McAfee®

VirusScan® Plus 2007

AntiVirus, Firewall & AntiSpyware

Gebruikershandleiding

Inhoud

HOOFDSTUK 1

Inleiding

McAfee VirusScan Plus Suite beschermt uw computer en bestanden tegen virussen, spyware en hackers. U kunt veilig en vertrouwd op internet surfen en bestanden downloaden, omdat McAfee altijd waakzaam is, altijd up-to-date wordt gehouden en altijd bescherming biedt. De vertrouwde bescherming van McAfee blokkeert bedreigingen en ontmoedigt hackers automatisch, zodat uw computer gezond en veilig blijft. Met McAfee wordt het tevens gemakkelijk om de beveiligingsstatus weer te geven, een scan uit te voeren op virussen en spyware, en ervoor te zorgen dat uw producten up-to-date zijn met behulp van het nieuw ontworpen McAfee SecurityCenter. Bovendien ontvangt u automatisch de meest recente McAfee-software en -updates bij het abonnement.

VirusScan Plus omvat de volgende programma's:

- SecurityCenter
- VirusScan
- Personal Firewall
- Network Manager
- EasyNetwork (alleen met licentie voor 3 gebruikers)
- SiteAdvisor

HOOFDSTUK 2

McAfee SecurityCenter

McAfee SecurityCenter biedt een gebruiksvriendelijke omgeving waarin u een abonnement op beveiligingsservices kunt nemen, beheren en configureren.

Daarnaast is SecurityCenter dé informatiebron voor viruswaarschuwingen, productinformatie, ondersteuning en abonnementsgegevens en biedt het directe toegang tot hulpprogramma's en nieuws op de website van McAfee.

In dit hoofdstuk

Eigenschappen

McAfee SecurityCenter bevat de volgende nieuwe functies en voordelen:

Vernieuwde beveiligingsstatus

Hiermee is het gemakkelijk om de beveiligingsstatus van de computer te inspecteren, te controleren op updates en potentiële beveiligingsproblemen op te lossen.

Doorlopende updates en upgrades

Automatisch installeren van dagelijkse updates. Wanneer een nieuwe versie van McAfee-software beschikbaar is, ontvangt u die gedurende de looptijd van uw abonnement automatisch zonder kosten. Zo bent u er zeker van dat uw beveiliging altijd up-to-date is.

Real-time waarschuwingen

Door middel van beveiligingswaarschuwingen wordt u op de hoogte gebracht van nieuwe virusuitbraken en veiligheidsrisico's en krijgt u de mogelijkheid aangeboden de bedreigingen te verwijderen, te neutraliseren of er meer informatie over te lezen.

Gemakkelijke bescherming

Een verscheidenheid aan vernieuwingsopties helpt uw McAfee-beveiliging actueel te houden.

Hulpmiddelen voor prestatieverbetering

Verwijder bestanden die niet worden gebruikt, defragmenteer bestanden die wel worden gebruikt en gebruik de functie Systeemherstel om ervoor te zorgen dat uw computer maximale prestaties blijft leveren.

Echte online Help

Maak gebruik van de ondersteuning door McAfee's computerbeveiligingsexperts, via chatten, e-mail en telefoon.

Bescherming voor veilig surfen

Indien u de browserinvoegapplicatie McAfee SiteAdvisor hebt geïnstalleerd, beschermt deze functie u tegen spyware, spam, virussen en online zwendel door aan de websites die u bezoekt of die worden opgehaald als zoekresultaat een veiligheidsbeoordeling toe te kennen. U kunt de veiligheidskwalificatiegegevens bekijken die aangeven hoe een website uit de test komt voor wat betreft e-mailpraktijken, downloads, online koppelingen en ergernissen zoals pop-ups en cookietracering van derden.

HOOFDSTUK 3

SecurityCenter gebruiken

U kunt SecurityCenter starten door op het pictogram van McAfee SecurityCenter te klikken in het systeemvak van Windows, uiterst rechts op de taakbalk.

Wanneer u SecurityCenter opent, wordt in het deelvenster Startpagina de beveiligingsstatus van uw computer weergegeven en kunt u van hieruit snel updates, scans (als McAfee VirusScan is geïnstalleerd) en andere veel voorkomende taken uitvoeren:

Koptekst

Help

Het Help-bestand van het programma weergeven.

Linkerkolom

Bijwerken

Uw product bijwerken, zodat uw computer altijd is beveiligd tegen de nieuwste risico's.

Scannen

Als McAfee VirusScan is geïnstalleerd, kunt u een handmatige scan van uw computer uitvoeren.

Algemene taken

Van hieruit kunt u veel voorkomende taken uitvoeren, zoals terugkeren naar het deelvenster Startpagina, recente gebeurtenissen weergeven, uw computernetwerk beheren (als u werkt op een computer met beheerfuncties voor dit netwerk), en onderhoudstaken voor uw computer uitvoeren. Als McAfee Data Backup is geïnstalleerd, kunt u ook een back-up van uw gegevens maken.

Geïnstalleerde onderdelen

Hier kunt u zien met welke beveiligingsservices uw computer wordt beschermd.

Hoofdvenster

Beveiligingsstatus

Onder **Is mijn computer beveiligd?** wordt het algemene beveiligingsniveau van uw computer weergegeven. Daaronder vindt u statusgegevens, uitgesplitst in beschermingscategorie en -type.

SecurityCenter-informatie

Hier ziet u wanneer uw computer voor het laatst is bijgewerkt, wanneer de laatste scan heeft plaatsgevonden (als McAfee VirusScan is geïnstalleerd), en wanneer uw abonnement afloopt.

In dit hoofdstuk

Informatie over SecurityCenter-pictogrammen

SecurityCenter-pictogrammen worden weergegeven in het systeemvak van Windows, uiterst rechts op de taakbalk. Aan de hand van deze pictogrammen kunt u zien of uw computer volledig wordt beschermd, wat de status is van een scan in uitvoering (als McAfee VirusScan is geïnstalleerd), kunt u controleren of er updates beschikbaar zijn, uw computer onderhouden en ondersteuning krijgen van de McAfee-website.

SecurityCenter openen en extra functies gebruiken

Wanneer SecurityCenter actief is, wordt het pictogram met de M van het SecurityCenter weergegeven in het systeemvak van Windows, uiterst rechts op de taakbalk.

Ga als volgt te werk om SecurityCenter te openen en de extra functies te gebruiken:

- Klik met de rechtermuisknop op het SecurityCenter-hoofdpictogram en klik op een van de volgende opties:
  - SecurityCenter openen
  - Updates
  - Snelkoppelingen

    Het submenu bevat koppelingen naar de startpagina, naar Recente gebeurtenissen weergeven, Netwerk beheren, Computer onderhouden en Data Backup (indien dit is geïnstalleerd).
  - Abonnement controleren

    (Dit onderdeel wordt weergegeven wanneer het abonnement op minstens één product is verlopen.)
  - Upgradecentrum
  - Klantenservice

Uw beschermingsstatus controleren

Als uw computer niet volledig wordt beschermd, wordt het pictogram van de beveiligingsstatus weergegeven in het systeemvak van Windows, uiterst rechts op de taakbalk. Dit pictogram kan rood of geel zijn, afhankelijk van de beschermingsstatus.

Ga als volgt te werk om uw beveiligingsstatus te controleren:

- Klik op het pictogram van de beveiligingsstatus om het SecurityCenter te openen en eventuele problemen te verhelpen.

De status van uw updates controleren

Als u controleert of er updates beschikbaar zijn, wordt het pictogram updates weergegeven in het systeemvak van Windows, uiterst rechts op de taakbalk.

Ga als volgt te werk om de status van uw updates te controleren:

- Wijs naar het pictogram Updates om de status van uw updates als knopinfo weer te geven.

Informatie over de beveiligingsstatus

De algehele beveiligingsstatus van uw computer wordt in SecurityCenter weergegeven onder **Is mijn computer beveiligd?**.

De beveiligingsstatus biedt u informatie over de mate waarin uw computer is beveiligd tegen de nieuwste beveiligingsrisico's, geeft aan of er mogelijk problemen zijn die aandacht vereisen, en biedt u de mogelijkheid om deze problemen op te lossen. Wanneer een probleem is aangetroffen dat gevolgen heeft voor meerdere beveiligingscategorieën, kan het oplossen van het probleem ertoe leiden dat meerdere categorieën de status "volledig beveiligd" krijgen.

Enkele factoren die van invloed zijn op de beveiligingsstatus zijn externe veiligheidsrisico's, de beveiligingsproducten die op uw computer zijn geïnstalleerd, producten die verbinding maken met internet en de wijze waarop deze beveiligings- en internetproducten zijn geconfigureerd.

Standaard is het zo dat als Spambeveiliging of Inhoud blokkeren niet zijn geïnstalleerd, deze niet-essentiële beveiligingsproblemen automatisch worden genegeerd en niet worden gevolgd in de algehele beveiligingsstatus. Als er bij de melding van een beveiligingsprobleem echter een koppeling **Negeren** staat, kunt u ervoor kiezen om het probleem te negeren als u zeker weet dat u dit niet wilt herstellen.

Is mijn computer beveiligd?

Onder **Is mijn computer beveiligd?** in SecurityCenter ziet u het algemene beveiligingsniveau van uw computer:

- **Ja** wordt weergegeven als uw computer volledig wordt beschermd (groen).
- **Nee** wordt weergegeven als uw computer gedeeltelijk wordt beschermd (geel) of niet wordt beschermd (rood).

Klik op **Herstellen** naast de beveiligingsstatus. Hiermee worden de meeste beveiligingsproblemen automatisch verholpen. Als een of meer beveiligingsproblemen zich echter blijven voordoen en uw aandacht vereisen, klikt u op de koppeling naast het probleem om de voorgestelde actiestap te ondernemen.

Informatie over beschermingscategorieën en -typen

In SecurityCenter kunt u onder **Is mijn computer beveiligd?** statusgegevens weergeven, uitgesplitst in de volgende beschermingscategorieën en -typen:

- Computer en bestanden
- Internet en netwerk
- E-mail en expresberichten
- Ouderlijk toezicht

Welke beschermingstypen in SecurityCenter worden weergegeven, hangt af van de producten die zijn geïnstalleerd. Het beveiligingstype Pc-status wordt bijvoorbeeld weergegeven als de software van McAfee Data Backup is geïnstalleerd.

Als er in een bepaalde categorie geen beveiligingsproblemen zijn, is de status van deze categorie Groen. Als u op een Groene categorie klikt, wordt aan de rechterzijde een lijst weergegeven met geactiveerde beveiligingscategorieën, gevolgd door een lijst met problemen waarvoor eerder is aangegeven dat deze kunnen worden genegeerd. Als er geen problemen zijn, verschijnt een virusadvies in plaats van eventuele problemen. U kunt ook klikken op **Configureren** om uw opties voor die categorie te wijzigen.

Als alle beveiligingscategorieën binnen een categorie de status Groen hebben, dan is de status van deze categorie Groen. Als alle beveiligingscategorieën de status Groen hebben, is de algehele beveiligingsstatus dus ook Groen.

Als er beveiligingscategorieën zijn met de status Geel of Rood, dan kunt u de beveiligingsproblemen oplossen door deze te herstellen of te negeren, waardoor de status verandert in Groen.

Informatie over beveiliging van computer en bestanden

De categorie Computer- en bestandenbeveiliging bestaat uit de volgende typen beveiliging:

- **Virusbeveiliging** -- Real-time scannen beschermt de computer tegen virussen, wormen, Trojaanse paarden, verdachte scripts, hybride aanvallen en andere bedreigingen. Er worden automatisch scans uitgevoerd en pogingen gedaan om gedetecteerde bestanden (zoals gecomprimeerde EXE-bestanden, opstartsector-, geheugen- en essentiële bestanden) op te schonen als deze door u of de computer worden geopend.
- **Spywarebeveiliging** -- Met spywarebeveiliging kunt u snel spyware, adware en andere programma's die uw persoonlijke gegevens verzamelen en verzenden zonder uw toestemming detecteren, blokkeren en verwijderen.
- **SystemGuards** -- SystemGuards detecteren wijzigingen op uw computer en waarschuwen u wanneer deze zich voordoen. U kunt deze wijzigingen vervolgens bekijken en beslissen of u ze al dan niet wilt toestaan.
- **Beveiliging van Windows** -- Met deze optie kunt u de status van Windows Update op uw computer bekijken. Als McAfee VirusScan is geïnstalleerd, is ook een bescherming tegen overschrijding van de bufferlimiet beschikbaar.

Externe virussen zijn een van de factoren die van invloed zijn op de Computer- en bestandenbeveiliging. Wordt u bijvoorbeeld beschermd door uw antivirussoftware als er een virusuitbraak plaatsvindt? Andere bepalende factoren zijn onder andere de configuratie van uw antivirussoftware en het feit of deze software regelmatig wordt bijgewerkt met de nieuwste signatuurbestanden voor detectie om uw computer tegen de nieuwste bedreigingen te beschermen.

Het deelvenster voor configureren van computer en bestanden openen

Wanneer er geen problemen zijn onder **Computer & bestanden** kunt u het configuratiedeelvenster openen vanuit het informatiedeelvenster.

Ga als volgt te werk om het configuratiedeelvenster voor computer en bestanden te openen:

1. Klik in het deelvenster Startpagina op **Computer & bestanden**.
2. Klik in het rechter deelvenster op **Configureren**.

Informatie over beveiliging van internet en netwerk

De categorie Internet- en netwerkbeveiliging bestaat uit de volgende typen beveiliging:

- **Firewallbescherming** -- Als u de firewallbescherming uitschakelt, is uw computer kwetsbaar voor inbraak en ongewenst netwerkverkeer. Hiermee kunt u alle inkomende en uitgaande internetverbindingen beheren.
- **Draadloze beveiliging** -- Draadloze beveiliging beschermt uw draadloze thuisnetwerk tegen inbraak en onderschepping van gegevens. Als u momenteel echter bent verbonden met een extern draadloos netwerk, varieert uw beveiliging, afhankelijk van het ingestelde beveiligingsniveau van dat netwerk.
- **Beveiliging van webgebruik** -- Met beveiliging van webgebruik verbergt u advertenties, pop-ups en webbugs op uw computer wanneer u een webbrowser gebruikt.
- **Bescherming tegen phishing** -- Bescherming tegen phishing helpt frauduleuze websites te blokkeren die via hyperlinks in e-mailberichten, instant messages, pop-ups en andere bronnen om persoonlijke gegevens vragen.
- **Beveiliging van persoonlijke gegevens** -- Met beveiliging van persoonlijke gegevens wordt de verspreiding van gevoelige en vertrouwelijke gegevens via internet geblokkeerd.

Het deelvenster voor configureren van internet en netwerk openen

Wanneer er geen problemen zijn onder **Internet & netwerk** kunt u het configuratiedeelvenster openen vanuit het informatiedeelvenster.

Ga als volgt te werk om het configuratiedeelvenster voor internet en netwerk te openen:

1. Klik in het deelvenster Startpagina op **Internet & netwerk**.
2. Klik in het rechter deelvenster op **Configureren**.

Informatie over Beveiliging van e-mail en expresberichten

De categorie Beveiliging van e-mail en expresberichten bestaat uit de volgende typen beveiliging:

- **E-mailbeveiliging** -- Met e-mailbeveiliging worden automatisch scans uitgevoerd en wordt geprobeerd virussen, spyware en mogelijke bedreigingen in inkomende en uitgaande e-mailberichten en bijlagen te verwijderen.
- **Spambeveiliging** -- Spambeveiliging helpt ongewenste e-mailberichten te filteren zodat deze niet in uw Postvak IN terechtkomen.
- **IM-beveiliging** -- Met beveiliging van expresberichten (Instant Messaging) worden automatisch scans uitgevoerd en wordt geprobeerd virussen, spyware en mogelijke bedreigingen in bijlagen bij inkomende expresberichten te verwijderen. Ook wordt voorkomen dat clients voor expresberichten ongewenste inhoud of persoonlijke gegevens uitwisselen via internet.
- **Bescherming voor veilig surfen** -- Indien u de browserinvoegapplicatie McAfee SiteAdvisor hebt geïnstalleerd, helpt deze u te beschermen tegen spyware, spam, virussen en online zwendel door aan de websites die u bezoekt of die worden opgehaald als zoekresultaat een veiligheidsbeoordeling toe te kennen. U kunt de veiligheidskwalificatiegegevens bekijken die aangeven hoe een website uit de test komt voor wat betreft e-mailpraktijken, downloads, online koppelingen en ergernissen zoals pop-ups en cookietracering van derden.

Het deelvenster voor configureren van e-mail en expresberichten openen

Wanneer er geen problemen zijn onder **E-mail- & expresberichten** kunt u het configuratiedeelvenster openen vanuit het informatiedeelvenster.

Ga als volgt te werk om het deelvenster voor configureren van e-mail en expresberichten te openen:

1. Klik in het deelvenster Startpagina op **E-mail & expresberichten**.
2. Klik in het rechter deelvenster op **Configureren**.

Informatie over beveiligingsinstellingen voor ouderlijk toezicht

De categorie Ouderlijk toezicht bestaat uit het volgende type beveiliging:

- **Ouderlijk toezicht** -- Inhoud blokkeren voorkomt dat gebruikers bepaalde ongewenste internetinhoud kunnen bekijken, door potentieel schadelijke websites te blokkeren. Daarnaast kunnen de activiteiten en het gebruik van het internet door gebruikers worden gevolgd en beperkt.

Open het deelvenster voor configuratie van ouderlijk toezicht

Wanneer er geen problemen zijn onder **Ouderlijk toezicht** kunt u het configuratiedeelvenster openen vanuit het informatiedeelvenster.

Ga als volgt te werk om het deelvenster voor configuratie van ouderlijk toezicht te openen:

1. Klik in het deelvenster Startpagina op **Ouderlijk toezicht**.
2. Klik in het rechter deelvenster op **Configureren**.

Beveiligingsproblemen herstellen

De meeste beveiligingsproblemen kunnen automatisch worden opgelost. Als er echter een of meer problemen zijn die zich blijven voordoen, dient u deze handmatig op te lossen.

Beveiligingsproblemen automatisch herstellen

De meeste beveiligingsproblemen kunnen automatisch worden opgelost.

Ga als volgt te werk om beveiligingsproblemen automatisch te herstellen:

- Klik op **Herstellen** naast de beveiligingsstatus.

Beveiligingsproblemen handmatig herstellen

Als een of meer beveiligingsproblemen niet automatisch kunnen worden opgelost, klikt u op de koppeling naast het probleem om de voorgestelde actiestap te ondernemen.

Ga als volgt te werk om beveiligingsproblemen handmatig te herstellen:

- Voer een van de volgende handelingen uit:
  - Als er de laatste dertig dagen geen volledige scan van uw computer is uitgevoerd, klikt u op **Scannen** links van de belangrijkste beveiligingsstatus om een handmatige scan uit te voeren. (Deze optie wordt weergegeven als u McAfee VirusScan hebt geïnstalleerd.)
  - Als uw virusdefinitiebestanden (DAT) verouderd zijn, klikt u op de koppeling **Bijwerken** links van de belangrijkste beveiligingsstatus om de bescherming bij te werken.
  - Als een bepaald programma niet is geïnstalleerd, klikt u op **Zorg voor volledige beveiliging** om het te installeren.
  - Als er componenten van een programma ontbreken, installeert u het programma opnieuw.
  - Als een programma moet worden geregistreerd om volledige beveiliging te krijgen, klikt u op **Nu registreren** om dit te registreren. (Deze optie wordt weergegeven als een of meer programma's zijn verlopen.)
  - Als een programma is verlopen, klikt u op **Mijn abonnement controleren** om uw accountstatus te controleren. (Deze optie wordt weergegeven als een of meer programma's zijn verlopen.)

Informatie over SecurityCenter weergeven

Onder het deelvenster met de beveiligingsstatus geeft de knop SecurityCenter-informatie toegang tot de opties van SecurityCenter en toont deze u de meest recente update, laatste uitgevoerde scan (als McAfee VirusScan is geïnstalleerd) en de vervaldatum van uw abonnementen op McAfee-producten.

Open het configuratiedeelvenster van SecurityCenter

Als u uw opties wilt wijzigen, kunt u dit desgewenst ook doen door het configuratiedeelvenster van SecurityCenter te openen vanuit het deelvenster Startpagina.

Ga als volgt te werk om het configuratiedeelvenster van SecurityCenter te openen:

- Klik in het deelvenster Startpagina onder **SecurityCenter-informatie** op **Configureren**.

Informatie over geïnstalleerde producten weergeven

U kunt een lijst met geïnstalleerde producten weergeven waarin het productversienummer wordt getoond en het moment waarop de meest recente update is uitgevoerd.

Ga als volgt te werk om informatie over uw McAfee-product weer te geven:

- Klik in het deelvenster Startpagina onder **SecurityCenter-informatie** op **Details weergeven** om het venster met productinformatie weer te geven.

Gebruik van het menu Geavanceerd

Wanneer u SecurityCenter voor het eerst opent, wordt het menu Basis weergegeven in de linkerkolom. Als u een gevorderde gebruiker bent, kunt u op **Menu Geavanceerd** klikken om in plaats van het basismenu een meer gedetailleerd opdrachtenmenu weer te geven. Voor uw gemak wordt standaard het laatst weergegeven menu geopend wanneer u SecurityCenter een volgende keer opent.

Het menu Geavanceerd bestaat uit de volgende onderdelen:

- Startpagina
- Rapporten en logboeken (inclusief de lijst met Recente gebeurtenissen en logboeken op type voor de afgelopen 30, 60 en 90 dagen)
- Configureren
- Herstellen
- Extra

HOOFDSTUK 4

Opties van SecurityCenter configureren

SecurityCenter toont de algehele beveiligingsstatus van uw computer, biedt u de mogelijkheid om McAfee-gebruikersaccounts aan te maken, installeert automatisch de nieuwste productupdates en brengt u standaard automatisch via waarschuwingsvensters en geluidssignalen op de hoogte van virusuitbraken, veiligheidsrisico's en productupdates.

in het deelvenster Configuratie van SecurityCenter kunt u uw SecurityCenter-opties aanpassen voor de volgende functies:

- Beveiligingsstatus
- Gebruikers
- Automatische updates
- Waarschuwingen

In dit hoofdstuk

De beveiligingsstatus configureren

De algehele beveiligingsstatus van uw computer wordt in SecurityCenter weergegeven onder **Is mijn computer beveiligd?**.

De beveiligingsstatus biedt u informatie over de mate waarin uw computer is beveiligd tegen de nieuwste beveiligingsrisico's, geeft aan of er mogelijk problemen zijn die aandacht vereisen, en biedt u de mogelijkheid om deze problemen op te lossen.

Standaard is het zo dat als Spambeveiliging of Inhoud blokkeren niet zijn geïnstalleerd, deze niet-essentiële beveiligingsproblemen automatisch worden genegeerd en niet worden gevolgd in de algehele beveiligingsstatus. Als er bij de melding van een beveiligingsprobleem echter een koppeling **Negeren** staat, kunt u ervoor kiezen om het probleem te negeren als u zeker weet dat u dit niet wilt herstellen. Als u achteraf besluit een eerder genegeerd probleem alsnog te herstellen, kunt u dit probleem opnemen in de beveiligingsstatus ter controle.

Genegeerde problemen configureren

U kunt opgeven dat problemen wel of niet moeten worden meegenomen in de controle, als onderdeel van de algehele beveiligingsstatus van uw computer. Als er bij de melding van een beveiligingsprobleem een koppeling **Negeren** staat, kunt u ervoor kiezen om het probleem te negeren als u zeker weet dat u dit niet wilt herstellen. Als u achteraf besluit een eerder genegeerd probleem alsnog te herstellen, kunt u dit probleem opnemen in de beveiligingsstatus ter controle.

Ga als volgt te werk om genegeerde problemen te configureren:

1. Klik onder **SecurityCenter-informatie** op **Configureren**.
2. Klik op de pijl naast **Beveiligingsstatus** om het bijbehorende deelvenster te vergroten en klik vervolgens op **Geavanceerd**.
3. Voer een van de volgende handelingen uit in het deelvenster Genegeerde problemen:
   - Als u eerder genegeerde problemen wilt opnemen in de beveiligingsstatus, schakelt u de desbetreffende selectievakjes uit.
   - Als u eerder genegeerde problemen wilt uitsluiten uit de beveiligingsstatus, schakelt u de desbetreffende selectievakjes in.
4. Klik op **OK**.

Gebruikersopties configureren

Als u McAfee-programma's uitvoert die gebruikersrechten vereisen, komen deze rechten standaard overeen met de Windows-gebruikersaccounts op uw computer. Teneinde het gebruikersbeheer voor deze programma's te vereenvoudigen kunt u op elk moment naar McAfee-gebruikersaccounts overschakelen.

Als u overschakelt naar het gebruik van McAfee-gebruikersaccounts, worden eventuele internet-restricties, gebruikersnamen en toegangsregels uit uw programma voor ouderlijk toezicht op gebruikers automatisch geïmporteerd. De eerste keer dat u overschakelt moet u echter een beheerdersaccount aanmaken. Daarna kunt u beginnen met het maken en configureren van andere McAfee-gebruikersaccounts.

Overschakelen naar McAfee-gebruikersaccounts

Standaard maakt u gebruik van Windows-gebruikersaccounts. Door over te schakelen naar McAfee-gebruikersaccounts wordt het echter onnodig om verder nog Windows-gebruikersaccounts aan te maken.

Ga als volgt te werk om over te schakelen naar McAfee-gebruikersaccounts:

1. Klik onder **SecurityCenter-informatie** op **Configureren**.
2. Klik op de pijl naast **Gebruikers** om het bijbehorende deelvenster te vergroten en klik vervolgens op **Geavanceerd**.
3. Als u McAfee-gebruikersaccounts wilt gaan gebruiken, klikt u op **Schakelen**.

Wanneer u bent overgeschakeld naar het gebruik van McAfee-gebruikersaccounts en deze voor het eerst wilt gaan gebruiken, moet u een beheerdersaccount maken (pagina 26).

Een beheerdersaccount maken

De eerste keer dat u overschakelt naar het gebruik van McAfee-gebruikers, wordt u gevraagd een beheerdersaccount te maken.

Ga als volgt te werk om een beheerdersaccount te maken:

1. Geef een wachtwoord op in het vak **Wachtwoord** en typ dit nogmaals in het vak **Bevestig het wachtwoord**.
2. Kies de vraag die moet worden gesteld als u het wachtwoord bent vergeten uit de lijst, en typ het antwoord op deze beveiligingsvraag in het vak **Antwoord**.
3. Klik op **Toepassen**.

   Wanneer u klaar bent, wordt het type gebruikersaccount in het deelvenster bijgewerkt met de bestaande gebruikersnamen en toegangsregels uit uw programma voor ouderlijk toezicht op gebruikers, als u een dergelijk programma gebruikt. Als u voor het eerst gebruikersaccounts configureert, verschijnt het deelvenster Gebruiker beheren.

Gebruikersopties configureren

Als u overschakelt naar het gebruik van McAfee-gebruikersaccounts, worden bestaande gebruikersnamen en toegangsregels uit uw programma voor ouderlijk toezicht op gebruikers automatisch geïmporteerd. De eerste keer dat u overschakelt moet u echter een beheerdersaccount aanmaken. Daarna kunt u beginnen met het maken en configureren van andere McAfee-gebruikersaccounts.

Ga als volgt te werk om gebruikersopties te configureren:

1. Klik op **Configureren** onder **SecurityCenter-informatie**.
2. Klik op de pijl naast **Gebruikers** om het bijbehorende deelvenster te vergroten en klik vervolgens op **Geavanceerd**.
3. Klik onder **Gebruikersaccounts** op **Toevoegen**.
4. Typ een gebruikersnaam in het vak **Gebruikersnaam**.
5. Geef een wachtwoord op in het vak **Wachtwoord** en typ dit nogmaals in het vak **Wachtwoord bevestigen**.
6. Schakel het selectievakje **Hoofdgebruiker** in als u wilt dat deze nieuwe gebruiker automatisch wordt aangemeld wanneer SecurityCenter wordt gestart.
7. Selecteer onder **Type gebruikersaccount** een type account voor deze gebruiker en klik vervolgens op **Maken**.

   Opmerking: Nadat u de gebruikersaccount hebt gemaakt, moet u onder Ouderlijk toezicht de instellingen configureren voor een Gebruiker met beperkte rechten.

8. Als u het wachtwoord, de automatisch aanmeldgegevens of het type account van een gebruiker wilt bewerken, selecteert u een gebruikersnaam in de lijst en klikt u op **Bewerken**.
9. Klik op **Toepassen** als u klaar bent.

Het beheerderswachtwoord opvragen

Als u het beheerderswachtwoord bent vergeten, kunt u het nog terugvinden.

Ga als volgt te werk om het beheerderswachtwoord op te vragen:

1. Klik met de rechtermuisknop op het pictogram met de M van het SecurityCenter, en klik vervolgens op **Andere gebruiker**.
2. Selecteer in de lijst **Gebruikersnaam** de optie **Beheerder**, en klik op **Wachtwoord vergeten?**.
3. Voer het antwoord in op de geheime vraag die u bij het aanmaken van uw beheerdersaccount hebt geselecteerd.
4. Klik op **Verzenden**.

   Het beheerderswachtwoord dat u was vergeten, verschijnt nu op uw scherm.

Het beheerderswachtwoord wijzigen

Als u er moeite mee hebt om het Beheerderswachtwoord te onthouden of vermoedt dat dit wachtwoord bekend is geworden bij derden, kunt u het wijzigen.

Ga als volgt te werk om het beheerderswachtwoord te wijzigen:

1. Klik met de rechtermuisknop op het pictogram met de M van SecurityCenter, en klik vervolgens op **Andere gebruiker**.
2. Selecteer in de lijst **Gebruikersnaam** de optie **Beheerder**, en klik op **Wachtwoord wijzigen**.
3. Geef uw bestaande wachtwoord op in het vak **Vorig wachtwoord**.
4. Geef uw nieuwe wachtwoord op in het vak **Wachtwoord** en typ dit nogmaals in het vak **Bevestig het wachtwoord**.
5. Klik op **OK**.

Update-opties configureren

SecurityCenter controleert, indien u bent verbonden met internet, om de vier uur automatisch op updates voor al uw McAfee-services en installeert vervolgens automatisch de nieuwste productupdates. U kunt echter op elk gewenst moment handmatig controleren of er updates beschikbaar zijn met behulp van het SecurityCenter-pictogram, dat wordt weergegeven in het systeemvak van Windows, uiterst rechts op de taakbalk.

Automatisch controleren op updates

SecurityCenter controleert automatisch elke vier uur op updates als u verbinding hebt met internet. U kunt SecurityCenter echter ook zodanig configureren dat u op de hoogte wordt gebracht voordat er updates worden gedownload of geïnstalleerd.

Ga als volgt te werk om automatisch te controleren op updates:

1. Klik op **Configureren** onder **SecurityCenter-informatie**.
2. Klik op de pijl naast de status **Automatische updates zijn ingeschakeld** om het bijbehorende deelvenster te vergroten en klik vervolgens op **Geavanceerd**.
3. Selecteer een van de volgende opties in het deelvenster Update-opties:
   - De updates automatisch installeren en een waarschuwing weergeven wanneer het product is bijgewerkt (aanbevolen) (pagina 30)
   - De updates automatisch downloaden en een waarschuwing weergeven wanneer ze gereed zijn voor installatie (pagina 31)
   - Een waarschuwing weergeven voordat updates worden gedownload (pagina 31)
4. Klik op **OK**.

Opmerking: Voor maximale beveiliging raadt McAfee u aan om SecurityCenter in te stellen op het automatisch controleren op en installeren van updates. Als u de beveiligingsservices echter alleen handmatig wilt bijwerken, kunt u het automatisch bijwerken uitschakelen (pagina 32).

Updates automatisch downloaden en installeren

Als u de optie **De updates automatisch installeren en een waarschuwing weergeven wanneer mijn services zijn bijgewerkt (aanbevolen)** selecteert in het venster Update-opties van SecurityCenter, worden updates voor SecurityCenter automatisch gedownload en geïnstalleerd.

Updates automatisch downloaden

Als u in SecurityCenter de update-optie **De updates automatisch downloaden en een waarschuwing weergeven wanneer ze gereed zijn voor installatie** selecteert, worden updates voor SecurityCenter automatisch gedownload en krijgt u bericht wanneer een update gereed is voor installatie. U kunt vervolgens beslissen of u de update wilt installeren of uitstellen (pagina 32).

Ga als volgt te werk om een automatisch gedownloade update te installeren:

1. Klik op **Nu een update voor mijn producten uitvoeren** in de waarschuwing en klik vervolgens op **OK**.

   Meld u desgevraagd aan bij de website als voor het downloaden van updates de status van uw abonnement moet worden gecontroleerd.

2. Nadat uw abonnement is gecontroleerd, klikt u op **Bijwerken** in het deelvenster Updates om de update te downloaden en te installeren. Als uw abonnement is verlopen, klikt u in het waarschuwingsbericht op **Mijn abonnement verlengen** en volgt u de aanwijzingen.

Opmerking: In sommige gevallen wordt u gevraagd de computer opnieuw op te starten om de update te voltooien. Sla al uw werk op en sluit alle programma's voordat u opnieuw opstart.

Waarschuwing laten weergeven voordat updates worden gedownload

Als u de optie **Een waarschuwing weergeven voordat updates worden gedownload** selecteert in het deelvenster Update-opties, stuurt SecurityCenter u bericht voordat een update wordt gedownload. U kunt vervolgens beslissen of u een update op de beveiligingsservices wilt downloaden en installeren om het risico van een aanval weg te nemen.

Ga als volgt te werk om een update te downloaden en te installeren:

1. Selecteer **Nu een update voor mijn producten uitvoeren** in de waarschuwing en klik vervolgens op **OK**.
2. Meld u aan bij de website als dit wordt gevraagd.

   De update wordt automatisch gedownload.
3. Klik op **OK** in het waarschuwingsbericht wanneer de update is geïnstalleerd.

Opmerking: In sommige gevallen wordt u gevraagd de computer opnieuw op te starten om de update te voltooien. Sla al uw werk op en sluit alle programma's voordat u opnieuw opstart.

Automatische updates uitschakelen

Voor maximale beveiliging raadt McAfee u aan om SecurityCenter in te stellen op het automatisch controleren op en installeren van updates. Als u de beveiligingsservices echter alleen handmatig wilt bijwerken, kunt u het automatisch bijwerken uitschakelen.

Opmerking: Het is raadzaam ten minste eenmaal per week handmatig op updates te controleren (pagina 33). Als u niet op updates controleert, is de computer niet beveiligd met de nieuwste beveiligingsupdates.

Ga als volgt te werk om automatisch bijwerken uit te schakelen:

1. Klik onder **SecurityCenter-informatie** op **Configureren**.
2. Klik op de pijl naast de status **Automatische updates zijn ingeschakeld** om het bijbehorende deelvenster te vergroten.
3. Klik op **Uit**.
4. Klik op **Ja** om de wijziging te bevestigen.

   De status in de koptekst wordt bijgewerkt.

Als u binnen zeven dagen nog niet handmatig hebt gecontroleerd of er updates zijn, wordt een waarschuwing weergegeven.

Het bijwerken uitstellen

Als u het te druk hebt om de beveiligingsservices bij te werken op het moment dat u de waarschuwing krijgt, kunt u aangeven dat u later een herinnering wilt krijgen of kunt u de waarschuwing negeren.

Ga als volgt te werk om het bijwerken uit te stellen:

- Voer een van de volgende handelingen uit:
  - Selecteer **Stuur later een herinnering** in de waarschuwing en klik vervolgens op **OK**.
  - Selecteer **Deze waarschuwing sluiten** en klik op **OK** om de waarschuwing te sluiten zonder actie te ondernemen.

Handmatig controleren op updates

SecurityCenter controleert, indien u bent verbonden met internet, om de vier uur automatisch op updates en installeert vervolgens de nieuwste productupdates. U kunt echter op elk gewenst moment handmatig controleren of er updates beschikbaar zijn met behulp van het SecurityCenter-pictogram, dat wordt weergegeven in het systeemvak van Windows, uiterst rechts op de taakbalk.

Opmerking: Voor maximale beveiliging raadt McAfee u aan om SecurityCenter in te stellen op het automatisch controleren op en installeren van updates. Als u de beveiligingsservices echter alleen handmatig wilt bijwerken, kunt u het automatisch bijwerken uitschakelen (pagina 32).

Ga als volgt te werk om handmatig te controleren op updates:

1. Zorg ervoor dat uw computer verbinding heeft met internet.
2. Klik met de rechtermuisknop op het pictogram met de M van het SecurityCenter in het systeemvak van Windows, uiterst rechts op de taakbalk en klik vervolgens op **Updates**.

   Terwijl er in SecurityCenter naar updates wordt gezocht, kunt u in het programma doorgaan met andere taken.

   In het systeemvak van Windows, uiterst rechts op de taakbalk, wordt een animatiepictogram weergegeven. Als SecurityCenter klaar is met zoeken, verdwijnt het pictogram automatisch.
3. Meld u aan bij de website als u wordt gevraagd om uw abonnement te controleren.

Opmerking: In sommige gevallen wordt u gevraagd de computer opnieuw op te starten om de update te voltooien. Sla al uw werk op en sluit alle programma's voordat u opnieuw opstart.

Configureren van waarschuwingsopties

SecurityCenter brengt u automatisch via waarschuwingsvensters en geluidssignalen op de hoogte van virusuitbraken, veiligheidsrisico's en productupdates. U kunt SecurityCenter echter ook zodanig configureren dat alleen waarschuwingen worden weergegeven die uw onmiddellijke aandacht vereisen.

Waarschuwingsopties configureren

SecurityCenter brengt u automatisch via waarschuwingsvensters en geluidssignalen op de hoogte van virusuitbraken, veiligheidsrisico's en productupdates. U kunt SecurityCenter echter ook zodanig configureren dat alleen waarschuwingen worden weergegeven die uw onmiddellijke aandacht vereisen.

Ga als volgt te werk om waarschuwingsopties te configureren:

1. Klik onder **SecurityCenter-informatie** op **Configureren**.
2. Klik op de pijl naast **Waarschuwingen** om het bijbehorende deelvenster te vergroten en klik vervolgens op **Geavanceerd**.
3. Selecteer een van de volgende opties in het deelvenster Waarschuwingsopties:
   - **Waarschuw mij wanneer een virusuitbraak of een veiligheidsrisico optreedt**
   - **Informatiewaarschuwingen weergeven wanneer de spelletjesmodus wordt gedetecteerd**
   - **Geluid afspelen wanneer er een waarschuwing optreedt**
   - **Opstartscherm van McAfee weergeven bij opstarten van Windows**
4. Klik op **OK**.

Opmerking: Als u toekomstige informatieve waarschuwingen wilt uitschakelen vanuit het waarschuwingsbericht zelf, selecteert u het selectievakje **Deze waarschuwing niet meer tonen**. U kunt deze later weer inschakelen vanuit het deelvenster Informatiewaarschuwingen.

Informatieve waarschuwingen configureren

Informatiewaarschuwingen worden weergegeven wanneer gebeurtenissen optreden waarop u niet direct hoeft te reageren. Als u toekomstige informatieve waarschuwingen uitschakelt vanuit het waarschuwingsbericht zelf, kunt u deze later weer inschakelen in het deelvenster Informatiewaarschuwingen.

Ga als volgt te werk om informatieve waarschuwingen te configureren:

1. Klik onder **SecurityCenter-informatie** op **Configureren**.
2. Klik op de pijl naast **Waarschuwingen** om het bijbehorende deelvenster te vergroten en klik vervolgens op **Geavanceerd**.
3. Klik onder **Configuratie van SecurityCenter** op **Informatiewaarschuwingen**.
4. Schakel het selectievakje **Informatiewaarschuwingen verbergen** uit en verwijder vervolgens de vinkjes bij alle selectievakjes voor waarschuwingen in de lijst die u wel wilt weergeven.
5. Klik op **OK**.

HOOFDSTUK 5

Algemene taken uitvoeren

U kunt hier veel voorkomende taken uitvoeren, zoals terugkeren naar het deelvenster Startpagina, recente gebeurtenissen weergeven, uw computernetwerk beheren (als u werkt op een computer met beheerfuncties voor dit netwerk), en onderhoudstaken voor uw computer uitvoeren. Als McAfee Data Backup is geïnstalleerd, kunt u ook een back-up van uw gegevens maken.

In dit hoofdstuk

Algemene taken uitvoeren

U kunt hier veel voorkomende taken uitvoeren, zoals terugkeren naar het deelvenster Startpagina, recente gebeurtenissen weergeven, uw computer onderhouden, uw netwerk beheren (als u werkt op een computer met beheerfuncties voor dit netwerk), en een back-up van uw gegevens maken (als McAfee Data Backup is geïnstalleerd).

Ga als volgt te werk om algemene taken uit te voeren:

- Voer in het menu Basis onder **Algemene taken** een van de volgende handelingen uit:
  - Als u wilt terugkeren naar het deelvenster Startpagina klikt u op **Startpagina**.
  - Als u wilt zien welke recente gebeurtenissen er door uw beveiligingssoftware zijn aangetroffen, klikt u op **Recente gebeurtenissen**.
  - Om ongebruikte bestanden te verwijderen, uw gegevens te defragmenteren en de oorspronkelijke instellingen van uw computer te herstellen, klikt u op **Computer onderhouden**.
  - Als u uw computernetwerk wilt beheren, klikt u op **Netwerk beheren** op een computer met beheerfuncties voor dit netwerk.

Network Manager controleert computers in uw netwerk op zwakke punten in de beveiliging, zodat u op eenvoudige wijze netwerkbeveiligingsproblemen kunt opsporen.

- Als u reservekopieën van uw bestanden wilt maken, klikt u op **Back-up gegevens**. Dit is alleen mogelijk als McAfee Data Backup is geïnstalleerd.

  Automatische back-up bewaart kopieën van uw meest waardevolle bestanden waar u maar wilt. De bestanden worden versleuteld en opgeslagen op een CD/DVD-, USB-, extern of netwerkstation.

Tip: Om het u gemakkelijker te maken, kunt u algemene taken ook uitvoeren vanuit twee andere locaties (onder **Startpagina** in het menu Geavanceerd, en in het menu **QuickLinks** dat u kunt openen via het pictogram M van SecurityCenter, uiterst rechts op de werkbalk. U kunt ook recente gebeurtenissen bekijken en uitgebreide logboeken op type weergeven onder **Rapporten en logboeken** in het menu Geavanceerd.

Recente gebeurtenissen weergeven

Recente gebeurtenissen worden vastgelegd in een logboek wanneer er wijzigingen aan uw computer plaatsvinden. Voorbeelden hiervan zijn gevallen waarin een beschermingstype wordt ingeschakeld of uitgeschakeld, een bedreiging wordt verwijderd of een poging tot maken van een internetverbinding wordt geblokkeerd. U kunt de twintig meest recente gebeurtenissen met de bijbehorende gegevens bekijken.

Zie het Help-bestand van het betreffende product voor meer informatie over de bijbehorende gebeurtenissen.

Ga als volgt te werk om recente gebeurtenissen weer te geven:

1. Klik met de rechtermuisknop op het hoofdpictogram van SecurityCenter, wijs naar **QuickLinks** en klik vervolgens op **Recente gebeurtenissen weergeven**.

   Alle recente gebeurtenissen worden weergegeven in de lijst, samen met de datum en een korte omschrijving.

2. Selecteer een gebeurtenis onder **Recente gebeurtenissen** als u meer informatie hierover wilt bekijken in het detailvenster.

   Onder **Ik wil...** worden eventuele beschikbare acties weergegeven.

3. Als u een meer uitgebreide lijst met gebeurtenissen wilt weergeven, klikt u op **Logboek weergeven**.

Uw computer handmatig onderhouden

Om kostbare schijfruimte vrij te maken en de prestaties van uw computer te optimaliseren, kunt u inplannen dat taken zoals QuickClean of Schijfdefragmentatie regelmatig worden uitgevoerd. Deze taken bestaan onder meer uit het verwijderen, vernietigen en defragmenteren van bestanden en mappen.

Ga als volgt te werk om uw computer automatisch te onderhouden:

1. Klik met de rechtermuisknop op het hoofdpictogram van SecurityCenter, wijs naar **QuickLinks** en klik vervolgens op **Computer onderhouden**.
2. Klik onder **Taakplanner** op **Start.**
3. Selecteer in de lijst met bewerkingen de optie **QuickClean** of **Schijfdefragmentatie**.
4. Voer een van de volgende handelingen uit:
   - Als u een bestaande taak wilt wijzigen, selecteert u de desbetreffende taak en klikt u op **Wijzigen**. Volg de instructies op het scherm.
   - Om een nieuwe taak te maken, geeft u de gewenste naam op in het vak **Taaknaam** en klikt u vervolgens op **Maken**. Volg de instructies op het scherm.
   - Als u een taak wilt verwijderen, selecteert u deze en klikt u vervolgens op **Verwijderen**.
5. Onder **Taakoverzicht** leest u wanneer de taak voor het laatst is uitgevoerd, wanneer deze de eerstvolgende keer weer wordt uitgevoerd en wat de status ervan is.

Uw computer handmatig onderhouden

U kunt handmatige onderhoudstaken uitvoeren om ongebruikte bestanden te verwijderen, uw gegevens te defragmenteren of de oorspronkelijke instellingen van uw computer te herstellen.

Ga als volgt te werk om uw computer handmatig te onderhouden:

- Voer een van de volgende handelingen uit:
  - Als u QuickClean wilt gebruiken, klikt u met de rechtermuisknop op het SecurityCenter-hoofdpictogram, wijst u naar **QuickLinks,** klikt u op **Computer onderhouden** en klikt u vervolgens op **Start**.
  - Als u Schijfdefragmentatie wilt gebruiken, klikt u met de rechtermuisknop op het SecurityCenter-hoofdpictogram, wijst u naar **QuickLinks,** klikt u op **Computer onderhouden** en klikt u vervolgens op **Analyseren**.
  - Als u Systeemherstel wilt gebruiken, klikt u in het menu Geavanceerd op **Extra**, klikt u op **Systeemherstel** en klikt u vervolgens op **Start**.

Ongebruikte bestanden en mappen verwijderen

Gebruik QuickClean om kostbare schijfruimte vrij te maken en de prestaties van uw computer te optimaliseren.

Ga als volgt te werk om ongebruikte bestanden en mappen te verwijderen:

1. Klik met de rechtermuisknop op het hoofdpictogram van SecurityCenter, wijs naar **QuickLinks** en klik vervolgens op **Computer onderhouden**.
2. Klik onder **QuickClean** op **Start**.
3. Volg de instructies op het scherm.

Bestanden en mappen defragmenteren

Bestanden raken gefragmenteerd naarmate er bestanden en mappen worden verwijderd en er nieuwe bestanden worden toegevoegd. Deze fragmentatie vertraagt de toegang tot de vaste schijf en verslechtert de algehele prestaties van uw computer, hoewel dit meestal niet van ernstige aard is.

Gebruik defragmentatie om delen van een bestand te herschrijven naar aangrenzende sectoren op een vaste schijf, zodat de snelheid van openen en ophalen van gegevens wordt verhoogd.

Ga als volgt te werk om bestanden en mappen te defragmenteren:

1. Klik met de rechtermuisknop op het hoofdpictogram van SecurityCenter, wijs naar **QuickLinks** en klik vervolgens op **Computer onderhouden**.
2. Klik onder **Schijfdefragmentatie** op **Analyseren**.
3. Volg de instructies op het scherm.

De oorspronkelijke instellingen van uw computer terugzetten

Herstelpunten zijn momentopnamen van uw computer die met regelmatige tussenpozen door Windows worden opgeslagen en op momenten dat er belangrijke gebeurtenissen plaatsvinden (zoals wanneer een programma of stuurprogramma wordt geïnstalleerd). U kunt echter op elk gewenst moment uw eigen herstelpunten maken en een naam geven.

Gebruik herstelpunten om schadelijke wijzigingen aan uw computer ongedaan te maken en de oorspronkelijke instellingen te herstellen.

Ga als volgt te werk om de oorspronkelijke instellingen van uw computer terug te zetten:

1. Klik in het menu Geavanceerd op **Extra** en klik vervolgens op **Systeem herstellen**.
2. Klik onder **Systeem herstellen** op **Start**.
3. Volg de instructies op het scherm.

Uw netwerk beheren

Als de computer die u gebruikt beheerfuncties voor dit netwerk heeft, kunt u computers in uw netwerk door Network Manager laten controleren op zwakke punten in de beveiliging, zodat u op eenvoudige wijze beveiligingsproblemen kunt opsporen.

Als de beveiligingsstatus van uw computer in dit netwerk niet wordt gecontroleerd, maakt uw computer ofwel geen deel uit van dit netwerk of is het een niet-beheerd onderdeel van dit netwerk. Zie het Help-bestand van Network Manager voor meer informatie.

Ga als volgt te werk om uw netwerk te beheren:

1. Klik met de rechtermuisknop op het hoofdpictogram van SecurityCenter, wijs naar **QuickLinks** en klik vervolgens op **Netwerk beheren**.
2. Klik op het pictogram dat deze computer aangeeft in het netwerkoverzicht.
3. Klilk onder **Ik wil...** op **Deze computer controleren**.

Meer informatie over virussen

Gebruik de Virus Information Library en de Virus Map om een van de volgende acties uit te voeren:

- Kom meer te weten over de nieuwste virussen, e-mailvirushoaxes en andere bedreigingen.
- Krijg gratis gereedschappen waarmee u virussen kunt verwijderen en uw computer kunt repareren.
- Haal een real-time, wereldwijd overzicht op met algemene informatie over de nieuwste virussen die computers infecteren.

Als u meer wilt weten over virussen:

1. Klik in het menu Geavanceerd op **Extra** en klik vervolgens op **Virusinformatie**.
2. Voer een van de volgende handelingen uit:
   - Zoek informatie over virussen op met behulp van de gratis McAfee Virus Information Library.
   - Zoek informatie over virussen op met behulp van de World Virus Map op de website van McAfee.

HOOFDSTUK 6

McAfee QuickClean

Wanneer u surft op internet, zorgt dit al snel voor een ophoping van overbodige bestanden op uw computer. Bescherm uw privacy en verwijder onnodige gegevens afkomstig van internet en uit e-mailberichten met QuickClean. Met QuickClean worden bestanden geïdentificeerd en verwijderd die worden verzameld tijdens het surfen, waaronder cookies, e-mails, downloads en geschiedenissen, kortom: gegevens die persoonlijke informatie over u bevatten. Uw privacy wordt beschermd doordat deze gevoelige informatie op veilige wijze wordt verwijderd.

Met QuickClean worden ook ongewenste programma's verwijderd. Geef de bestanden op die u wilt verwijderen, zodat de belangrijke gegevens behouden blijven en de ongewenste bestanden worden gewist.

In dit hoofdstuk

Functies van QuickClean

In dit gedeelte worden de functies van QuickClean beschreven.

Functies

QuickClean bevat een set met efficiënte en gemakkelijk te gebruiken functies die digitale rommel veilig opruimen. U kunt waardevolle schijfruimte vrijmaken en de prestaties van de computer verbeteren.

HOOFDSTUK 7

Opschonen van de computer

Met QuickClean kunt u bestanden en mappen op veilige wijze verwijderen.

Wanneer u surft op internet, kopieert uw browser elke internetpagina en de bijbehorende afbeeldingen naar een cachemap op de vaste schijf. Als u dan nogmaals terug gaat naar een pagina, kan de browser deze snel laden. Het opslaan van bestanden in het cachegeheugen is nuttig als u herhaaldelijk dezelfde internetpagina's bezoekt en de inhoud van deze pagina's niet regelmatig wordt gewijzigd. Meestal zijn de bestanden in het cachegeheugen echter niet nuttig en kunnen ze worden verwijderd.

Met de volgende opschoonprogramma's kunt u diverse items verwijderen.

- Prullenbak opschonen: Hiermee wordt de Prullenbak van Windows leeggemaakt.
- Tijdelijke bestanden opschonen: Hiermee worden bestanden verwijderd die zijn opgeslagen in tijdelijke mappen.
- Snelkoppelingen opschonen: Hiermee worden verbroken snelkoppelingen en snelkoppelingen waaraan geen programma is gekoppeld, verwijderd.
- Verloren bestandsfragmenten opschonen: Hiermee worden verloren bestandsfragmenten van de computer verwijderd.
- Register opschonen: Hiermee wordt Windows-registerinformatie verwijderd voor programma's die niet meer aanwezig zijn op de computer.
- Cache opschonen: Hiermee worden bestanden in het cachegeheugen verwijderd die worden verzameld wanneer u op internet surft. Bestanden van dit type worden meestal opgeslagen als tijdelijke internetbestanden.
- Cookies opschonen: Hiermee worden cookies verwijderd. Bestanden van dit type worden meestal opgeslagen als tijdelijke internetbestanden.
  Cookies zijn kleine bestanden die door uw webbrowser op verzoek van een webserver op de computer worden opgeslagen. Elke keer dat u een webpagina van de webserver bekijkt, stuurt de browser de cookie terug naar de server. Deze cookies kunnen fungeren als een label, waarmee de webserver kan bijhouden welke pagina's u bekijkt en hoe vaak u terugkeert naar de pagina's.
- Browsergeschiedenissen opschonen: Hiermee worden uw browsergeschiedenissen verwijderd.

- Opschonen van verwijderde en verstuurde e-mail in Outlook Express en Outlook: Hiermee worden e-mailberichten verwijderd uit de Outlook-mappen voor verzonden en verwijderde items.
- Recent gebruikte items opschonen: Hiermee worden recent gebruikte items verwijderd die zijn opgeslagen op de computer, zoals Microsoft Office-documenten.
- ActiveX en invoegtoepassingen opschonen: Hiermee worden ActiveX-besturingselementen en invoegtoepassingen verwijderd.
  ActiveX is een technologie die wordt gebruikt voor het implementeren van besturingselementen in een programma. Met een ActiveX-besturingselement kan een knop worden toegevoegd aan een programma-interface. De meeste van deze besturingselementen zijn onschadelijk. Sommige mensen kunnen ActiveX-technologie echter gebruiken om informatie van uw computer vast te leggen.
  Invoegtoepassingen zijn kleine softwareprogramma's die worden ingevoegd in grotere toepassingen om extra functionaliteiten toe te voegen. Dankzij invoegtoepassingen kan de webbrowser bestanden openen en uitvoeren die zijn ingesloten in HTML-documenten en een indeling hebben die de browser normaal gesproken niet zou herkennen (bijvoorbeeld animatie-, video- en audiobestanden).
- Systeemherstelpunten opschonen: Hiermee worden oude systeemherstelpunten van de computer verwijderd.

In dit hoofdstuk

QuickClean gebruiken

In dit gedeelte wordt beschreven hoe u QuickClean kunt gebruiken.

Uw computer opschonen

U kunt ongebruikte bestanden en mappen verwijderen, schijfruimte vrijmaken en ervoor zorgen dat uw computer beter functioneert.

Ga als volgt te werk om de computer op te schonen:

1. Klik in het menu Geavanceerd op **Extra**.
2. Klik op **Computer onderhouden** en vervolgens op **Start** onder **McAfee QuickClean**.
3. Voer een van de volgende handelingen uit:
   - Klik op **Volgende** om de standaardopschoonprogramma's in de lijst te accepteren.
   - Selecteer de gewenste opschoonprogramma's en klik op **Volgende.** Voor het programma Recent gebruikte items opschonen kunt u klikken op **Eigenschappen** om de selectie op te heffen van de programma's waarvan u de lijsten niet wilt opschonen.
   - Klik op **Standaardwaarden herstellen** als u de standaardopschoonprogramma's wilt herstellen en klik vervolgens op **Volgende.**
4. Nadat de analyse is uitgevoerd, klikt u op **Volgende** om de verwijdering van bestanden te bevestigen. U kunt deze lijst uitvouwen om te zien welke bestanden zullen worden verwijderd en op welke locatie deze zich bevinden.
5. Klik op **Volgende.**
6. Voer een van de volgende handelingen uit:
   - Klik op **Volgende** om de standaardoptie **Nee, ik wil bestanden op de standaardmanier van Windows verwijderen** te accepteren.
   - Klik op **Ja, ik wil mijn bestanden veilig wissen met Shredder** en geef het aantal cyclussen op. Bestanden die met Shredder worden gewist, kunnen niet meer worden hersteld.
7. Klik op **Voltooien**.
8. Bekijk onder **Overzicht van QuickClean** het aantal registerbestanden dat is verwijderd en hoeveel schijfruimte er is vrijgemaakt na de schijf- en internetopschoning.

HOOFDSTUK 8

McAfee Shredder

U kunt verwijderde bestanden altijd terugzetten, zelfs nadat u de Prullenbak hebt leeggemaakt. Als u een bestand verwijdert, wordt deze ruimte op de schijf in Windows aangegeven als niet langer in gebruik, maar het bestand is er nog wel. Met speciale hulpprogramma's kunnen belastingaangiften, cv's of andere documenten die u hebt verwijderd, worden teruggehaald. Met Shredder verwijdert u ongewenste bestanden veilig en definitief, waardoor uw privacy wordt gewaarborgd.

Als u een bestand definitief wilt verwijderen, moet u het herhaaldelijk overschrijven met nieuwe gegevens. In Microsoft® Windows worden bestanden niet veilig verwijderd, omdat elke bestandsbewerking daarmee erg traag zou worden. Als u een document vernietigt, wordt niet altijd voorkomen dat dit bestand wordt teruggezet. In bepaalde programma's worden namelijk verborgen kopieën gemaakt van geopende documenten. Als u alleen documenten vernietigt die in Windows® Verkenner worden weergegeven, hebt u mogelijk nog steeds tijdelijke kopieën van deze documenten.

Opmerking: er wordt geen reservekopie gemaakt van vernietigde bestanden. Bestanden die met Shredder worden gewist, kunnen niet meer worden hersteld.

In dit hoofdstuk

Functies van Shredder

In dit gedeelte worden de functies van Shredder beschreven.

Functies

Met Shredder kunt u de Prullenbak-inhoud, tijdelijke internetbestanden, webgeschiedenissen, bestanden, mappen en schijven wissen.

HOOFDSTUK 9

Ongewenste bestanden wissen met Shredder

Met Shredder worden ongewenste bestanden zoals de Prullenbak-inhoud, tijdelijke internetbestanden en websitegeschiedenissen veilig en definitief verwijderd, waardoor uw privacy wordt gewaarborgd. U kunt bestanden en mappen die u wilt vernietigen selecteren of er naartoe bladeren.

In dit hoofdstuk

Shredder gebruiken

In dit gedeelte wordt beschreven hoe u Shredder kunt gebruiken.

Bestanden, mappen en schijven vernietigen

Zelfs nadat u de Prullenbak hebt leeggemaakt, kunnen er bestanden achterblijven op uw computer. Als u bestanden echter vernietigt, worden de gegevens definitief verwijderd en hebben hackers hier geen toegang toe.

U vernietigt bestanden, mappen en schijven als volgt:

1. Klik in het menu Geavanceerd **Extra** en klik vervolgens op **Shredder**.
2. Voer een van de volgende handelingen uit:
   - Klik op **Bestanden en mappen wissen** als u bestanden en mappen wilt vernietigen.
   - Klik op **Volledige schijf wissen** als u schijven wilt vernietigen**.**
3. Selecteer een van de volgende vernietigingsniveaus:
   - **Snel**: Hiermee worden de geselecteerde items 1 keer vernietigd.
   - **Grondig**: Hiermee worden de geselecteerde items 7 keer vernietigd.
   - **Aangepast**: Hiermee worden de geselecteerde items maximaal 10 keer vernietigd. Door een groter aantal vernietigingscyclussen op te geven, wordt het niveau van veilige bestandsverwijdering verhoogd.
4. Klik op **Volgende**.
5. Voer een van de volgende handelingen uit:
   - Als u bestanden wilt vernietigen, klikt u op **Prullenbak-inhoud**, **Tijdelijke internetbestanden** of **Websitegeschiedenis** in de lijst **Selecteer te vernietigen bestanden**. Als u een schijf wilt vernietigen, klikt u op de schijf.
   - Klik op **Bladeren**, ga naar de bestanden die u wilt vernietigen en selecteer deze.
   - Typ het pad naar de bestanden die u wilt vernietigen in de lijst **Selecteer te vernietigen bestanden** .
6. Klik op **Volgende**.
7. Klik op **Voltooien** om de bewerking te voltooien.
8. Klik op **Gereed.**

HOOFDSTUK 10

McAfee Network Manager

McAfee® Network Manager biedt een grafische weergave van de computers en onderdelen in uw thuisnetwerk. Met Network Manager kunt u de beveiligingsstatus van elke beheerde computer in het netwerk op afstand controleren en gerapporteerde beveiligingsproblemen van deze beheerde computers op afstand oplossen.

Voordat u Network Manager gaat gebruiken, kunt u kennismaken met enkele van de meest gebruikte functies. Meer informatie over de configuratie en het gebruik van deze functies vindt u in de Help bij Network Manager.

In dit hoofdstuk

Functies

Network Manager biedt de volgende functies:

Grafisch netwerkoverzicht

Het netwerkoverzicht van Network Manager biedt een grafisch overzicht van de beveiligingsstatus van de computers en componenten waaruit uw thuisnetwerk bestaat. Wanneer u wijzigingen aanbrengt in uw netwerk (zoals wanneer u een computer toevoegt), herkent het netwerkoverzicht deze wijzigingen. U kunt het netwerkoverzicht vernieuwen, de naam van het netwerk wijzigen of uw weergave wijzigen door componenten van het netwerkoverzicht weer te geven of te verbergen. U kunt ook de details bekijken van elk onderdeel dat in het netwerkoverzicht wordt weergegeven.

Extern beheer

Gebruik het netwerkoverzicht van Network Manager om de beveiligingsstatus te beheren van de computers waaruit uw thuisnetwerk bestaat. U kunt een computer uitnodigen om lid te worden van het beheerde netwerk, de beveiligingsstatus van de beheerde computer controleren, en bekende zwakke punten in de beveiliging oplossen vanaf een externe computer in het netwerk.

Informatie over pictogrammen van Network Manager

In de volgende tabel worden de pictogrammen beschreven die worden gebruikt in het netwerkoverzicht van Network Manager.

Pictogram	Beschrijving
	Een online, beheerde computer
	Een offline, beheerde computer
	Een niet-beheerde computer waarop McAfee 2007-beveiligingssoftware is geïnstalleerd
	Een offline, niet-beheerde computer
	Een online computer waarop geen McAfee 2007-beveiligingssoftware is geïnstalleerd of een onbekend netwerkapparaat
	Een offline computer waarop geen McAfee 2007-beveiligingssoftware is geïnstalleerd of een offline, onbekend netwerkapparaat
	Het bijbehorende item is beveiligd en aangesloten
	Het bijbehorende item vereist uw aandacht
	Het bijbehorende item vereist uw aandacht en is niet aangesloten
	Een draadloze thuisrouter
	Een standaardthuisrouter
	Het internet, als u verbinding hebt
	Het internet, als u geen verbinding hebt

HOOFDSTUK 11

Een beheerd netwerk instellen

Als u een beheerd netwerk wilt instellen, werkt u met de items in het netwerkoverzicht en voegt u leden (computers) aan het netwerk toe.

In dit hoofdstuk

Werken met het netwerkoverzicht

Elke keer dat u een computer op het netwerk aansluit, wordt de status van het netwerk geanalyseerd met Network Manager om te bepalen of er (beheerde of niet-beheerde) leden zijn en wat de routerkenmerken en de internetstatus zijn. Als er geen leden worden gevonden, wordt aangenomen dat de momenteel aangesloten computer de eerste computer in het netwerk is en wordt de computer automatisch een beheerd lid met beheerrechten. De naam van het netwerk bestaat standaard uit de werkgroep- of domeinnaam van de eerste computer met McAfee 2007-beveiligingssoftware die op het netwerk wordt aangesloten. U kunt de naam van het netwerk echter op elk moment wijzigen.

Als u wijzigingen in het netwerk aanbrengt (bijvoorbeeld een computer toevoegt, kunt u het netwerkoverzicht aanpassen. Zo kunt u het netwerkoverzicht vernieuwen, de naam van het netwerk wijzigen, en onderdelen van het netwerkoverzicht weergeven of verbergen om de weergave aan te passen. U kunt ook de details bekijken van elk onderdeel dat in het netwerkoverzicht wordt weergegeven.

Het netwerkoverzicht openen

Als u een overzicht van het netwerk wilt weergeven, start u Network Manager vanuit de lijst met algemene taken in SecurityCenter. Het netwerkoverzicht biedt een grafische weergave van de computers en onderdelen in uw thuisnetwerk.

Ga als volgt te werk om het netwerkoverzicht te openen:

- Klik in het menu Basis of Geavanceerd op **Netwerk beheren**. Het netwerkoverzicht wordt nu weergegeven in het rechterdeelvenster.

Opmerking: De eerste keer dat u het netwerkoverzicht opent, wordt u gevraagd de andere computers in het netwerk te vertrouwen voordat het netwerkoverzicht verschijnt.

Het netwerkoverzicht vernieuwen

U kunt het netwerkoverzicht altijd vernieuwen, bijvoorbeeld nadat u een andere computer aan het beheerde netwerk hebt toegevoegd.

Het netwerkoverzicht vernieuwen:

1. Klik in het menu Basis of Geavanceerd op **Netwerk beheren**. Het netwerkoverzicht wordt nu weergegeven in het rechterdeelvenster.
2. Klik op **Het netwerkoverzicht vernieuwen** onder **Ik wil**.

Opmerking: de koppeling **Het netwerkoverzicht vernieuwen** is alleen beschikbaar als u geen items hebt geselecteerd in het netwerkoverzicht. Als u de selectie van een item wilt opheffen, klikt u op het geselecteerde item of op een leeg gedeelte in het netwerkoverzicht.

De naam van het netwerk wijzigen

De naam van het netwerk bestaat standaard uit de werkgroep- of domeinnaam van de eerste computer met McAfee 2007-beveiligingssoftware die op het netwerk wordt aangesloten. U kunt deze naam desgewenst wijzigen.

De naam van het netwerk wijzigen:

1. Klik in het menu Basis of Geavanceerd op **Netwerk beheren**. Het netwerkoverzicht wordt nu weergegeven in het rechterdeelvenster.
2. Klik op **De naam van het netwerk wijzigen** onder **Ik wil**.
3. Typ de gewenste naam van het netwerk in het vak **Naam van netwerk wijzigen**.
4. Klik op **OK**.

Opmerking: de koppeling **De naam van het netwerk wijzigen** is alleen beschikbaar als u geen items hebt geselecteerd in het netwerkoverzicht. Als u de selectie van een item wilt opheffen, klikt u op het geselecteerde item of op een leeg gedeelte in het netwerkoverzicht.

Items in het netwerkoverzicht weergeven of verbergen

Standaard worden alle computers en onderdelen in uw thuisnetwerk weergegeven in het netwerkoverzicht. Als u items hebt verborgen, kunt u deze op elk moment weer weergeven. U kunt alleen niet-beheerde items verbergen. Beheerde computers worden altijd weergegeven.

Om...	Klik in het menu Basis of Geavanceerd op **Netwerk beheren** en voer een van de volgende handelingen uit...
Een item in het netwerkoverzicht verbergen	Klik op een item in het netwerkoverzicht en vervolgens op **Dit item verbergen** onder **Ik wil**. Klik op **Ja** in het bevestigingsdialoogvenster.
Verborgen items in het netwerkoverzicht weergeven	Klik op **Verborgen items weergegeven** onder **Ik wil**.

Informatie over items bekijken

U kunt gedetailleerde informatie over elk onderdeel in uw netwerk bekijken door het onderdeel in het netwerkoverzicht te selecteren. Deze informatie bestaat uit de naam van het onderdeel, de beveiligingsstatus en andere gegevens die nodig zijn om het onderdeel te beheren.

De details van een item bekijken:

1. Klik op het pictogram van een item in het netwerkoverzicht.
2. Bekijk informatie over het item onder **Details**.

Lid worden van het beheerde netwerk

U kunt een computer alleen op afstand beheren of machtiging verlenen om andere computers in het netwerk op afstand te beheren als deze computer een vertrouwd lid van het netwerk is. Lidmaatschap van het netwerk wordt aan nieuwe computers verleend door bestaande leden (computers) met beheerrechten. Gebruikers van zowel de verlenende computer als de computer die wordt toegevoegd, moeten elkaar verifiëren om ervoor te zorgen dat alleen vertrouwde computers lid van het netwerk worden.

Als een computer aan het netwerk wordt toegevoegd, wordt de computer gevraagd de McAfee-beveiligingsstatus zichtbaar te maken voor andere computers in het netwerk. Zodra een computer de beveiligingsstatus beschikbaar maakt, wordt de computer een *beheerd* lid van het netwerk. Als een computer de beveiligingsstatus niet beschikbaar maakt, wordt de computer een *niet-beheerd* lid van het netwerk. Niet-beheerde leden van het netwerk zijn doorgaans gastcomputers die willen gebruikmaken van andere netwerkvoorzieningen (bijvoorbeeld het delen van bestanden of printers).

Opmerking: zodra een computer met andere netwerkprogramma's van McAfee (zoals McAfee Wireless Network Security of EasyNetwork) aan het netwerk is toegevoegd, wordt de computer eveneens herkend als beheerde computer in deze programma's. Het machtigingsniveau dat aan een computer wordt toegewezen Network Manager, wordt toegepast op alle McAfee-netwerkprogramma's. Raadpleeg de documentatie bij een programma voor meer informatie over de betekenis van gast-, beheer- en volledige machtigingen in andere McAfee-netwerkprogramma's.

Lid worden van een beheerd netwerk

Als u een uitnodiging krijgt om lid te worden van een beheerd netwerk, kunt u de uitnodiging accepteren of weigeren. U kunt ook aangeven of u wilt dat deze computer en andere computers in het netwerk elkaars beveiligingsinstellingen controleren (bijvoorbeeld of de virusbeveiligingsservices van een computer up-to-date zijn).

Ga als volgt te werk om lid te worden van een beheerd netwerk:

1. Schakel in het uitnodigingsdialoogvenster het selectievakje **Deze computer en andere computers in het netwerk toestaan elkaars beveiligingsinstellingen te controleren** om andere computers in het beheerde netwerk toe te staan de beveiligingsinstellingen van uw computer te controleren.
2. Klik op **Aanmelden**.
   Als u de uitnodiging accepteert, worden twee speelkaarten weergegeven.
3. Bevestig dat de speelkaarten overeenkomen met de speelkaarten op de computer die de uitnodiging heeft verstuurd om lid te worden van het beheerde netwerk.
4. Klik op **Bevestigen**.

Opmerking: als op de computer die u heeft uitgenodigd lid te worden van het beheerde netwerk niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een lek in de beveiliging van het beheerde netwerk. Als u lid wordt van het netwerk, kunt u uw computer in gevaar brengen. Klik daarom op **Weigeren** in het bevestigingsdialoogvenster.

Een computer uitnodigen om lid te worden van het beheerde netwerk

Als een computer wordt toegevoegd aan het beheerde netwerk of als het netwerk een andere, niet-beheerde computer bevat, kunt u deze computer uitnodigen om lid te worden van het beheerde netwerk. Alleen computers met beheerrechten voor het netwerk kunnen andere computers uitnodigen om lid van het netwerk te worden. In de uitnodiging kunt u tevens aangeven welk machtigingsniveau u wilt toewijzen aan de computer die wordt toegevoegd.

Ga als volgt te werk om een computer uit te nodigen om lid te worden van het beheerde netwerk:

1. Klik op het pictogram van een niet-beheerde computer in het netwerkoverzicht.
2. Klik op **Deze computer controleren** onder **Ik wil**.
3. Klik in het dialoogvenster Een computer uitnodigen om lid te worden van dit beheerde netwerk op een van de volgende opties:
   - **Gasttoegang verlenen**
     Met gasttoegang heeft de computer toegang tot het netwerk.
   - **Volledige toegang verlenen tot alle beheerde netwerktoepassingen**
     Met volledige toegang heeft de computer toegang tot het netwerk (net als met gasttoegang).
   - **Beheertoegang verlenen tot alle beheerde netwerktoepassingen**
     Met beheertoegang heeft de computer toegang tot het netwerk met beheerrechten. De computer kan dan tevens toegang verlenen aan andere computers die lid van het beheerde netwerk willen worden.

4 Klik op **Uitnodigen**.
Een uitnodiging om lid te worden van het beheerde netwerk wordt naar de computer verzonden. Zodra de computer de uitnodiging accepteert, worden twee speelkaarten weergegeven.

5 Bevestig dat de speelkaarten overeenkomen met de speelkaarten op de computer die u hebt uitgenodigd om lid te worden van het beheerde netwerk.

6 Klik op **Toegang verlenen**.

Opmerking: als op de computer die u hebt uitgenodigd lid te worden van het beheerde netwerk niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een lek in de beveiliging van het beheerde netwerk. Als u de computer toestaan om lid te worden van het netwerk, kunt u andere computers in gevaar brengen. Klik daarom op **Toegang weigeren** in het bevestigingsdialoogvenster.

Computers op het netwerk niet meer vertrouwen

Als u per ongeluk aangeeft dat u de andere computers in het netwerk wilt vertrouwen, kunt u dit ongedaan maken.

Ga als volgt te werk om het vertrouwen van computers in het netwerk ongedaan te maken:

- Klik op **Computers in dit netwerk niet vertrouwen** onder **Ik wil**.

Opmerking: de koppeling **Computers in dit netwerk niet vertrouwen** is alleen beschikbaar als geen andere beheerde computers lid zijn van het netwerk.

HOOFDSTUK 12

Het netwerk op afstand beheren

Nadat u het beheerde netwerk hebt ingesteld, kunt u de computers en onderdelen van het netwerk op afstand beheren van Network Manager. Zo kunt u de status en machtigingsniveaus van de computers en onderdelen op afstand controleren en beveiligingsproblemen op afstand oplossen.

In dit hoofdstuk

Status en machtigingen controleren

Een beheerd netwerk heeft twee soorten leden: beheerde leden en niet-beheerde leden. Beheerde leden staan andere computers in het netwerk toe hun McAfee-beveiligingsstatus te controleren. Niet-beheerde leden staan dit niet toe. Niet-beheerde leden zijn doorgaans gastcomputers die willen gebruikmaken van andere netwerkvoorzieningen (bijvoorbeeld het delen van bestanden of printers). Een beheerde computer in het netwerk kan een niet-beheerde computer uitnodigen om een beheerd lid te worden. Evenzo kan een beheerde computer niet-beheerd worden gemaakt.

Beheerde computers hebben beheer-, gast- of volledige machtiging voor het netwerk. Met een beheermachtiging kan de beheerde computer de beveiligingsstatus van alle andere beheerde computers in het netwerk beheren en andere computers lid van het netwerk maken. Met een gast- of volledige machtiging heeft een computer alleen toegang tot het netwerk. U kunt het machtigingsniveau van een computer op elk moment wijzigen.

Omdat een beheerd netwerk ook apparaten kan bevatten (zoals routers), kunt u deze eveneens met Network Manager beheren. Tevens kunt u de weergave-eigenschappen van een apparaat in het netwerkoverzicht configureren en wijzigen.

De beveiligingsstatus van een computer controleren

Als de beveiligingsstatus van een computer niet wordt gecontroleerd in het netwerk (omdat de computer geen lid of een onbeheerd lid van het netwerk is), kunt u een verzoek indienen om de computer te controleren.

Ga als volgt te werk om de beveiligingsstatus van een computer te controleren:

1. Klik op het pictogram van een niet-beheerde computer in het netwerkoverzicht.
2. Klik op **Deze computer controleren** onder **Ik wil**.

De controle van de beveiligingsstatus van een computer stoppen

U kunt de controle van de beveiligingsstatus van een beheerde computer in uw privé-netwerk stoppen. De computer wordt dan een niet-beheerde computer.

Ga als volgt te werk om de controle van de beveiligingsstatus van een computer te stoppen:

1. Klik op het pictogram van een beheerde computer in het netwerkoverzicht.
2. Klik op **Controle van deze computer stoppen** onder **Ik wil**.
3. Klik op **Ja** in het bevestigingsdialoogvenster.

Machtigingen van een beheerde computer wijzigen

U kunt de machtigingen van een beheerde computer op elk moment wijzigen. Zo kunt u de computers wijzigen die de beveiligingsstatus (beveiligingsinstellingen) van andere computers in het netwerk kunnen controleren.

Ga als volgt te werk om machtigingen van een beheerde computer te wijzigen:

1. Klik op het pictogram van een beheerde computer in het netwerkoverzicht.
2. Klik op **Machtigingen voor deze computer wijzigen** onder **Ik wil**.
3. Schakel in het dialoogvenster Machtigingen wijzigen het selectievakje in of uit om aan te geven of deze computer en andere computers in het beheerde netwerk elkaars beveiligingsstatus kunnen controleren.
4. Klik op **OK**.

Een apparaat beheren

U kunt een apparaat beheren door de beheerwebpagina van het apparaat te openen vanuit Network Manager.

Een apparaat beheren:

1. Klik op het pictogram van een apparaat in het netwerkoverzicht.
2. Klik op **Dit apparaat beheren** onder **Ik wil**.
   De webbrowser wordt geopend, waarin de beheerwebpagina van het apparaat wordt weergegeven.
3. Geef in de webbrowser uw aanmeldingsgegevens op en configureer de beveiligingsinstellingen van het apparaat.

Opmerking: als het apparaat een draadloze router of toegangspunt is die is beveiligd met Wireless Network Security, moet u de beveiligingsinstellingen van het apparaat configureren in Wireless Network Security.

De weergave-eigenschappen van een apparaat wijzigen

Als u de weergave-eigenschappen van een apparaat wijzigen, kunt u de apparaatnaam wijzigen die wordt weergegeven in het netwerkoverzicht en aangeven of het apparaat een draadloze router is.

Ga als volgt te werk om de weergave-eigenschappen van een apparaat te wijzigen:

1. Klik op het pictogram van een apparaat in het netwerkoverzicht.
2. Klik op **Apparaateigenschappen wijzigen** onder **Ik wil**.
3. Typ een naam in het vak **Naam** om de weergavenaam van het apparaat op te geven.
4. Als u het apparaattype wilt opgeven, klikt u op een van de volgende opties:
   - **Router**
     Een standaardthuisrouter.
   - **Draadloze router**
     Een draadloze thuisrouter.
5. Klik op **OK**.

Beveiligingsproblemen oplossen

Vanaf beheerde computers met beheerrechten kunt u de McAfee-beveiligingsstatus van andere beheerde computers in het netwerk op afstand controleren en gerapporteerde beveiligingsproblemen op afstand oplossen. Wanneer de McAfee-beveiligingsstatus van een beheerde computer bijvoorbeeld aangeeft dat VirusScan is uitgeschakeld, kunt u dit beveiligingsprobleem vanaf een andere beheerde computer met beheerrechten *oplossen* door VirusScan op afstand in te schakelen.

Als u beveiligingsproblemen op afstand oplost, worden de meeste gerapporteerde problemen automatisch hersteld met Network Manager. Voor bepaalde beveiligingsproblemen kan echter handmatige interventie op de lokale computer zijn vereist. In dit geval worden de problemen opgelost die op afstand kunnen worden hersteld, en wordt u vervolgens gevraagd de resterende problemen op te lossen door u aan te melden bij SecurityCenter op de kwetsbare computer en de aanbevolen handelingen uit te voeren. Soms wordt als mogelijke oplossing aanbevolen McAfee 2007-beveiligingssoftware op de externe computer of computers in uw netwerk te installeren.

Beveiligingsproblemen oplossen

Met Network Manager kunt u de meeste beveiligingsproblemen op externe beheerde computers automatisch oplossen. Als VirusScan bijvoorbeeld is uitgeschakeld op een externe computer, kunt u dit programma automatisch inschakelen met Network Manager.

Ga als volgt te werk om beveiligingsproblemen op te lossen:

1. Klik op het pictogram van een item in het netwerkoverzicht.
2. Bekijk de beveiligingsstatus van het item onder **Details**.
3. Klik op **Beveiligingsproblemen oplossen** onder **Ik wil**.
4. Klik op **OK** als u de beveiligingsproblemen hebt opgelost.

Opmerking: hoewel met Network Manager de meeste beveiligingsproblemen automatisch worden opgelost, vereisen bepaalde problemen dat u zicht aanmeldt bij SecurityCenter op de kwetsbare computer en de aanbevolen handelingen uitvoert.

McAfee-beveiligingssoftware installeren op externe computers

Als op een of meer computers in het netwerk geen McAfee 2007-beveiligingssoftware wordt uitgevoerd, kan de beveiligingsstatus van deze computers niet op afstand worden gecontroleerd. Als u deze computers op afstand wilt controleren, moet u de McAfee 2007-beveiligingssoftware ter plaatse op elke computer installeren.

McAfee-beveiligingssoftware installeren op een externe computer:

1. Ga in een browser op de externe computer naar http://download.mcafee.com/us/.
2. Volg de aanwijzingen op het scherm om McAfee 2007-beveiligingssoftware op de computer te installeren.

HOOFDSTUK 13

McAfee VirusScan

VirusScan biedt uitgebreide, betrouwbare en up-to-date beveiliging tegen virussen en spyware. VirusScan is gebaseerd op de veelgeprezen scantechnologie van McAfee en biedt bescherming tegen virussen, wormen, Trojaanse paarden, schadelijke scripts, rootkits, overschrijdingen van de bufferlimiet, hybride aanvallen, spyware, mogelijk ongewenste programma's en andere bedreigingen.

In dit hoofdstuk

Functies

Deze versie van VirusScan biedt de volgende functies.

Virusbeveiliging

Door real-time scannen worden bestanden gescand wanneer deze door u of de computer worden geopend.

Scannen

Zoeken naar virussen en andere bedreigingen op vaste schijven, diskettes en in afzonderlijke bestanden en mappen. U kunt ook met de rechtermuisknop op een item klikken om het te scannen.

Detectie van spyware en adware

VirusScan detecteert en verwijdert spyware, adware en andere programma's die uw privacy in gevaar kunnen brengen en de prestaties van uw computer nadelig kunnen beïnvloeden.

Automatische updates

Automatische updates beschermen u tegen de allernieuwste bekende en onbekende virussen.

Snel scannen op de achtergrond

Snelle, onopvallende scans detecteren en vernietigen virussen, Trojaanse paarden, wormen, spyware, adware, dialers en andere bedreigingen zonder uw werk te onderbreken.

Real-time beveiligingswaarschuwingen

Door middel van beveiligingswaarschuwingen wordt u op de hoogte gebracht van nieuwe virusuitbraken en veiligheidsrisico's en krijgt u de mogelijkheid aangeboden de bedreigingen te verwijderen, te neutraliseren of er meer informatie over te lezen.

Detecteren en opschonen op meerdere ingangspunten

VirusScan bewaakt en schoont uw computer op de belangrijkste ingangspunten op: e-mail, inkomende bijlagen bij expresberichten en downloads van internet.

E-mailbewaking op wormachtige activiteiten

WormStopper™ blokkeert Trojaanse paarden van e-mailwormen naar andere computers en vraagt u om toestemming voordat onbekende e-mailprogramma's e-mailberichten verzenden naar andere computers.

Scriptbewaking op wormachtige activiteiten

ScriptStopper™ voorkomt dat bekende, schadelijke scripts op de computer worden uitgevoerd.

McAfee X-ray for Windows

McAfee X-ray detecteert en elimineert rootkits en andere programma's die zich verborgen houden voor Windows.

Bescherming overschrijding bufferlimiet

Met bescherming tegen overschrijding van bufferlimieten wordt voorkomen dat de limieten van buffers worden overschreden. Overschrijdingen van de bufferlimiet treden op als verdachte programma's of processen proberen meer gegevens in een buffer (tijdelijke opslagruimte voor gegevens) op de computer op te slaan dan is toegestaan, waardoor geldige gegevens in nabijgelegen buffers worden beschadigd of overschreven.

McAfee SystemGuards

SystemGuards onderzoeken de computer op specifieke gedragingen die kunnen duiden op activiteiten van virussen, spyware of hackers.

HOOFDSTUK 14

Virusbeveiliging beheren

U kunt real-time SystemGuards, virus-, spyware- en scriptbeveiliging beheren. U kunt bijvoorbeeld scannen uitschakelen of opgeven wat moet worden gescand.

Alleen gebruikers met beheerdersrechten kunnen geavanceerde opties wijzigen.

In dit hoofdstuk

Virusbeveiliging gebruiken

Wanneer virusbeveiliging (real-time scannen) wordt gestart, wordt de computer constant gecontroleerd op virusactiviteiten. Door real-time scannen worden bestanden gescand elke keer dat ze door u of de computer worden geopend. Wanneer de virusbeveiliging een geïnfecteerd bestand aantreft, wordt er geprobeerd de infectie op te schonen of te verwijderen. Als een bestand niet kan worden opgeschoond of verwijderd, wordt u via een waarschuwing gevraagd verdere actie te ondernemen.

Verwante onderwerpen

- Beveiligingswaarschuwingen (pagina 109)

Virusbeveiliging uitschakelen

Als u virusbeveiliging uitschakelt, wordt de computer niet constant gecontroleerd op virusactiviteit. Als u de virusbeveiliging moet stoppen, moet u ervoor zorgen dat u geen verbinding hebt met internet.

Opmerking: Als u virusbeveiliging uitschakelt, wordt ook real-time beveiliging tegen spyware, van e-mail en van expresberichten uitgeschakeld.

Ga als volgt te werk om de virusbeveiliging uit te schakelen:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Virusbeveiliging** op **Uit**.
4. Ga op een van de volgende manieren te werk in het bevestigingsdialoogvenster:
   - Als u de virusbeveiliging na een opgegeven tijd weer wilt starten, schakelt u het selectievakje **Real-time scannen opnieuw inschakelen na** in en selecteert u een tijd in het menu.
   - Als u niet wilt dat de virusbeveiliging na een opgegeven tijd weer wordt gestart, schakelt u het selectievakje **Real-time scannen opnieuw inschakelen na** uit.

5 Klik op **OK**.

Als de real-time beveiliging zo is geconfigureerd dat deze wordt gestart wanneer Windows wordt gestart, wordt de computer weer beveiligd wanneer u de computer opnieuw opstart.

Verwante onderwerpen

- Real-time beveiliging configureren (pagina 80)

Virusbeveiliging inschakelen

Met virusbeveiliging wordt de computer constant gecontroleerd op virusactiviteiten.

U schakelt virusbeveiliging als volgt in:

1 Klik in het menu Geavanceerd op **Configureren**.

2 Klik in het deelvenster Configureren op **Computer en bestanden**.

3 Klik onder **Virusbeveiliging** op **Aan**.

Real-time beveiliging configureren

U kunt de real-time virusbeveiliging wijzigen. U kunt bijvoorbeeld alleen programmabestanden en documenten scannen, of real-time scannen uitschakelen wanneer Windows wordt gestart (wordt niet aanbevolen).

Real-time beveiliging configureren

U kunt de real-time virusbeveiliging wijzigen. U kunt bijvoorbeeld alleen programmabestanden en documenten scannen, of real-time scannen uitschakelen wanneer Windows wordt gestart (wordt niet aanbevolen).

Ga als volgt te werk om de real-time beveiliging te configureren:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Virusbeveiliging** op **Geavanceerd**.
4. Schakel de volgende selectievakjes in of uit:
   - **Scannen op onbekende virussen met behulp van heuristische technieken**: Bestanden worden vergeleken met handtekeningen van bekende virussen om tekenen van onbekende virussen te kunnen ontdekken. Met deze optie voert u de grondigste scanbewerking uit, maar dit duurt wel langer dan een normale scanbewerking.
   - **Diskettestation bij het uitschakelen scannen**: Wanneer u de computer uitschakelt, wordt het diskettestation gescand.
   - **Scannen op spyware en mogelijk ongewenste programma's**: Spyware, adware en andere programma's die mogelijk gegevens verzamelen en verzenden zonder uw toestemming, worden opgespoord en verwijderd.
   - **Trackingcookies scannen en verwijderen**: Cookies die mogelijk gegevens verzamelen en verzenden zonder uw toestemming, worden gedetecteerd en verwijderd. Een cookie zorgt voor de identificatie van gebruikers wanneer deze een webpagina bezoeken.
   - **Netwerkstations scannen**: Stations die zijn aangesloten op het netwerk, worden gescand.
   - **Bescherming overschrijding bufferlimiet inschakelen**: Als er een overschrijdingsactiviteit van de bufferlimiet wordt gedetecteerd, wordt deze activiteit geblokkeerd en ontvangt u een waarschuwing.
   - **Real-time scannen starten bij het starten van Windows (aanbevolen)**: Real-time beveiliging wordt ingeschakeld elke keer dat u de computer start, zelfs als u de beveiliging tijdens een sessie hebt uitgeschakeld.

5 Klik op een van de volgende knoppen:

- **Alle bestanden (aanbevolen)**: Elk bestandstype dat op de computer wordt gebruikt, wordt gescand. Wanneer deze optie is ingeschakeld, maakt u zo grondig mogelijk gebruik van de scanfunctie.
- **Alleen programmabestanden en documenten**: Alleen programmabestanden en documenten worden gescand.

6 Klik op **OK**.

Spywarebeveiliging gebruiken

Door spywarebeveiliging worden spyware, adware en andere mogelijk ongewenste programma's die gegevens verzamelen en verzenden zonder uw toestemming, verwijderd.

Spywarebeveiliging uitschakelen

Als u spywarebeveiliging uitschakelt, worden mogelijk ongewenste programma's die gegevens verzamelen en verzenden zonder uw toestemming, niet gedetecteerd.

U schakelt spywarebeveiliging als volgt uit:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Spywarebeveiliging** op **Uit**.

Spywarebeveiliging inschakelen

Door spywarebeveiliging worden spyware, adware en andere mogelijk ongewenste programma's die gegevens verzamelen en verzenden zonder uw toestemming, verwijderd.

U schakelt spywarebeveiliging als volgt in:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Spywarebeveiliging** op **Aan**.

SystemGuards gebruiken

SystemGuards detecteren mogelijk onbevoegde wijzigingen op de computer en waarschuwen u wanneer deze zich voordoen. U kunt deze wijzigingen vervolgens bekijken en beslissen of u ze al dan niet wilt toestaan.

SystemGuards worden als volgt ingedeeld in categorieën.

Programma

SystemGuards voor programma's detecteren wijzigingen in opstartbestanden, extensies en configuratiebestanden.

Windows

SystemGuards voor Windows detecteren wijzigingen in de instellingen van Internet Explorer, zoals browsereigenschappen en beveiligingsinstellingen.

Browser

SystemGuards voor browsers detecteren wijzigingen in Windows®-services, certificaten en configuratiebestanden.

SystemGuards uitschakelen

Als u SystemGuards uitschakelt, worden mogelijk onbevoegde wijzigingen op de computer niet gedetecteerd.

U schakelt alle SystemGuards als volgt uit:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **SystemGuard-beveiliging** op **Uit**.

SystemGuards inschakelen

SystemGuards detecteren mogelijk onbevoegde wijzigingen op de computer en waarschuwen u wanneer deze zich voordoen.

U schakelt SystemGuards als volgt in:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **SystemGuard-beveiliging** op **Aan**.

SystemGuards configureren

U kunt SystemGuards wijzigen. Voor elke wijziging die wordt gedetecteerd kunt u bepalen of u wilt worden gewaarschuwd en of de gebeurtenis moet worden geregistreerd in het logboek, of de gebeurtenis alleen moet worden geregistreerd in het logboek, of dat de SystemGuard moet worden uitgeschakeld.

SystemGuards configureren

U kunt SystemGuards wijzigen. Voor elke wijziging die wordt gedetecteerd kunt u bepalen of u wilt worden gewaarschuwd en of de gebeurtenis moet worden geregistreerd in het logboek, of de gebeurtenis alleen moet worden geregistreerd in het logboek, of dat de SystemGuard moet worden uitgeschakeld.

U configureert SystemGuards als volgt:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **SystemGuard-beveiliging** op **Geavanceerd**.
4. Klik in de SystemGuards-lijst op een categorie om een lijst weer te geven van SystemGuards en de bijbehorende status.
5. Klik op de naam van een SystemGuard.
6. Bekijk informatie over de SystemGuard onder **Details**.
7. Ga op een van de volgende manieren te werk onder **Ik wil**:
   - Klik op **Waarschuwingen weergeven** als u wilt worden gewaarschuwd wanneer er een verandering plaatsvindt en als u wilt dat de gebeurtenis wordt geregistreerd in het logboek.
   - Klik op **Wijzigingen alleen vastleggen in logboek** als u niet wilt dat er actie wordt ondernomen wanneer er een verandering wordt gedetecteerd. De verandering wordt alleen geregistreerd in het logboek.
   - Klik op **Deze SystemGuard uitschakelen** als u de SystemGuard wilt uitschakelen. U ontvangt geen waarschuwing wanneer er een verandering plaatsvindt en de gebeurtenis wordt niet geregistreerd in het logboek.
8. Klik op **OK**.

SystemGuards

SystemGuards detecteren mogelijk onbevoegde wijzigingen op de computer en waarschuwen u wanneer deze zich voordoen. U kunt deze wijzigingen vervolgens bekijken en beslissen of u ze al dan niet wilt toestaan.

SystemGuards worden als volgt ingedeeld in categorieën.

Programma

SystemGuards voor programma's detecteren wijzigingen in opstartbestanden, extensies en configuratiebestanden.

Windows

SystemGuards voor Windows detecteren wijzigingen in de instellingen van Internet Explorer, zoals browsereigenschappen en beveiligingsinstellingen.

Browser

SystemGuards voor browsers detecteren wijzigingen in Windows®-services, certificaten en configuratiebestanden.

Info over SystemGuards voor programma's

SystemGuards voor programma's detecteren de volgende items.

ActiveX-installaties

Hiermee worden ActiveX-programma's gedetecteerd die worden gedownload via Internet Explorer. ActiveX-programma's worden gedownload van websites en op de computer opgeslagen in C:\Windows\Downloaded Program Files of C:\Windows\Temp\Temporary Internet Files. Er wordt ook in het register naar verwezen aan de hand van hun CLSID (de lange reeks cijfers tussen accolades).

In Internet Explorer worden vele legitieme ActiveX-programma's gebruikt. Als u niet zeker bent van een ActiveX-programma, kunt u het verwijderen zonder schade toe te brengen aan de computer. Als u dit programma later opnieuw nodig hebt, wordt het automatisch door Internet Explorer gedownload de volgende keer dat u teruggaat naar een website die dit programma nodig heeft.

Opstartitems

Hiermee wordt gecontroleerd op wijzigingen in de registersleutels en mappen bij opstarten. Registersleutels voor opstarten zijn vermeldingen in het register van Windows waarin paden naar programma's op de computer worden opgeslagen. Programma's die op deze locaties staan vermeld, worden geladen wanneer Windows wordt gestart. Spyware of andere mogelijk ongewenste programma's proberen vaak automatisch te worden geladen bij het starten van Windows.

Windows-shell-uitvoeringshooks

Hiermee wordt gecontroleerd op wijzigingen die worden aangebracht in de lijst met programma's die in explorer.exe worden geladen. Een shell-uitvoeringshook is een programma dat in de Windows-shell van explorer.exe wordt geladen. Een shell-uitvoeringshook ontvangt alle uitvoeringsopdrachten die op een computer worden uitgevoerd. Elk programma dat in de shell van explorer.exe wordt geladen, kan een extra taak uitvoeren voordat een andere programma daadwerkelijk wordt gestart. Spyware of andere mogelijk ongewenste programma's kunnen shell-uitvoeringshooks gebruiken om te voorkomen dat beveiligingsprogramma's worden uitgevoerd.

Vertraagd laden Shell-serviceobject

Hiermee wordt gecontroleerd op wijzigingen aan bestanden die staan vermeld in Vertraagd laden Shell-serviceobject. Deze bestanden worden door explorer.exe geladen wanneer de computer wordt gestart. Aangezien explorer.exe de shell voor de computer vormt, wordt dit programma altijd gestart, waarbij de bestanden worden geladen waarnaar met in sleutel wordt verwezen. Deze bestanden worden in een vroegtijdig stadium van het opstartproces geladen voordat er sprake is van menselijke tussenkomst.

Info over SystemGuards voor Windows

SystemGuards voor Windows detecteren de volgende items.

Handlers voor contextmenu

Hiermee worden onbevoegde wijzigingen in contextmenu's van Windows voorkomen. Deze menu's stellen u in staat met de rechtermuisknop op een bestand te klikken en specifieke acties uit te voeren die relevant zijn voor het desbetreffende bestand.

AppInit DLLs

Hiermee worden onbevoegde wijzigingen in Windows AppInit.DLLs voorkomen. De registerwaarde AppInit_DLLs bevat een lijst met bestanden die worden geladen wanneer user32.dll wordt geladen. Bestanden in de waarde AppInit_DLLs worden in een vroeg stadium van de Windows-opstartroutine geladen, waardoor een mogelijk schadelijk .DDL-programma zich kan verbergen voordat er sprake is van menselijke tussenkomst.

Hosts-bestand van Windows

Hiermee wordt gecontroleerd op wijzigingen in het Hosts-bestand van de computer. Het Hosts-bestand wordt gebruikt voor het herleiden van bepaalde domeinnamen naar specifieke IP-adressen. Als u bijvoorbeeld een bezoek brengt aan www.voorbeeld.com, controleert de browser het Hosts-bestand, ziet een vermelding voor voorbeeld.com en verwijst naar het IP-adres voor dat domein. Bepaalde spywareprogramma's proberen het Hosts-bestand te wijzigen om de browser om te leiden naar een andere site of om te voorkomen dat software correct wordt bijgewerkt.

Winlogon-shell

Hiermee wordt de Winlogon-shell gecontroleerd. Deze shell wordt geladen wanneer een gebruiker zich aanmeldt bij Windows. De shell is de primaire gebruikersinterface die wordt gebruikt voor het beheren van Windows. Gewoonlijk is dit Windows Verkenner (explorer.exe). De Windows-shell kan echter gemakkelijk worden gewijzigd zodat naar een ander programma wordt verwezen. Als dit gebeurt, wordt een ander programma dan de Windows-shell gestart telkens wanneer een gebruiker zich aanmeldt.

Winlogon UserInit

Hiermee wordt gecontroleerd op wijzigingen in uw gebruikersinstellingen voor aanmelding bij Windows. Met de sleutel HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit wordt opgegeven welk programma wordt gestart nadat een gebruiker zich heeft aangemeld bij Windows. Het standaardprogramma herstelt uw profiel, lettertypen, kleuren en andere instellingen voor uw gebruikersnaam. Spyware en andere mogelijk ongewenste programma's kunnen proberen te worden gestart door zichzelf toe te voegen aan deze sleutel.

Windows-protocollen

Hiermee wordt gecontroleerd op wijzigingen in uw netwerkprotocollen. Spyware of andere mogelijk ongewenste programma's nemen de controle over van sommige van de manieren waarop de computer informatie verzendt en ontvangt. Dit wordt gedaan via de filters en handlers van de Windows-protocollen.

Gelaagde serviceproviders van Winsock

Hiermee wordt gecontroleerd op gelaagde serviceproviders, waarmee gegevens via het netwerk kunnen worden onderschept en kunnen worden gewijzigd of omgeleid. Legitieme gelaagde serviceproviders zijn bijvoorbeeld software voor ouderlijk toezicht, firewalls en andere beveiligingsprogramma's. Spyware kan gebruikmaken van gelaagde serviceproviders om uw internetactiviteiten in de gaten te houden en gegevens te wijzigen. Om te voorkomen dat u het besturingssysteem opnieuw moet installeren, moet u McAfee-programma's gebruiken om spyware en gevaarlijke gelaagde serviceproviders automatisch te verwijderen.

Open-opdrachten voor Windows-shell

Hiermee worden wijzigingen in de Open-opdrachten van de Windows-shell (explorer.exe) voorkomen. Met Open-opdrachten voor de shell kan een specifiek programma worden geactiveerd, telkens wanneer er een bepaald type bestand wordt uitgevoerd. Zo kan bijvoorbeeld worden geprobeerd automatisch een worm te activeren telkens wanneer een .exe-bestand wordt uitgevoerd.

Gedeelde taakplanner

Hiermee wordt de registersleutel SharedTaskScheduler gecontroleerd, die een lijst bevat met programma's die worden uitgevoerd wanneer Windows wordt gestart. Bepaalde spywaretoepassingen of andere mogelijk ongewenste programma's wijzigen deze sleutel en voegen zichzelf zonder uw toestemming toe aan de lijst.

Windows Messenger Service

Hiermee wordt de Windows Messenger Service gecontroleerd, een niet-beschreven functie van Windows Messenger die gebruikers in staat stelt pop-upberichten te verzenden. Bepaalde spywaretoepassingen of andere mogelijk ongewenste programma's proberen deze service in te schakelen om ongevraagde reclame te verzenden. Deze service kan daarnaast ook worden gebruikt om een bekende kwetsbaarheid uit te buiten of op afstand een programmacode uit te voeren.

Win.ini-bestand van Windows

Het win.ini-bestand is een tekstbestand dat een lijst van programma's bevat die moeten worden uitgevoerd wanneer Windows wordt gestart. De syntaxis voor het laden van deze programma's bevindt zich ook in het bestand dat wordt gebruikt om ondersteuning te bieden voor oudere versies van Windows. De meeste programma's maken geen gebruik van het bestand win.ini om programma's te laden: bepaalde spywaretoepassingen of andere ongewenste programma's zijn echter speciaal zo ontworpen dat ze misbruik maken van deze oude syntaxis en zichzelf laden wanneer Windows wordt gestart.

Info over SystemGuards voor browsers

SystemGuards voor browsers detecteren de volgende items.

Browser Helper-objecten

Hiermee wordt gecontroleerd op toevoegingen aan Browser Helper-objecten (BHO's). BHO's zijn programma's die fungeren als invoegtoepassingen voor Internet Explorer. Spyware en programma's die de controle over de browser overnemen maken vaak gebruik van BHO's om advertenties weer te geven of uw browsergewoonten bij te houden. BHO's worden tevens gebruikt door tal van legitieme programma's, zoals de bekende zoekbalken.

Internet Explorer-balken

Hiermee wordt gecontroleerd op wijzigingen in de lijst met balken in Internet Explorer. Een verkennersbalk is een deelvenster zoals de deelvensters Zoeken, Favorieten of Geschiedenis die worden weergegeven in Internet Explorer (IE) of Windows Verkenner.

Invoegtoepassingen voor Internet Explorer

Hiermee wordt voorkomen dat spyware invoegtoepassingen voor Internet Explorer installeert. Invoegtoepassingen voor Internet Explorer zijn softwaretoevoegingen die worden geladen wanneer Internet Explorer wordt gestart. Spyware maakt vaak gebruik van invoegtoepassingen voor Internet Explorer om advertenties weer te geven of uw browsergewoonten bij te houden. Legitieme invoegtoepassingen voegen functionaliteit toe aan Internet Explorer.

Internet Explorer ShellBrowser

Hiermee wordt gecontroleerd op wijzigingen in het Internet Explorer ShellBrowser-exemplaar. De Internet Explorer ShellBrowser bevat informatie over en instellingen voor een exemplaar van Internet Explorer. Als deze instellingen worden gewijzigd of een nieuwe ShellBrowser wordt toegevoegd, kan deze ShellBrowser de volledige controle over Internet Explorer overnemen en functies zoals werkbalken, menu's en knoppen toevoegen.

Internet Explorer WebBrowser

Hiermee wordt gecontroleerd op wijzigingen in het Internet Explorer WebBrowser-exemplaar. De Internet Explorer WebBrowser bevat informatie over en instellingen voor een exemplaar van Internet Explorer. Als deze instellingen worden gewijzigd of een nieuwe WebBrowser wordt toegevoegd, kan deze WebBrowser de volledige controle over Internet Explorer overnemen en functies zoals werkbalken, menu's en knoppen toevoegen.

Internet Explorer-hooks voor zoeken van URL's

Hiermee wordt gecontroleerd op wijzigingen in de hook voor het zoeken van URL's in Internet Explorer. Een hook voor het zoeken van URL's wordt gebruikt als u een adres typt in het locatieveld van de browser zonder een protocol zoals http:// of ftp:// op te geven in het adres. Als u een dergelijk adres invoert, maakt de browser mogelijk gebruik van de UrlSearchHook om op het internet te zoeken naar de ingevoerde locatie.

Internet Explorer-URL's

Hiermee wordt gecontroleerd op wijzigingen in de vooraf ingestelde URL's voor Internet Explorer. Zo wordt voorkomen dat spyware of andere mogelijk ongewenste programma's uw browserinstellingen wijzigen zonder uw toestemming.

Internet Explorer-restricties

Hiermee worden Internet Explorer-restricties gecontroleerd, waarmee een computerbeheerder kan voorkomen dat een gebruiker de startpagina of andere opties in Internet Explorer kan wijzigen. Deze opties worden alleen weergegeven als de beheerder deze met opzet heeft ingesteld.

Beveiligde zones in Internet Explorer

Hiermee worden beveiligde zones in Internet Explorer beheerd. Internet Explorer heeft vier vooraf gedefinieerde beveiligingszones: Internet, Lokaal intranet, Vertrouwde websites en Websites met beperkte toegang. Elke beveiligingszone heeft zijn eigen beveiligingsinstellingen die vooraf zijn gedefinieerd of die kunnen worden aangepast. Beveiligingszones zijn het doelwit van bepaalde spywaretoepassingen of andere ongewenste programma's omdat deze waarschuwingen kunnen voorkomen en ongestoord te werk kunnen gaan als het beveiligingsniveau wordt verlaagd.

Vertrouwde sites van Internet Explorer

Hiermee worden vertrouwde sites van Internet Explorer gecontroleerd. De lijst met vertrouwde websites bevat alle websites die u vertrouwt. Bepaalde spywaretoepassingen of andere mogelijk ongewenste programma's proberen deze lijst te beïnvloeden om er zo voor te zorgen dat verdachte websites zonder meer worden vertrouwd zonder dat u dat weet.

Internet Explorer-policy

Hiermee worden de policy's van Internet Explorer gecontroleerd. Deze instellingen worden normaal gesproken gewijzigd door systeembeheerders. Spyware kan echter ook van deze instellingen gebruikmaken. Wijzigingen kunnen ervoor zorgen dat u niet langer een andere startpagina kunt instellen of dat in het dialoogvenster Internet-opties, dat u via het menu Extra kunt openen, bepaalde tabbladen worden verborgen.

Scripts scannen gebruiken

Een script kan bestanden maken, kopiëren of verwijderen. Het kan tevens het Windows-register openen.

Scripts scannen voorkomt automatisch dat bekende, schadelijke scripts op de computer worden uitgevoerd.

Scripts scannen uitschakelen

Als u Scripts scannen uitschakelt, worden verdachte scriptuitvoeringen niet gedetecteerd.

U schakelt Scripts scannen als volgt uit:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Scripts scannen** op **Uit**.

Scannen van scripts inschakelen

Scripts scannen waarschuwt u als het uitvoeren van een script resulteert in het maken, kopiëren of verwijderen van bestanden, of in het openen van het Windows-register.

U schakelt Scripts scannen als volgt in:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Scripts scannen** op **Aan**.

E-mailbeveiliging gebruiken

E-mailbeveiliging detecteert en blokkeert bedreigingen in inkomende (POP3) en uitgaande (SMTP) e-mailberichten en bijlagen, waaronder virussen, Trojaanse paarden, wormen, spyware, adware en ander bedreigingen.

E-mailbeveiliging uitschakelen

Als u e-mailbeveiliging uitschakelt, worden mogelijke bedreigingen in inkomende (POP3) en uitgaande (SMTP) e-mailberichten niet gedetecteerd.

U schakelt e-mailbeveiliging als volgt uit:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **E-mail en expresberichten**.
3. Klik onder **E-mailbeveiliging** op **Uit**.

E-mailbeveiliging inschakelen

E-mailbeveiliging detecteert bedreigingen in inkomende (POP3) en uitgaande (SMTP) e-mailberichten en bijlagen

U schakelt e-mailbeveiliging als volgt in:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **E-mail en expresberichten**.
3. Klik onder **E-mailbeveiliging** op **Aan**.

E-mailbeveiliging configureren

Met de opties voor e-mailbeveiliging kunt u inkomende e-mailberichten, uitgaande e-mailberichten en wormen scannen. Wormen vermenigvuldigen zich en gebruiken systeembronnen, waardoor de computer langzamer wordt of taken worden gestopt. Wormen kunnen kopieën van zichzelf verzenden via e-mailberichten. Ze kunnen bijvoorbeeld probeeren om e-mailberichten door te sturen naar personen in het adresboek.

E-mailbeveiliging configureren

Met de opties voor e-mailbeveiliging kunt u inkomende e-mailberichten, uitgaande e-mailberichten en wormen scannen.

U configureert e-mailbeveiliging als volgt:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **E-mail en expresberichten**.
3. Klik onder **E-mailbeveiliging** op **Geavanceerd**.
4. Schakel de volgende selectievakjes in of uit:
   - **Inkomende e-mailberichten scannen**: Inkomende (POP3) berichten worden gescand op potentiële bedreigingen.
   - **Uitgaande e-mailberichten scannen**: Uitgaande (SMTP) berichten worden gescand op potentiële bedreigingen.
   - **WormStopper inschakelen**: WormStopper blokkeert wormen in e-mailberichten.
5. Klik op **OK**.

Beveiliging van expresberichten gebruiken

Met beveiliging van expresberichten worden bedreigingen in bijlagen bij inkomende expresberichten gedetecteerd.

Beveiliging van expresberichten uitschakelen

Als u beveiliging van expresberichten uitschakelt, worden bedreigingen in bijlagen bij inkomende expresberichten niet gedetecteerd.

U schakelt de beveiliging van expresberichten als volgt uit:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **E-mail en expresberichten**.
3. Klik onder **Beveiliging van expresberichten** op **Uit**.

Beveiliging van expresberichten inschakelen

Met beveiliging van expresberichten worden bedreigingen in bijlagen bij inkomende expresberichten gedetecteerd.

U schakelt de beveiliging van expresberichten als volgt in:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **E-mail en expresberichten**.
3. Klik onder **Beveiliging van expresberichten** op **Aan**.

HOOFDSTUK 15

De computer handmatig scannen

U kunt zoeken naar virussen en andere bedreigingen op vaste schijven, diskettes en in afzonderlijke bestanden en mappen. Wanneer VirusScan een verdacht bestand aantreft, wordt geprobeerd het bestand op te schonen, tenzij het een mogelijk ongewenst programma is. Als VirusScan het bestand niet kan opschonen, kunt u het in quarantaine plaatsen of verwijderen.

In dit hoofdstuk

Handmatig scannen

U kunt op elk gewenst moment handmatig scannen. Als u bijvoorbeeld zojuist VirusScan hebt geïnstalleerd, kunt u een scan uitvoeren om er zeker van te zijn dat de computer nog geen virussen of andere bedreigingen bevat. Als u real-time scannen hebt uitgeschakeld, kunt u bijvoorbeeld ook een scan uitvoeren om er zeker van de zijn dat de computer nog steeds veilig is.

Scannen met de handmatige scaninstellingen

Bij dit type scan worden de handmatige scaninstellingen gebruikt die u opgeeft. Met VirusScan wordt gescand in gecomprimeerde bestanden (met de extensie .zip, .cab, enz.), maar wordt een gecomprimeerd bestand beschouwd als één bestand. Het aantal gescande bestanden kan ook variëren als u tijdelijke internetbestanden hebt verwijderd sinds de laatste scanbewerking.

Scannen met de handmatige scaninstellingen gaat als volgt:

1. Klik in het menu Basis op **Scannen**. Wanneer de scan is voltooid, wordt er een overzicht weergegeven met het aantal gescande en gedetecteerde bestanden, het aantal opgeschoonde items en wanneer de laatste scan is uitgevoerd.
2. Klik op **Voltooien**.

Verwante onderwerpen

- Handmatige scans configureren (pagina 100)

Scannen zonder de handmatige scaninstellingen

Bij dit type scan worden de handmatige scaninstellingen die u opgeeft niet gebruikt. Met VirusScan wordt gescand in gecomprimeerde bestanden (met de extensie .zip, .cab, enz.), maar wordt een gecomprimeerd bestand beschouwd als één bestand. Het aantal gescande bestanden kan ook variëren als u tijdelijke internetbestanden hebt verwijderd sinds de laatste scanbewerking.

Ga als volgt te werk om te scannen zonder de handmatige scaninstellingen:

1. Klik in het menu Geavanceerd op**Startpagina**.
2. Klik in het deelvenster Startpagina op **Scannen**.
3. Schakel onder **Te scannen locaties** de selectievakjes in naast de bestanden, mappen en stations die u wilt scannen.
4. Schakel onder **Opties** de selectievakjes in naast de typen bestanden die u wilt scannen.
5. Klik op **Nu scannen**. Wanneer de scan is voltooid, wordt er een overzicht weergegeven met het aantal gescande en gedetecteerde bestanden, het aantal opgeschoonde items en wanneer de laatste scan is uitgevoerd.
6. Klik op **Voltooien**.

Opmerking: Deze opties worden niet opgeslagen.

Scannen in Windows Verkenner

U kunt scannen op virussen en andere bedreigingen in geselecteerde bestanden, mappen of stations in Windows Verkenner.

Ga als volgt te werk om bestanden te scannen in Windows Verkenner:

1. Open Windows Verkenner.
2. Klik met de rechtermuisknop het bestand, de map of het station dat u wilt scannen en klik vervolgens op **Scannen**. Alle standaardscanopties worden geselecteerd om te zorgen voor een grondige scan

Handmatige scans configureren

Wanneer u een handmatige of geplande scan uitvoert, kunt u opgeven welke typen bestanden moeten worden gescand, welke locaties moeten worden gescand en wanneer een scan moet worden uitgevoerd.

Configureren welke bestandstypen moeten worden gescand

U kunt configureren welke bestandstypen moeten worden gescand.

Ga als volgt te werk om te configureren welke bestandstypen moeten worden gescand:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Virusbeveiliging** op **Geavanceerd**.
4. Klik in het deelvenster Virusbeveiliging op **Handmatig scannen**.
5. Schakel de volgende selectievakjes in of uit:
   - **Scannen op onbekende virussen met behulp van heuristische technieken**: Bestanden worden vergeleken met handtekeningen van bekende virussen om tekenen van onbekende virussen te kunnen ontdekken. Met deze optie voert u de grondigste scanbewerking uit, maar dit duurt wel langer dan een normale scanbewerking.
   - **ZIP- en andere archiefbestanden scannen**: Detecteert en verwijdert virussen in zip-bestanden en andere archiefbestanden. Soms plaatsen virusmakers een virus in een zip-bestand en wordt dat zip-bestand vervolgens opgenomen in een zip-bestand in een poging virusscanners te omzeilen.
   - **Scannen op spyware en mogelijk ongewenste programma's**: Spyware, adware en andere programma's die mogelijk gegevens verzamelen en verzenden zonder uw toestemming, worden opgespoord en verwijderd.
   - **Trackingcookies scannen en verwijderen**: Cookies die mogelijk gegevens verzamelen en verzenden zonder uw toestemming, worden gedetecteerd en verwijderd. Een cookie zorgt voor de identificatie van gebruikers wanneer deze een webpagina bezoeken.
   - **Scannen op rootkits en andere stealth-programma's**: Detecteert en verwijdert eventuele rootkits of andere programma's die verborgen zijn voor Windows.

6 Klik op een van de volgende knoppen:

- **Alle bestanden (aanbevolen)**: Elk bestandstype dat op de computer wordt gebruikt, wordt gescand. Wanneer deze optie is ingeschakeld, maakt u zo grondig mogelijk gebruik van de scanfunctie.
- **Alleen programmabestanden en documenten**: Alleen programmabestanden en documenten worden gescand.

7 Klik op **OK**.

Configureren welke locaties moeten worden gescand

U kunt configureren welke locaties moeten worden gescand voor handmatige of geplande scans.

U configureert als volgt waar moet worden gescand:

1 Klik in het menu Geavanceerd op **Configureren**.

2 Klik in het deelvenster Configureren op **Computer en bestanden**.

3 Klik onder **Virusbeveiliging** op **Geavanceerd**.

4 Klik in het deelvenster Virusbeveiliging op **Handmatig scannen**.

5 Selecteer onder **Standaardlocatie voor scannen** de bestanden, mappen en stations die u wilt scannen.

Als u een zo grondig mogelijke scan wilt uitvoeren, moet u ervoor zorgen dat **Essentiële bestanden** is ingeschakeld.

6 Klik op **OK**.

Scans plannen

U kunt scans plannen om de computer op geplande tijdstippen grondig te controleren op virussen en andere bedreigingen.

U plant een scanbewerking als volgt:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Virusbeveiliging** op **Geavanceerd**.
4. Klik in het deelvenster Virusbeveiliging op **Geplande scan**.
5. Zorg ervoor dat **Gepland scannen inschakelen** wordt ingeschakeld.
6. Schakel de selectievakjes in naast de dag van de week waarop de scan moet worden uitgevoerd.
7. Klik op waarden in de lijsten met begintijden om een begintijd op te geven.
8. Klik op **OK**.

Tip: Als u het standaardschema wilt gebruiken, klikt u op **Opnieuw instellen.**

HOOFDSTUK 16

VirusScan beheren

U kunt items verwijderen uit lijsten met vertrouwde items, bestanden in quarantaine, cookies en bestanden beheren, gebeurtenissen en logboeken bekijken, en verdachte activiteiten melden aan McAfee.

In dit hoofdstuk

Lijsten met vertrouwde items beheren

Wanneer u een SystemGuard, programma, overschrijding van de bufferlimiet of e-mailprogramma vertrouwt, wordt het item toegevoegd aan een lijst met vertrouwde items, zodat het niet meer wordt gedetecteerd.

Als u een programma per ongeluk hebt vertrouwd of als u wilt dat het programma wordt gedetecteerd, moet u het uit deze lijst verwijderen.

Lijsten met vertrouwde items beheren

Wanneer u een SystemGuard, programma, overschrijding van de bufferlimiet of e-mailprogramma vertrouwt, wordt het item toegevoegd aan een lijst met vertrouwde items, zodat het niet meer wordt gedetecteerd.

Als u een programma per ongeluk hebt vertrouwd of als u wilt dat het programma wordt gedetecteerd, moet u het uit deze lijst verwijderen.

U verwijdert items als volgt uit de lijsten met vertrouwde items:

1. Klik in het menu Geavanceerd op **Configureren**.
2. Klik in het deelvenster Configureren op **Computer en bestanden**.
3. Klik onder **Virusbeveiliging** op **Geavanceerd**.
4. Klik in het deelvenster Virusbeveiliging op **Lijsten met vertrouwde items**.
5. Selecteer in de lijst een vertrouwde SystemGuard, programma, overschrijding van de bufferlimiet of e-mailprogramma om de bijbehorende items en de vertrouwensstatus ervan te bekijken.
6. Bekijk informatie over het item onder **Details**.
7. Klik op een actie onder **Ik wil**.
8. Klik op **OK**.

Programma's, cookies en bestanden in quarantaine beheren

U kunt programma's, cookies en bestanden in quarantaine herstellen, verwijderen of naar McAfee verzenden voor verdere analyse.

Programma's, cookies en bestanden in quarantaine terugzetten

Indien gewenst kunt u programma's, cookies en bestanden in quarantaine terugzetten.

U zet programma's, cookies en bestanden in quarantaine als volgt:

1. Klik in het menu Geavanceerd op **Terugzetten**.
2. Klik in het deelvenster Terugzetten op **Programma's en cookies** of **Bestanden**, afhankelijk van de situatie.
3. Selecteer de programma's, cookies of bestanden in quarantaine die u wilt terugzetten.
4. Als u meer informatie wilt over het virus dat in quarantaine is geplaatst, klikt u op de detectienaam onder **Details**. De Virus Information Library verschijnt, met een beschrijving van het virus.
5. Klik op een actie onder **Ik wil** op **Terugzetten**.

Programma's, cookies en bestanden in quarantaine verwijderen

U kunt programma's, cookies en bestanden in quarantaine verwijderen.

U kunt programma's, cookies en bestanden in quarantaine als volgt verwijderen:

1. Klik in het menu Geavanceerd op **Terugzetten**.
2. Klik in het deelvenster Terugzetten op **Programma's en cookies** of **Bestanden**, afhankelijk van de situatie.
3. Selecteer de programma's, cookies of bestanden in quarantaine die u wilt terugzetten.
4. Als u meer informatie wilt over het virus dat in quarantaine is geplaatst, klikt u op de detectienaam onder **Details**. De Virus Information Library verschijnt, met een beschrijving van het virus.
5. Klik op een actie onder **Ik wil** op **Verwijderen**.

Programma's, cookies en bestanden in quarantaine naar McAfee verzenden

U kunt programma's, cookies en bestanden in quarantaine verzenden naar McAfee voor verdere analyse.

Opmerking: Als het bestand in quarantaine dat u verzendt een maximumgrootte overschrijdt, kan het bestand worden geweigerd. Meestal is dit niet het geval.

U verzendt programma's of bestanden in quarantaine als volgt naar McAfee:

1. Klik in het menu Geavanceerd op **Terugzetten**.
2. Klik in het deelvenster Terugzetten op **Programma's en cookies** of **Bestanden**, afhankelijk van de situatie.
3. Selecteer de programma's, cookies of bestanden in quarantaine die u naar McAfee wilt verzenden.
4. Als u meer informatie wilt over het virus dat in quarantaine is geplaatst, klikt u op de detectienaam onder **Details**. De Virus Information Library verschijnt, met een beschrijving van het virus.
5. Klik op een actie onder **Ik wil** op **Verzenden naar McAfee**.

Recente gebeurtenissen en logboeken bekijken

In recente gebeurtenissen en logboeken worden gebeurtenissen weergegeven van alle geïnstalleerde McAfee-producten.

Onder Recente gebeurtenissen kunt u de laatste 30 belangrijke gebeurtenissen zien die hebben plaatsgevonden op de computer. U kunt geblokkeerde programma's terugzetten, real-time scannen opnieuw inschakelen en overschrijdingen van bufferlimieten vertrouwen.

Tevens kunt u logboeken bekijken, waarin elke gebeurtenis wordt geregistreerd die de afgelopen 30 dagen heeft plaatsgevonden.

Gebeurtenissen weergeven

Onder Recente gebeurtenissen kunt u de laatste 30 belangrijke gebeurtenissen zien die hebben plaatsgevonden op de computer. U kunt geblokkeerde programma's terugzetten, real-time scannen opnieuw inschakelen en overschrijdingen van bufferlimieten vertrouwen.

U kunt gebeurtenissen als volgt weergeven:

1. Klik in het menu Geavanceerd op **Rapportenen logboeken**.
2. Klik in het deelvenster Rapporten en logboeken op **Recente gebeurtenissen**.
3. Selecteer de gebeurtenissen die u wilt weergeven.
4. Bekijk informatie over de gebeurtenis onder **Details**.
5. Klik op een actie onder **Ik wil**.

Logboeken weergeven

In logboeken wordt elke gebeurtenis geregistreerd die de afgelopen 30 dagen heeft plaatsgevonden.

U kunt logboeken als volgt weergeven:

1. Klik in het menu Geavanceerd op **Rapportenen logboeken**.
2. Klik in het deelvenster Rapporten en logboeken op **Recente gebeurtenissen**.
3. Klik in het deelvenster Recente gebeurtenissen op **Logboek weergeven**.
4. Selecteer het type logboek dat u wilt weergeven en selecteer vervolgens een logboek.
5. Bekijk informatie over het logboek onder **Details**.

Anonieme informatie automatisch rapporteren

U kunt informatie over virussen, mogelijk ongewenste programma's en de activiteiten van hackers anoniem melden aan McAfee. Deze optie is alleen beschikbaar tijdens de installatie.

Er worden geen persoonlijke identificatiegegevens verzameld.

Rapporteren aan McAfee

U kunt informatie over virussen, mogelijk ongewenste programma's en de activiteiten van hackers melden aan McAfee. Deze optie is alleen beschikbaar tijdens de installatie.

U kunt anonieme informatie als volgt automatisch rapporteren:

1. Accepteer tijdens de installatie van VirusScan de standaardinstelling **Informatie anoniem versturen**.
2. Klik op **Volgende**.

Beveiligingswaarschuwingen

Als er een bedreiging wordt gedetecteerd tijdens real-time scannen, wordt er een waarschuwing weergegeven. Bij de meeste virussen, Trojaanse paarden en wormen wordt het bestand automatisch opgeschoond tijdens real-time scannen en wordt u gewaarschuwd. Bij mogelijk ongewenste programma's en SystemGuards wordt tijdens real-time scannen het bestand of de wijziging gedetecteerd en wordt u gewaarschuwd. Bij overschrijdingen van de bufferlimiet, trackingcookies en scriptactiviteiten wordt de activiteit automatisch geblokkeerd tijdens real-time scannen en wordt u gewaarschuwd.

Deze waarschuwingen kunnen worden ingedeeld in drie basistypen.

- Rode waarschuwing
- Gele waarschuwing
- Groene waarschuwing

U kunt vervolgens kiezen hoe gedetecteerde bestanden, gedetecteerde e-mail, verdachte scripts, mogelijke wormen, mogelijk ongewenste programma's, SystemGuards of overschrijdingen van de bufferlimiet moeten worden beheerd.

Waarschuwingen beheren

McAfee gebruikt een reeks waarschuwingen waarmee u uw beveiliging beter kunt beheren. Deze waarschuwingen kunnen worden ingedeeld in drie basistypen.

- Rode waarschuwing
- Gele waarschuwing
- Groene waarschuwing

Rode waarschuwing

Bij een rode waarschuwing is een reactie van u vereist. In sommige gevallen kan McAfee niet bepalen hoe automatisch moet worden gereageerd op een bepaalde activiteit. In dergelijke gevallen wordt in de rode waarschuwing beschreven om welke activiteit het gaat en kunt u kiezen uit een of meer opties.

Gele waarschuwing

Een gele waarschuwing is een niet-kritieke melding waarbij meestal een reactie van u vereist is. In de gele waarschuwing wordt beschreven om welke activiteit het gaat en kunt u kiezen uit een of meer opties.

Groene waarschuwing

Een groene waarschuwing geeft meestal basisinformatie over een gebeurtenis waar u niet op hoeft te reageren.

Waarschuwingsopties configureren

Als u ervoor kiest een waarschuwing niet meer weer te geven en later van gedachten verandert, kunt u de configuratie wijzigen zodat die waarschuwing weer wordt weergegeven. Raadpleeg de documentatie van SecurityCenter voor meer informatie over het configureren van waarschuwingsopties.

HOOFDSTUK 17

Aanvullende Help

In dit hoofdstuk worden veelgestelde vragen en scenario's voor het oplossen van problemen behandeld.

In dit hoofdstuk

Veelgestelde vragen

In dit gedeelte vindt u antwoorden op de meeste veelgestelde vragen.

Er is een bedreiging gedetecteerd. Wat moet ik doen?

McAfee gebruikt waarschuwingen waarmee u uw beveiliging beter kunt beheren. Deze waarschuwingen kunnen worden ingedeeld in drie basistypen.

- Rode waarschuwing
- Gele waarschuwing
- Groene waarschuwing

U kunt vervolgens kiezen hoe gedetecteerde bestanden, gedetecteerde e-mail, verdachte scripts, mogelijke wormen, mogelijk ongewenste programma's, SystemGuards of overschrijdingen van de bufferlimiet moeten worden beheerd.

Raadpleeg de Virus Information Library voor meer informatie over het beheren van specifieke bedreigingen. U kunt deze vinden op: http://us.mcafee.com/virusInfo/default.asp?affid=.

Verwante onderwerpen

- Beveiligingswaarschuwingen (pagina 109)

Kan ik VirusScan gebruiken met de browsers van Netscape, Firefox en Opera?

U kunt Netscape, Firefox of Opera gebruiken als uw standaardinternetbrowser, maar Microsoft® Internet Explorer 6.0 of hoger moet wel op de computer zijn geïnstalleerd.

Moet ik verbinding hebben met internet om een scan uit te voeren?

U hoeft geen verbinding te hebben met internet om een scan uit te voeren, maar u moet wel minstens eenmaal per week verbinding maken om updates van McAfee te ontvangen.

Kan ik met VirusScan e-mailbijlagen scannen?

Als u real-time scannen en e-mailbeveiliging hebt ingeschakeld, worden alle bijlagen gescand wanneer het e-mailbericht binnenkomt.

Kan ik met VirusScan zip-bestanden scannen?

Met VirusScan worden zip-bestanden en andere archiefbestanden gescand.

Waarom treden er fouten op bij het scannen van uitgaande e-mail?

Bij het scannen van uitgaande e-mailberichten kunnen de volgende fouten optreden:

- Protocolfout. De e-mailserver heeft een e-mailbericht geweigerd.
  Als er een protocolfout of systeemfout optreedt, worden de resterende e-mailberichten voor die sessie verwerkt en naar de server verzonden.
- Verbindingsfout. De verbinding met de e-mailserver is verbroken.
  Als er een verbindingsfout optreedt, controleert u of de computer een verbinding met internet heeft en probeert u het bericht vervolgens nogmaals te verzenden vanuit de lijst **Verzonden items** in uw e-mailprogramma.
- Systeemfout. Er is een bestandsverwerkingsfout of andere systeemfout opgetreden.
- Fout bij gecondeerde SMTP-verbinding. Er is een gecodeerde SMTP-verbinding voor uw e-mailprogramma gedetecteerd. Als er een fout optreedt bij een gecodeerde SMTP-verbinding, schakelt u de gecodeerde SMTP-verbinding in uw e-mailprogramma uit zodat de e-mailberichten worden gescand.

Als er timeouts optreden bij het verzenden van e-mailberichten, schakelt u de optie voor het scannen van uitgaande e-mail uit, of schakelt u gecodeerde SMTP-verbindingen uit in uw e-mailprogramma.

Verwante onderwerpen

- E-mailbeveiliging configureren (pagina 94)

Problemen oplossen

In dit gedeelte vindt u hulp bij algemene problemen waarmee u te maken kunt krijgen.

Een virus kan niet worden opgeschoond of verwijderd

Voor sommige virussen moet u de computer handmatig opschonen. Probeer de computer opnieuw op te starten en de scan vervolgens nogmaals uit te voeren.

Als de computer een virus niet kan opschonen of verwijderen, raadpleegt u de Virus Information Library op: http://us.mcafee.com/virusInfo/default.asp?affid=.

Als u aanvullende hulp nodig hebt, raadpleegt u de klantenservice van McAfee op de McAfee-website.

Opmerking: Virussen kunnen niet worden opgeschoond als deze op cd-rom's, dvd's en diskettes met schrijfbeveiliging staan.

Nadat de computer opnieuw is opgestart, kan een item nog steeds niet worden verwijderd

Na het scannen en verwijderen van items moet de computer in bepaalde situaties opnieuw worden opgestart.

Als het item niet wordt verwijderd nadat de computer opnieuw is opgestart, stuurt u het bestand op naar McAfee.

Opmerking: Virussen kunnen niet worden opgeschoond als deze op cd-rom's, dvd's en diskettes met schrijfbeveiliging staan.

Verwante onderwerpen

- Programma's, cookies en bestanden in quarantaine beheren (pagina 105)

Onderdelen ontbreken of zijn beschadigd

In bepaalde situaties kan VirusScan onjuist worden geïnstalleerd:

- Er is onvoldoende vrije schijfruimte of geheugen beschikbaar op de computer. Controleer of de computer voldoet aan de systeemvereisten voor het uitvoeren van deze software.
- De internetbrowser is niet goed geconfigureerd.
- De internetverbinding is niet in orde. Controleer de verbinding. Probeer anders op een later tijdstip opnieuw verbinding te maken.
- Bestanden ontbreken of de installatie is mislukt.

De beste oplossing hiervoor is om de bovenstaande problemen op te lossen en VirusScan vervolgens opnieuw te installeren.

HOOFDSTUK 18

McAfee Personal Firewall

Personal Firewall biedt geavanceerde beveiliging voor uw computer en uw persoonlijke gegevens. Personal Firewall vormt een barrière tussen uw computer en internet, waarbij het internetverkeer wordt gecontroleerd op verdachte activiteiten, zonder dat hiervan melding wordt gemaakt.

In dit hoofdstuk

Voorzieningen

Personal Firewall biedt volledige inkomende en uitgaande firewallbeveiliging en vertrouwt automatisch bekende goede programma's en helpt spyware, Trojaanse paarden en programma's voor het vastleggen van toetsaanslagen te blokkeren. Firewall biedt u bescherming tegen toegangspogingen en aanvallen van hackers, controleert op internet- en netwerkactiviteiten, waarschuwt u bij mogelijk vijandige of verdachte gebeurtenissen, verschaft informatie over internetverkeer en vormt een aanvulling op uw antivirusprogramma´s.

Standaard en aangepaste beveiligingsniveaus

Bescherm uzelf tegen aanvallen en verdachte activiteiten met behulp van de standaardwaarden van uw firewallbescherming of pas Firewall aan aan uw eigen beveiligingsbehoeften.

Real-time beveiligingswaarschuwingen

Ontvang dynamisch gegenereerde aanbevelingen om u te helpen bepalen of aan programma's internettoegang moet worden verleend en of netwerkverkeer kan worden vertrouwd.

Intelligent toegangsbeheer voor programma's

Beheer de internettoegang voor programma's, door middel van waarschuwingen en gebeurtenislogboeken, of configureer toegangsrechten voor specifieke programma's vanuit het deelvenster Programmamachtigingen van Firewall.

Spelbeveiliging

Voorkom dat u tijdens spellen die u schermvullend speelt wordt gestoord door waarschuwingen over inbraakpogingen en verdachte activiteiten en configureer Firewall zodanig dat waarschuwingen pas worden weergegeven nadat u het computerspel hebt voltooid.

Bescherming van uw computer tijdens het opstarten

Voordat Windows wordt gestart, beschermt Firewall uw computer tegen inbraakpogingen, ongewenste programma's en ongewenst netwerkverkeer.

Controle van systeemservicepoort

Systeemservicepoorten kunnen indringers ongemerkt toegang geven tot uw computer. Met Firewall kunt u de geopende en gesloten systeemservicepoorten beheren die voor sommige programma's nodig zijn.

Computerverbindingen beheren

Vertrouw of blokkeer externe verbindingen en IP-adressen die een verbinding met uw computer kunnen maken.

Integratie van HackerWatch-informatie

HackerWatch is een verzamelpunt voor beveiligingsinformatie dat wereldwijde inbraakactiviteiten en -patronen volgt en daarnaast de meest actuele informatie verstrekt over programma's op uw computer. U kunt mondiale statistieken over beveiligingsgebeurtenissen en internetpoortactiviteiten weergeven.

Firewall vergrendelen

Hiermee kunt u direct al het inkomend en uitgaand internetverkeer tussen uw computer en internet blokkeren.

De standaardwaarden van Firewall herstellen

Stel de oorspronkelijke beveiligingsinstellingen van Firewall opnieuw in. Als Personal Firewall ongewenst gedrag vertoont dat u niet kunt corrigeren, kunt u de oorspronkelijke standaardinstellingen van Firewall weer terugzetten.

Geavanceerde opsporing van Trojaanse paarden

In deze functie is het beheer van toepassingsverbindingen gecombineerd met een verbeterde database. Met behulp hiervan worden mogelijk schadelijke toepassingen, zoals Trojaanse paarden, opgespoord en wordt voorkomen dat ze toegang krijgen tot internet en uw persoonlijke gegevens doorgeven.

Logboekregistratie

Hiermee kunt u instellen of u logboekregistratie wilt inschakelen of uitschakelen. Als u logboekregistratie inschakelt, kunt u bovendien instellen welke typen gebeurtenissen u in een logboek wilt vastleggen. Het vastleggen van gebeurtenissen in logboeken stelt u in staat om recente inkomende en uitgaande gebeurtenissen weer te geven. Daarnaast kunt u tevens door het inbraakdetectiesysteem gedetecteerde gebeurtenissen weergeven.

Internetverkeer controleren

Raadpleeg gemakkelijk leesbare grafische kaarten die de bron van vijandige aanvallen en verkeer wereldwijd aangeven. Hier vindt u ook gedetailleerde eigenaargegevens en geografische gegevens van de bron-IP-adressen. U kunt ook het inkomende en uitgaande verkeer analyseren, de bandbreedte van programma's controleren en het gedrag van programma's in het oog houden.

Inbraakpreventie

Bescherm uw privacy dankzij de preventie van inbraakpogingen via het internet. Met behulp van heuristische functionaliteit biedt McAfee een derde beschermingslaag door items te blokkeren die de kenmerken van een aanval of een hackpoging vertonen.

Geavanceerde verkeersanalyse

Controleer zowel inkomend als uitgaand internetverkeer en programmaverbindingen, waaronder programma's die actief 'luisteren' naar geopende verbindingen. Zo kunt u zien welke programma's kwetsbaar zijn voor inbraak en desgewenst actie ondernemen.

Firewall starten

Zodra u Firewall hebt geïnstalleerd, is uw computer beschermd tegen inbraak en ongewenst netwerkverkeer. Bovendien kunt u dan reageren op waarschuwingen en kunt u inkomende en uitgaande internettoegang voor bekende en onbekende programma's beheren. 'Slimme aanbevelingen' en het beveiligingsniveau 'Standaard' zijn automatisch ingeschakeld.

Het is mogelijk om Firewall uit te schakelen via het deelvenster 'Internet- en netwerkconfiguratie'. Uw computer is dan echter niet langer beschermd tegen inbraak en ongewenst netwerkverkeer. Bovendien is het dan niet meer mogelijk om inkomende en uitgaande netwerkverbindingen op effectieve wijze te beheren. Als u de firewall moet uitschakelen, doe dat dan tijdelijk en uitsluitend wanneer het nodig is. U kunt Firewall ook weer inschakelen via het deelvenster 'Internet- en netwerkconfiguratie'.

Wanneer Windows® Firewall is geïnstalleerd, wordt deze automatisch door Firewall uitgeschakeld en wordt Firewall ingesteld als de standaardfirewall.

Opmerking: Als u Firewall wilt configureren, opent u het deelvenster Netwerk en internetconfiguratie.

Firewallbescherming starten

Met een firewall beschermt u uw computer tegen inbraak en ongewenst netwerkverkeer. Ook kunt u er in- en uitgaande internetverbindingen mee beheren.

Ga als volgt te werk om firewallbescherming in te schakelen:

1. Ga in het deelvenster McAfee SecurityCenter op een van de volgende manieren te werk:
   - Klik op **Internet en netwerk** en vervolgens op **Configureren**.
   - Klik op **Menu Geavanceerd**. Klik in het deelvenster **Startpagina** op **Configureren** en wijs vervolgens **Internet en netwerk** aan.
2. Klik in het deelvenster **Internet- en netwerkconfiguratie** onder **Firewallbescherming** op **Aan**.

Firewallbescherming stoppen

Als u de firewallbescherming uitschakelt, is uw computer kwetsbaar voor inbraak en ongewenst netwerkverkeer. Als de firewallbescherming is uitgeschakeld, kunt u inkomende en uitgaande netwerkverbindingen niet beheren.

Ga als volgt te werk om firewallbescherming uit te schakelen:

1. Ga in het deelvenster McAfee SecurityCenter op een van de volgende manieren te werk:
   - Klik op **Internet en netwerk** en vervolgens op **Configureren**.
   - Klik op **Menu Geavanceerd**. Klik in het deelvenster **Startpagina** op **Configureren** en wijs vervolgens **Internet en netwerk** aan.
2. Klik in het deelvenster **Internet- en netwerkconfiguratie** onder **Firewallbescherming** op **Uit**.

Werken met waarschuwingen

Firewall kent een breed scala aan waarschuwingen dat u ondersteunt bij het beheren van uw beveiliging. Deze waarschuwingen kunnen worden onderverdeeld in vier basistypen.

- De waarschuwing Trojaans paard geblokkeerd
- Rode waarschuwing
- Gele waarschuwing
- Groene waarschuwing

Waarschuwingen kunnen ook informatie bevatten waarmee de gebruiker kan bepalen hoe de waarschuwing moet worden afgehandeld of hoe informatie kan worden opgehaald over programma's die op de computer worden uitgevoerd.

Informatie over waarschuwingen

Firewall kent vier basistypen waarschuwingen. Sommige van deze waarschuwingen bevatten informatie over hoe u meer te weten kunt komen over programma's die op uw computer worden uitgevoerd.

De waarschuwing Trojaans paard geblokkeerd

Trojaanse paarden lijken legitieme programma's, maar deze programma's kunnen de werking van uw computer onderbreken, gegevens beschadigen en toegang tot uw gegevens verlenen aan onbevoegde personen. Deze waarschuwing wordt weergegeven als de Firewall een Trojaans paard op uw computer detecteert en blokkeert. Vervolgens wordt u aangeraden om uw computer op andere bedreigingen te scannen. Deze waarschuwing wordt op elk beveiligingsniveau weergegeven, behalve op het niveau Open en in gevallen waarin Slimme aanbevelingen is uitgeschakeld.

Rode waarschuwingen

De meestvoorkomende waarschuwingen zijn rode waarschuwingen. Over het algemeen vereisen dergelijke waarschuwingen een reactie van de gebruiker. Firewall is in sommige gevallen niet in staat om automatisch te bepalen welke handelswijze in het geval van een activiteit van een programma of een netwerkgebeurtenis de voorkeur verdient. In dergelijke gevallen bevat de waarschuwing een beschrijving van de activiteit van het programma of de netwerkgebeurtenis en een of meer mogelijkheden waaruit u kunt kiezen. Als Slimme aanbevelingen is ingeschakeld, worden programma's toegevoegd aan het deelvenster Programmamachtigingen.

Hierna volgt een aantal veelvoorkomende waarschuwingen:

- **Programma verzoekt om toegang tot internet**: Firewall heeft een programma gedetecteerd dat toegang tot internet probeert te verkrijgen.
- **Programma is gewijzigd**: Firewall heeft een programma gedetecteerd dat is gewijzigd. Dit kan het resultaat zijn van een online update.
- **Programma geblokkeerd**: Firewall heeft een programma geblokkeerd omdat het desbetreffende programma wordt vermeld in het deelvenster Programmamachtigingen.

De volgende opties kunnen worden weergegeven, afhankelijk van uw instellingen en van de activiteit van het programma of van de netwerkgebeurtenis:

- **Toegang verlenen**: Kies deze optie als u een programma op uw computer toegang tot internet wilt verlenen. Als u deze

optie kiest, wordt er een regel toegevoegd op de pagina Programmamachtigingen.

- **Eenmalig toegang verlenen**: Kies deze optie als u een programma op uw computer tijdelijk toegang tot internet wilt verlenen. Het kan bijvoorbeeld zijn dat u tijdens de installatie van een nieuw programma het desbetreffende programma eenmalig toegang tot internet moet verlenen.
- **Toegang blokkeren**: Kies deze optie als u de toegang van een programma tot internet wilt blokkeren.
- **Alleen uitgaande toegang verlenen**: Kies deze optie als u alleen een uitgaande verbinding met internet wilt toestaan. Deze optie is gewoonlijk beschikbaar als de beveiligingsniveaus Strikt en Stealth zijn ingesteld.
- **Dit netwerk vertrouwen**: Kies deze optie als u al het inkomende en uitgaande verkeer van een netwerk wilt toestaan. Het netwerk wordt vervolgens toegevoegd aan de lijst met vertrouwde IP-adressen.
- **Dit netwerk momenteel niet vertrouwen**: Kies deze optie als u al het inkomende en uitgaande verkeer van een netwerk wilt blokkeren.

Gele waarschuwingen

Gele waarschuwingen zijn niet-kritieke berichten waarin u wordt geïnformeerd over een netwerkgebeurtenis die door Firewall is gedetecteerd. De waarschuwing **Nieuw netwerk aangetroffen** wordt bijvoorbeeld weergegeven wanneer Firewall voor de eerste keer op een computer wordt uitgevoerd en als een computer waarop Firewall is geïnstalleerd, wordt verbonden met een nieuw netwerk. U kunt kiezen of u het netwerk wel of niet wilt vertrouwen. Als u het netwerk vertrouwt, wordt verkeer van en naar andere computers in het netwerk toegestaan en wordt het netwerk toegevoegd aan de lijst met vertrouwde IP-adressen.

Groene waarschuwingen

Groene waarschuwingen bevatten meestal basisinformatie over een gebeurtenis en vergen geen handelingen van de gebruiker. Groene waarschuwingen worden gewoonlijk weergegeven in gevallen waarin de beveiligingsniveaus Standaard, Strikt en Vergrendelen zijn ingesteld. Hierna volgen de groene waarschuwingen en hun beschrijvingen:

- **Programma is gewijzigd**: Dit bericht informeert u over het feit dat een programma waaraan u toegang tot internet hebt verleend, is gewijzigd. U kunt ervoor kiezen om het programma te blokkeren. Als u niets doet, verdwijnt het bericht echter van het scherm en blijft het programma toegang tot internet houden.
- **Toegang tot internet verleend aan programma**: Deze waarschuwing stelt u in kennis van het feit dat aan een

programma internettoegang is verleend. U kunt ervoor kiezen om het programma te blokkeren. Als u niets doet, verdwijnt het bericht echter van het scherm en blijft het programma toegang tot internet houden.

Hulp voor gebruikers

Veel Firewall-waarschuwingen bevatten aanvullende informatie die u bij het beheren van de beveiliging van uw computer van dienst kan zijn, waaronder:

- **Meer informatie over dit programma**: Hiermee start u de McAfee-website over mondiale beveiliging, zodat er informatie kan worden opgehaald over een programma dat Firewall op uw computer heeft gedetecteerd.
- **McAfee op de hoogte stellen van dit programma**: Hiermee kunt u informatie over een onbekend bestand dat door Firewall op uw computer is gedetecteerd naar McAfee verzenden.
- **McAfee raadt aan**: Hiermee geeft u advies weer over hoe waarschuwingen moeten worden afgehandeld. Het kan bijvoorbeeld zijn dat u via een bericht wordt aangeraden om een programma toegang te verlenen.

Informatieve waarschuwingen beheren

Firewall biedt u de mogelijkheid om informatieve waarschuwingen voor bepaalde gebeurtenissen weer te geven en te verbergen.

Waarschuwingen weergeven tijdens het spelen spelletjes

Firewall voorkomt standaard de weergave van informatieve waarschuwing wanneer u spelletjes schermvullend speelt. U kunt Firewall echter zo configureren dat informatieve berichten tijdens het spelen van spelletjes worden weergegeven in gevallen waarin er inbraakpogingen of verdachte activiteiten worden gedetecteerd.

Waarschuwingen weergeven tijdens het spelen van spelletjes:

1. Klik in het deelvenster Algemene taken op het menu **Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het deelvenster Configuratie van SecurityCenter op **Waarschuwingen**.
4. Klik op **Geavanceerd**.
5. Selecteer in het deelvenster **Waarschuwingsopties** de optie **Informatiewaarschuwingen weergeven wanneer de spelletjesmodus wordt gedetecteerd**.

Informatieve waarschuwingen verbergen

Informatieve waarschuwingen worden weergegeven wanneer er gebeurtenissen optreden waarop u niet direct hoeft te reageren.

Informatieve waarschuwingen verbergen:

1. Klik in het deelvenster Algemene taken op het menu **Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het deelvenster Configuratie van SecurityCenter op **Waarschuwingen**.
4. Klik op **Geavanceerd**.
5. Klik in het deelvenster **Configuratie van SecurityCenter** op **Informatiewaarschuwingen**.
6. Ga in het deelvenster **Informatiewaarschuwingen** op een van de volgende manieren te werk:
   - Selecteer een waarschuwingstype dat u wilt verbergen.
   - Selecteer **Informatieve waarschuwingen verbergen** als u alle informatieve waarschuwingen wilt verbergen.
7. Klik op **OK**.

HOOFDSTUK 19

Het beveiligingsniveau van Firewall configureren

Firewall biedt een aantal methoden voor het beheren van de beveiliging, waarbij u de wijze waarop er op beveiligingsgebeurtenissen en waarschuwingen moet worden gereageerd, kunt aanpassen.

Nadat u Firewall voor de eerste keer hebt geïnstalleerd, wordt het beveiligingsniveau ingesteld op Standaardbeveiliging. In veel gevallen voorziet deze instelling in alle beveiligingsbehoeften van de desbetreffende gebruiker. Firewall biedt echter ook andere beveiligingsniveaus die uiteenlopen van zeer restrictief tot zeer tolerant.

Daarnaast biedt Firewall u de mogelijkheid om aanbevelingen bij waarschuwingen en bij internettoegang voor programma's weer te geven.

In dit hoofdstuk

Beveiligingsniveaus van Firewall beheren

U kunt beveiligingsniveaus instellen waarmee u kunt aangeven hoe er op waarschuwingen moet worden gereageerd als Firewall ongewenst netwerkverkeer en inkomende en uitgaande netwerkverbindingen detecteert. Standaard is het beveiligingsniveau 'Standaard' ingeschakeld.

Als het beveiligingsniveau is ingesteld op 'Standaard' en als 'Slimme aanbevelingen' is ingeschakeld, bieden rode waarschuwingen opties waarmee u voor onbekende of aangepaste programma's toegang kunt verlenen of weigeren. Als bekende programma's worden gedetecteerd, verschijnen er groene informatieve waarschuwingen en wordt er automatisch toegang verleend. Als er toegang wordt verleend, mag een programma uitgaande verbindingen maken en luisteren naar ongevraagde inkomende verbindingen.

Over het algemeen geldt dat hoe restrictiever het beveiligingsniveau is ('Stealth' en 'Strikt'), hoe meer opties en waarschuwingen er worden weergegeven, die u vervolgens moet afhandelen.

Firewall heeft zes beveiligingsniveaus. Dit zijn de beveiligingsniveaus in volgorde van afnemende restrictiviteit:

- **Vergrendelen**: hiermee worden alle internetverbindingen geblokkeerd.
- **Stealth**: hiermee worden alle inkomende internetverbindingen geblokkeerd.
- **Strikt**: hiermee wordt via waarschuwingen uw toestemming gevraagd bij elke aanvraag voor een inkomende of uitgaande internetverbinding.
- **Standaard**: hiermee wordt u via waarschuwingen op de hoogte gesteld wanneer onbekende of nieuwe programma's internettoegang nodig hebben.
- **Vertrouwend**: hiermee worden alle inkomende en uitgaande internetverbindingen toegestaan en worden deze automatisch toegevoegd aan het deelvenster 'Programmamachtigingen'.
- **Open**: hiermee worden alle inkomende en uitgaande internetverbindingen toegestaan.

Met Firewall is het ook mogelijk om het beveiligingsniveau 'Standaard' rechtstreeks in te stellen in het deelvenster 'Standaardwaarden van firewallbescherming herstellen'.

Beveiligingsniveau instellen op 'Vergrendelen'

Als u het beveiligingsniveau van de firewall instelt op 'Vergrendelen', worden alle inkomende en uitgaande netwerkverbindingen geblokkeerd, waaronder toegang tot websites, e-mail en beveiligingsupdates. Dit beveiligingsniveau heeft hetzelfde resultaat als het loskoppelen van de internetverbinding. U kunt deze instelling gebruiken om poorten te blokkeren die u in het deelvenster 'Systeemservices' hebt ingesteld op 'Open'. Tijdens 'Vergrendelen' blijven er waarschuwingen verschijnen die u vragen of programma's moeten worden geblokkeerd.

Het beveiligingsniveau van de firewall instellen op 'Vergrendelen':

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Verplaats de schuifregelaar in het deelvenster 'Beveiligingsniveau' zodat **Vergrendelen** wordt weergegeven als het huidige niveau.
3. Klik op **OK**.

Beveiligingsniveau instellen op 'Stealth'

Als u het beveiligingsniveau van de firewall instelt op 'Stealth', worden alle inkomende en uitgaande netwerkverbindingen geblokkeerd, met uitzondering van open poorten. Met deze instelling is de computer volledig onzichtbaar op internet. Als het beveiligingsniveau is ingesteld op 'Stealth', wordt u gewaarschuwd als nieuwe programma's proberen uitgaande internetverbindingen tot stand te brengen of aanvragen voor inkomende verbindingen ontvangen. Geblokkeerde en toegevoegde programma's worden weergegeven in het deelvenster 'Programmamachtigingen'.

Het beveiligingsniveau van de firewall instellen op 'Stealth':

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Verplaats de schuifregelaar in het deelvenster 'Beveiligingsniveau' zodat **Stealth** wordt weergegeven als het huidige niveau.
3. Klik op **OK**.

Beveiligingsniveau instellen op 'Strikt'

Als u het beveiligingsniveau instelt op 'Strikt', wordt u geïnformeerd als nieuwe programma's proberen uitgaande internetverbindingen tot stand te brengen of aanvragen voor inkomende verbindingen ontvangen. Geblokkeerde en toegevoegde programma's worden weergegeven in het deelvenster 'Programmamachtigingen'. Als het beveiligingsniveau is ingesteld op 'Strikt', vraagt een programma alleen het type toegang aan dat op dat moment is vereist, bijvoorbeeld alleen uitgaande toegang. U kunt deze toegang verlenen of blokkeren. Als het programma later zowel een inkomende als een uitgaande verbinding nodig heeft, kunt u via het deelvenster 'Programmamachtigingen' volledige toegang voor het programma verlenen.

Het beveiligingsniveau van de firewall instellen op 'Strikt':

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Verplaats de schuifregelaar in het deelvenster 'Beveiligingsniveau' zodat **Strikt** wordt weergegeven als het huidige niveau.
3. Klik op **OK**.

Beveiligingsniveau instellen op 'Standaard'

Het standaardbeveiligingsniveau is 'Standaard' (aanbevolen).

Als u het beveiligingsniveau instelt op 'Standaard', worden inkomende en uitgaande internetverbindingen gecontroleerd en wordt u gewaarschuwd wanneer nieuwe programma's internettoegang proberen te krijgen. Geblokkeerde en toegevoegde programma's worden weergegeven in het deelvenster 'Programmamachtigingen'.

Ga als volgt te werk om het beveiligingsniveau van de firewall in te stellen op 'Standaard':

1. Klik in het deelvenster voor configuratie van internet en netwerk op **Geavanceerd**.
2. Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Standaard** wordt weergegeven als het huidige niveau.
3. Klik op **OK**.

Beveiligingsniveau instellen op 'Vertrouwend'

Als u het beveiligingsniveau van de firewall instelt op 'Vertrouwend', worden alle inkomende en uitgaande verbindingen toegestaan. Als het beveiligingsniveau is ingesteld op 'Vertrouwend', wordt automatisch toegang verleend voor alle programma's en worden deze toegevoegd aan de lijst van toegestane programma's in het deelvenster 'Programmamachtigingen'.

Het beveiligingsniveau van de firewall instellen op 'Vertrouwend':

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Verplaats de schuifregelaar in het deelvenster 'Beveiligingsniveau' zodat **Vertrouwend** wordt weergegeven als het huidige niveau.
3. Klik op **OK**.

'Slimme aanbevelingen' configureren voor waarschuwingen

Waarschuwingen met betrekking tot programma's die proberen toegang tot internet te krijgen, kunnen vergezeld gaan van aanbevelingen. U kunt instellen of deze aanbevelingen moeten worden toegevoegd, uitgesloten of weergegeven.

Met behulp van 'Slimme aanbevelingen' kunt u besluiten hoe u moet reageren op waarschuwingen. Als 'Slimme aanbevelingen' is ingeschakeld (en als het beveiligingsniveau is ingesteld op 'Standaard'), wordt voor bekende programma's automatisch toegang verleend of geblokkeerd en wordt u gewaarschuwd als er onbekende of potentieel schadelijke programma's worden gedetecteerd. U krijgt ook aanbevelingen over wat u dan het beste kunt doen.

Als 'Slimme aanbevelingen' is uitgeschakeld, wordt internettoegang niet automatisch toegestaan of geblokkeerd en worden er ook geen aanbevelingen gedaan over wat u het beste kunt doen.

Als u hebt ingesteld dat slimme aanbevelingen alleen moeten worden weergegeven, wordt u via een waarschuwing gevraagd om toegang te verlenen of te blokkeren, en krijgt u aanbevelingen over wat u het beste kunt doen.

'Slimme aanbevelingen' inschakelen

Met behulp van 'Slimme aanbevelingen' kunt u besluiten hoe u moet reageren op waarschuwingen. Als 'Slimme aanbevelingen' is ingeschakeld, wordt automatisch toegang verleend voor programma's of blokkeert deze. Bovendien wordt u gewaarschuwd over onbekende en potentieel schadelijke programma's.

'Slimme aanbevelingen' inschakelen:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Selecteer in het deelvenster 'Beveiligingsniveau', onder **Slimme aanbevelingen**, de optie **Slimme aanbevelingen inschakelen**.
3. Klik op **OK**.

'Slimme aanbevelingen' uitschakelen

Als u 'Slimme aanbevelingen' uitschakelt, worden waarschuwingen niet meer vergezeld van aanbevelingen over de manier waarop u met waarschuwingen moet omgaan en over het beheren van toegang voor programma's. Als 'Slimme aanbevelingen' is uitgeschakeld, wordt nog steeds toegang verleend voor programma's of worden deze geblokkeerd. Bovendien wordt u gewaarschuwd over onbekende en potentieel schadelijke programma's. En als er een nieuw programma wordt gedetecteerd dat verdacht is of dat bekend staat als potentieel schadelijk, wordt voor dat programma automatisch de toegang tot internet geblokkeerd.

'Slimme aanbevelingen' uitschakelen:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Selecteer in het deelvenster 'Beveiligingsniveau', onder **Slimme aanbevelingen**, de optie **Slimme aanbevelingen uitschakelen**.
3. Klik op **OK**.

'Slimme aanbevelingen' alleen weergeven

Als u 'Slimme aanbevelingen' weergeeft, wordt u geholpen bij het reageren op waarschuwingen met betrekking tot onbekende en potentieel schadelijke programma's. Als 'Slimme aanbevelingen' is ingesteld op **Alleen weergeven**, wordt er informatie gegeven over het afhandelen van waarschuwingen. Maar in tegenstelling tot de optie **Slimme aanbevelingen inschakelen** worden de aanbevelingen niet automatisch toegepast en wordt voor programma's niet automatisch toegang verleend of geblokkeerd. In plaats hiervan gaan de waarschuwingen vergezeld van aanbevelingen die u helpen bij uw beslissing om voor programma's toegang te verlenen of te blokkeren.

Ga als volgt te werk om 'Slimme aanbevelingen' alleen weer te geven:

1. Klik in het deelvenster voor configuratie van internet en netwerk op **Geavanceerd**.
2. Selecteer in het deelvenster 'Beveiligingsniveau', onder **Slimme aanbevelingen**, de optie **Alleen weergeven**.
3. Klik op **OK**.

Firewall-beveiliging optimaliseren

Er zijn vele manieren waarop de veiligheid van uw computer in gevaar kan komen. Er zijn bijvoorbeeld programma's die proberen om toegang tot internet te krijgen voordat Windows® is gestart. Verder zijn er handige computergebruikers die een ping naar uw computer kunnen uitvoeren om vast te stellen of deze op een netwerk is aangesloten. Met Firewall kunt u uw computer verdedigen tegen beide typen inbraken, doordat u opstartbeveiliging kunt inschakelen en ICMP-pingaanvragen kunt blokkeren. Met de eerste instelling kunnen programma's tijdens het starten van Windows geen toegang krijgen tot internet. Met de tweede instelling worden pingaanvragen geblokkeerd waarmee andere gebruikers uw computer op een netwerk kunnen detecteren.

Standaard installatie-instellingen zijn onder andere het automatisch detecteren van de meest voorkomende inbraakpogingen, zoals Denial of Service-aanvallen of -misbruik. Door gebruik te maken van de standaard installatie-instellingen zorgt u ervoor dat u wordt beschermd tegen dergelijke aanvallen en scans. U kunt de automatische detectie echter ook uitschakelen voor een of meer aanvallen en scans in het deelvenster Inbraakdetectie

Computer beveiligen tijdens het opstarten

Met Firewall kunt u de computer beveiligen tijdens het starten van Windows. Met 'Opstartbeveiliging' worden alle nieuwe programma's geblokkeerd waarvoor nog niet eerder toegang tot internet is verleend. Na het starten van Firewall worden relevante waarschuwingen weergegeven voor programma's die tijdens het opstarten toegang tot internet hebben aangevraagd. U kunt de toegang toestaan of blokkeren. Deze optie is niet beschikbaar als het beveiligingsniveau is ingesteld op 'Open' of 'Vergrendelen'.

De computer beveiligen tijdens het opstarten:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Selecteer in het deelvenster 'Beveiligingsniveau', onder 'Beveiligingsinstellingen', **Opstartbeveiliging inschakelen**.
3. Klik op **OK**.

Opmerking: als opstartbeveiliging is ingeschakeld, worden geblokkeerde verbindingen en inbraken niet geregistreerd.

Instellingen voor pingaanvragen configureren

Computergebruikers kunnen een pingprogramma gebruiken dat ICMP-echoaanvraagberichten verzendt en ontvangt en waarmee kan worden vastgesteld of een bepaalde computer op het netwerk is aangesloten. U kunt in Firewall instellen dat uw computer wel of niet kan worden gepingd.

Instellingen voor ICMP-pingaanvragen configureren:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. In het deelvenster 'Beveiligingsniveau', onder **Beveiligingsinstellingen**, gaat u op een van de volgende manieren te werk:
   - Selecteer **ICMP-pingaanvragen toestaan** als u wilt toestaan dat uw computer op het netwerk kan worden gedetecteerd door middel van pingaanvragen.
   - Maak de selectie van **ICMP-pingaanvragen toestaan** ongedaan als u wilt voorkomen dat uw computer op het netwerk kan worden gedetecteerd door middel van pingaanvragen.
3. Klik op **OK**.

Inbraakdetectie configureren

Het inbraakdetectiesysteem (IDS) controleert gegevenspakketten en gaat na of er sprake is van een verdachte gegevensoverdracht of van verdachte overdrachtsmethoden. Het IDS analyseert gegevensverkeer en gegevenspakketten en gaat na of er sprake is van specifieke patronen die door aanvallers worden gebruikt. Wanneer Firewall bijvoorbeeld ICMP-pakketten detecteert, worden deze geanalyseerd en wordt er door de ICMP-pakketten te vergelijken met bekende aanvalspatronen nagegaan of er sprake is van verdachte aanvalspatronen. De pakketten worden door Firewall vergeleken met een database met handtekeningen. Als er een verdacht of schadelijk pakket wordt gedetecteerd, worden de pakketten die van de verdachte computer afkomstig zijn automatisch geblokkeerd en wordt de gebeurtenis, als u dat hebt ingesteld, in het logboek vastgelegd.

Standaard installatie-instellingen zijn onder andere het automatisch detecteren van de meest voorkomende inbraakpogingen, zoals Denial of Service-aanvallen of -misbruik. Door gebruik te maken van de standaard installatie-instellingen zorgt u ervoor dat u wordt beschermd tegen dergelijke aanvallen en scans. U kunt de automatische detectie echter ook uitschakelen voor een of meer aanvallen en scans in het deelvenster Inbraakdetectie

De inbraakdetectie configureren:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik op **Inbraakdetectie** in het deelvenster Firewall.
3. Ga onder **Pogingen tot indringing detecteren** op een van de volgende manieren te werk:
   - Selecteer een naam als u de aanval of scan automatisch wilt laten detecteren.
   - Wis een naam als u het automatisch detecteren van de aanval of scan wilt uitschakelen.
4. Klik op **OK**.

De instellingen van de beveiligingsstatus van Firewall configureren

In SecurityCenter worden problemen bijgehouden als onderdeel van de algehele beveiligingsstatus van de computer. U kunt Firewall echter zo configureren dat specifieke problemen op uw computer die van invloed zijn op uw beveiligingsstatus worden genegeerd. U kunt in SecurityCenter instellen dat de beveiligingsstatus moet worden genegeerd als Firewall is ingesteld op het beveiligingsniveau Open, als de Firewall-service niet wordt uitgevoerd of als een firewall voor alleen uitgaande verbindingen niet op uw computer is geïnstalleerd.

De instellingen van de beveiligingsstatus van Firewall configureren:

1. Klik in het deelvenster Algemene taken op het menu **Geavanceerd**.
2. Klik op **Configureren**.
3. Klik in het deelvenster Configuratie van SecurityCenter op **Waarschuwingen**.
4. Klik op **Geavanceerd**.
5. Klik in het deelvenster Algemene taken op het menu **Geavanceerd**.
6. Klik op **Configureren**.
7. Klik in het deelvenster Configuratie van SecurityCenter op **Beveiligingstatus**.
8. Klik op Geavanceerd.
9. Selecteer in het deelvenster Genegeerde problemen een of meer van de volgende opties:
   - **Firewall is ingesteld op het beveiligingsniveau Open.**
   - **Firewallservice wordt niet uitgevoerd.**
   - **Geen uitgaande firewall geïnstalleerd op uw computer.**
10. Klik op **OK**.

Firewall vergrendelen en problemen oplossen

De vergrendelingsfunctie is nuttig tijdens noodgevallen op de computer, waarin gebruikers al het verkeer willen blokkeren, zodat zij een probleem op hun computer kunnen isoleren of in gevallen waarin de gebruiker eerst wil uitzoeken hoe de internettoegang van een programma moet worden beheerd.

Firewall onmiddellijk vergrendelen

Als u Firewall onmiddellijk vergrendelt, wordt direct al het inkomende en uitgaande netwerkverkeer tussen uw computer en internet geblokkeerd. Externe verbindingen krijgen geen toegang meer tot uw computer en de programma's op uw computer hebben geen toegang meer tot internet.

Firewall onmiddellijk vergrendelen en al het netwerkverkeer blokkeren:

1. Klik in het deelvenster Start of Algemene taken terwijl het menu **Basis** of **Geavanceerd** is ingeschakeld op **Firewall vergrendelen**.
2. Klik in het deelvenster Firewall vergrendelen op **Vergrendelen**.
3. Klik in het weergegeven dialoogvenster op **Ja** om te bevestigen dat u al het inkomende en uitgaande verkeer onmiddellijk wilt blokkeren.

Firewall onmiddellijk ontgrendelen

Als u Firewall onmiddellijk vergrendelt, wordt direct al het inkomende en uitgaande netwerkverkeer tussen uw computer en internet geblokkeerd. Externe verbindingen krijgen geen toegang meer tot uw computer en de programma's op uw computer hebben geen toegang meer tot internet. Nadat u Firewall hebt vergrendeld, kunt u het programma weer ontgrendelen, zodat netwerkverkeer opnieuw mogelijk wordt.

Firewall onmiddellijk ontgrendelen en netwerkverkeer toestaan:

1. Klik in het deelvenster Start of Algemene taken terwijl het menu **Basis** of **Geavanceerd** is ingeschakeld op **Firewall vergrendelen**.
2. Klik in het deelvenster Vergrendelen ingeschakeld op **Ontgrendelen**.
3. Klik in het weergegeven dialoogvenster op **Ja** om te bevestigen dat u Firewall wilt ontgrendelen en dat u uitgaand verkeer wilt toestaan.

Firewall opnieuw op de standaardwaarden instellen

U kunt Firewall opnieuw op de oorspronkelijke beveiligingsinstellingen instellen. U stelt hierdoor het beveiligingsniveau opnieuw in op Standaard. Verder wordt de optie Slimme aanbevelingen ingeschakeld en worden de vertrouwde en verboden IP-adressen opnieuw op de oorspronkelijke instellingen ingesteld. Daarnaast worden alle programma's verwijderd uit het deelvenster Programmamachtigingen.

Firewall opnieuw op de oorspronkelijke instellingen instellen:

1. Klik in het deelvenster Start of Algemene taken terwijl het menu **Basis** of **Geavanceerd** is ingeschakeld op **Standaardwaarden van firewall herstellen**.
2. Klik in het deelvenster Standaardwaarden van firewall herstellen op **Standaardwaarden herstellen**.
3. Klik in het dialoogvenster Standaardwaarden van firewall herstellen op **Ja** om te bevestigen dat u de firewallconfiguratie opnieuw op de standaardwaarden wilt instellen.

Beveiligingsniveau instellen op 'Open'

Als u het beveiligingsniveau van de firewall instelt op 'Open', wordt toegang verleend aan alle inkomende en uitgaande netwerkverbindingen. Via het deelvenster 'Programmamachtigingen' kunt u toegang verlenen voor programma's die voorheen waren geblokkeerd.

Het beveiligingsniveau van de firewall instellen op 'Open':

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Verplaats de schuifregelaar in het deelvenster Beveiligingsniveau zodat **Open** wordt weergegeven als het huidige niveau.
3. Klik op **OK**.

Opmerking: voorheen geblokkeerde programma's blijven geblokkeerd als het beveiligingsniveau van de firewall wordt ingesteld op **Open**. Dit kunt u voorkomen door de toegangsregel voor deze programma's in te stellen op **Volledige toegang**.

HOOFDSTUK 20

Programma's en toegangsregels beheren

Met Firewall kunt u toegangsregels instellen en beheren voor bestaande en nieuwe programma's die inkomende en uitgaande internettoegang nodig hebben. Met Firewall kunt u volledige toegang of alleen uitgaande toegang verlenen voor programma's. U kunt de toegang voor programma's ook blokkeren.

In dit hoofdstuk

Internettoegang voor programma's verlenen

Sommige programma's, zoals internetbrowsers, hebben toegang tot internet nodig om naar behoren te kunnen functioneren.

In Firewall kunt u via de pagina 'Programmamachtigingen' het volgende doen:

- Toegang voor programma's verlenen
- Alleen uitgaande toegang voor programma's verlenen
- Toegang voor programma's blokkeren

Het is ook mogelijk om volledige toegang en alleen uitgaande toegang te verlenen vanuit de logboeken 'Uitgaande gebeurtenissen' en 'Recente gebeurtenissen'.

Volledige toegang voor een programma verlenen

Voor veel programma's op de computer is inkomende en uitgaande internettoegang vereist. Personal Firewall bevat een lijst met programma's waarvoor automatisch volledige toegang is toegestaan. U kunt deze toegangsregels echter wijzigen.

Ga als volgt te werk om volledige internettoegang voor een programma te verlenen:

1. Klik in het deelvenster voor configuratie van internet en netwerk op **Geavanceerd**.
2. Klik in het deelvenster Firewall op **Programmamachtigingen**.
3. Selecteer onder **Programmamachtigingen** een programma met **Geblokkeerd** of **Alleen uitgaande toegang**.
4. Klik onder **Actie** op **Volledige toegang verlenen**.
5. Klik op **OK**.

Volledige toegang voor een nieuw programma verlenen

Voor veel programma's op de computer is inkomende en uitgaande internettoegang vereist. Firewall bevat een lijst met programma's waarvoor automatisch volledige toegang wordt verleend. U kunt echter nieuwe programma's aan deze lijst toevoegen en de bijbehorende machtigingen wijzigen.

Ga als volgt te werk om een nieuw programma volledige internettoegang te verlenen:

1. Klik in het deelvenster voor configuratie van internet en netwerk op **Geavanceerd**.
2. Klik in het deelvenster **Firewall** op **Programmamachtigingen**.
3. Klik onder **Programmamachtigingen** op **Toegestaan programma toevoegen**.
4. Blader via het dialoogvenster **Programma toevoegen** naar het programma dat u wilt toevoegen en selecteer het programma.
5. Klik op **Openen**.
6. Klik op **OK**.

   Het zojuist toegevoegde programma wordt nu weergegeven onder **Programmamachtigingen**.

Opmerking: het wijzigen van machtigingen van nieuw toegevoegde programma's gaat op dezelfde manier als bij bestaande programma's: selecteer het programma en klik vervolgens onder **Actie** op **Alleen uitgaande toegang verlenen** of op **Toegang blokkeren**.

Volledige toegang toekennen vanuit het logboek voor recente gebeurtenissen

Een groot aantal programma's op uw computer heeft inkomende en uitgaande toegang tot internet nodig. U kunt een programma selecteren in het logboek voor recente gebeurtenissen en dit volledige toegang tot internet verlenen.

Een programma volledige toegang tot internet verlenen vanuit het logboek voor recente gebeurtenissen:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Selecteer de beschrijving van de gebeurtenis onder Recente gebeurtenissen en klik vervolgens op **Volledige toegang verlenen**.
3. Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen dat u aan het programma volledige internettoegang wilt verlenen.

Verwante onderwerpen

- Uitgaande gebeurtenissen weergeven (pagina 178)

Volledige toegang toekennen vanuit het logboek voor uitgaande gebeurtenissen

Een groot aantal programma's op uw computer heeft inkomende en uitgaande toegang tot internet nodig. U kunt een programma selecteren in het logboek voor uitgaande gebeurtenissen en dit volledige toegang tot internet verlenen.

Een programma volledige toegang tot internet verlenen vanuit het logboek voor uitgaande gebeurtenissen:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Selecteer **Netwerk & internet** en vervolgens **Uitgaande gebeurtenissen**.
4. Selecteer in het deelvenster Uitgaande gebeurtenissen een bron-IP-adres en klik vervolgens op **Toegang verlenen**.
5. Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen dat u aan het programma volledige internettoegang wilt verlenen.

Verwante onderwerpen

- Uitgaande gebeurtenissen weergeven (pagina 178)

Alleen uitgaande toegang aan programma's verlenen

Sommige programma's op uw computer hebben alleen uitgaande toegang tot internet nodig. U kunt in Firewall aan dergelijke programma's alleen uitgaande toegang tot internet verlenen.

Alleen uitgaande toegang voor een programma verlenen

Voor veel programma's op de computer is inkomende en uitgaande internettoegang vereist. Personal Firewall bevat een lijst met programma's waarvoor automatisch volledige toegang is toegestaan. U kunt deze toegangsregels echter wijzigen.

Ga als volgt te werk om een programma alleen uitgaande toegang tot internet te verlenen:

1. Klik in het deelvenster voor configuratie van internet en netwerk op **Geavanceerd**.
2. Klik in het deelvenster Firewall op **Programmamachtigingen**.
3. Selecteer onder **Programmamachtigingen** een programma met **Geblokkeerd** of **Volledige toegang**.
4. Klik onder **Actie** op **Alleen uitgaande toegang verlenen**.
5. Klik op **OK**.

Alleen uitgaande toegang toekennen vanuit het logboek voor recente gebeurtenissen

Een groot aantal programma's op uw computer heeft inkomende en uitgaande toegang tot internet nodig. U kunt een programma selecteren in het logboek voor recente gebeurtenissen en dit alleen uitgaande toegang tot internet verlenen.

Een programma alleen uitgaande toegang tot internet verlenen vanuit het logboek voor recente gebeurtenissen:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Selecteer de beschrijving van de gebeurtenis onder Recente gebeurtenissen en klik vervolgens op **Alleen uitgaande toegang verlenen**.
3. Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen dat u aan het programma alleen uitgaande internettoegang wilt verlenen.

Verwante onderwerpen

- Uitgaande gebeurtenissen weergeven (pagina 178)

Alleen uitgaande toegang toekennen vanuit het logboek voor uitgaande gebeurtenissen

Een groot aantal programma's op uw computer heeft inkomende en uitgaande toegang tot internet nodig. U kunt een programma selecteren in het logboek voor uitgaande gebeurtenissen en dit alleen uitgaande toegang tot internet verlenen.

Een programma alleen uitgaande toegang tot internet verlenen vanuit het logboek voor uitgaande gebeurtenissen:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Selecteer **Netwerk & internet** en vervolgens **Uitgaande gebeurtenissen**.
4. Selecteer in het deelvenster Uitgaande gebeurtenissen een bron-IP-adres en klik vervolgens op **Alleen uitgaande toegang verlenen**.
5. Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen dat u aan het programma alleen uitgaande internettoegang wilt verlenen.

Verwante onderwerpen

- Uitgaande gebeurtenissen weergeven (pagina 178)

Internettoegang voor programma's blokkeren

Met Firewall kunt u de internettoegang voor bepaalde programma's blokkeren. Controleer dat het blokkeren van een programma niet tot gevolg heeft dat uw netwerkverbinding wordt onderbroken, of dat een programma dat verbinding met internet nodig heeft, niet meer naar behoren kan functioneren.

Toegang voor een programma blokkeren

Voor veel programma's op de computer is inkomende en uitgaande internettoegang vereist. Personal Firewall bevat een lijst met programma's waarvoor automatisch volledige toegang is toegestaan. U kunt de toegang echter blokkeren.

Ga als volgt te werk om internettoegang voor een programma te blokkeren:

1. Klik in het deelvenster voor configuratie van internet en netwerk op **Geavanceerd**.
2. Klik in het deelvenster Firewall op **Programmamachtigingen**.
3. Selecteer onder **Programmamachtigingen** een programma met **Volledige toegang** of **Alleen uitgaande toegang**.
4. Klik onder **Actie** op **Toegang blokkeren**.
5. Klik op **OK**.

Toegang voor een nieuw programma blokkeren

Voor veel programma's op de computer is inkomende en uitgaande internettoegang vereist. Personal Firewall bevat een lijst met programma's waarvoor automatisch volledige toegang wordt verleend. U kunt echter nieuwe programma's aan deze lijst toevoegen en vervolgens de internettoegang voor die programma's blokkeren.

Ga als volgt te werk om internettoegang voor een nieuw programma te blokkeren:

1. Klik in het deelvenster voor configuratie van internet en netwerk op **Geavanceerd**.
2. Klik in het deelvenster Firewall op **Programmamachtigingen**.
3. Klik onder **Programmamachtigingen** op **Geblokkeerd programma toevoegen**.
4. Blader via het dialoogvenster **Programma toevoegen** naar het programma dat u wilt toevoegen en selecteer het programma.
5. Klik op **Openen**.
6. Klik op **OK**.

   Het zojuist toegevoegde programma wordt nu weergegeven onder **Programmamachtigingen**.

Opmerking: het wijzigen van machtigingen van nieuw toegevoegde programma's gaat op dezelfde manier als bij bestaande programma's: selecteer het programma en klik vervolgens onder **Actie** op **Alleen uitgaande toegang verlenen** of op **Volledige toegang verlenen**.

De toegang tot internet blokkeren vanuit het logboek voor recente gebeurtenissen

Een groot aantal programma's op uw computer heeft inkomende en uitgaande toegang tot internet nodig. U kunt er echter voor kiezen om de toegang van programma's tot internet vanuit het logboek voor recente gebeurtenissen te blokkeren.

De toegang tot internet blokkeren vanuit het logboek voor recente gebeurtenissen:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Selecteer de beschrijving van de gebeurtenis onder Recente gebeurtenissen en klik vervolgens op **Toegang blokkeren**.
3. Klik in het dialoogvenster Programmamachtigingen op **Ja** om te bevestigen dat u het programma wilt blokkeren.

Verwante onderwerpen

- Uitgaande gebeurtenissen weergeven (pagina 178)

Toegangsrechten voor programma's verwijderen

Controleer voordat u de toegangrechten voor een programma verwijdert, of deze actie geen nadelige gevolgen heeft voor de functionaliteit van de computer of de netwerkverbinding.

Programmamachtigingen verwijderen

Voor veel programma's op de computer is inkomende en uitgaande internettoegang vereist. Personal Firewall bevat een lijst met programma's waarvoor automatisch volledige toegang wordt verleend. U kunt echter programma's uit deze lijst verwijderen, die er automatisch of handmatig aan zijn toegevoegd.

Een machtiging voor een nieuw programma verwijderen:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
3. Selecteer een programma onder **Programmamachtigingen**.
4. Klik onder **Actie** op **Programmamachtiging verwijderen**.
5. Klik op **OK**.

   Het programma wordt uit het deelvenster 'Programmamachtigingen' verwijderd.

Opmerking: sommige programma's kunt u niet wijzigen. Uitgeschakelde acties worden in dat geval lichter weergegeven.

Informatie over programma's

Als u onzeker bent over de keuze van de machtigingen voor een bepaald programma, kunt u op de HackerWatch-website van McAfee informatie over dat programma vinden die u kan helpen bij het nemen van een beslissing.

Informatie over programma's raadplegen

Voor veel programma's op de computer is inkomende en uitgaande internettoegang vereist. Personal Firewall bevat een lijst met programma's waarvoor automatisch volledige toegang is toegestaan. U kunt deze toegangsregels echter wijzigen.

Via Firewall kunt u hulp krijgen bij het nemen van een beslissing over het verlenen of weigeren van internettoegang voor een bepaald programma. Controleer dat de computer is aangesloten op internet, zodat de browser de HackerWatch-website van McAfee kan openen. Deze site biedt actuele informatie over programma's, vereisten voor internettoegang en beveiligingsrisico's.

Informatie over programma's raadplegen:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Klik in het deelvenster 'Firewall' op **Programmamachtigingen**.
3. Selecteer een programma onder **Programmamachtigingen**.
4. Klik onder **Actie** op **Meer informatie**.

Informatie over een programma opvragen vanuit het logboek voor uitgaande gebeurtenissen

Firewall stelt u in staat om informatie op te halen over programma's die in het logboek voor uitgaande gebeurtenissen worden weergegeven.

U moet als u dergelijke informatie wilt ophalen over een internetverbinding en een internetbrowser beschikken.

Informatie over een programma ophalen vanuit het logboek voor uitgaande gebeurtenissen

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Selecteer **Netwerk & internet** en vervolgens **Uitgaande gebeurtenissen**.
4. Selecteer in het deelvenster Uitgaande gebeurtenissen een bron-IP-adres en klik vervolgens op **Meer informatie**.

   U kunt informatie over het programma weergeven op de HackerWatch-website. HackerWatch biedt actuele informatie over programma's, internettoegangsvereisten en beveiligingsbedreigingen.

Verwante onderwerpen

- Uitgaande gebeurtenissen weergeven (pagina 178)

HOOFDSTUK 21

Systeemservices beheren

Bepaalde programma's (waaronder webservers en serverprogramma's voor het delen van bestanden) werken alleen als deze ongevraagde verbindingen van andere computers via toegewezen poorten van systeemservices accepteren. Deze servicepoorten worden gewoonlijk door Firewall gesloten omdat deze het meest risicovolle element in de beveiliging van uw systeem vormen. Voor het accepteren van verbindingen van externe computers moeten de servicepoorten echter geopend zijn.

In deze lijst worden de standaardpoorten voor algemene services weergegeven.

- Poort 20-21 voor File Transfer Protocol (FTP)
- Poort 143 voor e-mailserver (IMAP)
- Poort 110 voor e-mailserver (POP3)
- Poort 25 voor e-mailserver (SMTP)
- Poort 445 voor Microsoft Directory Server (MSFT DS)
- Poort 1433 voor Microsoft SQL-server (MSFT SQL)
- Poort 3389 voor Hulp op afstand / Terminal Server (RDP)
- Poort 135 voor Remote Procedure Calls (RPC)
- Poort 443 voor beveiligde webserver (HTTPS)
- Poort 5000 voor Universal Plug and Play (UPnP)
- Poort 80 voor webserver (HTTP)
- Poort 137-139 voor NETBIOS (delen van bestanden in Windows)

In dit hoofdstuk

Poorten voor systeemservices configureren

Als u externe toegang tot een service op uw computer wilt toestaan, moet u instellen dat de service en de bijbehorende poort worden geopend. Selecteer alleen een service en een poort als u zeker weet dat deze moeten worden geopend. Het is zelden nodig dat er een poort moet worden geopend.

Toegang tot een bestaande poort voor een systeemservice toestaan

U kunt via het deelvenster Systeemservices een bestaande poort openen of sluiten om externe toegang tot een netwerkservice op uw computer toe te staan of te weigeren. Een geopende poort voor een systeemservice kan uw computer kwetsbaar maken voor van internet afkomstige bedreigingen van de beveiliging. U moet daarom alleen poorten openen als dat echt nodig is.

Toegang tot een bestaande poort voor een systeemservice toestaan:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik op **Systeemservices** in het deelvenster Firewall.
3. Selecteer de servicepoort die u wilt openen onder **Poort voor systeemservice openen**.
4. Klik op **OK**.

De toegang tot een bestaande poort voor een systeemservice blokkeren

U kunt via het deelvenster Systeemservices een bestaande poort openen of sluiten om externe toegang tot een netwerkservice op uw computer toe te staan of te weigeren. Een geopende poort voor een systeemservice kan uw computer kwetsbaar maken voor van internet afkomstige bedreigingen van de beveiliging. U moet daarom alleen poorten openen als dat echt nodig is.

De toegang tot een bestaande poort voor een systeemservice blokkeren:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik onder het deelvenster Firewall op **Systeemservices**.
3. Schakel onder **Poort voor systeemservice openen** het selectievakje uit van de servicepoort die u wilt sluiten.
4. Klik op **OK**.

Een nieuwe poort voor een systeemservice openen

U kunt via het deelvenster Systeemservices een nieuwe poort voor een systeemservice toevoegen, die u vervolgens kunt openen als u externe toegang tot een netwerkservice op uw computer wilt toestaan en die u kunt sluiten als u externe toegang tot een netwerkservice op uw computer wilt weigeren. Een geopende poort voor een systeemservice kan uw computer kwetsbaar maken voor van internet afkomstige bedreigingen van de beveiliging. U moet daarom alleen poorten openen als dat echt nodig is.

Een nieuwe poort voor een systeemservice maken en configureren:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik op **Systeemservices** in het deelvenster Firewall.
3. Klik op **Toevoegen**.
4. Specificeer onder **Poortconfiguratie toevoegen** het volgende:
   - De programmanaam
   - Inkomende TCP/IP-poorten
   - Uitgaande TCP/IP-poorten
   - Inkomende UDP-poorten
   - Uitgaande UDP-poorten
5. Voeg eventueel een beschrijving voor de nieuwe configuratie toe.
6. Klik op **OK**.

   De nieuwe poort voor de systeemservice wordt weergegeven onder **Poort voor systeemservice openen**.

Een poort voor een systeemservice wijzigen

Een geopende poort maakt toegang tot een netwerkservice op uw computer mogelijk, terwijl een gesloten poort ervoor zorgt dat de toegang tot de desbetreffende netwerkservice op uw computer wordt geweigerd. U kunt inkomende en uitgaande informatie voor een bestaande poort wijzigen via het deelvenster Systeemservices. Als de poortinformatie niet juist is ingevoerd, mislukt het uitvoeren van de systeemservice.

Een poort voor een systeemservice wijzigen:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik op **Systeemservices** in het deelvenster Firewall.
3. Selecteer een systeemservice en klik op **Bewerken**.
4. Specificeer onder **Poortconfiguratie toevoegen** het volgende:
   - De programmanaam
   - Inkomende TCP/IP-poorten
   - Uitgaande TCP/IP-poorten
   - Inkomende UDP-poorten
   - Uitgaande UDP-poorten
5. Voeg eventueel een beschrijving voor de gewijzigde configuratie toe.
6. Klik op **OK**.

   De gewijzigde poort voor de systeemservice wordt weergegeven onder **Poort voor systeemservice openen**.

Een poort voor een systeemservice verwijderen

Een geopende poort maakt toegang tot een netwerkservice op uw computer mogelijk, terwijl een gesloten poort ervoor zorgt dat de toegang tot de desbetreffende netwerkservice op uw computer wordt geweigerd. U kunt een bestaande poort en de bijbehorende systeemservice verwijderen via het deelvenster Systeemservices. Nadat u een poort en de bijbehorende systeemservice via het deelvenster Systeemservices hebt verwijderd, hebben externe computers geen toegang meer tot de netwerkservice op uw computer.

Een poort voor een systeemservice verwijderen:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik op **Systeemservices** in het deelvenster Firewall.
3. Selecteer een systeemservice en klik vervolgens op **Verwijderen**.
4. Klik in het dialoogvenster **Systeemservices** op **Ja** om te bevestigen dat u de systeemservice wilt verwijderen.

   De poort voor de systeemservice wordt vervolgens niet meer weergegeven in het deelvenster Systeemservices.

HOOFDSTUK 22

Computerverbindingen beheren

U kunt Firewall configureren voor het beheren van specifieke externe verbindingen naar uw computer door middel van regels die zijn gebaseerd op IP-adressen (Internet Protocol) van externe computers. Computers waaraan een vertrouwd IP-adres is gekoppeld, kunnen worden vertrouwd om toegang te krijgen tot uw computer. Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Wanneer u een verbinding toestaat, dient u te controleren of de door u vertrouwde computer veilig is. Als een computer die u vertrouwt, is geïnfecteerd met een worm of een ander mechanisme, kan uw computer hierdoor worden blootgesteld aan een besmettingsrisico. Daarnaast raadt McAfee u aan om te controleren of de computer(s) die u vertrouwt, ook beveiligd zijn met een firewall en een actueel antiviruspakket.Verkeer dat afkomstig is van IP-adressen uit de lijst met vertrouwde IP-adressen, wordt niet in het logboek geregistreerd. Ook worden voor deze adressen geen gebeurteniswaarschuwingen gegenereerd.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om IP-adressen te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke dreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server of andere servers bij uw internetprovider. Afhankelijk van uw beveiligingsinstellingen, krijgt u mogelijk een waarschuwing van Firewall als deze een gebeurtenis van een verboden computer detecteert.

In dit hoofdstuk

Computerverbindingen vertrouwen

In het deelvenster 'Vertrouwde en verboden IP-adressen' kunt u onder **Vertrouwde IP-adressen** vertrouwde IP-adressen toevoegen, bewerken en verwijderen.

Met de lijst met **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen' kunt u alle verkeer van een specifieke computer toegang geven tot uw computer. Verkeer dat afkomstig is van IP-adressen die voorkomen in de lijst **Vertrouwde IP-adressen** wordt niet in het logboek geregistreerd. Ook worden voor deze adressen geen gebeurteniswaarschuwingen gegenereerd.

Alle geselecteerde IP-adressen in de lijst worden vertrouwd. Dat betekent dat verkeer vanaf een vertrouwd IP-adres via de firewall of via een van de poorten altijd wordt toegestaan. Gebeurtenissen van vertrouwde IP-adressen worden niet geregistreerd. In Firewall worden activiteiten tussen uw computer en de computer met een vertrouwd IP-adres niet gefilterd of geanalyseerd.

Wanneer u een verbinding toestaat, dient u te controleren of de door u vertrouwde computer veilig is. Als een computer die u vertrouwt, is geïnfecteerd met een worm of een ander mechanisme, kan uw computer hierdoor worden blootgesteld aan een besmettingsrisico. Daarnaast raadt McAfee u aan om te controleren of de computer(s) die u vertrouwt, ook beveiligd zijn met een firewall en een actueel antiviruspakket.

Vertrouwde computerverbinding toevoegen

U kunt via Firewall een vertrouwde computerverbinding en het bijbehorende IP-adres toevoegen.

Met de lijst met **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen' kunt u alle verkeer van een specifieke computer toegang geven tot uw computer. Verkeer dat afkomstig is van IP-adressen die voorkomen in de lijst **Vertrouwde IP-adressen** wordt niet in het logboek geregistreerd. Ook worden voor deze adressen geen gebeurteniswaarschuwingen gegenereerd.

Computers die horen bij een vertrouwd IP-adres kunnen altijd verbinding met uw computer maken. Voordat u een vertrouwd IP-adres toevoegt, bewerkt of verwijdert moet u controleren of dit een adres is waarmee veilige communicatie mogelijk is. Zo niet, dan dient u dit adres te verwijderen.

Een vertrouwde computerverbinding toevoegen:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
3. Selecteer **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
4. Klik op **Toevoegen**.
5. Voer onder **Regel vertrouwd IP-adres toevoegen** een van de volgende handelingen uit:
   - Selecteer een **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
   - Selecteer een **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**.
6. Selecteer eventueel **Regel verloopt over** waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
7. Ook kunt u eventueel een beschrijving van de regel opgeven.
8. Klik op **OK**.
9. Klik in het dialoogvenster 'Regel vertrouwd IP-adres toevoegen' op **Ja** om te bevestigen dat u een vertrouwde computerverbinding wilt toevoegen.

   Het zojuist toegevoegde IP-adres verschijnt onder **Vertrouwde IP-adressen**.

Een vertrouwde computer toevoegen vanuit het logboek voor inkomende gebeurtenissen

U kunt een vertrouwde computerverbinding en het bijbehorende IP-adres toevoegen vanuit het logboek voor inkomende gebeurtenissen.

Computers die horen bij een vertrouwd IP-adres kunnen altijd verbinding met uw computer maken. Voordat u een vertrouwd IP-adres toevoegt, bewerkt of verwijdert moet u controleren of dit een adres is waarmee veilige communicatie mogelijk is. Zo niet, dan dient u dit adres te verwijderen.

Een vertrouwde computer toevoegen vanuit het logboek voor inkomende gebeurtenissen:

1. Controleer of het menu Geavanceerd actief is. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Klik op **Netwerk & internet** en vervolgens op **Inkomende gebeurtenissen**.
4. Selecteer in het deelvenster Inkomende gebeurtenissen een bron-IP-adres en klik vervolgens op **Dit adres vertrouwen**.
5. Klik in het dialoogvenster Regel vertrouwd IP-adres toevoegen op **Ja** om te bevestigen dat u het IP-adres wilt instellen als een vertrouwd adres.

   Het zojuist toegevoegde IP-adres wordt vervolgens weergegeven onder **Vertrouwde IP-adressen**.

Verwante onderwerpen

- Logboekregistratie (pagina 176)

Vertrouwde computerverbinding bewerken

U kunt via Firewall een vertrouwde computerverbinding en het bijbehorende IP-adres bewerken.

Computers die horen bij een vertrouwd IP-adres kunnen altijd verbinding met uw computer maken. Voordat u een vertrouwd IP-adres toevoegt, bewerkt of verwijdert moet u controleren of dit een adres is waarmee veilige communicatie mogelijk is. Zo niet, dan dient u dit adres te verwijderen.

Een vertrouwde computerverbinding bewerken:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
3. Selecteer **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
4. Selecteer een IP-adres en klik vervolgens op **Bewerken**.
5. Voer onder **Regel vertrouwd IP-adres toevoegen** een van de volgende handelingen uit:
   - Selecteer een **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
   - Selecteer een **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de vakken **Eerste IP-adres** en **Laatste IP-adres**.
6. Selecteer eventueel **Regel verloopt over**, waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
7. Ook kunt u eventueel een beschrijving van de regel opgeven.
8. Klik op **OK**.

   Het gewijzigde IP-adres verschijnt onder **Vertrouwde IP-adressen**.

Vertrouwde computerverbinding verwijderen

U kunt via Firewall een vertrouwde computerverbinding en het bijbehorende IP-adres verwijderen.

Computers die horen bij een vertrouwd IP-adres kunnen altijd verbinding met uw computer maken. Voordat u een vertrouwd IP-adres toevoegt, bewerkt of verwijdert moet u controleren of dit een adres is waarmee veilige communicatie mogelijk is. Zo niet, dan dient u dit adres te verwijderen.

Een vertrouwde computerverbinding verwijderen:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
3. Selecteer **Vertrouwde IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
4. Selecteer een IP-adres en klik vervolgens op **Verwijderen**.
5. Klik in het dialoogvenster **Vertrouwde en verboden IP-adressen** op **Ja** om te bevestigen dat u een vertrouwd IP-adres onder **Vertrouwde IP-adressen** wilt verwijderen.

Computerverbindingen verbieden

In het deelvenster 'Vertrouwde en verboden IP-adressen' kunt u onder **Verboden IP-adressen** vertrouwde IP-adressen toevoegen, bewerken en verwijderen.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om IP-adressen te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke dreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server of andere servers bij uw internetprovider. Afhankelijk van uw beveiligingsinstellingen, krijgt u mogelijk een waarschuwing van Firewall als deze een gebeurtenis van een verboden computer detecteert.

Verboden computerverbinding toevoegen

U kunt via Firewall een verboden computerverbinding en het bijbehorende IP-adres toevoegen.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om IP-adressen te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke dreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server of andere servers bij uw internetprovider. Afhankelijk van uw beveiligingsinstellingen, krijgt u mogelijk een waarschuwing van Firewall als deze een gebeurtenis van een verboden computer detecteert.

Een verboden computerverbinding toevoegen:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
3. Selecteer **Verboden IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
4. Klik op **Toevoegen**.
5. Voer onder 'Regel verboden IP-adres toevoegen' een van de volgende handelingen uit:
   - Selecteer een **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
   - Selecteer een **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de velden **Eerste IP-adres** en **Laatste IP-adres**.
6. Selecteer eventueel **Regel verloopt over**, waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
7. Ook kunt u eventueel een beschrijving van de regel opgeven.
8. Klik op **OK**.
9. Klik in het dialoogvenster **Regel verboden IP-adres toevoegen** op **Ja** om te bevestigen dat u een verboden computerverbinding wilt toevoegen.

   Het zojuist toegevoegde IP-adres verschijnt onder **Verboden IP-adressen**.

Een verboden computerverbinding bewerken

U kunt via Firewall een verboden computerverbinding en het bijbehorende IP-adres bewerken.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om IP-adressen te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke dreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server of andere servers bij uw internetprovider. Afhankelijk van uw beveiligingsinstellingen, krijgt u mogelijk een waarschuwing van Firewall als deze een gebeurtenis van een verboden computer detecteert.

Een verboden computerverbinding bewerken:

1. Klik in het deelvenster 'Internet- en netwerkconfiguratie' op **Geavanceerd**.
2. Klik in het deelvenster 'Firewall' op **Vertrouwde en verboden IP-adressen**.
3. Selecteer **Verboden IP-adressen** in het deelvenster 'Vertrouwde en verboden IP-adressen'.
4. Selecteer een IP-adres en klik vervolgens op **Bewerken**.
5. Voer onder **Regel verboden IP-adres toevoegen** een van de volgende handelingen uit:
   - Selecteer een **Enkelvoudig IP-adres** en voer vervolgens het IP-adres in.
   - Selecteer een **IP-adresbereik** en voer vervolgens het eerste en laatste IP-adres in in de velden **Eerste IP-adres** en **Laatste IP-adres**.
6. Selecteer eventueel **Regel verloopt over**, waarna u kunt invullen gedurende hoeveel dagen deze regel moet worden uitgevoerd.
7. Ook kunt u eventueel een beschrijving van de regel opgeven.

   Klik op **OK**. Het gewijzigde IP-adres verschijnt onder **Verboden IP-adressen**.

Een verbinding met een verboden computer verwijderen

U kunt Firewall gebruiken als u een verbinding met een verboden computer en het bijbehorende IP-adres wilt verwijderen.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om IP-adressen te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke dreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server of andere servers bij uw internetprovider. Afhankelijk van uw beveiligingsinstellingen, krijgt u mogelijk een waarschuwing van Firewall als deze een gebeurtenis van een verboden computer detecteert.

Een verbinding met een verboden computer verwijderen:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik op **Vertrouwde en verboden IP-adressen** in het deelvenster Firewall.
3. Selecteer **Verboden IP-adressen** in het deelvenster Vertrouwde en verboden IP-adressen.
4. Selecteer een IP-adres en klik op **Verwijderen**.
5. Klik in het dialoogvenster **Vertrouwde en verboden IP-adressen** op **Ja** om te bevestigen dat u het IP-adres wilt verwijderen uit de lijst **Verboden IP-adressen**.

Een computer blokkeren vanuit het logboek voor inkomende gebeurtenissen

U kunt een vertrouwde computerverbinding en het bijbehorende IP-adres blokkeren vanuit het logboek voor inkomende gebeurtenissen.

IP-adressen die in het logboek voor inkomende gebeurtenissen worden weergegeven, zijn geblokkeerd. Het blokkeren van een adres resulteert dan ook niet een verdergaande mate van bescherming, behalve als uw computer gebruikmaakt van poorten die opzettelijk zijn geopend of als er op uw computer een programma staat waaraan internettoegang is verleend.

Voeg alleen een IP-adres toe aan de lijst met **verboden IP-adressen** als een of meer poorten opzettelijk zijn geopend en als er aanleiding is om te voorkomen dat het adres toegang krijgt tot de geopende poorten.

De pagina Inkomende gebeurtenissen bevat u een lijst met al het inkomende internetverkeer, die u kunt gebruiken om een IP-adres te blokkeren dat u ervan verdenkt de bron te zijn van een verdachte of ongewenste internetactiviteit.

Een vertrouwde computerverbinding blokkeren vanuit het logboek voor inkomende gebeurtenissen:

1. Controleer of het menu Geavanceerd actief is. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Klik op **Netwerk & internet** en vervolgens op **Inkomende gebeurtenissen**.
4. Selecteer in het deelvenster Inkomende gebeurtenissen een bron-IP-adres en klik vervolgens op **Dit adres blokkeren**.
5. Klik in het dialoogvenster **Regel verboden IP-adres toevoegen** op **Ja** om te bevestigen dat u het IP-adres wilt blokkeren.

   Het zojuist toegevoegde IP-adres wordt vervolgens weergegeven in de lijst met **verboden IP-adressen**.

Verwante onderwerpen

- Logboekregistratie (pagina 176)

Een computer blokkeren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem

U kunt een computerverbinding en het bijbehorende IP-adres blokkeren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem.

Computers waaraan een onbekend, verdacht of onvertrouwd IP-adres is gekoppeld, kunnen worden uitgesloten van verbinding met uw computer.

Aangezien Firewall al het ongewenste verkeer blokkeert, is het normaal gesproken niet nodig om IP-adressen te blokkeren. U moet een IP-adres alleen blokkeren wanneer u zeker weet dat een internetverbinding een specifieke dreiging oplevert. Zorg ervoor dat u geen belangrijke IP-adressen blokkeert, zoals de DNS- of DHCP-server of andere servers bij uw internetprovider. Afhankelijk van uw beveiligingsinstellingen, krijgt u mogelijk een waarschuwing van Firewall als deze een gebeurtenis van een verboden computer detecteert.

Een computer blokkeren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Klik op **Netwerk & internet** en klik vervolgens op **Gebeurtenissen inbraakdetectie**.
4. Selecteer in het deelvenster Gebeurtenissen inbraakdetectie een bron-IP-adres en klik vervolgens op **Dit adres blokkeren**.
5. Klik in het dialoogvenster **Regel verboden IP-adres toevoegen** op **Ja** om te bevestigen dat u het IP-adres wilt blokkeren.

   Het zojuist toegevoegde IP-adres wordt vervolgens weergegeven in de lijst met **verboden IP-adressen**.

Verwante onderwerpen

- Logboekregistratie (pagina 176)

HOOFDSTUK 23

Logbestanden, controles en analyses

Firewall voorziet in veelomvattende en gebruikersvriendelijke mogelijkheden voor logboekregistratie, controles en analyses voor internetverkeer en gebeurtenissen. Inzicht in internetverkeer en -gebeurtenissen stelt u in staat om uw internetverbindingen beter te beheren.

In dit hoofdstuk

Logboekregistratie

U kunt in Firewall instellen of u logboekregistratie wilt inschakelen of uitschakelen. Als u logboekregistratie inschakelt, kunt u bovendien instellen welke typen gebeurtenissen u in een logboek wilt vastleggen. Het vastleggen van gebeurtenissen in logboeken stelt u in staat om recente inkomende en uitgaande gebeurtenissen weer te geven. Daarnaast kunt u tevens door het inbraakdetectiesysteem gedetecteerde gebeurtenissen weergeven.

De instellingen voor het gebeurtenislogboek configureren

Als u firewallgebeurtenissen en firewallactiviteiten wilt volgen, kunt u instellen welke typen gebeurtenissen u wilt weergeven.

Het vastleggen van gebeurtenissen configureren:

1. Klik op **Geavanceerd** in het deelvenster Netwerk en internetconfiguratie.
2. Klik op **Instellingen gebeurtenislogboek** in het deelvenster Firewall.
3. Ga in het deelvenster Instellingen gebeurtenislogboek op een van de volgende manieren te werk:
   - Selecteer **Gebeurtenis registreren in logboek** als u het vastleggen van gebeurtenissen wilt inschakelen.
   - Selecteer **Gebeurtenis niet registreren in logboek** als u het vastleggen van gebeurtenissen wilt uitschakelen.
4. Geef onder **Instellingen gebeurtenislogboek** op welke gebeurtenistypen u in een logboek wilt vastleggen. Het betreft de volgende gebeurtenistypen:
   - ICMP-pings
   - Verkeer van verboden IP-adressen
   - Gebeurtenissen op systeemservicepoorten
   - Gebeurtenissen op onbekende poorten
   - Gebeurtenissen in het inbraakdetectiesysteem (IDS)
5. Selecteer **Gebeurtenissen op de volgende poort(en) niet vastleggen** en voer afzonderlijke poortnummers gescheiden door komma's of poortbereiken gescheiden door streepjes in (bijvoorbeeld `137-139, 445, 400-5000`), als u logboekregistratie op specifieke poorten wilt voorkomen.
6. Klik op **OK**.

Recente gebeurtenissen weergeven

Als het logbestand is ingeschakeld, kunt u recente gebeurtenissen weergeven. In het deelvenster Recente gebeurtenissen worden datums en beschrijvingen van recente gebeurtenissen weergegeven. In het deelvenster Recente gebeurtenissen worden alleen activiteiten weergegeven van programma's waarvoor de toegang tot internet nadrukkelijk is geblokkeerd.

Recente gebeurtenissen van Firewall weergeven:

- Klik in het menu **Geavanceerd** onder het deelvenster Algemene taken op **Rapporten en logboeken** of op **Recente gebeurtenissen weergeven**. U kunt ook in het menu Basis onder het deelvenster Algemene taken op **Recente gebeurtenissen weergeven** klikken.

Inkomende gebeurtenissen weergeven

Als het logbestand is ingeschakeld, kunt u inkomende gebeurtenissen weergeven en sorteren.

In het logbestand voor inkomende gebeurtenissen worden de volgende gegevens vastgelegd:

- De datum en de tijd
- Het bron-IP-adres
- De hostnaam
- Informatie en het gebeurtenistype

De inkomende gebeurtenissen van uw firewall weergeven:

1. Controleer of het menu Geavanceerd actief is. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Klik op **Netwerk & internet** en vervolgens op **Inkomende gebeurtenissen**.

Opmerking: U kunt IP-adressen die in het logboek voor inkomende gebeurtenissen zijn vastgelegd, vertrouwen, blokkeren en traceren.

Verwante onderwerpen

- Een vertrouwde computer toevoegen vanuit het logboek voor inkomende gebeurtenissen (pagina 166)
- Een computer blokkeren vanuit het logboek voor inkomende gebeurtenissen (pagina 173)
- Een computer traceren vanuit het logboek voor inkomende gebeurtenissen (pagina 182)

Uitgaande gebeurtenissen weergeven

Als het logbestand is ingeschakeld, kunt u uitgaande gebeurtenissen weergeven. In het logbestand voor uitgaande gebeurtenissen wordt onder meer het volgende vastgelegd: de naam van het programma dat heeft geprobeerd om een uitgaande verbinding tot stand te brengen, de datum en het tijdstip waarop de gebeurtenis plaatsvond en de locatie van het desbetreffende programma op uw computer.

De uitgaande gebeurtenissen van uw firewall weergeven:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Selecteer **Netwerk & internet** en vervolgens **Uitgaande gebeurtenissen**.

Opmerking: U kunt aan een programma in het logboek voor uitgaande gebeurtenissen volledige toegang of alleen uitgaande toegang toekennen. Daarnaast beschikt u over de mogelijkheid om aanvullende informatie over het desbetreffende programma weer te geven.

Verwante onderwerpen

- Volledige toegang toekennen vanuit het logboek voor uitgaande gebeurtenissen (pagina 146)
- Alleen uitgaande toegang toekennen vanuit het logboek voor uitgaande gebeurtenissen (pagina 149)
- Informatie over een programma opvragen vanuit het logboek voor uitgaande gebeurtenissen (pagina 155)

Gebeurtenissen van het inbraakdetectiesysteem weergeven

Als het logbestand is ingeschakeld, kunt u inkomende gebeurtenissen weergeven. Voor gebeurtenissen van het inbraakdetectiesysteem worden de datum en de tijd en het bron-IP-adres en de hostnaam van de gebeurtenis weergegeven. Daarnaast bevat het logboek een beschrijving van het type gebeurtenis.

Gebeurtenissen van het inbraakdetectiesysteem weergeven:

1. Klik onder het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder Recente gebeurtenissen op **Logboek weergeven**.
3. Klik op **Netwerk & internet** en klik vervolgens op **Gebeurtenissen inbraakdetectie**.

Opmerking: U kunt IP-adressen die in het logboek voor gebeurtenissen van het inbraakdetectiesysteem zijn vastgelegd, vertrouwen, blokkeren en traceren.

Verwante onderwerpen

- Een computer blokkeren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem (pagina 174)
- Een computer traceren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem (pagina 183)

Werken met statistieken

Firewall voorziet u via de HackerWatch-beveiligingswebsite van McAfee van mondiale statistieken over aan gerelateerde beveiligingsgebeurtenissen en poortactiviteiten.

Mondiale statistieken over beveiligingsgebeurtenissen weergeven

HackerWatch houdt wereldwijde beveiligingsgebeurtenissen met betrekking tot internet bij. U kunt deze gegevens weergeven via SecurityCenter. De informatie die u kunt weergeven omvat lijsten met incidenten die in de afgelopen 24 uur, 7 dagen of 30 dagen aan HackerWatch zijn gerapporteerd.

Mondiale statistieken over beveiligingsgebeurtenissen weergeven:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **HackerWatch** in het deelvenster Gereedschappen.
3. De statistieken worden weergegeven onder **Tracering van gebeurtenissen**.

Mondiale internetpoortactiviteiten weergeven

HackerWatch houdt wereldwijde beveiligingsgebeurtenissen met betrekking tot internet bij. U kunt deze gegevens weergeven via SecurityCenter. De weergegeven informatie omvat de belangrijkste gebeurtenissen met poorten die in de afgelopen zeven dagen aan HackerWatch zijn gerapporteerd. Hierbij wordt er standaard informatie weergegeven over HTTP-, TCP- en UDP-poorten.

Mondiale poortactiviteiten weergeven:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **HackerWatch** in het deelvenster Gereedschappen.
3. De belangrijkste gebeurtenissen worden weergegeven onder **Recente poortactiviteit**.

Internetverkeer traceren

Firewall biedt een aantal opties voor het traceren van internetverkeer. Deze opties stellen u in staat om een netwerkcomputer geografisch te traceren, om domein- en netwerkinformatie op te vragen en om computers vanuit de logboeken voor inkomende gebeurtenissen en voor gebeurtenissen in het inbraakdetectiesysteem te traceren.

Een netwerkcomputer geografisch traceren

Als u aan de hand van de naam of het IP-adres van een computer die verbinding maakt of die verbinding probeert te maken met uw computer de geografische locatie van de desbetreffende computer wilt achterhalen, kunt u de visuele traceerfunctie gebruiken. U kunt de visuele traceerfunctie ook gebruiken om netwerk- en registratie-informatie weer te geven. Als u de visuele traceerfunctie uitvoert, wordt er een wereldkaart weergegeven waarop de meest waarschijnlijke route van de broncomputer naar uw computer wordt afgebeeld.

Een computer geografisch traceren:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **Visual Tracer** in het deelvenster Gereedschappen.
3. Typ het IP-adres van de computer en klik op **Dit adres traceren**.
4. Selecteer onder **Visual Tracer** de optie **Weergave kaart**.

Opmerking: Het is niet mogelijk om gebeurtenissen met herhalende, privé- of ongeldige IP-adressen te traceren.

Computerregistratie-informatie ophalen

U kunt via SecurityCenter met Visual Trace computerregistratie-informatie ophalen. Deze informatie omvat de domeinnaam, de naam en het adres van de geregistreerd en de contactgegevens.

De domeininformatie van een computer ophalen:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **Visual Tracer** in het deelvenster Gereedschappen.
3. Typ het IP-adres van de desbetreffende computer en klik vervolgens op **Dit adres traceren**.
4. Selecteer onder **Visual Tracer** de optie **Weergave geregistreerde**.

De netwerkinformatie van een computer ophalen

U kunt via SecurityCenter met Visual Trace netwerkregistratie-informatie ophalen. Deze netwerkinformatie omvat details over het netwerk waarin het domein zich bevindt.

De netwerkinformatie van een computer ophalen:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **Visual Tracer** in het deelvenster Gereedschappen.
3. Typ het IP-adres van de desbetreffende computer en klik vervolgens op **Dit adres traceren**.
4. Selecteer onder **Visual Tracer** de optie **Weergave netwerk**.

Een computer traceren vanuit het logboek voor inkomende gebeurtenissen

U kunt vanuit het deelvenster Inkomende gebeurtenissen een IP-adres traceren dat wordt weergegeven in het logboek voor inkomende gebeurtenissen.

Het IP-adres van een computer traceren vanuit het logboek voor inkomende gebeurtenissen:

1. Controleer of het menu Geavanceerd actief is. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Klik op **Netwerk & internet** en vervolgens op **Inkomende gebeurtenissen**.
4. Selecteer in het deelvenster Inkomende gebeurtenissen een bron-IP-adres en klik vervolgens op **Dit adres traceren**.
5. Klik in het deelvenster Visual Tracer op een van de volgende opties:
   - **Weergave kaart**: Hiermee kunt u een computer met het geselecteerde IP-adres geografisch traceren.
   - **Weergave geregistreerde**: Hiermee kunt u informatie weergeven over het domein dat het geselecteerde IP-adres gebruikt.
   - **Weergave netwerk**: Hiermee kunt u informatie weergeven over het netwerk dat het geselecteerde IP-adres gebruikt.
6. Klik op **Gereed**.

Verwante onderwerpen

- Internetverkeer traceren (pagina 181)
- Inkomende gebeurtenissen weergeven (pagina 177)

Een computer traceren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem

U kunt vanuit het deelvenster Gebeurtenissen inbraakdetectie een IP-adres traceren dat wordt weergegeven in het logboek voor gebeurtenissen van het inbraakdetectiesysteem.

Het IP-adres van een computer traceren vanuit het logboek voor gebeurtenissen van het inbraakdetectiesysteem:

1. Klik in het deelvenster Algemene taken op **Rapporten en logboeken**.
2. Klik onder **Recente gebeurtenissen** op **Logboek weergeven**.
3. Klik op **Netwerk & internet** en klik vervolgens op **Gebeurtenissen inbraakdetectie**. Selecteer in het deelvenster Gebeurtenissen inbraakdetectie een bron-IP-adres en klik vervolgens op **Dit adres traceren**.
4. Klik in het deelvenster Visual Tracer op een van de volgende opties:
   - **Weergave kaart**: Hiermee kunt u een computer met het geselecteerde IP-adres geografisch traceren.
   - **Weergave geregistreerde**: Hiermee kunt u informatie weergeven over het domein dat het geselecteerde IP-adres gebruikt.
   - **Weergave netwerk**: Hiermee kunt u informatie weergeven over het netwerk dat het geselecteerde IP-adres gebruikt.
5. Klik op **Gereed**.

Verwante onderwerpen

- Internetverkeer traceren (pagina 181)
- Logbestanden, controles en analyses (pagina 175)

Een gecontroleerd IP-adres traceren

U kunt een gecontroleerd IP-adres traceren. Als u het IP-adres traceert, wordt er een wereldkaart weergegeven waarop de meest waarschijnlijke route van de gegevens van de broncomputer naar uw computer wordt afgebeeld. Daarnaast kunt u registratie- en netwerkinformatie over het desbetreffende IP-adres ophalen.

Een gecontroleerd IP-adres traceren:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
3. Klik onder **Verkeersmonitor** op **Actieve programma's**.
4. Selecteer een programma en klik vervolgens op het IP-adres dat onder de naam van het programma wordt weergegeven.
5. Klik onder **Activiteit van programma** op **Dit IP-adres traceren**.
6. Er wordt vervolgens onder **Visual Tracer** een wereldkaart weergegeven waarop de meest waarschijnlijke route van de gegevens van de broncomputer naar uw computer wordt afgebeeld. Daarnaast kunt u registratie- en netwerkinformatie over het desbetreffende IP-adres ophalen.

Opmerking: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Visual Tracer** op **Vernieuwen**.

Verwante onderwerpen

- Internetverkeer controleren (pagina 185)

Internetverkeer controleren

Firewall voorziet in een aantal methoden voor het controleren van het internetverkeer, waaronder:

- **De grafiek Verkeersanalyse**: Hiermee geeft u het recente inkomende en uitgaande internetverkeer weer.
- **De grafiek Verkeersgebruik**: Hiermee geeft u het percentage van de bandbreedte weer dat in de afgelopen 24 uur door de meest actieve toepassingen op uw computer is gebruikt.
- **Actieve Programma's**: Hiermee geeft u de programma's op uw computer weer die momenteel de meeste netwerkverbindingen gebruiken en u geeft de IP-adressen weer die door deze programma's zijn benaderd.

Informatie over de grafiek Verkeersanalyse

De grafiek Verkeersanalyse geeft een numerieke en een grafische weergave weer van inkomend en uitgaand internetverkeer. Bovendien geeft de Verkeersmonitor weer welke toepassingen momenteel de meeste netwerkverbindingen op uw computer gebruiken en welke IP-adressen door de toepassingen worden geopend.

U kunt vanuit het deelvenster Verkeersanalyse recent inkomend en uitgaand internetverkeer en huidige, gemiddelde en maximale overdrachtssnelheden weergeven. U kunt bovendien het verkeersvolume weergeven (inclusief het verkeersvolume sinds u Firewall hebt gestart) en u kunt de totale hoeveelheid verkeer voor de huidige maand en de vorige maand weergeven.

Het deelvenster Verkeersanalyse geeft de realtime internetactiviteit op uw computer weer, inclusief het volume en de snelheid van het recente inkomende en uitgaande internetverkeer op uw computer. Daarnaast worden tevens de verbindingssnelheid en het aantal bytes dat via internet is overgedragen, weergegeven.

De groene lijn vertegenwoordigt de huidige overdrachtssnelheid voor inkomend verkeer. De groene stippellijn vertegenwoordigt de gemiddelde overdrachtssnelheid voor inkomend verkeer. Als de huidige en de gemiddelde overdrachtssnelheid gelijk zijn, wordt de stippellijn niet in de grafiek weergegeven. De weergegeven lijn vertegenwoordigt in een dergelijk geval zowel de gemiddelde als de huidige overdrachtssnelheid.

De rode lijn vertegenwoordigt de huidige overdrachtssnelheid voor uitgaand verkeer. De rode stippellijn vertegenwoordigt de gemiddelde overdrachtssnelheid voor uitgaand verkeer. Als de huidige en de gemiddelde overdrachtssnelheid gelijk zijn, wordt de stippellijn niet in de grafiek weergegeven. De weergegeven lijn vertegenwoordigt in een dergelijk geval zowel de gemiddelde als de huidige overdrachtssnelheid.

Verwante onderwerpen

- Het inkomende en uitgaande verkeer analyseren (pagina 186)

Het inkomende en uitgaande verkeer analyseren

De grafiek Verkeersanalyse geeft een numerieke en een grafische weergave weer van inkomend en uitgaand internetverkeer. Bovendien geeft de Verkeersmonitor weer welke toepassingen momenteel de meeste netwerkverbindingen op uw computer gebruiken en welke IP-adressen door de toepassingen worden geopend.

Het inkomende en uitgaande verkeer analyseren:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
3. Klik onder **Verkeersmonitor** op **Verkeersanalyse**.

Tip: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Verkeersanalyse** op **Vernieuwen**.

Verwante onderwerpen

- Informatie over de grafiek Verkeersanalyse (pagina 185)

De bandbreedte van programma's controleren

U kunt een cirkeldiagram weergeven waarin bij benadering het percentage aan bandbreedte wordt getoond dat in de afgelopen 24 uur door de meest actieve programma's op uw computer is gebruikt. Een cirkeldiagram voorziet in een grafische weergave van de relatieve hoeveelheid bandbreedte die door de programma's is gebruikt.

Het bandbreedtegebruik van programma's controleren:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
3. Klik onder **Verkeersmonitor** op **Verkeersgebruik**.

Tip: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Verkeersgebruik** op **Vernieuwen**.

Activiteiten van programma's controleren

U kunt inkomende en uitgaande activiteiten van programma's weergeven. Hierbij worden de verbindingen met externe computers en poorten weergegeven.

De activiteiten van programma's controleren:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **Verkeersmonitor** in het deelvenster Gereedschappen.
3. Klik onder **Verkeersmonitor** op **Actieve programma's**.
4. U kunt de volgende informatie weergeven:
   - Een grafiek van de activiteiten van een programma: Selecteer een programma als u een grafiek van de activiteiten van het programma wilt weergeven.
   - Luisterende verbindingen: Selecteer een item onder de naam van het programma.
   - Computerverbindingen: Selecteer een IP-adres onder de naam van het programma, het systeemproces of de service.

Opmerking: Als u de meest actuele statistieken wilt weergeven, klikt u onder **Actieve programma's** op **Vernieuwen**.

HOOFDSTUK 24

Informatie over internetbeveiliging

Firewall voorziet u via de HackerWatch-beveiligingswebsite van McAfee van actuele informatie over programma's en mondiale internetactiviteiten. HackerWatch biedt daarnaast een HTML-zelfstudie over Firewall.

In dit hoofdstuk

De HackerWatch-zelfstudie starten

Als u meer wilt leren over Firewall, kunt u de HackerWatch-zelfstudie starten vanuit SecurityCenter.

De HackerWatch-zelfstudie starten:

1. Schakel het menu Geavanceerd in en klik vervolgens op **Gereedschappen**.
2. Klik op **HackerWatch** in het deelvenster Gereedschappen.
3. Klik onder **HackerWatch-bronnen** op **Zelfstudie weergeven**.

HOOFDSTUK 25

McAfee EasyNetwork

McAfee® EasyNetwork ondersteunt het veilig delen van bestanden, maakt het gemakkelijk bestanden over te dragen en verzorgt automatisch het delen van printers tussen vertrouwde computers in uw thuisnetwerk.

Voordat u begint met het gebruik van EasyNetwork kunt u kennismaken met enkele van de meest gebruikte functies. Meer informatie over het configureren en gebruik van deze functies vindt u in de Help van EasyNetwork.

In dit hoofdstuk

Functies

EasyNetwork biedt de volgende functies.

Bestanden delen

Met EasyNetwork is het eenvoudig om bestanden op uw computer te delen met andere computers in het netwerk. Wanneer u bestanden deelt, verleent u daarmee andere computers toestemming om deze bestanden te mogen lezen (alleen-lezen). Alleen computers die lid zijn van het beheerde netwerk (dat wil zeggen computers met volledige of beheerdersrechten) kunnen bestanden delen of bestanden openen die door andere leden worden gedeeld.

Bestandsoverdracht

U kunt bestanden verzenden naar andere computers die lid zijn van het beheerde netwerk. Wanneer u een bestand ontvangt, verschijnt deze in uw Postvak IN van EasyNetwork. Het Postvak IN is een tijdelijke opslagplaats voor alle bestanden die naar u worden verzonden door andere computers in het netwerk.

Automatisch delen van printers

Nadat u zich hebt aangemeld bij een beheerd netwerk, deelt EasyNetwork automatisch de beschikbare lokale printers die aan uw computer zijn verbonden. Hierbij wordt de huidige naam van de printer gebruikt als naam voor de gedeelde printer. EasyNetwork controleert ook of er printers beschikbaar zijn die worden gedeeld door andere computers in uw netwerk, en staat u toe om deze printers te configureren en te gebruiken.

HOOFDSTUK 26

EasyNetwork installeren

Voordat u de functies van EasyNetwork kunt gebruiken, moet u eerst het programma starten en u aanmelden bij het beheerde netwerk. Nadat u zich hebt aangemeld, kunt u het netwerk op elk gewenst moment weer verlaten.

In dit hoofdstuk

EasyNetwork starten

Standaard wordt u onmiddellijk na het installeren van EasyNetwork gevraagd of u dit programma wilt starten. U kunt EasyNetwork echter ook op een later tijdstip starten.

EasyNetwork starten

Standaard wordt u onmiddellijk na het installeren van EasyNetwork gevraagd of u dit programma wilt starten. U kunt EasyNetwork echter ook op een later tijdstip starten.

Ga als volgt te werk om EasyNetwork te starten:

- Wijs in het menu **Start** de optie **Programma's** aan, wijs **McAfee** aan klik vervolgens op **McAfee EasyNetwork**.

Tip: Als u er tijdens de installatie toestemming voor hebt gegeven om een bureaubladpictogram en een snelstartpictogram aan te maken, kunt u EasyNetwork ook starten door te dubbelklikken op het pictogram van McAfee EasyNetwork op uw bureaublad of door te klikken op het pictogram van McAfee EasyNetwork in het systeemvak van Windows, rechts op de taakbalk.

Lid worden van een beheerd netwerk

Nadat u SecurityCenter hebt geïnstalleerd, wordt aan uw computer een netwerkagent toegevoegd die op de achtergrond wordt uitgevoerd. In EasyNetwork is de netwerkagent verantwoordelijk voor het opsporen van een geldige netwerkverbinding, het opsporen van lokale printers die worden gedeeld, en het controleren van de netwerkstatus.

Als er in het netwerk waarop u momenteel bent aangesloten geen andere computer wordt aangetroffen waarop de netwerkagent wordt uitgevoerd, wordt u automatisch aangemeld als lid van het netwerk en wordt u gevraagd om aan te geven of het netwerk vertrouwd is. Als uw computer de eerste is die lid wordt van het netwerk, wordt de naam van uw computer automatisch opgenomen in de netwerknaam. U kunt dit netwerk echter altijd een andere naam geven.

Wanneer een computer verbinding maakt met het netwerk, wordt een aanmeldingsverzoek gestuurd naar alle andere computers die op dat moment op het netwerk zijn aangesloten. Het verzoek kan worden ingewilligd door elke computer die over de juiste beheerdersrechten voor het netwerk beschikt. De toegangsverlener kan ook het het machtigingsniveau bepalen voor de computer die momenteel lid wordt van het netwerk. Machtigingsniveaus zijn bijvoorbeeld: gast (uitsluitend gemachtigd tot bestandsoverdracht) of volledige/beheerdersrechten (zowel gemachtigd tot bestandsoverdracht als tot het uitwisselen van bestanden). In EasyNetwork kunnen computers met beheerdersrechten toegang verlenen aan andere computers en machtigingen beheren (dat wil zeggen computers hoger of lager in de hiërarchie plaatsen); computers met volledige toegangsrechten mogen deze beheerderstaken niet uitvoeren. Voordat de computer lid mag worden, wordt ook eerst een beveiligingscontrole uitgevoerd.

Opmerking: Nadat u lid bent geworden, en indien u andere McAfee-netwerkprogramma's hebt geïnstalleerd (bijvoorbeeld McAfee Wireless Network Security of Network Manager), wordt de computer door deze programma's ook herkend als een beheerde computer. Het machtigingsniveau dat aan een computer is toegewezen, geldt voor alle McAfee-netwerkprogramma's. Raadpleeg de documentatie bij een programma voor meer informatie over de betekenis van gast-, beheer- en volledige machtigingen in andere McAfee-netwerkprogramma's.

Lid worden van het netwerk

De eerste keer dat een computer waarop EasyNetwork is geïnstalleerd verbinding maakt met een vertrouwd netwerk, wordt er gevraagd of u lid wil worden van het beheerde netwerk. Wanneer de computer toestemming verleent om lid te worden, wordt een aanmeldingsverzoek gestuurd naar alle andere computers met beheerdersrechten. Dit verzoek moet worden verleend voordat de computer printers of bestanden kan delen, of bestanden kan versturen of kopiëren over het netwerk. Als de computer de eerste computer in het netwerk is, worden er automatisch beheerdersmachtigingen voor het netwerk aan deze computer verleend.

Ga als volgt te werk om lid te worden van het netwerk:

1. Klik in het venster Gedeelde bestanden op **Ja, nu aanmelden bij dit netwerk**.
   Wanneer een computer voor netwerkbeheer uw verzoek inwilligt, verschijnt een bericht waarin u wordt gevraagd of u deze computer en andere computers in het netwerk wilt toestaan om elkaars beveiligingsinstellingen te beheren.
2. Als u wilt toestaan dat deze computer en andere computers in het netwerk elkaars beveiligingsinstellingen beheren, klikt u op **Ja**; zo niet, dan klikt u op **Nee**.
3. Bevestig dat de computer die toegang verleent de speelkaarten weergeeft die momenteel worden weergegeven in het bevestigingsdialoogvenster, en klik vervolgens op **Bevestigen**.

Opmerking: Als er op de computer die toegang verleent niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een inbreuk op de beveiliging van het beheerde netwerk. Als u lid wordt van het netwerk, kunt u uw computer in gevaar brengen. Klik daarom op **Weigeren** in het bevestigingsdialoogvenster.

Toegang verlenen tot het netwerk

Wanneer een computer een verzoek indient om lid te worden van het beheerde netwerk, wordt een bericht gestuurd naar de andere computers in het netwerk die over beheerdersrechten beschikken. De eerste computer die dit bericht beantwoordt, wordt de toegangsverlener. Als toegangsverlener bent u verantwoordelijk voor het besluit of u het gewenste type toegang aan de computer in kwestie wilt verlenen: gast, volledig of beheerder.

Ga als volgt te werk om toegang te verlenen tot het netwerk:

1. Schakel één van de volgende selectievakjes van het waarschuwingsbericht in:
   - **Gasttoegang verlenen**: Hiermee kan de gebruiker bestanden versturen naar andere computers, maar geen bestanden delen.
   - **Volledige toegang verlenen tot alle beheerde netwerktoepassingen**: Hiermee kan de gebruiker zowel bestanden versturen als bestanden delen.
   - **Beheertoegang verlenen tot alle beheerde netwerktoepassingen**: Hiermee kan de gebruiker bestanden versturen en delen, toegang verlenen tot andere computers en de machtigingsniveaus van andere computers wijzigen.
2. Klik op **Toegang verlenen**.
3. Bevestig dat op uw computer dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, en klik vervolgens op **Bevestigen**.

Opmerking: Als er op uw computer niet dezelfde speelkaarten worden weergegeven als in het bevestigingsdialoogvenster, is er sprake van een inbreuk op de beveiliging van het beheerde netwerk. Door deze computer toegang te verlenen tot het netwerk zou u uw computer kunnen blootstellen aan een beveiligingsrisico. We raden u dan ook aan om te klikken op **Weigeren** in het bevestigingsdialoogvenster Beveiliging.

De naam van het netwerk wijzigen

Standaard is de naam van de eerste computer die zich bij het netwerk heeft aangemeld opgenomen in de naam van het netwerk. U kunt de naam van het netwerk echter altijd nog wijzigen. Wanneer u het netwerk een andere naam geeft, wijzigt u de netwerkomschrijving die wordt weergegeven in EasyNetwork.

De naam van het netwerk wijzigen:

1. Klik in het menu **Opties** op **Configureren**.
2. In het dialoogvenster Configureren typt u de naam van het netwerk in het vak **Netwerknaam**.
3. Klik op **OK**.

U afmelden bij een beheerd netwerk

Als u zich hebt aangemeld bij een beheerd netwerk en vervolgens besluit dat u niet langer lid wenst te zijn, kunt u het netwerk verlaten. Nadat u uw lidmaatschap hebt opgezegd kunt u daarna vervolgens altijd weer lid worden. U dient zich dan echter wel weer opnieuw aan te melden, er moet u opnieuw toestemming worden verleend en u moet de beveiligingscontrole opnieuw doorlopen. Zie Lid worden van een beheerd netwerk (pagina 195) voor meer informatie.

U afmelden bij een beheerd netwerk

U kunt zich afmelden bij een beheerd netwerk waarbij u zich eerder hebt aangemeld.

Ga als volgt te werk om u af te melden bij een beheerd netwerk:

1. Klik in het menu **Extra** op **Netwerk verlaten**.
2. In het dialoogvenster Netwerk verlaten selecteert u de naam van het netwerk waarvoor u zich wilt afmelden.
3. Klik op **Netwerk verlaten**.

HOOFDSTUK 27

Bestanden delen en versturen

Met EasyNetwork wordt het eenvoudig om bestanden op uw computer te delen met en te versturen naar andere computers in het netwerk. Wanneer u bestanden deelt, verleent u daarmee andere computers toestemming om deze bestanden te mogen lezen. Alleen computers die lid zijn van het beheerde netwerk (dat wil zeggen computers met volledige of beheerdersrechten) kunnen bestanden delen of bestanden openen die door andere lidcomputers worden gedeeld.

In dit hoofdstuk

Bestanden delen

Met EasyNetwork wordt het eenvoudig om bestanden op uw computer te delen met andere computers in het netwerk. Wanneer u bestanden deelt, verleent u daarmee andere computers toestemming om deze bestanden te mogen lezen. Alleen computers die lid zijn van het beheerde netwerk (dat wil zeggen computers met volledige of beheerdersrechten) kunnen bestanden delen of bestanden openen die door andere lidcomputers worden gedeeld. Als u een map deelt, worden alle bestanden in die map en in de submappen daarvan gedeeld. Als u vervolgens bestanden toevoegt aan die map worden deze echter niet automatisch gedeeld. Als een gedeeld bestand of een gedeelde map wordt verwijderd, wordt deze ook verwijderd uit het venster Gedeelde bestanden. U kunt het delen van een bestand op elk gewenst moment opheffen.

U kunt een gedeeld bestand op twee manieren openen: Door het bestand rechtstreeks te openen vanuit EasyNetwork of door het bestand te kopiëren naar een locatie op uw computer en het vervolgens te openen. Als uw lijst met gedeelde bestanden te lang wordt, kunt u zoeken op een of meer gedeelde bestanden die u wilt openen.

Opmerking: Bestanden die worden gedeeld met behulp van EasyNetwork kunnen niet vanuit andere computers worden geopend met behulp van Windows Verkenner. Het delen van bestanden met EasyNetwork verloopt via veilige verbindingen.

Een bestand delen

Wanneer u een bestand deelt, wordt dit automatisch beschikbaar gesteld aan alle andere leden met volledige of beheerdersrechten voor het beheerde netwerk.

Ga als volgt te werk om een bestand te delen:

1. Zoek in Windows Verkenner het bestand dat u wilt delen.
2. Sleep het bestand vanuit de locatie in Windows Verkenner naar het venster Gedeelde bestanden in EasyNetwork.

Tip: U kunt een bestand ook delen door te klikken op **Bestanden delen** in het menu **Extra**. Navigeer in het dialoogvenster Delen naar de map waarin het bestand dat u wilt delen is opgeslagen, selecteer het bestand en klik vervolgens op **Delen**.

Het delen van een bestand opheffen

Als u een bestand deelt op het beheerde netwerk, kunt u het delen van dat bestand op elk gewenst moment opheffen. Wanneer u stopt met het delen van een bestand kunnen andere leden van het beheerde netwerk dat bestand niet langer openen.

Ga als volgt te werk om het delen van een bestand te stoppen:

1. Klik in het menu **Extra** op **Stoppen met bestanden delen**.
2. Selecteer in het dialoogvenster Stoppen met bestanden delen het bestand dat u niet langer wilt delen.
3. Klik op **Niet delen**.

Een gedeeld bestand kopiëren

U kunt gedeelde bestanden vanaf elke computer in het beheerde netwerk kopiëren naar uw eigen computer. Als de computer stopt met het delen van een bestand hebt u dan zelf nog altijd een exemplaar.

Ga als volgt te werk om een bestand te kopiëren:

- Sleep een bestand vanuit het venster Gedeelde bestanden in EasyNetwork naar een locatie in Windows Verkenner of naar het Windows-bureaublad.

Tip: U kunt een gedeeld bestand ook kopiëren door het bestand te selecteren in EasyNetwork, en vervolgens te klikken op **Kopiëren naar** in het menu **Extra**. Navigeer in het dialoogvenster 'Kopiëren naar map' de map waarnaar u het bestand wilt kopiëren, selecteer de betreffende map en klik vervolgens op **Opslaan**.

Een gedeeld bestand zoeken

U kunt zoeken naar een bestand dat door u of door een ander lid van het netwerk is gedeeld. Terwijl u uw zoekcriteria typt, geeft EasyNetwork automatisch de bijbehorende resultaten weer in het venster Gedeelde bestanden.

Ga als volgt te werk om een gedeeld bestand te zoeken:

1. Klik in het venster Gedeelde bestanden op **Zoeken**.
2. Klik op een van de volgende opties in de lijst **Bevat**:
   - **Bevat alle volgende woorden**: Zoekt de naam van het bestand of het pad dat alle woorden bevat die u opgeeft in de lijst **Bestandsnaam of pad**, in willekeurige volgorde.

- **Bevat een of meer van de volgende woorden**: Zoekt de naam van het bestand of het pad dat een of meer van de woorden bevat die u opgeeft in de lijst **Bestandsnaam of pad**.
- **Bevat exact de volgende tekenreeks**: Zoekt de naam van het bestand of het pad dat exact dezelfde woordenreeks bevat die u opgeeft in de lijst **Bestandsnaam of pad**.

3 Typ een deel van de bestandsnaam of van het pad of de gehele bestandsnaam of het gehele pad in de lijst **Bestandsnaam of pad**.

4 Klik op een van de volgende bestandstypen in de lijst **Type**:

- **Willekeurig**: Doorzoekt alle gedeelde bestandstypen.
- **Document**: Doorzoekt alle gedeelde documenten.
- **Afbeelding**: Doorzoekt alle gedeelde afbeeldingsbestanden.
- **Video**: Doorzoekt alle gedeelde videobestanden.
- **Audio**: Doorzoekt alle gedeelde audiobestanden.

5 Klik in de lijsten **Van** en **t/m** op datums die het datumbereik aangeven waarbinnen het gezochte bestand is aangemaakt.

Bestanden naar andere computers verzenden

U kunt bestanden verzenden naar andere computers die lid zijn van het beheerde netwerk. Voordat u een bestand verstuurt, bevestigt EasyNetwork dat er voldoende vrije schijfruimte beschikbaar is op de computer die het bestand ontvangt.

Wanneer u een bestand ontvangt, verschijnt dit in uw Postvak IN van EasyNetwork. Het Postvak IN is een tijdelijke opslagplaats voor alle bestanden die naar u worden verzonden door andere computers in het netwerk. Als u EasyNetwork geopend hebt wanneer u een bestand ontvangt, verschijnt het bestand direct in uw Postvak IN. Als u EasyNetwork niet geopend hebt, verschijnt er een bericht in het systeemvak van Windows, rechts op de taakbalk. Als u geen waarschuwingsberichten wenst te ontvangen, kunt u deze functie uitschakelen. Als er in het Postvak IN al een bestand voorkomt met dezelfde naam, krijgt het nieuwe bestand een nummer achter de naam. Bestanden blijven in uw Postvak IN staan totdat u deze accepteert (dat wil zeggen totdat u deze naar een locatie op uw computer kopieert).

Een bestand naar een een andere computer verzenden

U kunt een bestand rechtstreeks naar een andere computer op het beheerde netwerk sturen zonder dat u het bestand hoeft te delen. Voordat een gebruiker op de ontvangende computer het bestand kan bekijken, moet deze het bestand eerst opslaan in een lokale locatie. Zie Een bestand van een andere computer accepteren (pagina 206) voor meer informatie.

Ga als volgt te werk om een bestand naar een andere computer te verzenden:

1. Zoek in Windows Verkenner het bestand dat u wilt verzenden.
2. Sleep het bestand vanuit de locatie in Windows Verkenner naar het pictogram van een actieve computer in EasyNetwork.

Tip: U kunt meerdere bestanden tegelijk naar een computer verzenden door de toets Ctrl (Control) ingedrukt te houden terwijl u de bestanden selecteert. U kunt ook bestanden verzenden door te klikken op **Verzenden** in het menu **Extra**, de bestanden te selecteren en vervolgens te klikken op **Verzenden**.

Een bestand van een andere computer accepteren

Als een andere computer in het beheerde netwerk u een bestand stuurt, moet u dit accepteren (door het bestand op te slaan in een map op uw computer). Als u EasyNetwork niet geopend hebt of als het niet in de voorgrond wordt uitgevoerd wanneer er een bestand naar uw computer wordt gestuurd, ontvangt u een bericht hierover in het systeemvak van Windows, rechts op de taakbalk. Klik op dit bericht om EasyNetwork te openen en toegang te krijgen tot het bestand.

Ga als volgt te werk om een bestand van een andere computer te ontvangen:

- Klik op **Ontvangen** en sleep vervolgens een bestand vanuit uw Postvak IN van EasyNetwork naar een map in Windows Verkenner.

Tip: U kunt ook een bestand van een andere computer ontvangen door het bestand te selecteren uw Postvak IN van EasyNetwork, en vervolgens te klikken op **Accepteren** in het menu **Extra**. Blader in het dialoogvenster Accepteren in map naar de map waarin u de bestanden die u ontvangt wilt opslaan, selecteer de gewenste map en klik vervolgens op **Opslaan**.

Bericht ontvangen wanneer een bestand wordt verzonden

U kunt desgewenst bericht ontvangen telkens wanneer een andere computer op het beheerde netwerk u een bestand stuurt. Als u EasyNetwork momenteel niet geopend hebt of als EasyNetwork niet op de voorgrond van uw bureaublad wordt weergegeven, verschijnt er een bericht in het systeemvak van Windows, rechts op de taakbalk.

Ga als volgt te werk om bericht te ontvangen wanneer een bestand wordt verzonden:

1. Klik in het menu **Opties** op **Configureren**.
2. Schakel in het dialoogvenster Configureren het selectievakje **Waarschuwen wanneer een andere computer mij bestanden stuurt** in.
3. Klik op **OK**.

HOOFDSTUK 28

Printers delen

Nadat u zich hebt aangemeld bij een beheerd netwerk, deelt EasyNetwork automatisch de beschikbare lokale printers die aan uw computer zijn verbonden. EasyNetwork controleert ook of er printers beschikbaar zijn die worden gedeeld door andere computers in uw netwerk, en staat u toe om deze printers te configureren en te gebruiken.

In dit hoofdstuk

Werken met gedeelde printers

Nadat u zich hebt aangemeld bij een beheerd netwerk, deelt EasyNetwork automatisch de beschikbare lokale printers die aan uw computer zijn verbonden. Hierbij wordt de huidige naam van de printer gebruikt als naam voor de gedeelde printer. EasyNetwork controleert ook of er printers beschikbaar zijn die worden gedeeld door andere computers in uw netwerk, en staat u toe om deze printers te configureren en te gebruiken. Als u een printer zodanig hebt geconfigureerd dat deze afdrukt via een netwerk-afdrukserver (zoals een draadloze USB-afdrukserver), beschouwt EasyNetwork de printer als een lokale printer en zal EasyNetwork de printer deze automatisch delen in het netwerk. U kunt het delen van een printer op elk gewenst moment opheffen.

EasyNetwork spoort ook printers op die worden gedeeld door alle andere computers in het netwerk. Als EasyNetwork een externe printer aantreft die nog niet met uw computer verbonden is, verschijnt de koppeling **Beschikbare netwerkprinters** in het venster Gedeelde bestanden wanneer u EasyNetwork voor het eerst opent. Hiermee kunt u beschikbare printers installeren of de installatie opheffen van printers die al met uw computer zijn verbonden. U kunt de lijst met beschikbare printers die zijn aangetroffen in dit netwerk ook vernieuwen.

Als u zich nog niet hebt aangemeld bij het beheerde netwerk maar er wel op bent aangesloten, kunt u de gedeelde printers openen via het venster Printers en faxapparaten onder het menu Configuratiescherm van Windows.

Het delen van een printer opheffen

U kunt het delen van een printer op elk gewenst moment opheffen. Leden die de printer hebben geïnstalleerd zullen in het vervolg niet meer met deze printer kunnen afdrukken.

Ga als volgt te werk om het delen van een printer op te heffen:

1. Klik in het menu **Extra** op **Printers**.
2. Selecteer in het dialoogvenster Netwerkprinters beheren de printer die u niet langer wilt delen.
3. Klik op **Niet delen**.

Een beschikbare netwerkprinter installeren

Als lid van een beheerd netwerk kunt u toegang krijgen tot de printers die via het netwerk worden gedeeld. Om een gedeelde printer te kunnen gebruiken, moet u het printerstuurprogramma installeren dat door de printer wordt gebruikt. Als de eigenaar het delen van de printer opheft nadat u het stuurprogramma hebt geïnstalleerd, kunt u voortaan niet meer afdrukken op deze printer.

Ga als volgt te werk om een beschikbare netwerkprinter te installeren:

1. Klik in het menu **Extra** op **Printers**.
2. Klik in het dialoogvenster Beschikbare netwerkprinters op de naam van een printer.
3. Klik op **Installeren**.

HOOFDSTUK 29

Naslag

De Verklarende woordenlijst van termen geeft een overzicht en definitie van de beveiligingstermen die in McAfee-producten het meeste worden gebruikt.

Onder Informatie over McAfee vindt u de juridische kennisgevingen van McAfee Corporation.

Verklarende woordenlijst

8

802.11

Een reeks IEEE-standaarden voor draadloze LAN-technologie. 802.11 definieert een interface via de lucht tussen een draadloze client en een basisstation, of tussen twee draadloze clients. Er zijn meerdere 802.11-specificaties, zoals 802.11a, een standaard voor een maximale netwerksnelheid van 54 Mbps in de 5-GHz band, 802.11b, een standaard voor een maximale netwerksnelheid van 11 Mbps in de 2,4-GHz band, 802.11g, een standaard voor een maximale netwerksnelheid van 54 Mbps in de 2,4-GHz band, en 802.11i, een reeks beveiligingsstandaarden voor alle draadloze Ethernet-netwerken.

802.11a

Een uitbreiding van 802.11 voor draadloze LAN's, waarbij gegevens worden verzonden met een maximumsnelheid van 54 Mbps in de 5-GHz band. De transmissiesnelheid is weliswaar hoger dan bij 802.11b maar de maximumafstand is veel kleiner.

802.11b

Een uitbreiding van 802.11 voor draadloze LAN's, waarbij gegevens worden verzonden met een maximumsnelheid van 11 Mbps in de 2,4-GHz band. 802.11b wordt momenteel beschouwd als de standaard voor draadloze netwerken.

802.11g

Een uitbreiding van 802.11 voor draadloze LAN's, waarbij gegevens worden verzonden met een maximumsnelheid van 54 Mbps in de 2,4-GHz band.

802.1x

Wordt niet ondersteund door Wireless Home Network Security. Een IEEE-standaard voor verificatie op draadloze en kabelnetwerken. Deze standaard wordt echter vooral gebruikt in combinatie met 802.11 voor draadloze netwerken. Deze standaard biedt sterke, wederzijdse verificatie tussen een client en een verificatieserver. Daarnaast kan 802.1x dynamisch WEP-sleutels bieden die worden gewijzigd per gebruiker en per sessie, zodat u zich niet met het intensieve beheer en de beveiligingsrisico's van statische WEP-sleutels hoeft bezig te houden.

A

Aanval met grof geweld

Wordt ook kraken met grof geweld genoemd. Dit is een 'met vallen en opstaan'-methode die door toepassingsprogramma's wordt gebruikt om gecodeerde gegevens zoals wachtwoorden te decoderen via niet-aflatende pogingen (met gebruik van grof geweld) in plaats van via intelligente strategieën. Net zoals een crimineel een kluis kan proberen te openen (of te kraken) door alle mogelijke combinaties te proberen, probeert een toepassing voor kraken met grof geweld alle mogelijke combinaties van toegestane tekens achter elkaar. Dit type van aanval neemt weliswaar veel tijd in beslag, maar wordt als onfeilbaar beschouwd.

Archiveren

Een lokale kopie maken van bewaakte bestanden op cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf.

Archiveren

Een lokale kopie maken van bewaakte bestanden op cd, dvd, een USB-station, een externe vaste schijf of een netwerkschijf.

B

Back-up maken

Een kopie maken van uw bewaakte bestanden op een beveiligde online server.

Bandbreedte

De hoeveelheid gegevens die binnen een bepaalde periode kan worden verzonden of ontvangen. Voor digitale apparaten wordt de bandbreedte doorgaans uitgedrukt in bits per seconde (bps) of bytes per seconde. Voor analoge apparaten wordt de bandbreedte uitgedrukt in cycli per seconde, of hertz (Hz).

Beeldanalyse

Blokkeert afbeelding die mogelijk ongeschikt zijn. Afbeeldingen worden geblokkeerd voor alle gebruikers behalve leden van de leeftijdsgroep voor volwassenen.

beheerd netwerk

Een thuisnetwerk dat twee typen leden kan hebben: beheerde leden en niet-beheerde leden. Beheerde leden staan andere computers in het netwerk toe hun McAfee-beveiligingsstatus te controleren. Niet-beheerde leden staan dit niet toe.

bewaakte bestandstypen

De bestandtypen (bijvoorbeeld .doc, .xls, enz.) waarvan met Data Backup een back-up wordt gemaakt of die worden gearchiveerd in de bewaakte locaties.

bewaakte locaties

De mappen op uw computer die door Data Backup worden bewaakt.

bibliotheek

Het online opslaggebied voor bestanden die door gebruikers van Data Backup zijn gepubliceerd. De bibliotheek is een website op internet die toegankelijk is voor iedereen met toegang tot internet.

browser

Een clientprogramma dat HTTP (Hypertext Transfer Protocol) gebruikt om aanvragen in te dienen bij webservers op internet. In een webbrowser wordt inhoud grafisch weergegeven.

C

Client

Een toepassing die op een pc of werkstation wordt uitgevoerd en afhankelijk is van een server voor de uitvoering van bepaalde acties. Bijvoorbeeld: een e-mailclient is een toepassing waarmee u e-mail kunt verzenden en ontvangen.

codering

Een proces waarbij tekst wordt omgezet in code. Hierdoor worden de gegevens gemaskeerd zodat deze onleesbaar wordt voor iedereen die niet weet hoe de informatie moet worden gedecodeerd.

Codetekst

Gegevens die zijn gecodeerd. Codetekst is onleesbaar totdat deze met behulp van een sleutel is geconverteerd (gedecodeerd) naar normale tekst.

compressie

Een proces waarbij gegevens (bestanden) worden gecomprimeerd naar een formaat dat minder ruimte inneemt bij het opslaan of versturen.

cookie

Op het World Wide Web: een blok met gegevens dat door een webserver wordt opgeslagen op een clientsysteem. Wanneer een gebruiker terugkeert naar dezelfde website, stuurt de browser een kopie van de cookie terug naar de server. Cookies worden gebruikt om gebruikers te identificeren, om de server op te dragen een aangepaste versie van de opgevraagde webpagina te verzenden, om accountgegevens van de gebruiker in te dienen en voor andere beheerdoeleinden.

Een website kan aan de hand van cookies onthouden wie u bent, hoeveel mensen de website hebben bezocht en wanneer, en welke pagina's werden bekeken. Met cookies kan een bedrijf ook zijn website op u afstemmen. Veel websites vereisen een gebruikersnaam en wachtwoord voor toegang tot bepaalde pagina's. Er wordt een cookie naar uw computer verzonden zodat u zich niet telkens opnieuw hoeft aan te melden. Cookies kunnen echter ook worden misbruikt. Internetreclamebureaus gebruiken vaak cookies om te bepalen welke websites u vaak bezoekt. Vervolgens worden reclames op uw favoriete websites geplaatst. Voordat u cookies van een site toestaat, moet u zeker weten of u de site kunt vertrouwen.

Cookies zijn een informatiebron voor legitieme bedrijven, maar kunnen ook een informatiebron voor hackers zijn. Veel websites met online winkels gebruiken cookies voor het onthouden van creditcardgegevens en andere persoonlijke informatie om het online winkelen te vergemakkelijken. Er kunnen helaas beveiligingsproblemen optreden waardoor hackers toegang hebben tot de informatie van cookies die zijn opgeslagen op de computers van de klanten.

D

delen

Een handeling waarbij ontvangers van een e-mailbericht een beperkte periode geselecteerde back-upbestanden kunnen openen. Als u een bestand deelt, verstuurt u een back-upexemplaar van het bestand aan de e-mailontvangers die u opgeeft. De ontvangers ontvangen een e-mailbericht van Data Backup met de melding dat er bestanden met hen worden gedeeld. Het e-mailbericht bevat ook een koppeling naar de gedeelde bestanden.

Denial of Service (DoS)

Op internet is een DoS-aanval een voorval waarbij een gebruiker of organisatie geen toegang meer heeft tot een service waartoe deze normaal gesproken toegang moet hebben. Het verlies van service bestaat meestal uit het niet beschikbaar zijn van een bepaalde netwerkservice, bijvoorbeeld e-mail, of het tijdelijke verlies van alle netwerkverbindingen en services. In het slechtste geval kan bijvoorbeeld een website met miljoenen bezoekers nu en dan worden gedwongen om tijdelijk offline te gaan. Een DoS-aanval kan ook programma's en bestanden in een computersysteem vernietigen. In de meeste situaties worden deze aanvallen opzettelijk en met kwade bedoelingen uitgevoerd, maar soms treden ze ook per ongeluk op. Een DoS-aanval is een type van veiligheidslek in een computersysteem dat doorgaans niet leidt tot diefstal van informatie of andere beveiligingsproblemen. Deze aanvallen kunnen het slachtoffer of het betrokken bedrijf echter veel tijd en geld kosten.

DNS

Acroniem voor Domain Name System. Het hiërarchische systeem waarin hosts op internet zowel een domeinnaamadressen (zoals bluestem.prairienet.org) als IP-adressen (zoals 192.17.3.4) hebben. Het domeinnaamadres wordt gebruikt door menselijke gebruikers en wordt automatisch vertaald naar het numerieke IP-adres, dat wordt gebruikt door de software voor het routeren van pakketten. DNS-namen bestaan uit een hoofdniveaudomein (zoals .com, .org en .net), een domein op het tweede niveau (de sitenaam van een bedrijf, een organisatie of een persoon) en mogelijk een of meer subdomeinen (servers binnen een domein op het tweede niveau). Zie ook DNS-server en IP-adres.

DNS-server

Korte naam voor Domain Name System-server. Een computer die DNS-query's kan beantwoorden. De DNS-server houdt een database bij van hostcomputers en de bijbehorende IP-adressen. Als de DNS-server bijvoorbeeld de naam apex.com krijgt aangeboden, wordt het IP-adres geretourneerd van het hypothetische bedrijf Apex. Ook wel naamserver genoemd. Zie ook DNS en IP-adres.

Domein

Een adres van een netwerkverbinding waarmee de eigenaar van dat adres wordt geïdentificeerd in een hiërarchische indeling: server.organisatie.type. Bijvoorbeeld, met www.wittehuis.gov wordt de webserver van het Witte Huis geïdentificeerd, die deel uitmaakt van de Amerikaanse overheid.

Draadloze adapter

Bevat de elektronica die een computer of een ander apparaat nodig heeft om te communiceren met een draadloze router (om verbinding te maken met een draadloos netwerk). Draadloze adapters kunnen geïntegreerd zijn in de hoofdelektronica van een hardwareapparaat, of ontworpen als aparte insteekmodule die via de overeenkomstige poort in een apparaat kan worden geplaatst.

Draadloze PCI-adapterkaarten

Kaarten die een desktopcomputer verbinden met een netwerk. De kaart wordt in een PCI-uitbreidingssleuf in de computer geplaatst.

Draadloze USB-adapterkaarten

Bieden een uitbreidbare, seriële, Plug-and-Play interface. Deze interface biedt een goedkope, draadloze standaardaansluiting voor randapparatuur zoals toetsenborden, muizen, joysticks, printers, scanners, opslagapparatuur en videoconferentiecamera's.

E

E-mail

Elektronische post, berichten die worden verzonden via internet of binnen het LAN of WAN van een bedrijf. E-mailbijlagen in de vorm van EXE-bestanden (uitvoerbare bestanden) of VBS-bestanden (Visual Basic-scripts) worden steeds vaker gebruikt voor de verspreiding van virussen en Trojaanse paarden.

E-mailclient

Een e-mailaccount, bijvoorbeeld Microsoft Outlook of Eudora.

ESS (Extended Service Set)

Een set van twee of meer netwerken die één subnetwerk vormen.

externe vaste schijf

Een vaste schijf die zich buiten de computerbehuizing bevindt.

F

Firewall

Een systeem dat is ontworpen om ongeoorloofde toegang tot of vanaf een privé-netwerk onmogelijk te maken. Firewalls kunnen hardware- of softwarematig, of een combinatie van beide zijn. Firewalls worden vaak gebruikt om niet-geautoriseerde internetgebruikers de toegang te weigeren tot privé-netwerken (vooral intranetten) die met internet zijn verbonden. Alle berichten die het intranet binnenkomen of verlaten, passeren de firewall. De firewall controleert alle berichten en blokkeert berichten die niet voldoen aan de ingestelde beveiligingscriteria. Een firewall wordt beschouwd als de eerste verdedigingslinie bij de bescherming van privé-informatie. Voor meer veiligheid kunnen de gegevens worden gecodeerd.

G

Gebeurtenis

Gebeurtenissen van 0.0.0.0

Als u gebeurtenissen ziet van IP-adres 0.0.0.0, zijn hier twee mogelijke oorzaken voor. De eerste en meest voorkomende oorzaak is dat uw computer een onjuist samengesteld pakket heeft ontvangen. Het internet is niet altijd 100% betrouwbaar en er kunnen ongeldige pakketten voorkomen. Aangezien de firewall de pakketten ziet voordat deze door TCP/IP kunnen worden gevalideerd, worden deze pakketten mogelijk gerapporteerd als een gebeurtenis.

De andere situatie treedt op wanneer het bron-IP-adres wordt vervalst. Vervalste pakketten kunnen erop wijzen dat iemand een scan uitvoert op zoek naar Trojaanse paarden en dat daarbij is geprobeerd uw computer te scannen. Vergeet niet dat de firewall de poging blokkeert.

Gebeurtenissen van 127.0.0.1

Voor sommige gebeurtenissen is het bron-IP-adres 127.0.0.1. Dit IP-adres is speciaal en wordt het loopback-adres genoemd.

Ongeacht welke computer u gebruikt, 127.0.0.1 verwijst altijd naar de lokale computer. Het adres heet ook wel localhost, omdat de localhost van de computernaam altijd wordt omgezet naar het IP-adres 127.0.0.1. Betekent dit dat uw computer zelf aan het hacken is? Neemt een Trojaans paard of spyware uw computer over? Dat is niet waarschijnlijk. Veel legitieme programma's gebruiken het loopback-adres voor de communicatie tussen onderdelen. Veel persoonlijke mail- of webservers kunt u bijvoorbeeld configureren via een webinterface die meestal toegankelijk is via een adres zoals http://localhost/.

De firewall staat echter verkeer van deze programma's toe, dus als u gebeurtenissen ziet van 127.0.0.1, betekent dit hoogstwaarschijnlijk dat het bron-IP-adres is vervalst. Vervalste pakketten duiden er meestal op dat er iemand scant op Trojaanse paarden. Vergeet niet dat de firewall deze poging blokkeert. Het rapporteren van gebeurtenissen met 127.0.0.1 als bron heeft natuurlijk geen nut.

Voor bepaalde programma's, met name Netscape 6.2 en hoger, moet u 127.0.0.1 echter toevoegen aan de lijst **Vertrouwde IP-adressen**. De onderdelen van deze programma's communiceren op een zodanige wijze met elkaar dat de firewall niet kan bepalen of het verkeer lokaal is.

Als u bij Netscape 6.2 het adres 127.0.0.1 niet vertrouwt, kunt u de buddylijst niet gebruiken. Als u dus verkeer ziet van 127.0.0.1 en alle programma's op de computer werken op de normale wijze, is het veilig om dit verkeer te blokkeren. Als een programma (zoals Netscape) echter problemen heeft, voegt u 127.0.0.1 toe aan de lijst **Vertrouwde IP-adressen** in de firewall en kijkt u of het probleem is opgelost.

Als het probleem is opgelost door 127.0.0.1 in de lijst **Vertrouwde IP-adressen** te plaatsen, moet u het volgende overwegen: als u 127.0.0.1 vertrouwt, werkt uw programma, maar bent u kwetsbaarder voor aanvallen met een vervalst IP-adres. Als u het adres niet vertrouwt, werkt het programma niet, maar bent u nog wel beveiligd tegen dergelijk schadelijk verkeer.

Gebeurtenissen van computers op uw LAN

Voor de meeste instelling voor bedrijfs-LAN's geldt dat u alle computers in uw LAN kunt vertrouwen.

Gebeurtenissen van privé-IP-adressen

IP-adressen met de indeling 192.168.xxx.xxx, 10.xxx.xxx.xxx en 172.16.0.0 - 172.31.255.255 worden niet-routeerbare of privé-IP-adressen genoemd. In principe mogen deze IP-adressen uw netwerk nooit verlaten en kunnen ze meestal worden vertrouwd.

Het blok 192.168 wordt gebruikt voor de voorziening Internetverbinding delen van Microsoft. Als u gebruikmaakt van Internetverbinding delen en u gebeurtenissen ziet van dit IP-blok, kunt u het IP-adres 192.168.255.255 toevoegen aan uw lijst **Vertrouwde IP-adressen**. U vertrouwt dan het volledige blok 192.168.xxx.xxx.

Als u zich niet op een privé-netwerk bevindt en u gebeurtenissen ziet uit deze IP-bereiken, kan het bron-IP-adres vervalst zijn. Vervalste pakketten duiden er meestal op dat iemand op zoek is naar Trojaanse paarden. Vergeet niet dat de firewall deze poging blokkeert.

Aangezien privé-IP-adressen niet hetzelfde zijn als IP-adressen op het internet, heeft het geen zin om deze gebeurtenissen te rapporteren.

Gedeeld geheim

Zie ook RADIUS. Beveiligt gevoelige delen van RADIUS-berichten. Dit gedeelde geheim is een wachtwoord dat op een veilige manier wordt gedeeld tussen de verificator en de verificatieserver.

Geïntegreerde gateway

Een apparaat dat de functies van een toegangspunt, router en firewall combineert. Sommige apparaten kunnen ook beveiligingsfuncties en bridgingvoorzieningen bieden.

Groepen met inhoudsrestricties

Leeftijdsgroepen waartoe een gebruiker behoort. Inhoud wordt beoordeeld (met andere woorden: beschikbaar gesteld of geblokkeerd) op basis van de groep met inhoudsrestricties waartoe de gebruiker behoort. De groepen met inhoudsrestricties zijn: jong kind, kind, jongere tiener, oudere tiener en volwassene.

Hotspot

Een specifieke geografische locatie waar een toegangspunt mobiele bezoekers via een draadloos netwerk toegang biedt tot openbare, draadloze breedbandservices. Hotspots bevinden zich doorgaans op plaatsen met veel mensen, zoals luchthavens, spoorwegstations, bibliotheken, jachthavens, congrescentra en hotels. Hotspots hebben gewoonlijk een klein toegangsbereik.

Internet

Het internet bestaat uit een groot aantal onderling verbonden netwerken die de TCP/IP-protocollen gebruiken om gegevens te vinden en over te zetten. Het internet is voortgekomen uit een aantal aan elkaar gekoppelde computers op universiteiten en colleges (aan het eind van de jaren zestig en aan het begin van de jaren zeventig van de vorige eeuw) die waren gefinancierd door het Amerikaanse ministerie van defensie. Dit netwerk werd het ARPANET genoemd. Vandaag de dag is het internet een wereldwijd netwerk dat bestaat uit bijna 100.000 onafhankelijke netwerken.

intranet

Een privé-netwerk, meestal binnen een organisatie, dat functioneert zoals het internet. Gewoonlijk verlenen deze intranetten toegang aan zelfstandige computers die op een andere locatie door studenten of werknemers worden gebruikt. Voor een goede beveiliging zijn firewalls, aanmeldingsprocedures en wachtwoorden vereist.

IP-adres

Een uniek nummer dat bestaat uit vier delen die door middel van een punt van elkaar zijn gescheiden (bijvoorbeeld 63.227.89.66). Elke computer op het internet, van de grootste server tot een laptop die via een mobiele telefoon communiceert, heeft een uniek IP-nummer. Hoewel niet elke computer een domeinnaam heeft, heeft elke computer een IP-adres.

Hieronder volgen enkele ongebruikelijke typen IP-adressen:

- Niet-routeerbare IP-adressen: Deze worden ook 'Privé-IP-ruimte' genoemd. Het betreft IP-adressen die niet op internet kunnen worden gebruikt. Privé-IP-adressen zijn 10.x.x.x, 172.16.x.x - 172.31.x.x en 192.168.x.x.
- Loopback-IP-adressen**:** Loopback-adressen worden gebruikt voor testdoeleinden. Verkeer dat naar deze IP-adressen wordt verstuurd, komt weer terug naar het apparaat dat het pakket heeft gegenereerd. Het verkeer verlaat het apparaat niet en wordt alleen gebruikt voor het testen van de hardware en software. Het loopback-IP-adres is 127.x.x.x.

Null-IP-adres: Dit is een ongeldig adres. Dit adres geeft aan dat het verkeer een blanco IP-adres had. Dit is uiteraard niet normaal en het geeft meestal aan dat de afzender opzettelijk probeert de bron van het verkeer te maskeren. De afzender kan geen antwoord op het verkeer ontvangen, tenzij het pakket wordt ontvangen door een toepassing die de inhoud begrijpt van het pakket, dat specifieke instructies voor die toepassing bevat. Elk adres dat begint met 0 (0.x.x.x) is een null-adres. 0.0.0.0 is bijvoorbeeld een null-IP-adres.

IP-spoofing

De IP-adressen in een IP-pakket vervalsen. Dit wordt toegepast in vele typen aanvallen, inclusief session hijacking (kapen van een sessie). Het wordt ook vaak gebruikt om de e-mailheader van spam te vervalsen, zodat de afzender niet goed kan worden opgespoord.

Knooppunt

Eén computer die met een netwerk is verbonden.

Koptekst

Een koptekst is informatie die in de loop van het bestaan van een bericht aan het kopgedeelte van het bericht wordt toegevoegd. De koptekst bevat instructies waarmee internetsoftware het bericht kan bezorgen, het adres waar antwoorden naartoe moeten worden gestuurd, een uniek identificatienummer voor uw bericht en andere administratieve gegevens. Voorbeelden van koptekstvelden zijn: Aan, van, CC, Datum, Onderwerp, Bericht-ID en Ontvangen.

LAN (Local Area Network)

Een computernetwerk dat een relatief klein gebied omvat. De meeste LAN's zijn beperkt tot één gebouw of een groep gebouwen. Een LAN kan echter over een willekeurige afstand met andere LAN's zijn verbonden via telefoonlijnen en radiogolven. Een systeem van LAN's die op deze manier zijn verbonden, wordt een WAN (Wide Area Network) genoemd. De meeste LAN's verbinden werkstations en pc's doorgaans via gewone hubs of switches met elkaar. Elk knooppunt (individuele computer) in een LAN heeft zijn eigen processor voor de uitvoering van programma's. Een knooppunt heeft echter ook toegang tot gegevens en apparaten (zoals printers) op een willekeurige plaats binnen het LAN. Dit betekent dat vele gebruikers dure apparaten (zoals laserprinters) en gegevens gemeenschappelijk kunnen delen. Gebruikers kunnen het LAN ook gebruiken om met elkaar te communiceren, bijvoorbeeld door e-mails te verzenden of deel te nemen aan een chatsessie.

Locatie voor grondige bewaking

Een map (en alle submappen) op uw computer die door Data Backup worden gecontroleerd op wijzigingen. Als u een locatie voor grondige bewaking instelt, maakt Data Backup back-ups van de bewaakte bestandstypen in die map en de bijbehorende submappen.

locaties voor oppervlakkige bewaking

Een map op uw computer die door Data Backup worden gecontroleerd op wijzigingen. Als u een locatie voor oppervlakkige bewaking instelt, maakt Data Backup back-ups van de bewaakte bestandstypen in die map, maar niet van de bijbehorende submappen.

MAC (Media Access Control of Message Authenticator Code)

Zie MAC-adres voor de eerste betekenis. De tweede betekenis is een code die wordt gebruikt om een bepaald bericht (bijvoorbeeld een RADIUS-bericht) te identificeren. De code is doorgaans een cryptografisch sterk versleutelde inhoud van het bericht, met een unieke waarde om afspelen te voorkomen.

MAC-adres (Media Access Control)

Een adres op laag niveau, dat wordt toegewezen aan het fysieke apparaat dat toegang vraagt tot het netwerk.

Man-in-het-midden-aanval

De aanvaller onderschept berichten bij de uitwisseling van een openbare sleutel en verzendt ze vervolgens opnieuw, waarbij de gevraagde sleutel wordt vervangen door hun eigen openbare sleutel, zodat de twee oorspronkelijke partijen nog altijd direct met elkaar lijken te communiceren. De aanvaller gebruikt een programma dat zich voordoet als server voor de client, en als client voor de server. Mogelijk wordt de aanval slechts gebruikt om toegang te krijgen tot de berichten, maar het is ook mogelijk dat de aanvaller de berichten wijzigt voordat hij ze opnieuw verzendt. De term is afgeleid van het balspel waarbij een aantal spelers een bal rechtstreeks naar elkaar gooien terwijl één speler in het midden de bal probeert te onderscheppen.

MAPI-account

Acroniem voor Messaging Application Programming Interface. De Microsoft-interfacespecificatie waarmee verschillende bericht- en werkgroeptoepassingen (inclusief e-mail, voicemail en fax) via één enkele client kunnen werken, zoals de Exchange-client. Om deze reden wordt MAPI vaak gebruikt in zakelijke omgevingen, in bedrijven die gebruikmaken van Microsoft® Exchange Server. Veel mensen gebruiken Microsoft Outlook echter voor hun persoonlijke internet-e-mail.

Mogelijk ongewenst programma

Mogelijk ongewenste programma's zijn onder andere spyware, adware en andere programma's die zonder uw toestemming uw gegevens verzamelen en verzenden.

MSN-account

Acroniem voor Microsoft Network. Een online service en internetportal. Dit is een op het web gebaseerde account.

netwerk

Wanneer u twee of meer computers met elkaar verbindt, ontstaat er een netwerk.

Netwerkkaart

Een kaart die in een laptopcomputer of een ander apparaat wordt geplaatst om verbinding te maken met het LAN.

netwerkoverzicht

In Network Manager wordt hiermee een grafisch overzicht aangeduid van de beveiligingsstatus van de computers en componenten waaruit uw thuisnetwerk bestaat.

Netwerkstation

Een station of schijf die is verbonden met een server op een netwerk met meerdere gebruikers. Netwerkstations worden soms externe stations genoemd.

Normale tekst

Een willekeurig bericht dat niet is gecodeerd.

Onbetrouwbare toegangspunten

Een toegangspunt waarvoor een bedrijf geen gebruikstoestemming verleent. Het probleem is dat onbetrouwbare toegangspunten vaak niet voldoen aan de voorwaarden van het beveiligingsbeleid voor draadloze LAN's (WLAN's). Een onbetrouwbaar toegangspunt biedt een open, onveilige interface met het bedrijfsnetwerk vanaf een locatie die zich niet binnen het fysiek gecontroleerde gebouw bevindt.

Binnen een goed beveiligd WLAN kunnen onbetrouwbare toegangspunten meer schade aanrichten dan onbetrouwbare gebruikers. Onbevoegde gebruikers die toegang proberen te krijgen tot een WLAN bereiken doorgaans geen belangrijke bedrijfsgegevens als effectieve verificatiemechanismen worden gebruikt. Er kunnen echter grote problemen optreden als een werknemer of hacker verbinding maakt met een onbetrouwbaar toegangspunt. Het onbetrouwbare toegangspunt biedt een willekeurige persoon met een apparaat waarop 802.11 is geactiveerd, toegang tot het bedrijfsnetwerk. Dit betekent dat de afstand tot uiterst belangrijke gegevens heel klein wordt.

online opslagplaats

De locatie op de online server waar uw bewaakte bestanden worden opgeslagen nadat er een back-up van is gemaakt.

ouderlijk toezicht

Instellingen waarmee u inhoudsrestricties kunt configureren, waarmee u de websites en inhoud beperkt die een gebruiker kan bekijken. Ook kunt u tijdslimieten voor internet configureren, waarmee u de periode en tijdsduur kunt opgeven waarin een gebruiker toegang tot internet heeft. Met de opties voor ouderlijk toezicht kunt u ook de toegang tot specifieke websites beperken en toegang verlenen en blokkeren op basis van leeftijdsgroepen en bijbehorende trefwoorden.

Overschrijding van de bufferlimiet

Overschrijdingen van de bufferlimiet doen zich voor als verdachte programma's of processen proberen meer gegevens in een buffer (tijdelijke opslagruimte voor gegevens) op de computer op te slaan dan is toegestaan, waardoor geldige gegevens worden beschadigd of overschreven in nabijgelegen buffers.

Phishing

Wordt uitgesproken als het Engelse 'fishing'. Dit is een zwendellist om waardevolle informatie zoals creditcardnummers, sofi-nummers, gebruikers-id's en wachtwoorden te stelen. Mogelijke slachtoffers ontvangen een officieel ogend e-mailbericht waarin wordt gedaan alsof dit afkomstig is van hun internetaanbieder, bank of een winkel. E-mails kunnen worden verzonden naar mensen op geselecteerde lijsten of op een willekeurige lijst, waarbij wordt verwacht dat een bepaald percentage van de geadresseerden ook daadwerkelijk een account heeft bij de echte organisatie.

poort

Een plaats waar informatie de computer verlaat of binnenkomt. Een conventionele analoge modem is bijvoorbeeld aangesloten op een seriële poort. De poortnummers bij TCP/IP-communicatie zijn virtuele waarden aan de hand waarvan verkeer wordt gesplitst in toepassingsspecifieke gegevensstromen. Poorten worden toegewezen aan standaardprotocollen, zoals SMTP of HTTP, zodat programma's weten op welke poort ze een verbinding moeten proberen. De doelpoort voor TCP-pakketten geeft aan naar welke toepassing of server wordt gezocht.

pop-ups

Kleine vensters die op de voorgrond voor andere vensters worden weergegeven op het beeldscherm van de computer. Pop-upvensters worden vaak gebruikt om advertenties weer te geven in webbrowsers. McAfee blokkeert pop-upvensters die automatisch worden geladen wanneer een webpagina in de browser wordt geladen. Pop-upvensters die worden geladen wanneer u op een koppeling klikt, worden niet geblokkeerd door McAfee.

POP3-account

Acroniem voor Post Office Protocol 3. De meeste particuliere gebruikers hebben een account van dit type. Dit is de huidige versie van de Post Office Protocol-standaard die veel wordt gebruikt in TCP/IP-netwerken. Ook bekend als een standaard-e-mailaccount.

PPPoE

Point-to-Point Protocol Over Ethernet. PPPoE wordt door vele DSL-aanbieders gebruikt. Het ondersteunt de protocollagen en verificatie die veel worden gebruikt in PPP en maakt point-to-point-verbindingen mogelijk binnen de Ethernet-architectuur (die normaal gesproken multipoint is).

Protocol

Een indeling voor de gegevenstransmissie tussen twee apparaten, waarover wordt onderhandeld voordat de verbinding tot stand wordt gebracht. Vanuit het oogpunt van gebruikers is het enige belangrijke aspect van protocollen, dat hun computer of apparaat de juiste protocollen moet ondersteunen als ze willen communiceren met andere computers. Het protocol kan hardware- of softwarematig zijn geïmplementeerd.

proxy

Een computer (of de software die erop wordt uitgevoerd) die fungeert als een barrière tussen een netwerk en het internet door slechts één netwerkadres door te geven aan externe sites. Doordat de proxy alle interne computers vertegenwoordigt, worden de netwerkidentiteiten beveiligd, terwijl er wel internettoegang wordt verschaft. Zie ook proxyserver.

proxyserver

Een onderdeel van een firewall waarmee het internetverkeer van en naar een LAN (Local Area Network) wordt beheerd. Een proxyserver kan de prestaties verbeteren, doordat deze veelgevraagde gegevens levert (zoals een populaire webpagina) en aanvragen kan filteren en negeren die door de eigenaar als ongewenst worden beschouwd, zoals aanvragen voor ongeoorloofde toegang tot bestanden.

publiceren

Een back-upbestand openbaar beschikbaar maken op internet.

Quarantaine

Wanneer verdachte bestanden worden gedetecteerd, worden deze in quarantaine geplaatst. Vervolgens kunt u zelf de noodzakelijke actie ondernemen.

RADIUS (Remote Access Dial-In User Service)

Een protocol dat gebruikersverificatie biedt, doorgaans bij externe toegang. Het protocol is oorspronkelijk gedefinieerd voor gebruik bij servers voor inbeltoegang, maar wordt nu voor een heel gamma van verificatieomgevingen gebruikt, inclusief 802.1x-verificatie van het gedeelde geheim van WLAN-gebruikers.

Real-time scannen

Bestanden worden gescand op virussen en andere activiteiten zodra ze door uzelf of de computer worden geopend.

Roaming

De mogelijkheid om van het ene toegangspunt naar een ander te gaan zonder onderbreking van de service of verbreking van de verbinding.

Router

Een netwerkapparaat dat pakketten doorstuurt van het ene netwerk naar een ander. Op basis van interne routeringstabellen lezen routers elk inkomend pakket en beslissen ze hoe het wordt doorgestuurd. De routerinterface waarnaar uitgaande pakketten worden verzonden, kan worden bepaald door een willekeurige combinatie van bron- en doeladres, evenals de huidige verkeersomstandigheden zoals belasting, kosten en kwaliteit van de lijn. Wordt soms ook toegangspunt genoemd.

Script

Scripts kunnen bestanden maken, kopiëren of verwijderen. Ze kunnen tevens het Windows-register openen.

server

Een computer of software die specifieke services verleent aan software die op andere computers wordt uitgevoerd. De 'mailserver' bij uw internetprovider is software waarmee alle inkomende en uitgaande mail wordt verwerkt voor alle bij de internetprovider aangesloten gebruikers. Een server op een LAN is hardware die het hoofdknooppunt in het netwerk vormt. Hierop kan ook software worden uitgevoerd waarmee bepaalde services, gegevens of andere voorzieningen worden geleverd aan alle clientcomputers die ermee zijn verbonden.

Sleutel

Een reeks letters en/of cijfers voor de verificatie van de communicatie tussen twee apparaten. Beide apparaten moeten over de sleutel beschikken. Zie ook WEP, WPA, WPA2, WPA-PSK en WPA2- PSK.

SMTP-server

Acroniem voor Simple Mail Transfer Protocol. Een TCP/IP-protocol voor het verzenden van berichten van de ene computer naar de andere in een netwerk. Dit protocol wordt op internet gebruikt voor het routeren van e-mail.

snelle archivering

Alleen de bewaakte bestanden archiveren die zijn gewijzigd sinds de vorige volledige of snelle archivering.

SSID (Service Set Identifier)

Netwerknaam voor de apparaten op een subsysteem van een draadloos LAN. Dit is een normale tekenreeks van 32 tekens die wordt toegevoegd aan de header van elk WLAN-pakket. De SSID zorgt voor unieke identificatie van elk WLAN, zodat alle gebruikers van een netwerk dezelfde SSID moeten opgeven om toegang te krijgen tot een bepaald toegangspunt. Het gebruik van SSID's blokkeert de toegang van alle clientapparaten die niet beschikken over de SSID. Toegangspunten verzenden echter standaard hun SSID via hun beacon. Zelfs als het verzenden van SSID's is uitgeschakeld, kan een hacker de SSID detecteren via sniffing.

SSL (Secure Sockets Layer)

Een protocol dat door Netscape is ontwikkeld voor het verzenden van privé-documenten via internet. SSL werkt met een openbare sleutel voor het coderen van gegevens die via de SSL-verbinding worden overgebracht. Zowel Netscape Navigator als Internet Explorer gebruiken en ondersteunen SSL, en vele websites gebruiken het protocol bij het opvragen van vertrouwelijke gebruikersgegevens, zoals creditcardnummers. In overeenstemming met het protocol beginnen URL's waarvoor een SSL-verbinding is vereist, met https: in plaats van http:

Standaard-e-mailaccount

De meeste particuliere gebruikers hebben een account van dit type. Zie ook POP3-account.

synchroniseren

Verschillen oplossen tussen de back-up bestanden en de bestanden op uw lokale computer. U synchroniseert de bestanden wanneer de versie van het bestand in de online opslagplaats nieuwer is dan de versie van het bestand die zich op de andere computers bevindt. Door synchroniseren wordt de kopie van het bestand op uw computers bijgewerkt met de versie van het bestand in de online opslagplaats.

SystemGuard

SystemGuards detecteren onbevoegde wijzigingen op uw computer en waarschuwen u wanneer deze zich voordoen.

terugzetten

Een kopie van het bestand ophalen uit de online opslagplaats of uit een archief.

TKIP (Temporal Key Integrity Protocol)

Een snelle reparatiemethode om de kenmerkende zwakke plekken van WEP-beveiliging te versterken, met name bij het opnieuw gebruiken van coderingssleutels. TKIP wijzigt de tijdelijke sleutels elke 10.000 pakketten en biedt op die manier een dynamische distributiemethode die de beveiliging van het netwerk aanzienlijk verbetert. Het TKIP-(beveiligings)proces begint met een tijdelijke 128-bits sleutel die wordt gedeeld tussen clients en toegangspunten. TKIP combineert de tijdelijke sleutel met het MAC-adres (van de clientcomputer) en voegt vervolgens een relatief grote 16-byte initialisatievector toe om de sleutel voor het coderen van de gegevens te genereren. Deze procedure garandeert dat elk station andere sleutelstromen gebruikt om de gegevens te coderen. TKIP gebruikt RC4 voor het uitvoeren van de codering. RC4 wordt ook gebruikt door WEP.

Toegangspunt

Een netwerkapparaat dat door 802.11-clients wordt gebruikt om verbinding te maken met een lokaal netwerk (LAN). Toegangspunten breiden het fysieke bereik van de service voor een draadloze gebruiker uit. Wordt soms ook draadloze router genoemd.

trefwoord

Een woord dat u kunt toewijzen aan een back-upbestand om duidelijk te maken dat het bestand hoort bij de andere bestanden met hetzelfde trefwoord. Door het toewijzen van trefwoorden wordt het eenvoudiger om bestanden te vinden die u op internet hebt gepubliceerd.

Trojaans paard

Trojaanse paarden zijn programma's die zich voordoen als bonafide toepassingen. Trojaanse paarden zijn geen virussen omdat ze zichzelf niet vermenigvuldigen, maar ze kunnen even schadelijk zijn.

URL

Uniform Resource Locator. Dit is de standaardindeling voor internetadressen.

Verificatie

Het proces waarbij een persoon wordt geïdentificeerd, doorgaans op basis van een gebruikersnaam en een wachtwoord. Verificatie controleert of de persoon is wie hij/zij zegt te zijn, maar oordeelt niet over de toegangsrechten van de persoon.

volledige archivering

Hiermee archiveert u een volledige gegevensset die is gebaseerd op de bewaakte bestandstypen en locaties die u hebt ingesteld.

VPN (Virtual Private Network)

Een netwerk waarbij het openbare kabelnetwerk wordt gebruikt om knooppunten met elkaar te verbinden. Er zijn bijvoorbeeld een aantal systemen waarmee u netwerken kunt creëren door internet te gebruiken als medium voor gegevenstransport. Deze systemen gebruiken codering en andere beveiligingsmechanismen om te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot het netwerk en de gegevens niet kunnen worden onderschept.

wachtwoord

Een code (meestal alfanumeriek) waarmee u toegang krijgt tot uw computer, een bepaald programma of een website.

Wachtwoordkluis

Een veilig opslaggebied voor uw persoonlijke wachtwoorden. Hierin kunt u wachtwoorden opslaan met de zekerheid dat geen enkele andere gebruiker (zelfs geen McAfee- of netwerkbeheerder) ze kan bekijken.

Wardriver

Indringers die gewapend met laptopcomputers, speciale software en geïmproviseerde hardware door steden, voorsteden en bedrijvencentra rijden om verkeer via draadloze LAN's te onderscheppen.

Webbugs

Kleine grafische bestanden die kunnen worden ingesloten in uw HTML-pagina's en waarmee een onbevoegde bron cookies kan instellen op uw computer. Deze cookies worden vervolgens gebruikt om informatie naar de onbevoegde bronnen over te brengen. Webbugs worden ook wel webbeacons, pixeltags, doorzichtige GIF's of onzichtbare GIF's genoemd.

WEP (Wired Equivalent Privacy)

Een coderings- en verificatieprotocol dat is gedefinieerd in de 802.11-standaard. De eerste versies waren gebaseerd op RC4-codeertekst en vertoonden belangrijke zwakheden. WEP probeert de beveiliging te verbeteren door gegevens via radiogolven te coderen, zodat ze veilig zijn tijdens het transport van het ene eindpunt naar het andere. WEP blijkt echter niet zo veilig als men oorspronkelijk dacht.

Wi-Fi (Wireless Fidelity)

Wordt als algemene term gebruikt om te verwijzen naar een willekeurig type 802.11-netwerk, ongeacht of het 802.11b, 802.11a, dubbele-band, enzovoort is. De term wordt gebruikt door de Wi-Fi Alliance.

Wi-Fi Alliance

Een organisatie die bestaat uit grote fabrikanten van draadloze apparatuur en software, met als doel (1) alle op 802.11 gebaseerde producten te certificeren als compatibel met elkaar, en (2) de term Wi-Fi op alle markten te promoten als wereldwijde merknaam voor willekeurige, op 802.11 gebaseerde, draadloze LAN-producten. De organisatie fungeert als consortium, testlaboratorium en coördinatiecentrum voor leveranciers die compatibiliteit en de groei van de industrie willen bevorderen.

Weliswaar worden alle 802.11a/b/g-producten Wi-Fi genoemd, maar alleen producten die de tests van de Wi-Fi Alliance hebben doorstaan, mogen worden voorzien van het label Wi-Fi Certified (een gedeponeerd handelsmerk). Voor producten die de tests hebben doorstaan, moet een identificatiezegel op de verpakking worden aangebracht, met daarop de vermelding Wi-Fi Certified en de gebruikte radiofrequentieband. De groep was vroeger bekend onder de naam Wireless Ethernet Compatibility Alliance (WECA) maar veranderde zijn naam in oktober 2002 om duidelijker aan te geven welk merk (Wi-Fi) de groep wil laten accepteren als standaard.

Wi-Fi Certified

Alle producten die door de Wi-Fi Alliance zijn getest en zijn goedgekeurd als Wi-Fi Certified (een geregistreerd handelsmerk), worden gecertificeerd als compatibel met elkaar, zelfs als ze door verschillende fabrikanten zijn geproduceerd. Een gebruiker met een Wi-Fi Certified-product kan een toegangspunt van een willekeurig merk gebruiken in combinatie met clienthardware van een willekeurig ander merk, op voorwaarde dat ook deze hardware is gecertificeerd. Wi-Fi-producten die dezelfde radiofrequentie gebruiken (bijvoorbeeld 2,4 GHz voor 802.11b of 11g, 5 GHz voor 802.11a), werken echter doorgaans met willekeurige andere Wi-Fi-producten, zelfs als deze niet het label Wi-Fi Certified hebben.

Witte lijst

Een lijst met websites die mogen worden bezocht omdat ze niet als frauduleus worden beschouwd.

WLAN (Wireless Local Area Network)

Zie ook LAN. Een lokaal netwerk dat voor de verbindingen gebruikmaakt van een draadloos medium. Een WLAN gebruikt hoogfrequente radiogolven in plaats van kabels voor de communicatie tussen knooppunten.

Woordenboekaanval

Bij deze aanvallen wordt een hele reeks woorden uit een lijst ingevoerd om te proberen iemands wachtwoord te kraken. De aanvallers voeren niet handmatig alle combinaties in maar hebben programma's die iemands wachtwoord automatisch proberen te kraken.

Worm

Een worm is een zichzelf vermenigvuldigend virus dat zich in het actieve geheugen nestelt en via e-mailberichten kopieën van zichzelf kan verspreiden. Wormen vermenigvuldigen zich en gebruiken systeembronnen, waardoor de computer langzamer wordt of taken worden gestopt.

WPA (Wi-Fi Protected Access)

Een specificatiestandaard die de gegevensbeveiliging en toegangscontrole voor bestaande en toekomstige draadloze LAN-systemen aanzienlijk verbetert. WPA, dat is ontworpen om als software-upgrade te worden geïnstalleerd op bestaande hardware, is afgeleid van en compatibel met de IEEE-standaard 802.11i. Wanneer WPA correct is geïnstalleerd, biedt het gebruikers van draadloze LAN's een hoog niveau van garantie dat hun gegevens veilig zijn en dat alleen geautoriseerde gebruikers toegang hebben tot het netwerk.

WPA-PSK

Een speciale WPA-modus die is ontworpen voor particuliere gebruikers die geen sterke beveiliging van bedrijfsniveau nodig hebben en geen toegang hebben tot verificatieservers. In deze modus moet de particuliere gebruiker handmatig het initiële wachtwoord invoeren om WPA (Wi-Fi Protected Access) in de modus PSK (Pre-Shared Key, oftewel vooraf-gedeelde sleutel) te activeren. Vervolgens moet de wachtzin op elke draadloze computer en elk draadloos toegangspunt regelmatig worden gewijzigd. Zie ook WPA2-PSK en TKIP.

WPA2

Zie ook WPA. WPA2 is een update van de WPA-beveiligingsstandaard en is gebaseerd op de 802.11i IEEE-standaard.

WPA2-PSK

Zie ook WPA-PSK en WPA2. WPA2-PSK is vergelijkbaar met WPA-PSK en is gebaseerd op de WPA2-standaard. Een veelvoorkomende eigenschap van WPA2-PSK is dat apparaten vaak meerdere coderingsmodi (bijvoorbeeld AES, TKIP) tegelijkertijd ondersteunen, terwijl oudere apparaten doorgaans slechts één enkele coderingsmodus tegelijk ondersteunden (d.w.z. dat alle clients dezelfde coderingsmodus zouden moeten gebruiken).

Zwarte lijst

Een lijst met websites die als schadelijk worden beschouwd. Een website kan op een zwarte lijst worden geplaatst omdat deze een frauduleuze bewerking uitvoert of misbruik maakt van kwetsbaarheden in een browser om mogelijk ongewenste programma's naar de gebruiker te sturen.

Informatie over McAfee

McAfee, Inc. is gevestigd in Santa Clara, Californië en is de wereldwijde leider op het gebied van inbraakpreventie en beveiligingsrisicobeheer. McAfee levert proactieve, bewezen oplossingen en diensten waarmee systemen en netwerken over de hele wereld worden beveiligd. Dankzij de ongeëvenaarde expertise op het gebied van beveiliging en het continue streven naar innovatie geeft McAfee thuisgebruikers, bedrijven, de publieke sector en serviceproviders de mogelijkheid om aanvallen te weren, uitval te voorkomen en doorlopend de beveiliging te controleren en te verbeteren.

Copyright

Index

D

E

F

G

H

I

K

L

M

N

O

P

W

Z