerheden, er der sket et sikkerhedsbrud på det administrerede netværk. Det kan være risikabelt at tilslutte computeren til netværket. Derfor skal du klikke på **Annuller** i dialogboksen til bekræftelse af sikkerheden.

Give adgang til netværket

Når en computer anmoder om at blive tilsluttet til det administrerede netværk, sendes en meddelelse til de andre computere på netværket, der har administratoradgang. Den første computer, der svarer på meddelelsen, bliver tildeleren. Som tildeler er du ansvarlig for at afgøre, hvilken type adgang computeren skal have: gæst, fuld eller administrator.

1. Klik på det relevante adgangsniveau i beskeden.
2. I dialogboksen Inviter en computer til at deltage i dette administrerede netværk skal du gøre et af følgende:
   - Klik på **Giv gæsteadgang til administrerede netværksprogrammer** for at give computeren adgang til netværket (du kan bruge denne indstilling for midlertidige brugere i dit hjem).
   - Klik på **Giv fuld adgang til administrerede netværksprogrammer** for at give computeren adgang til netværket.
   - Klik på **Giv administratoradgang til administrerede netværksprogrammer** for at give computeren adgang til netværket med administratorrettigheder. Det giver også computeren adgang til at tildele adgangstilladelser til andre computere, der ønsker at deltage i det administrerede netværk.
3. Klik på **OK**.
4. Bekræft, at computeren viser de spillekort, der i øjeblikket vises i dialogboksen til sikkerhedsbekræftelse, og klik derefter på **Tildel adgang**.

Bemærk! Hvis computeren ikke viser de samme spillekort, som vises i dialogboksen til sikkerhedsbekræftelse, har der været en sikkerhedsbrist i det administrerede netværk. Det kan derfor udsætte din computer for risiko at give denne computer adgang til netværket, og du bør i stedet klikke på **Afvis adgang** i dialogboksen til sikkerhedsbekræftelse.

Omdøbe netværket

Som standard inkluderer netværksnavnet navnet på den første computer, der tilsluttede til det. Du kan dog til enhver tid ændre netværksnavnet. Når du omdøber netværket, ændrer du den netværksbeskrivelse, der vises i EasyNetwork.

1. Klik på **Konfigurer** i menuen **Indstillinger**.
2. Angiv navnet på netværket i feltet **Netværksnavn** i dialogboksen til konfiguration.
3. Klik på **OK**.

Forlade et administreret netværk

Hvis du tilslutter til et administreret netværk og derefter beslutter, at du ikke længere vil være medlem, kan du forlade netværket. Når du har forladt det administrerede netværk, kan du altid tilslutte dig igen. Så skal du dog have tilladelse igen. Flere oplysninger om at tilslutte sig finder du under Tilslutte til et administreret netværk (side 228).

Forlade et administreret netværk

Du kan forlade et administreret netværk, som du tidligere har tilsluttet til.

1. Afbryd forbindelsen mellem computeren og netværket.
2. Klik på **Forlad netværk** i menuen **Værktøjer** i EasyNetwork.
3. Vælg navnet på det netværk, du vil forlade, i dialogboksen Forlad netværk.
4. Klik på **Forlad netværk**.

KAPITEL 49

Dele og sende filer

EasyNetwork gør det nemt at dele og sende filer på computeren mellem andre computere på netværket. Når du deler filer, giver du andre computere læseadgang til disse filer. Det er kun computere, der er medlemmer af det administrerede netværk (dvs. med fuld eller administrativ adgang), der kan dele eller få adgang til filer, der deles af andre medlemscomputere.

Bemærk! Hvis du deler mange filer, kan det påvirke computerens ressourcer.

I dette kapitel

Dele filer

Det er kun computere, der er medlemmer af det administrerede netværk (dvs. med fuld eller administrativ adgang), der kan dele eller få adgang til filer, der deles af andre medlemscomputere. Hvis du deler en mappe, deles alle filer i denne mappe samt i undermapperne. Filer, der efterfølgende føjes til mappen, deles dog ikke automatisk. Hvis en delt fil eller mappe slettes, fjernes den automatisk fra vinduet Delte filer. Du kan til enhver til stoppe delingen af en fil.

Hvis du vil have adgang til en delt fil, skal du filen direkte fra EasyNetwork eller kopiere den til din computer og derefter åbne den. Hvis din liste over delte filer er lang, og det er svært at se, hvor filen er, kan du søge efter den.

Bemærk! Filer, der deles vha. EasyNetwork, kan ikke åbnes fra andre computere ved hjælp af Windows Stifinder, fordi EasyNetwork-fildeling skal ske via sikre forbindelser.

Dele en fil

Når du deler en fil, er den automatisk tilgængelig for alle andre medlemmer med fuld eller administrativ adgang til det administrerede netværk.

1. Find den fil, du vil dele, i Windows Stifinder.
2. Træk filen fra dens placering i Windows Stifinder til vinduet Delte filer i EasyNetwork.

Tip! Du kan også dele en fil ved at klikke på **Del filer** i menuen **Værktøjer**. Gå til den mappe i dialogboksen til fildeling, hvor filen, du vil dele, er gemt, marker filen, og klik derefter på **Del**.

Stoppe deling af en fil

Hvis du deler en fil i det admininstrerede netværk, kan du til enhver tid stoppe delingen. Når du stopper delingen af en fil, kan andre medlemmer af det administrerede netværk ikke længere åbne den.

1. Klik på **Stop deling af filer** i menuen **Værktøjer**.
2. Marker den fil, du ikke længere vil dele, i dialogboksen Stop deling af filer
3. Klik på **OK**.

Kopiere en delt fil

Du kan kopiere en delt fil, så du stadig har den, når den ikke længere er delt. Du kan kopiere en delt fil fra enhver computer i det administrerede netværk.

- Træk en fil fra vinduet Delte filer i EasyNetwork til en placering i Windows Stifinder eller til Windows-skrivebordet.

Tip! Du kan også kopiere en delt fil ved at vælge filen i EasyNetwork og derefter klikke på **Kopier til** i menuen **Værktøjer**. Gå til mappen, som filen skal kopieres til, i dialogboksen til kopiering til mappe, marker mappen, og klik derefter på **Gem**.

Søge efter en delt fil

Du kan søge efter en fil, der er blevet delt af dig selv eller ethvert andet netværksmedlem. Når du angiver søgekriterierne, viser EasyNetwork automatisk de tilsvarende resultater i vinduet Delte filer.

1. Klik på **Søg** i vinduet Delte filer.
2. Klik på den relevante indstilling (side 235) på listen **Indeholder**.
3. Angiv en del af filnavnet, hele filnavnet eller stien på listen **Fil- eller stinavn**.
4. Klik på den relevante filtype (side 235) på listen **Type**.
5. Klik på de datoer på listerne **Fra** og **Til**, der angiver det datointerval, som filen blev oprettet inden for.

Søgekriterier

I følgende tabeller beskrives de søgekriterier, du skal angive, når du søger efter delte filer.

Navn på fil eller sti

Indeholder	Beskrivelse
Indeholder alle ordene	Søger efter fil- eller stinavne, der indeholder alle de ord, du angiver på listen **Fil- eller stinavn** i vilkårlig rækkefølge.
Indeholder et af ordene	Søger efter fil- eller stinavne, der indeholder et eller flere af de ord, du angiver på listen **Fil- eller stinavn**.
Indeholder den nøjagtige streng	Søger efter fil- eller stinavne, der indeholder det præcise udtryk, du angiver på listen **Fil- eller stinavn**.

Filtype

Type	Beskrivelse
Alle	Søger i alle typer delte filer.
Dokument	Søger i alle delte dokumenter.
Billede	Søger i alle delte billedfiler.
Video	Søger i alle delte videofiler.
Audio	Søger i alle delte audiofiler.
Komprimeret	Søger i alle komprimerede filer (f.eks. .zip-filer).

Sende filer til andre computere

Du kan sende filer til andre computere, der er medlemmer af det administrerede netværk. Før du sender en fil, bekræfter EasyNetwork, at den computer, der skal modtage filen, har tilstrækkelig fri diskplads.

Når du modtager en fil, vises den i EasyNetwork-indbakken. Indbakken er en midlertidig lagerplacering for alle filer, der sendes til dig af andre computere på netværket. Hvis du har EasyNetwork åben, når du modtager en fil, vises filen straks i indbakken. Ellers vises en besked i meddelelsesområdet til højre på Windows-proceslinjen. Hvis du ikke ønsker at modtage beskeder, kan du slå dem fra (hvis de f.eks. afbryder dit arbejde). Hvis der allerede findes en fil med det samme navn i indbakken, omdøbes den nye fil med et numerisk suffiks. Filerne bliver i indbakken, indtil du accepterer dem (dvs. kopierer dem til en placering på computeren).

Sende en fil til en anden computer

Du kan sende en fil direkte til en anden computer i det administrerede netværk uden at dele den. Før en bruger på den modtagende computer kan se filen, skal den gemmes lokalt. Flere oplysninger finder du i Acceptere en fil fra en anden computer (side 237).

1. Find den fil, du vil sende, i Windows Stifinder.
2. Træk filen fra dens placering i Windows Stifinder til et aktivt computerikon i EasyNetwork.

Tip! Du kan sende flere filer til en computer ved at holde CTRL-tasten nede, mens du vælger filerne. Du kan også sende filer ved at klikke på **Send** i menuen **Værktøjer**, vælge filerne og derefter klikke på **Send**.

Acceptere en fil fra en anden computer

Hvis en anden computer i det administrerede netværk sender en fil til dig, skal du acceptere den ved at gemme den på din computer. Hvis EasyNetwork ikke er åben eller ligger i forgrunden, når der sendes en fil til din computer, modtager du en besked i meddelelsesområdet til højre for proceslinjen. Klik på beskeden for at åbne EasyNetwork og åbne filen.

- Klik på **Modtaget**, og træk derefter filen fra EasyNetwork-indbakken til en mappe i Windows Stifinder.

Tip! Du kan også modtage en fil fra en anden computer ved at vælge filen i EasyNetwork-indbakken og derefter klikke på **Accepter** i menuen **Værktøjer**. I dialogboksen Accepter til mappe, skal du navigere til den mappe, hvor du vil gemme de filer, du modtager, markere mappen, og derefter klikke på **Gem**.

Modtage besked, når en fil er sendt

Du kan modtage en besked, når en anden computer i det administrerede netværk sender en fil til dig. Hvis EasyNetwork ikke kører, vises beskeden i meddelelsesområdet længst til højre på proceslinjen.

1. Klik på **Konfigurer** i menuen **Indstillinger**.
2. Marker afkrydsningsfeltet **Giv mig besked, når en anden computer sender mig filer** i konfigurationsdialogboksen.
3. Klik på **OK**.

KAPITEL 50

Dele printere

Når du har tilsluttet til et administreret netværk, deler EasyNetwork automatisk alle lokale printere, der er knyttet til computeren, og bruger printerens aktuelle navn som navnet på den delte printer. EasyNetwork registrerer også printere, der deles af andre computere på netværket, og giver dig mulighed for at konfigurere og bruge disse printere.

Hvis du har konfigureret en printerdriver til at udskrive gennem en netværksprinterserver (f.eks. en trådløs USB-printerserver), opfatter EasyNetwork printeren som en lokal printer og deler den automatisk på netværket. Du kan til enhver tid stoppe delingen af en printer.

I dette kapitel

Arbejde med delte printere

EasyNetwork registrerer printere, der deles af alle de andre computere på netværket. Hvis EasyNetwork registrerer en fjernprinter, der ikke allerede er knyttet til computeren, vises linket **Tilgængelige netværksprintere** i vinduet Delte filer, når du åbner EasyNetwork første gang. Dette gør det muligt for dig at installere tilgængelige printere eller afinstallere printere, der allerede er tilknyttet computeren. Du kan også opdatere listen over printere for at sikre, at opdaterede oplysninger vises.

Hvis du ikke har tilsluttet til det administrerede netværk, men er forbundet til det, kan du få adgang til de delte printere fra printerkontrolpanelet i Windows.

Stoppe deling af en printer

Når du stopper delingen af en printer, kan medlemmerne ikke bruge den.

1. Klik på **Printere** i menuen **Værktøjer**.
2. Klik på navnet på den printer, du ikke længere vil dele, i dialogboksen Administrer netværksprintere.
3. Klik på **Ophæv deling**.

Installere en tilgængelig netværksprinter

Hvis du er medlem af det administrerede netværk, kan du få adgang til de printere, der deles. Du skal dog installere den printerdriver, der bruges af printeren. Hvis ejeren af printeren stopper delingen af printeren, kan du ikke bruge den.

1. Klik på **Printere** i menuen **Værktøjer**.
2. Klik på et printernavn i dialogboksen med tilgængelige netværksprintere.
3. Klik på **Installer**.

Reference

Ordlisten viser og definerer de mest almindeligt anvendte sikkerhedstermer, der findes i McAfees produkter.

Ordliste

8

802.11

Et sæt standarder for overførsel af data via et trådløst netværk. 802.11 kaldes ofte Wi-Fi.

802.11a

En udvidelse af 802.11, der overfører data med op til 54 Mbps over 5 GHz-båndet. Selvom overførselshastigheden er hurtigere end 802.11b, er den afstand, der dækkes, meget mindre.

802.11b

En udvidelse af 802.11, der overfører data med op til 11 Mbps over 2,4 GHz-båndet. Selvom overførselshastigheden er langsommere end 802.11a, er den afstand, der dækkes, større.

802.1x

En standard for godkendelse på faste og trådløse netværk. 802.1x bruges ofte med 802.11 trådløst netværk. Se også godkendelse (side 245).

A

ActiveX-objekt

En softwarekomponent, der bruges af programmer eller websider til at tilføje funktionalitet, der fremstår som en normal del af programmet eller websiden. De fleste ActiveX-objekter er harmløse, men der er dog nogle, som kan opsnappe oplysninger fra din computer.

adgangskode

En kode (der normalt består af bogstaver og tal), som du bruger til at få adgang til computeren, et program eller et websted.

adgangskodeboks

Et sikkert lagringsområde til dine personlige adgangskoder. Den giver dig mulighed for at opbevare dine adgangskoder, så der er tillid til, at ingen andre brugere kan få adgang til dem (heller ikke en administrator).

adgangspunkt (access point - AP)

En netværksenhed (ofte kaldet en trådløs router), der tilsluttes en Ethernet-hub eller -switch for at udvide den fysiske tjenesteradius for en trådløs bruger. Når trådløse brugere roamer med deres mobilenheder, skifter overførslen fra et adgangspunkt til et andet for at opretholde forbindelsen.

almindelig tekst

Tekst, som ikke er krypteret. Se også kryptering (side 246).

arkivere

At oprette en kopi af vigtige filer på cd, dvd, USB-drev, ekstern harddisk eller netværksdrev. Sammenlign med back up (side 251).

B

browser

Et program, der bruges til at få vist websider på internettet. Populære webbrowsere omfatter Microsoft Internet Explorer og Mozilla Firefox.

bufferoverløb

En tilstand, der opstår i et operativsystem eller et program, når mistænkelige programmer eller processer forsøger at gemme flere data i en buffer (opbevaringsområde for midlertidige data), end der er plads til. Bufferoverløb beskadiger hukommelsen, eller overskriver data i nærliggende buffere.

båndbredde

Mængden af data (gennemløb), som kan transmitteres inden for et fastlagt tidsrum.

C

cache

Et midlertidigt opbevaringsområde på din computer til ofte eller for nylig åbnede data. For at øge hastigheden og effektiviteten på din internetsøgning kan din browser f.eks. hente en webside fra sin cache-mappe (i stedet for fra en fjernserver), næste gang du vil have den vist.

cookie

En lille tekstfil, der bruges af mange websteder til at opbevare oplysninger om besøgte sider, som gemmes på computeren af personer, som surfer på internettet. Den kan f.eks. indeholde login- eller registreringsoplysninger, oplysninger om indkøbsvogn eller brugerdefinerede indstillinger. Cookies bruges hovedsagelig af websider til at identificere brugere, som tidligere har registreret sig på eller besøgt siden. De kan dog også fungere som en informationskilde for hackere.

D

DAT

Registreringsdefinitionsfiler, også kaldet virusdefinitioner, som indeholder definitioner, som identificerer, finder og reparerer virus, trojanske heste, spyware, adware og andre potentielt uønskede programmer (PUP).

dele

At give e-mail-modtagere adgang til udvalgte sikkerhedskopierede filer i et begrænset stykke tid. Når du deler en fil, sender du sikkerhedskopien af filen til de e-mail-modtagere, som du angiver. Modtagerne får en e-mail-meddelelse fra Backup og Restore, der angiver, at filerne er blevet delt med dem. Denne e-mail indeholder også et link til de delte filer.

delt hemmelighed (shared secret)

En streng eller nøgle (normalt en adgangskode), som to parter, der kommunikerer med hinanden, har udvekslet, inden kommunikationen blev initieret. Bruges til at beskytte følsomme dele af RADIUS-meddelelser. Se også RADIUS (side 250).

denial of service-angreb (DOS)

En type angreb mod en computer, server eller et netværk, som bremser eller stopper netværkstrafikken. Det forekommer, når et netværk oversvømmes af så mange anmodninger, at almindelig trafik bremses eller afbrydes helt. Et denial of service-angreb overbebyrder sit mål med falske forbindelsesanmodninger, så målet ignorerer legitime anmodninger.

DNS

Domain Name System Et databasesystem, som oversætter en IP-adresse, f.eks. 11.2.3.44 til et domænenavn, f.eks. www.mcafee.com.

domæne

Et lokalt undernetværk eller en deskriptor for websteder på internettet. På et lokalt netværk (LAN) er et domæne et undernetværk bestående af klient- og servercomputere, der kontrolleres af én sikkerhedsdatabase. Et domæne udgør en del af alle websteder på internettet. F.eks. udgør mcafee domænet i www.mcafee.com.

E

e-mail

Elektronisk post. Meddelelser, der sendes og modtages elektronisk via et computernetværk. Se også webmail (side 253).

e-mail-klient

Et program, du kører på computeren for at sende og modtage e-mail (f.eks. Microsoft Outlook).

ekstern harddisk

En harddisk, som befinder sig uden for computeren.

ESS

Extended service set. To eller flere netværk, der udgør et undernetværk.

F

filfragmenter

Rester af en fil, der er spredt ud over disken. Filfragmentering sker, når filer tilføjes eller slettes, og kan sænke computerens effektivitet.

firewall

Et system (hardware, software eller begge dele), som er designet til at blokere uønsket adgang til eller fra et privat netværk. Firewalls bliver ofte brugt til at forhindre uautoriserede internetbrugere i at få adgang til private netværk, der har forbindelse til internettet, specielt intranet. Alle meddelelser, der modtages eller sendes fra intranettet, går gennem firewallen, som undersøger hver meddelelse og blokerer dem, som ikke opfylder de angivne sikkerhedskrav.

frit adgangspunkt

Et uautoriseret adgangspunkt Frie adgangspunkter kan installeres på et sikkert virksomhedsnetværk for at tildele netværksadgang til uautoriserede personer. De kan også oprettes for at tillade en angriber at gennemføre et smørklat-angreb.

G

genvej

En fil, der kun indeholder placeringen af en anden fil på computeren.

godkendelse

Bekræftelse af digital identitet af senderen af elektronisk kommunikation.

H

hjemmenetværk

To eller flere computere, der er forbundet i et hjem, så de kan dele filer og internetadgang. Se også LAN (side 246).

hotspot

Et geografisk område, der er dækket af et Wi-Fi (802.11)-adgangspunkt (AP). Brugere, der går ind i et hotspot med en trådløs bærbar computer, kan oprette forbindelse til internettet, hvis det pågældende hotspot sender signaler (beaconing), dvs. annoncerer dets tilstedeværelse, og godkendelse ikke er påkrævet. Hotspots er ofte placeret i områder med mange mennesker, f.eks. lufthavne.

hændelse

En hændelse eller forekomst i et system eller program, som kan opdages af sikkerhedssoftware på baggrund af foruddefinerede kriterier. En hændelse vil typisk udløse en handling såsom afsendelse af en påmindelse eller tilføjelse af en post til en hændelseslogfil.

I

indholdsbedømmelsesgruppe

De aldersgrupper, som en bruger hører ind under, i Forældrestyring. Indhold gøres tilgængeligt eller blokeres ud fra den indholdsbedømmelsesgruppe, brugeren tilhører. Indholdsbedømmelsesgrupperne omfatter: små børn, større børn, ung teenager, ældre teenager og voksen.

integreret gateway

En enhed, som kombinerer funktionerne fra et adgangspunkt (AP), en router og en firewall. Visse enheder kan også indeholde sikkerhedsforbedringer og brobyggende funktioner.

intranet

Et privat computernetværk normalt inden for en organisation, der kun kan benyttes af autoriserede brugere.

IP-adresse

Internet Protocol-adresse. En adresse, som bruges til at identificere en computer eller en enhed på et TCP/IP-netværk. En IP-adresses format er en 32-bit numerisk adresse, der er skrevet som fire tal adskilt af punktummer. Hvert tal kan være fra 0 til 255 (f.eks. 192.168.1.100).

IP-forfalskning

At forfalske IP-adresserne i en IP-pakke. Dette bliver brugt i mange typer angreb som f.eks. sessionskapring. Det bliver også brugt til at forfalske meddelelsesoverskrifterne i spam-beskeder, så de ikke kan spores korrekt.

K

karantæne

Påtvungen isolation af en fil eller en mappe, der mistænkes for at indeholde virus, spam, mistænkeligt indhold eller potentielt uønskede programmer (PUP'er), som gør, at filen eller mappen ikke kan åbnes eller køres.

klient

Et program, der kører på en pc eller en arbejdsstation, og som er afhængig af en server til visse opgaver. For eksempel er en e-mail-klient et program, der gør det muligt for dig at sende og modtage e-mail.

komprimering

En proces, der komprimerer filer til en form, som minimerer pladsbehovet til opbevaring eller overførsel.

krigschauffør (wardriver)

En person, der søger efter Wi-Fi (802.11)-netværk ved at køre gennem byer bevæbnet med en Wi-Fi-computer og speciel hardware eller software.

krypteret tekst

Krypterede data. Krypteret tekst er ulæselig, indtil den er blevet konverteret til almindelig tekst (dekrypteret). Se også kryptering (side 246).

kryptering

En metode til kodning af oplysninger for at forhindre uautoriseret adgang. Når oplysningerne er kodede, bruges der en "nøgle" og matematiske algoritmer. Krypterede oplysninger kan ikke dekrypteres uden den rette nøgle. Virus benytter sig nogle gange af kryptering i et forsøg på at undgå at blive registreret.

L

LAN

Lokalt netværk. Et computernetværk, som dækker et relativt lille område (f.eks. en enkelt bygning). Computere på et LAN kan kommunikere indbyrdes og dele ressourcer, f.eks. printere og filer.

launchpad

En U3-grænsefladekomponent, der fungerer som startpunkt for start og administration af U3 USB-programmer.

liste med elementer, der er tillid til

En liste med elementer, du har tillid til, og som ikke registreres. Hvis du kommer til at tilføje et element (f.eks. et potentielt uønsket program), eller du ønsker, at et program igen skal registreres, skal du fjerne det fra denne liste.

M

MAC-adresse

Media Access Control-adresse. Et entydigt serienummer, som er tilknyttet en fysisk enhed (netværksgrænsefladekort, NIC) med adgang til netværket.

MAPI

Messaging Application Programming Interface. En Microsoft-grænsefladespecifikation, som tillader forskellige meddelelsessystemer og arbejdsgruppeprogrammer (herunder e-mail, voicemail og fax) at fungere gennem en enkelt klient, såsom Exchange-klienten.

message authentication code (MAC)

En sikkerhedskode, der bruges til at kryptere meddelelser, der sendes mellem computere. Meddelelsen accepteres, hvis computeren genkender den afkrypterede kode som gyldig.

midlertidig fil

En fil, der er oprettet i hukommelse eller på disken af operativsystemet eller et andet program, og som skal bruges under en session og derefter kasseres.

MSN

Microsoft Network. En gruppe af webbaserede tjenester fra Microsoft Corporation, herunder søgemaskine, e-mail, onlinemeddelelser og portal.

N

netværk

En samling af IP-baserede systemer (såsom routere, omskiftere, servere og firewalls), som er grupperet som en logisk enhed. F.eks. kan et "økonominetværk" omfatte alle servere, routere og systemer som benyttes i en økonomiafdeling. Se også hjemmenetværk (side 245).

netværksdrev

En disk eller et bånd, som er forbundet til en server eller et netværk, der deles af flere brugere. Netværksdrev kaldes nogle gange for "fjerndrev".

netværkskort

En grafisk visning af de computere og komponenter, der udgør et hjemmenetværk.

NIC

Nætværksgrænsefladekort (Network Interface Card). Et kort, som kan sættes i en bærbar computer eller en anden enhed, og som tilslutter enheden til LAN-netværket.

node

En enkelt computer, der er tilsluttet et netværk.

nøgle

En række bogstaver og tal, som bruges af to enheder til at godkende deres kommunikation. Begge enheder skal have nøglen. Se også WEP (side 253), WPA (side 254), WPA2 (side 254), WPA2-PSK (side 254), WPA-PSK (side 254).

O

offentliggøre

At gøre en sikkerhedskopieret fil offentligt tilgængelig på internettet. Du kan få adgang til offentliggjorte filer ved at søge i bibliotekerne Backup og Restore.

opkaldsprogrammer

Software, der omdirigerer internetforbindelser til en anden part end brugerens standardinternetudbyder (Internet service provider, ISP) for at skabe yderligere tilslutningsgebyrer for en indholdsudbyder, leverandør eller tredjepart.

ordbogsangreb

En type råstyrkeangreb, der bruger almindelige ord til at afsløre en adgangskode.

orm

En virus, som spredes ved, at den kopierer sig selv til andre drev, systemer eller netværk. En mass-mailing-orm kræver handling fra brugeren for at kunne spredes, via f.eks. åbning af en vedhæftet fil eller ved at køre en dowloadet fil. Størstedelen af e-mail-virus i dag er orme. En selvforplantende orm kræver ingen handling fra brugerens side for at spredes. Eksempler på selvforplantende orme er Blaster og Sasser.

overvågede filtyper

De filtyper (f.eks. .doc, .xls), som Backup og Restore sikkerhedskopierer eller arkiverer inden for overvågningsplaceringerne.

overvågningsplaceringer

De mapper, som Backup og Restore overvåger på computeren.

P

Papirkurv

Et simuleret affaldsspand til slettede filer og mapper i Windows.

phishing

En metode, hvor man på uhæderlig vis indsamler personlige oplysninger såsom adgangskoder, personnumre og kreditkortoplysninger ved at sende fup-e-mails, der ser ud, som om de kommer fra en pålidelig kilde, f.eks. en bank eller et legitimt firma. I en phishing-e-mail bliver man typisk bedt om at klikke på linket i e-mailen for at bekræfte eller opdatere kreditkortoplysninger.

plug-in

Et lille softwareprogram, som tilføjer funktioner til eller forbedrer et større stykke software. Plug-ins giver f.eks. internetbrowseren mulighed for at indlæse og køre filer, der er integreret i HTML-dokumenter, og som er i formater, som browseren normalt ikke ville genkende, f.eks. animationer, video og lydfiler.

pop op-vinduer

Små vinduer, som dukker op oven i andre vinduer på computerskærmen. Pop op-vinduer bruges ofte i internetbrowsere til at vise reklamer.

POP3

Post Office Protocol 3. En grænseflade mellem et e-mail-klientprogram og e-mail-serveren. De fleste hjemmebrugere har en POP3-e-mail-konto, der også kaldes en standard-e-mail-konto.

port

En hardwareplacering til at sende data til og fra en computerenhed. Pc'er har forskellige typer af porte, herunder interne porte til tilslutning af diskdrev, skærme og tastaturer og eksterne porte til tilslutning af modem, printere, mus og andre ydre enheder.

positivliste

En liste med websteder eller e-mailadresser, der betragtes som sikre. Websteder på positivlisten er dem som brugeren har adgang til. E-mail-adresser på positivlisten er fra kilder, der er tillid til, og som du ønsker at modtage. Sammenlign med sortliste (side 251).

potentielt uønsket program (PUP)

Et softwareprogram, som muligvis er uønsket, selvom brugeren muligvis har givet tilladelse til at hente det. Det kan ændre indstillingerne for sikkerhed eller beskyttelse af personlige oplysninger på den computer, hvor det er installeret. PUP'er kan indeholde, men indeholder ikke altid spyware, adware og opkaldsprogrammer, og kan hentes sammen med det program brugeren ønsker.

PPPoE

Point-to-Point Protocol Over Ethernet. En metode til at bruge opkaldsprotokollen Point-to-Point Protocol (PPP) med Ethernet som transport.

protokol

Et regelsæt, der gør det muligt for computere eller enheder at udveksle data. I en lagdelt netværksarkitektur (Open Systems Interconnection-model) har hvert enkelt lag sine egne protokoller, der angiver, hvordan der kommunikeres på det givne niveau. Computeren eller enheden skal understøtte den korrekte protokol, hvis du vil kommunikere med andre computere. Se også Open Systems Interconnection (OSI).

proxy

En computer (eller den software, der kører på den), der fungerer som en barriere mellem et netværk og internettet ved kun at vise en enkelt netværksadresse for eksterne websteder. Ved at repræsentere alle interne computere beskytter proxy'en netværksidentiteter og giver samtidig adgang til internettet. Se også proxyserver (side 250).

proxyserver

En firewall-komponent, der styrer internettrafik til og fra et LAN (lokalnetværk). En proxyserver kan forbedre ydeevnen ved at levere data, der hyppigt anmodes om, f.eks. en populær webside, og kan filtrere og afvise anmodninger, ejeren ikke accepterer, f.eks. anmodninger om uautoriseret adgang til beskyttede filer.

R

RADIUS

Remote Access Dial-In User Service. En protokol, som tillader godkendelse af brugere. Det er som regel i forbindelse med fjernadgang. Denne protokol blev oprindelig udviklet til brug med eksterne opkaldsservere, men bruges nu til en række godkendelsesmiljøer, f.eks 802.1x-godkendelse af en WLAN-brugers "delte hemmelighed" (Shared Secret). Se også delt hemmelighed.

registreringsdatabase

En database, der bruges af Windows til at opbevare konfigurationsoplysninger for hver enkelt bruger, systemhardware, installerede programmer og indstillinger for egenskaber. Databasen er opdelt i nøgler, som hver har en fastsat værdi. Uønskede programmer kan ændre værdien af registreringsdatabasenøgler eller skabe nye nøgler for at køre skadelige koder.

roaming

At gå fra dækningsområdet for et adgangspunkt til et andet uden afbrydelse i tjenesterne eller tab af forbindelse.

rootkit

En samling værktøjer (programmer), som giver en bruger administratoradgang til en computer eller et computernetværk. Rootkits kan indeholde spyware og andre potentielt uønskede programmer, der kan skabe yderligere sikkerheds- eller fortrolighedsrisici for data og personlige oplysninger på din computer.

router

En netværksenhed, som videresender datapakker fra et netværk til et andet. Routere læser hver enkelt indgående pakke og afgør, hvordan den skal videresendes ud fra kilde- og destinationsadresserne og aktuelle trafikforhold. En router kaldes også et adgangspunkt (AP).

råstyrkeangreb (brute-force attack)

En hacking-metode, der bruges til at finde adgangskoder eller krypteringsnøgler ved at afprøve enhver mulig kombination af karakterer, indtil de brydes.

S

scanning i realtid

At scanne filer og mapper for virus og andre aktiviteter, når de anvendes af dig eller din computer.

scanning på forespørgsel

En planlagt undersøgelse af udvalgte filer, programmer eller netværksenheder for at finde en trussel, svaghed eller en anden potentielt uønsket kode. Den kan foretages straks, på et planlagt tidspunkt i fremtiden eller med regelmæssigt planlagte mellemrum. Sammenlign med scanning ved åbning. Se også sårbarhed.

script

En liste over kommandoer, der kan udføres automatisk (dvs. uden brugerinteraktion). I modsætning til programmer lagres scripts oftest i almindeligt tekstformat og kompileres, hver gang de kører. Makroer og batchfiler kaldes også scripts.

server

En computer eller et program, der accepterer forbindelser fra andre computere eller programmer og returnerer passende svar. Dit e-mail-program opretter f.eks. forbindelse til en e-mail-server, hver gang du sender eller modtager e-mail.

sikkerhedskopiere

At oprette en kopi af vigtige filer, typisk på en sikker onlineserver. Sammenlign med arkiv (side 242).

smart drive

Se USB-drev (side 253).

SMTP

Simple Mail Transfer Protocol. En TCP/IP-protokol til at sende beskeder fra en computer til en anden via et netværk. Denne protokol bruges på internettet til at route e-mail.

smørklat-angreb (man-in-the-middle attack)

En metode til at opfange og muligvis modificere meddelelser mellem to parter, uden at nogen af parterne ved, at deres kommunikationslink er blevet brudt.

sortliste

En liste med e-mail-adresser i Anti-Spam, som du ikke ønsker at modtage meddelelser fra, fordi du tror, det vil være spam. En liste over websteder, som bliver anset for at være bedrageriske, i forbindelse med anitphishing. Sammenlign med positivliste (side 249).

SSID

Service Set Identifier. En token (hemmelig nøgle), der identificerer et Wi-Fi (802.11)-netværk. SSID konfigureres af netværksadministratoren og skal angives af brugere, der ønsker at komme på netværket.

SSL

Secure Sockets Layer. En protokol, som Netscape har udviklet til at transmittere private dokumenter via internettet. SSL virker ved at bruge en offentlig nøgle til at kryptere data, som så overføres over SSL-forbindelsen. URL'er, der kræver en SSL-forbindelse, starter med HTTPS i stedet for HTTP.

standard-e-mail-konto

Se POP3 (side 249).

synkronisere

At fjerne uoverensstemmelser mellem sikkerhedskopierede filer og de filer, der er gemt på den lokale computer. Du synkroniserer filer, når versionen i sikkerhedskopieringslagret er nyere end den version, som måtte findes på andre computere.

Systembeskyttelse

McAfee-alarmer, der registrerer uautoriserede ændringer på computeren og underretter dig, når de opstår.

systemgendannelsespunkt

Et øjebliksbillede af indholdet af computerens hukommelse eller en database. Windows opretter regelmæssigt gendannelsespunkter og ved vigtige systemhændelser (f.eks. når et program eller en driver installeres). Du kan også oprette og navngive dine egne gendannelsespunkter når som helst.

T

TKIP

Temporal Key Integrity Protocol (udtales tee-kip). En del af 803.11i-krypteringsstandarden for trådløse lokalnetværk. TKIP er næste generation af WEP, som bruges til at sikre trådløse 802.11-lokalnetværk. TKIP giver nøgleblanding pr. pakke, et beskedintegritetscheck og en nøgleomdannelsesmekanisme og udbedrer dermed WEPs mangler.

Trojanske heste

Et program, som ikke kopierer sig selv, men som forårsager skade eller kompromitterer computerens sikkerhed. Det vil typisk være en person, som sender en trojansk hest. Den sender ikke sig selv. Du kan også, uden du er vidende om det, downloade en trojansk hest fra et websted eller via peer-to-peer-netværk.

trådløs adapter

En enhed, der føjer trådløs funktionalitet til en computer eller PDA. Den tilsluttes via en USB-port, PC Card-slot (CardBus), hukommelseskortslot eller internt i PCI-bussen.

Trådløst PCI-adapterkort

Peripheral Component Interconnect. Et trådløst adapterkort, der sættes i en PCI-udvidelsesport i computeren.

Trådløst USB-adapterkort

Et trådløst adapterkort, der sættes i en USB-indgang i computeren.

U

U3

Dig: Forenklet, smartere, mobil. En platform, der kører Windows 2000- eller Windows XP-programmer direkte fra et USB-drev. U3-initiativet blev grundlagt i 2004 af M-Systems og SanDisk og giver brugere mulighed for at køre U3-programmer på en Windows-computer uden at installere eller lagre data eller indstillinger på computeren.

URL-adresse

Uniform Resource Locator. Standardformatet for internetadresser

USB

Universal Serial Bus. Et standardstik på de fleste moderne computere, som forbinder en række enheder, lige fra tastaturer og mus til webcams, scannere og printere.

USB-drev

Et lille hukommelsesdrev, der sættes i en computers USB-port. Et USB-drev fungerer som et lille diskdrev og gør det nemt at overføre filer fra en computer til en anden.

V

virus

Et computerprogram, der kan kopiere sig selv og inficere en computer uden brugerens tilladelse eller vidende.

VPN

Virtual Private Network. Et privat kommunikationsnetværk, der konfigureres gennem et værtsnetværk såsom internettet. De data, der sendes via en VPN-forbindelse er krypterede og besidder stærke sikkerhedsforanstaltninger.

W

web bugs

Små grafikfiler, som kan lejre sig i dine HTML-sider og give en uautoriseret kilde mulighed for at gemme cookies på din computer. Disse cookies kan overføre oplysninger til den uautoriserede kilde. Web bugs kendes også som websignaler, pixel tags, gennemsigtige GIF'er eller usynlige GIF'er.

webmail

Web-baseret post. Elektronisk mailtjeneste, som åbnes via en webbrowser og ikke gennem en computerbaseret e-mail-klient som f.eks. Microsoft Outlook. Se også e-mail (side 244).

WEP

Wired Equivalent Privacy. En protokol til kryptering og godkendelse, der er defineret som en del af standarden for Wi-Fi (802.11). De første versioner er baseret på RC4-koder og har betydelige svagheder. WEP forsøger at give sikkerhed ved at kryptere data over radiobølger, så de bliver beskyttet under transmissionen fra et endepunkt til et andet. Det er imidlertid blevet opdaget, at WEP ikke er så sikkert, som man engang troede.

Wi-Fi

Wireless Fidelity. En term, der bruges af Wi-Fi Alliance for enhver type af 802.11-netværk.

Wi-Fi Alliance

En organisation, der udgøres af førende leverandører af trådløs hardware og software. Wi-Fi Alliance arbejder for at certificere alle 802.11-baserede produkter med hensyn til interoperabilitet og fremme termen Wi-Fi som det globale brand på tværs af alle markeder for alle 802.11-baserede trådløse LAN-produkter. Organisationen fungerer som konsortium, testlaboratorium og afregningskontor for forhandlere, som ønsker at promovere industriens vækst.

Wi-Fi Certified

At være testet og godkendt af Wi-Fi Alliance. Wi-Fi-certificerede produkter betragtes som havende indbyrdes kompatibilitet, selvom de kommer fra forskellige producenter. En bruger med et Wi-Fi-certificeret produkt kan bruge adgangspunkter af alle mærker sammen med ethvert andet mærke af klienthardware, så længe det også er certificeret.

WLAN

Trådløst lokalnetværk (Wireless Local Area Network) Et lokalt netværk med trådløs forbindelse. Et WLAN bruger højfrekvente radiobølger i stedet for ledninger til kommunikation mellem knudepunkter.

WPA

Wi-Fi Protected Access. En specifikationsstandard, som kraftigt forøger sikkerheden omkring databeskyttelse og adgangskontrol, både i eksisterende og fremtidige LAN-systemer. Er designet til at køre på eksisterende hardware som en softwareopgradering og er udledt af og kompatibel med 802.11i-standarden. Når den er installeret rigtigt, giver WPA-standarden trådløse LAN-brugere stor sikkerhed for, at deres data forbliver beskyttede, og at det kun er muligt for autoriserede netværksbrugere at få adgang til netværket.

WPA-PSK

En speciel WPA-tilstand udviklet til hjemmebrugere, som ikke kræver kraftfuld sikkerhed på virksomhedsniveau, og som ikke har adgang til godkendelsesservere. I denne tilstand kan hjemmebrugeren manuelt indtaste startadgangskoden, der aktiverer beskyttet Wi-Fi adgang i forhåndsdelt nøgletilstand, og bør regelmæssigt ændre adgangsfrasen på hver trådløs computer og adgangspunkt. Se også WPA2-PSK (side 254), TKIP (side 252).

WPA2

En opdatering af WPA-sikkerhedsstandarden, som er baseret på 802.11i-standarden.

WPA2-PSK

En særlig WPA-tilstand, der minder om WPA-PSK og er baseret på WPA2-standarden. En udbredt funktion i WPA2-PSK er, at enheder ofte understøtter flere krypteringsmetoder (f.eks. AES, TKIP) samtidig, mens ældre enheder generelt kun understøttede en enkelt krypteringsmetode ad gangen (dvs. at alle klienter var tvunget til at bruge samme krypteringsmetode).

Om McAfee

McAfee, Inc., som har hovedsæde i Santa Clara i Californien, er førende på markedet for løsninger til beskyttelse mod indtrængen og styring af sikkerhedsrisici og leverer proaktive og gennemprøvede løsninger og tjenester til sikring af systemer og netværk i hele verden. Med udgangspunkt i denne uovertrufne sikkerhedsekspertise og vilje til innovation kan McAfee give hjemmebrugere, virksomheder, den offentlige sektor og internetudbydere mulighed for at blokere angreb, undgå nedbrud og løbende følge op på og forbedre sikkerheden.

Licens

Copyright

KAPITEL 51

Kundeservice og teknisk support

SecurityCenter rapporterer kritiske og ikke-kritiske beskyttelsesproblemer, så snart de registreres. Kritiske beskyttelsesproblemer kræver øjeblikkelig handling og kompromitterer din beskyttelsesstatus (ændrer farven til rød). Ikke-kritiske beskyttelsesproblemer kræver ikke øjeblikkelig handling og muligvis kompromittere din beskyttelsesstatus (afhængigt af typen af problem). For at opnå grøn beskyttelsesstatus skal du løse alle kritiske problemer og enten løse eller ignorere alle ikke-kritiske problemer. Hvis du har brug for hjælp til at diagnosticere beskyttelsesproblemer, kan du køre McAfee Virtual Technician. Se Hjælp i McAfee Virtual Technician for at få flere oplysninger om McAfee Virtual Technician.

Hvis du har købt din sikkerhedssoftware fra en partner eller en anden leverandør end McAfee, skal du åbne en webbrowser og gå til www.mcafeehelp.com. Under Partner Links skal du vælge din partner eller leverandør for at få adgang til McAfee Virtual Technician.

Bemærk! Hvis du vil installere og køre McAfee Virtual Technician, skal du logge ind på din computer som Windows Administrator. Hvis du ikke gør det, kan MVT evt. ikke løse dine problemer. Du kan finde oplysninger om at logge ind som Windows Administrator i Windows Hjælp. I Windows Vista™ vises en meddelelse, når du kører MVT. Hvis det sker, skal du klikke på **Accepter**. Virtual Technician fungerer ikke med Mozilla® Firefox.

I dette kapitel

Brug af McAfee Virtual Technician

Som en personlig, teknisk supportmedarbejder indsamler Virtual Technician oplysninger om dine SecurityCenter-programmer for at hjælpe dig med at løse computerens sikkerhedsproblemer. Når du kører Virtual Technician, kontrollerer den, at dine SecurityCenter-programmer fungerer korrekt. Hvis den registrerer problemer, tilbyder Virtual Technician at løse dem for dig eller give dig flere detaljerede oplysninger om dem. Når Virtual Technician er færdig, vises resultaterne af analysen, og du kan søge yderligere teknisk support hos McAfee, hvis det er nødvendigt.

For at opretholde sikkerheden og integriteten for computeren og filerne indsamler Virtual Technician ikke personligt identificerbare oplysninger.

Bemærk! Klik på ikonet **Hjælp** i Virtual Technician for at få flere oplysninger om Virtual Technician.

Starte Virtual Technician

Virtual Technician indsamler oplysninger om dine SecurityCenter-programmer for at hjælpe dig med at løse computerens sikkerhedsproblemer. For at beskytte dine personlige oplysninger indeholder disse oplysninger ikke personligt identificerbare oplysninger.

1. Klik på **McAfee Virtual Technician** under **Almindelige opgaver**.
2. Følg anvisningerne på skærmen for at downloade og køre Virtual Technician.

Se følgende tabeller for oplysninger om McAfee Support- og Download-websteder i dit land eller område, herunder brugerhåndbøger.

Support og downloads

Land/område	McAfee Support	McAfee Downloads
Australien	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
Brasilien	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
Canada (engelsk)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Canada (fransk)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Danmark	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp

Finland	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
Frankrig	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
Grækenland	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Italien	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
Japan	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
Kina (forenklet kinesisk)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
Korea	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
Mexico	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
Norge	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
Polen	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
Portugal	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
Rusland	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
Slovakiet	www.mcafeehelp.com	de.mcafee.com/root/downloads.asp
Spanien	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
Storbritannien	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
Sverige	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
Taiwan	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
Tjekkiet	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
Tyrkiet	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
Tyskland	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
Ungarn	www.mcafeehelp.com	de.mcafee.com/root/downloads.asp
USA	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection-brugerhåndbøger

Land/område	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/da/MTP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
Frankrig	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
Grækenland	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Holland	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
Rusland	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slovakiet	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf

Sverige	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
Tjekkiet	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
Tyrkiet	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security-brugerhåndbøger

Land/område	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/da/MIS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
Frankrig	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
Grækenland	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
Holland	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf

Mexico	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
Rusland	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
Slovakiet	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
Tjekkiet	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
Tyrkiet	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus-brugerhåndbøger

Land/område	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/da/VSP_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf

Frankrig	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
Grækenland	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
Holland	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
Rusland	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
Slovakiet	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
Sverige	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
Tjekkiet	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
Tyrkiet	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan-brugerhåndbøger

Land/område	McAfee-brugerhåndbøger
Australien	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
Brasilien	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
Canada (engelsk)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
Canada (fransk)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
Danmark	download.mcafee.com/products/manuals/da/VS_userguide_2008.pdf
Finland	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
Frankrig	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
Grækenland	download.mcafee.com/products/manuals/el/VS_userguide_2008.pdf
Holland	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
Italien	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
Japan	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
Kina (forenklet kinesisk)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
Korea	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
Mexico	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
Norge	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
Polen	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
Portugal	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
Rusland	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
Slovakiet	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
Spanien	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
Storbritannien	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf

Sverige	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
Taiwan	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
Tjekkiet	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
Tyrkiet	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
Tyskland	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
Ungarn	download.mcafee.com/products/manuals/hu/VS_userguide_2008.pdf
USA	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

Se følgende tabel for oplysninger om McAfee Threat Center- og Virus Information-websteder i dit land eller område.

Land/område	Sikkerhedshovedkvarter	Virusoplysninger
Australien	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
Brasilien	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
Canada (engelsk)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Canada (fransk)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
Danmark	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
Finland	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
Frankrig	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
Grækenland	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
Holland	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
Italien	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
Japan	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
Kina (forenklet kinesisk)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo

Korea	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
Mexico	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
Norge	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
Polen	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
Portugal	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
Rusland	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
Slovakiet	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
Spanien	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
Storbritannien	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
Sverige	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
Taiwan	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
Tjekkiet	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
Tyrkiet	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
Tyskland	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
Ungarn	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
USA	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

Se følgende tabel for oplysninger om HackerWatch-websteder i dit land eller område.

Land/område	HackerWatch
Australien	www.hackerwatch.org
Brasilien	www.hackerwatch.org/?lang=pt-br
Canada (engelsk)	www.hackerwatch.org
Canada (fransk)	www.hackerwatch.org/?lang=fr-ca
Danmark	www.hackerwatch.org/?lang=da
Finland	www.hackerwatch.org/?lang=fi
Frankrig	www.hackerwatch.org/?lang=fr

Grækenland	www.hackerwatch.org/?lang=el
Holland	www.hackerwatch.org/?lang=nl
Italien	www.hackerwatch.org/?lang=it
Japan	www.hackerwatch.org/?lang=jp
Kina (forenklet kinesisk)	www.hackerwatch.org/?lang=zh-cn
Korea	www.hackerwatch.org/?lang=ko
Mexico	www.hackerwatch.org/?lang=es-mx
Norge	www.hackerwatch.org/?lang=no
Polen	www.hackerwatch.org/?lang=pl
Portugal	www.hackerwatch.org/?lang=pt-pt
Rusland	www.hackerwatch.org/?lang=ru
Slovakiet	www.hackerwatch.org/?lang=sk
Spanien	www.hackerwatch.org/?lang=es
Storbritannien	www.hackerwatch.org
Sverige	www.hackerwatch.org/?lang=sv
Taiwan	www.hackerwatch.org/?lang=zh-tw
Tjekkiet	www.hackerwatch.org/?lang=cs
Tyrkiet	www.hackerwatch.org/?lang=tr
Tyskland	www.hackerwatch.org/?lang=de
Ungarn	www.hackerwatch.org/?lang=hu
USA	www.hackerwatch.org

Indeks

N

O

P

R

S

T

U

V

W

Æ

Å