

Onderhoud en beveiliging

Wanneer onderhoud datgene is dat nodig is om een werkend systeem optimaal te laten werken, dan is beveiling daar een onderdeel van.

Onderhoud

Waar?

Onderhoud en beveiliging begint eigenlijk al bij de inrichting van de PC. Waarbij we ons af moeten vragen of we de harde schijf in meerdere partities moeten verdelen of niet en of we software zullen installeren in de aangeboden map C:\Program Files of dat we daar liever iets anders voor bedenken indien die mogelijkheid wordt geboden?

Een voordeel van een indeling met meerdere schijven of partities kan zijn dat het praktischer is een image (zie onder imaging) van alleen maar een systeempartitie te maken i.p.v. de gehele harde schijf. Dit omdat imagers meestal ook per partitie kunnen werken. Een tweede reden zou kunnen zijn dat de image die van een (systeem)partitie gemaakt is bij voorkeur niet op diezelfde partitie bewaard moet worden. Is het de partitie die faalt, dan kan een image snel vanaf een andere partitie terug worden geschreven. Harde schijven zijn veelal sneller dan externe bronnen als netwerken of cd-roms of dvds. Is het de harde schijf die instort dan zijn we ondanks de meerdere partities op een enkele hard disk toch zuur.

Uit bovenstaande kan een aanbeveling worden afgeleid voor het bewaren van een image:

- Meerdere harde schijven
- Meerdere partities
- Externe harde schijf/schijven
    - Netwerk

Maar als we dan toch over meerdere partities of liever ook nog harde schijven beschikken, dan kunnen we die ook nuttig gebruiken door bijvoorbeeld een systeemdeel, een programmadeel en een datadeel in te richten.

Houd bij het toedelen van de ruimte voor het systeemdeel rekening met alle updates, service packs en beveiligingspatches die Microsoft met grote regelmaat uitbrengt. Kijk niet raar op wanneer je na enige tijd een groei van het systeemdeel waarneemt vanaf de start met pakweg 1 GB tot bijna 10 GB. De snelle groei van de systeempartitie is mede het gevolg van het feit dat we weliswaar gemakkelijk de map Mijn Documenten naar een ander deel kunnen verleggen (data), maar dat het een stuk lastiger is om de hele struktuur van C:\Documents and Settings\<gebruikersnaam>\Onderliggende_mappen te verplaatsen. Des te meer gebruikers de pc heeft des te sneller zal de systeempartitie daarmee groeien.

Begeeft Windows het (crash), dan hoeft in het gunstigste geval alleen het systeemdeel te worden teruggezet.

Wat: Programma's

Helaas maakt Windows het niet echt gemakkelijk om alle programma's op een apart deel te installeren en dus een strikte scheiding tussen systeem en andere programmatuur te maken. Dat zullen we dus zelf moeten regelen.

Er zijn echter ook nog steeds programma's die geen keus laten waar iets geïnstalleerd kan worden. Daarmee komt het dan bijna altijd op C:\Program Files\... terecht.

In het andere geval hoeft het nog niet meteen duidelijk te zijn dat er een keuze is. In die gevallen moet dan gekozen worden voor een optie die vaak als 'geavanceerd', 'handmatig' of 'custom' wordt aangeduid. Pas dan kunnen we opgeven waar precies we willen dat het terecht komt.

Wat: Data

Het verdient absoluut aanbeveling alle gegevens die een gebruiker produceert op een eigen schijf te bewaren. Opnieuw maakt Windows het niet gemakkelijk omdat het allerlei specifieke gebruikersinstellingen in de map C:\Documents and Settings\<gebruikersnaam>\ bewaart.

Daarnaast is er ook nog een map toegankelijk voor alle gebruikers – gedeelde map - die slecht te verplaatsen is en dus op het systeemdeel blijft staan. Zelfs TweakUI.exe, een hulpprogramma uitgegeven door Microsoft, kan dit niet. Wie echter even zoekt vindt op http://windowsxp.mvps.org/ een tooltje genaamd 'folder redirector' dat dat wel kan.

Bij data op een aparte schijf bewaard kunnen we die gehele schijf ook uitnemen en zo in een nieuw systeem hangen. Maar los van deze misschien extreme vorm van onderhoud is het nu eenmaal overzichtelijker om bijvoorbeeld een backup te maken van een apart exclusief deel dan van een map op de systeempartitie. In geval windows crasht en de data op de systeempartitie stond zijn bij een herinstallatie ook meteen **alle** gebruikersgegevens foetsie. Tegenwoordig zijn dat dan vaak ook de muziek- en videobestanden.

Wie?

Onder andere vanuit de ervaringen opgedaan met de zakelijke serversoftware van Windows NT heeft het idee postgevat dat het helemaal niet handig is wanneer iedere gebruiker van een systeem altijd maar alles mag.

In de recente versies van Windows is dan ook altijd een gebruiker met de naam Administrator die in principe wel alles mag op een systeem.

Minder slim is dat andere gebruikers die tijdens de installatie (kunnen) worden aangemaakt nog steeds standaard ook **alle rechten** krijgen om van alles en nog wat te doen, i.c. beheerdersrechten hebben.

Dit zal volgens Microsoft in de komende Windows Vista niet langer het geval zijn. Gelukkig hebben we in de afgelopen jaren ook verantwoordelijke leveranciers gezien die aangepaste installaties leverden waarbij gebruikers die aangemaakt werden niet standaard alle rechten kregen, maar gebruikers met beperkte rechten aanmaakten.

Niet alleen is dit van belang vanuit het gezichtspunt van onderhoud maar nog veel meer vanuit beveiligingsoogpunt. Programma's werken namelijk standaard met de rechten van de gebruiker die ze heeft gestart. Mocht een of ander kwalijk programma dus weten te starten dan doet het dat met de rechten van die specifieke gebruiker.
Nu mag een gebruiker met beperkte rechten geen programma's installeren of de windows systeemmappen beheren. Een virus is een programma. Programma's die starten met de rechten van een beperkte gebruiker zullen dan niet in staat zijn zich te nestelen in het systeem!
Een belangrijk aspect van het bovenstaande is dat iedere gebruiker uit het oogpunt van veiligheid eigenlijk een wachtwoord zou moeten gebruiken. Een deugdelijk wachtwoord bestaat uit **minimaal** 6 karakters en bevat bij voorkeur ook nog HoofdLetters en c1jfer5.

Wachtwoorden

Een veelvoorkomend probleem is dat een gebruiker zijn wachtwoord vergeet.
Gelukkig kan de beheerder, maar ook de gebruiker met beperkte rechten daar zelf iets tegen doen.
Het is mogelijk een zogenaamde hersteldiskette voor wachtwoorden aan te maken. Daarvoor moet de gebruiker naar het configuratiescherm gaan en daar de ingang gebruikersaccounts te volgen

Jammer dat het alleen op floppies kan.

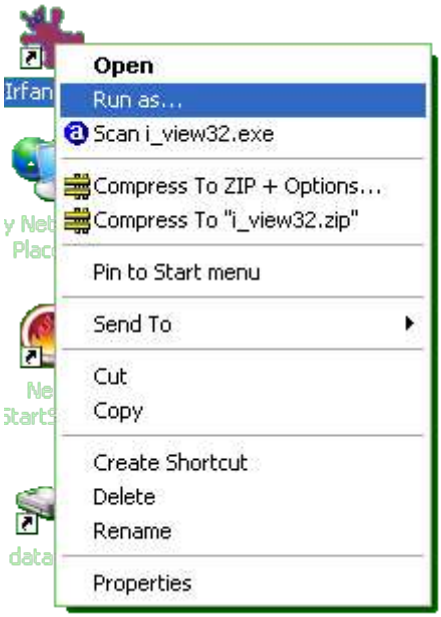
Werken met beperkte rechten

Windows XP wordt helaas door de meeste bedrijven afgeleverd met instellingen waar iedere gebruiker alles mag op het systeem. Dit is uitermate

onveilig en ook niet gewenst. Bovendien kan het gemakkelijk anders geregeld worden.
Hiervoor is het noodzakelijk dat de zogenaamde snelle gebruikerswisseling wordt uitgeschakeld. Daarnaast moet iedere gebruiker zich netjes met gebruikersnaam en wachtwoord aanmelden.
Alleen wanneer er nieuwe programma's geïnstalleerd moeten worden of wanneer er belangrijke wijzigingen in het systeem gemaakt moeten worden is het noodzakelijk om u aan te melden als beheerder van het systeem, m.a.w. met administrator rechten.
Met andere woorden:

- Er is dus een gebruiker met alle beheersrechten
- en er is/zijn een of meer gebruikers met beperkte rechten met hun eigen wachtwoord(en).

- De bedoeling van de verschillende gebruikers met hun al dan niet beperkte rechten is dat u en andere gebruikers zo veilig mogelijk kunnen werken.
  Soms levert dat een beperking op die gemakkelijk kan worden overwonnen door tijdelijk bijv. met beheerderrechten in te loggen. Die gebruiker heeft namelijk wel alle rechten en kan dus ook nieuwe programma's of drivers installeren!



- Een andere methode die tijdelijk meer rechten verschaft aan de gebruiker is de toepassing met de **rechter**muisknop aan te klikken en te kiezen voor Uitvoeren als.../Run as...

In het vervolgschermpje kiest u dan onderaan (waar nu Administrator staat) voor de gebruiker en geeft het wachtwoord voor die gebruiker.

Wanneer een programma per se beheerderrechten nodig heeft om zijn werk goed te kunnen doen en de gebruiker met beperkte rechten dat programma wil uitvoeren kan het programma standaard met beheerderrechten worden gestart. Er verschijnt dan een zogenaamde box met commandoprompt

waarin alleen nog het wachtwoord moet worden getypt dat hoort bij die gebruiker met beheerderrechten.
Een voorbeeld is het starten van het programma HitmanPro.

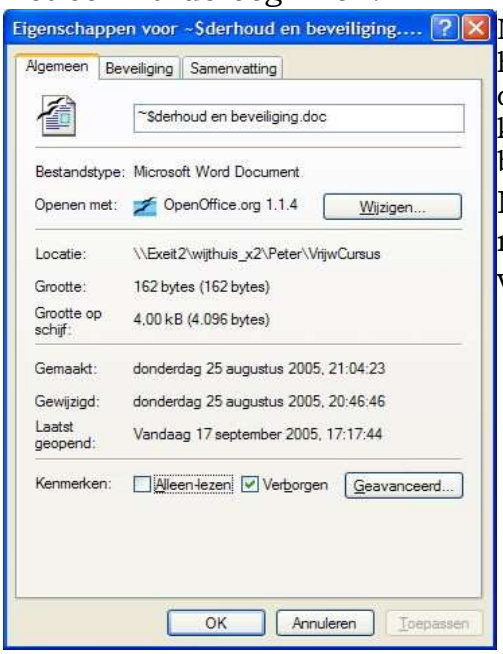
Het wachtwoord dat u hier nu moet typen ziet u niet!

Samenvattend:

Wanneer u al tevoren weet dat u nieuwe programma's moet installeren log dan in als een gebruiker met beheerderrechten.
Wanneer u als gebruiker met beperkte rechten aan het werk bent en tijdelijk meer rechten nodig hebt, klik dan met de rechtermuisknop en kies voor Uitvoeren als…
Wanneer een programma altijd beheerderrechten nodig heeft en gestart moet worden onder het account van een gebruiker met beperkte rechten kies dan voor de optie om een snelkoppeling te maken met andere rechten. Zie hiervoor de snelkoppeling van HitmanPro.

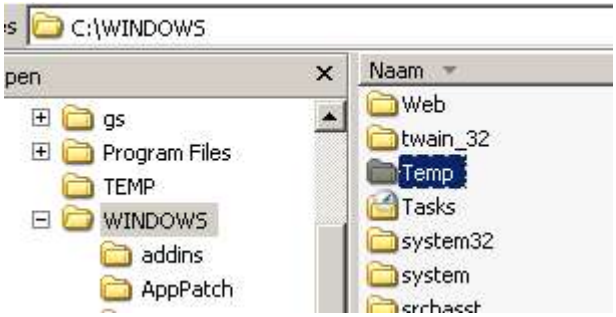
Opruimen

Onderhoud kan zo simpel en effectief zijn als het verwijderen van overbodige of oude bestanden. Daaronder vallen in ieder geval alle bestanden die in Windows de extensie .tmp hebben of beginnen met een tilde (~dit bestand.tmp). Een zoekaktie naar deze bestanden levert in het algemeen tientallen bestanden op die klakkeloos gewist kunnen worden. De Microsoft tekstverwerker Word laat regelmatig tijdelijke bestanden staan die met een ~tilde beginnen.



Maar wie tijdens het tekstverwerken probeert om het tijdelijke bestand dat hoort bij het document dat bewerkt wordt te wissen komt van een koude kermis thuis. Tijdens het werken zijn tijdelijke bestanden soms gewoon nodig.
Met andere woorden: dit soort onderhoud moet u niet doen terwijl u met uw 'normale' werk bezig bent.

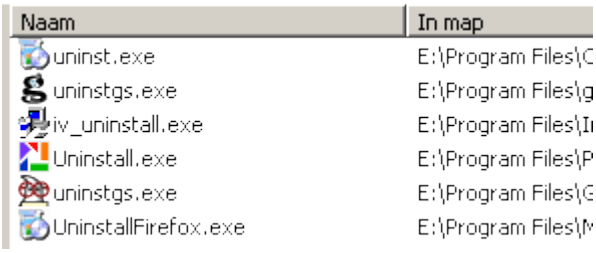
Tijdelijke mappen en bestanden



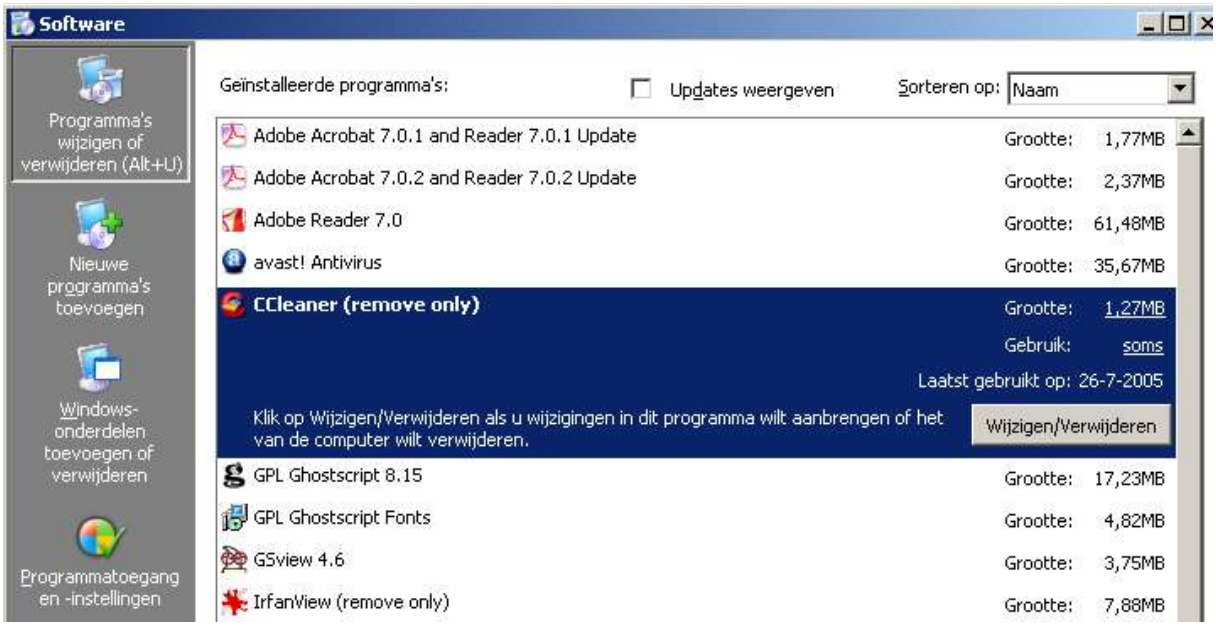
Windows kent een aantal mappen die gebruikt worden voor tijdelijke opslag.
Deze mappen genaamd \temp of \tmp kunnen zich zowel in de root van een partitie bevinden of binnen de map waarin Windows geïnstalleerd is.
In principe kan alles dat zich in die mappen bevindt gewist worden.
Een andere map voor tijdelijke bestanden is de map voor Tijdelijke Internetbestanden (Temporary Internet Files) die zich in de persoonlijke map Mijn Documenten bevindt – meestal in C:\Documents and Settings\<gebruikersnaam>\Local Settings\.

Software

Ook het verwijderen of deïnstalleren van overbodige software is onderhoud. Het kan helemaal geen kwaad om regelmatig na te denken of u nog steeds dat programma gebruikt dat u enige tijd geleden geïnstalleerd hebt.
Maar dat wil niet zeggen dat u nu de programmabestanden meteen moet gaan wissen.
Installatie van programma's brengt vaak met zich mee dat er in het register iets wordt geschreven. Klakkeloos wissen van programmabestanden laat die registersleutels gewoon staan en dus verkeert windows dan nog steeds in de veronderstelling dat dat programma nog ergens bestaat. Dit kan er bijvoorbeeld toe leiden dat u een waarschuwing krijgt dat een bestand niet gevonden kan worden.
De aangewezen weg om een programma te verwijderen is eerst eens een blik te werpen in de programmamap om te zien of er misschien een bestand is dat unwise.exe, uninst.exe of zoiets heet. Zie de voorbeelden hieronder.



Daarna is het zaak om in Windows naar het Configuratiescherm te gaan en te kiezen voor de categorie Software.
Komt de te verwijderen software in deze lijst voor dan kan gekozen worden voor Wijzigen/Verwijderen.



Configuratiescherm - Software

Komt het programma niet in de lijst voor dan staat ons niets anders open dan het eerder gevonden deïnstallatieprogramma (uninstaller) te gebruiken voor verwijdering.
Het kan voorkomen dat na het deïnstalleren de deïnstallatietoepassing met een dialoogvenster eindigt waarin het mogelijk is gedetailleerd te zien wat er gebeurd is. Het is uitermate zinnig de tijd en moeite te nemen dit even te bekijken omdat vaak blijkt dat het verwijderingsprogramma niet in staat is geweest hetregister naar behoren aan te passen. De achtergebleven ingangen in het register kunnen dan alsnog met de hand worden verwijderd. Het best gaat dat met Regedit dat u via Start→Uitvoeren in het invoervak in kunt geven om het register Editor te starten door *regedit* in te typen en een enter te geven.

NOTA BENE: Het aanpassen van het register is een gevaarlijke en gevoelige zaak. Nog steeds neemt Microsoft geen verantwoordelijkheid voor het niet functioneren van het een of ander wanneer er in het register gerommeld is. Dit ondanks het feit dat Microsoft regelmatig zelf adviseert om iets in het register aan te passen!

Het zijn meestal niet de beste programma's die zich alleen maar laten verwijderen door de bijbehorende map te wissen. Men zou de afwezigheid van een duidelijke deïnstallateur zelfs kunnen zien als een aanwijzing voor de kwaliteit van een programma.
Aan de andere kant zijn er uitermate nuttige programma's als HijackThisexe of de tooltjes van www.sysinternals.com die bijvoorbeeld alleen maar uit een enkel uitvoerbaar programma (*.exe) bestaan. Hier volstaat wissen van die enkele exe-file en eventueel de map waarin het bestand zich bevond.

Registry - register

De 'registry' of het register van windows is een speciale database waarin, van alles en nog wat dat voor het functioneren van het systeem van belang is, wordt opgeslagen en bijgehouden. Zonder een deugdelijke registry geen goed functionerend systeem! Het register bestond voorheen uit twee bestanden genaamd *user.dat* en *system.dat*. Onder windows XP trof ik per gebruiker alleen een *NTUSER.dat* aan….

Het register is volgens Microsoft Nederland (van hun website geplukt):

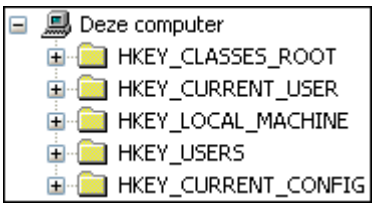
"**Het Windows Register bevat allerlei gegevens over instellingen van Windows, de hardware in uw computer en de softwareprogramma's die u gebruikt. Met behulp van de ingebouwde Register-editor kan men deze instellingen wijzigen of aanvullen en zo de werking van Windows XP beïnvloeden. Ook zijn er hulpprogramma's om deze (vaak verborgen) speciale instellingen te bereiken. In dit artikel leest u hoe dat allemaal in zijn werk gaat.**"

http://www.microsoft.com/netherlands/ondernemers/techniek_techniek/windows_register_aanpassen.aspx

"Het register is opgebouwd volgens een hiërarchische boomstructuur. Het hoogste niveau bestaat uit vijf ingangen:

1. HKEY_CLASSES_ROOT
2. HKEY_CURRENT_USER
3. HKEY_LOCAL_MACHINE
4. HKEY_USERS
5. HKEY_CURRENT_CONFIG

Onder elke hoofdingang bevinden zich diverse *sleutels*, die op hun beurt ook weer *subsleutels* kunnen bevatten. Een subsleutel kan waarde-ingangen bevatten. Deze bestaan uit een naam, een type en de uiteindelijke waarde. De applicaties en Windows zelf gebruiken deze waarden onder meer om gebruikers- en programma-instellingen te bewaren en uit te lezen."



Optimalistaties

Er is al heel wat afgeschreven over optimalisaties van Windows. Heeft het zin bepaalde diensten/services uit te schakelen? Kan het geheugengebruik nog verder geoptimaliseerd? Welnu, het Duitse vakblad C'T heeft er in augustus 2005 aandacht aan besteed.

De resultaten zijn op een bepaalde manier wel schokkend te noemen. Het advies is namelijk alles gewoon te laten zoals de firma Microsoft het bedacht heeft.

Wel heeft het zin zo min mogelijk toepassingen te draaien. Wat je niet nodig hebt hoef je niet te gebruiken. Kijk daarom eens kritisch naar de lijst met aktieve toepassingen. En daarmee moeten we ook een blik werpen op alles wat er in het systeemvak, links van de tijd/datum in de taakbalk, allemaal al aktief is. Kan dat niet wat minder? Zie hiervoor verderop onder het kopje Updates.

Een andere overweging zou kunnen zijn om met verschillende hardware profielen te werken. Wanneer niet altijd alle hardware/apparaten ook gebruikt wordt, zoals digitale camera's, infrarood- of Bluetoothverbindingen of eenZipdisk kun je overwegen om verschillende hardwareprofielen te gebruiken. Een kale voor wat je meestal gebruikt en een luxe voor als je die andere toepassing(en) wilt gebruiken. Hardwareprofielen vind u onder Configuratiescherm→(Prestaties & onderhoud)→Systeem→tabblad Hardware, onderaan Hardwareprofielen. Is een en ander uitgegrijsd, dan hebt u niet voldoende rechten om hardwareprofielen te maken/wijzigen. Log dan aan onder een account met beheerdersrechten.

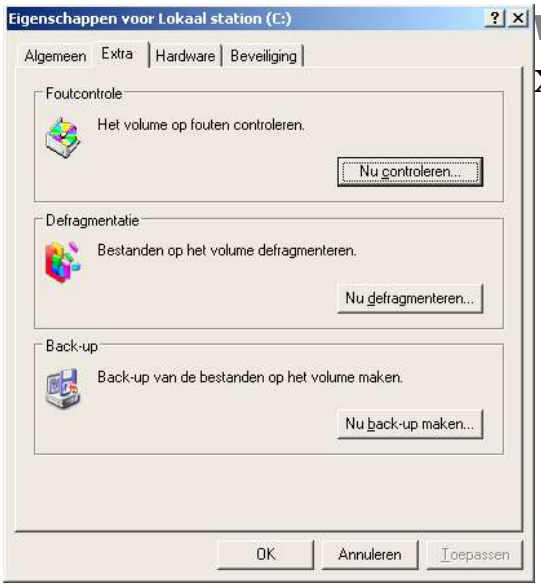
U kunt instellen welk hardwareprofiel als standaard moet worden gebruikt en of die automatisch na zoveel seconden moet starten.

Het handigst is een bestaand profiel te kopiëren, de opstartinstelling aan te passen, windows af te sluiten en dan de keuze voor het hardwareprofiel te maken. Onder dat hardware profiel schakelt u dan onder Systeem→apparaatbeheer alles uit dat niet nodig is of aan dat wel nodig is.

Zo kan voor ieder apparaat bepaald worden of de benodigde drivers etc. wel in het geheugen moeten zijn. Zo kunt u dus ook de toegang tot de diskette, USB-apparaten, netwerkkaart etc. verhinderen. Regelmatig wordt achteraf besloten de onboard video-, geluids- of netwerkkaart te vervangen door iets beters. De oude drivers hoeven dan niet meer geladen te worden en kunnen langs deze weg uitgeschakeld worden.

Updates

Er zijn talrijke nuttige programma's die aanbieden om op Internet te kijken of er niet net een nieuwe versie is verschenen die nog makkelijker of beter is. Die programma's vallen je niet lastig met meldingen dat ze nu even het web opgaan. Ze doen het gewoon. Daarnaast hebben deze gemaksopties nog een ander nadeel. Ze laten een dienst of proces lopen in ons belangrijke werkgeheugen en bezorgen zo de processor ook nog eens werk. Bovendien is nieuwer lang niet altijd beter. De meeste systeembeheerders werken volgens het principe dat je aan een winnend team niet moet sleutelen. Dat houd je zoals het is.

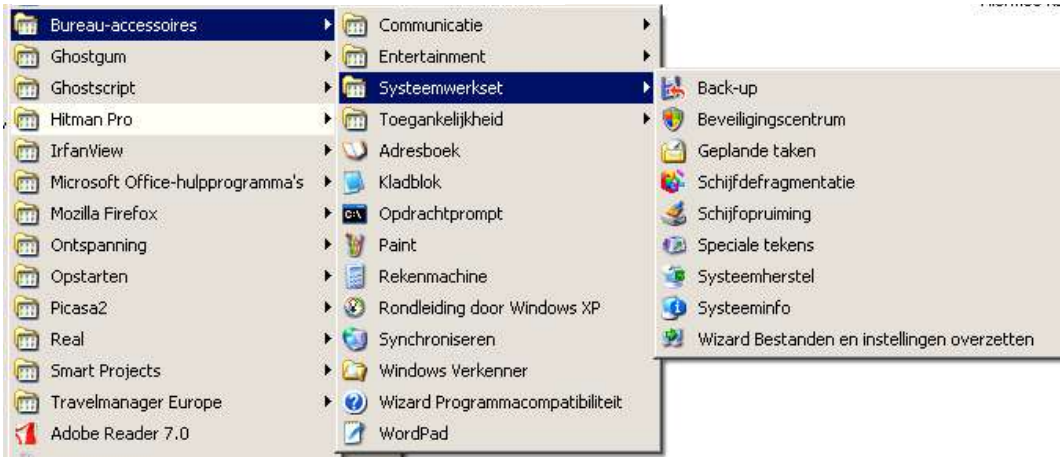


Eigenschappenblad van harde schijf

Wat biedt Windows XP ons?

XP biedt ons:

- Defragmentatie (bestanden netjes in volgorde plaatsen)
- Schijffoutherstel, Foutcontrole
- Schijfopruiming
- Back-ups maken
- Systeemherstel



Start→ Bureau-accessoires→ Systeemwerkset

Back-ups

Zolang u met dezelfde windows blijft werken kunt u de back-up van windows zonder al te veel problemen gebruiken. Microsoft heeft echter in het verleden getoond zo'n beetje bij iedere nieuwe versie van windows een incompatibele versie van back-up te leveren. Dus u gaat naar een nieuwere windows en u kunt uw oude backups niet inlezen/terugzetten.
Het vertrouwen in dit product is daarom niet al te groot. Maar beter iets dan niets.

Back-ups kunnen gemaakt worden op diskettes, zip-drives, harde (externe) schijven, en tape-drives. De tweetrapsversie van een backup op de harde schijf branden op cd-rom of dvd is een vrij algemene.

Het is goed om te beseffen dat u zonder dezelfde windows **niets** aan uw back-ups hebt. Crasht uw systeem dan kunnen uw back-ups u **niet** snel weer op de been brengen.

Systeemherstel

Ook voor systeemherstel gelden soortgelijke overwegingen als bij back-ups. Zonder een werkende windows kunt u uw systeem er niet mee redden. Alleen

een nog werkende windows kan gebruikt worden om terug te gaan naar een eerdere versie/configuratie van het systeem. We hebben het dan over de aanstuursoftware van apparaten (=drivers) en systeembestanden (die door bijv. een virus is vervangen).

Schijfopruiming

Is de ideale eerste stap om opruiming in het systeem te houden. Schijfopruiming werkt per partitie en toont na een korte analyse wat er opgeruimd kan worden.

Een nog beter programma is CrapCleaner van www.ccleaner.com dat ook meteen aanbiedt om huishoudelijk werk in het register te doen. Een echte aanrader dus.

Systeemherstel

Microsoft adviezen

De volgorde van de te bewandelen stappen is:

1. Gebruik als eerste de LKGF of Last Known Good Configuration. Die vindt u door tijdens het starten van Windows op F8 te drukken. In het menu dat dan verschijnt kiest u voor deze optie LKGF, die de laatste instelling bevat waarmee de computer het nog deed. Deze optie moet u dan ook echt meteen als eerste mogelijkheid kiezen in geval het systeem problemen ondervindt!
2. Als 1. maar nu kiest u voor de Veilige Modus om het probleem op te lossen
3. Herstelconsole gebruiken
   Er is nog een versie van systeemherstel. die onder de naam herstelconsole schuil gaat. Deze reparatiemogelijkheid van een systeem zien we slechts wanneer we zeer aandachtig de (eerste) installatie van een systeem uitvoeren.
   In geval van een crash leggen we de oorspronkelijke installatie-CD in de lade en volgen gewoon de eerste stappen van het installeren van een nieuw systeem. Nadat de bestanden gekopieerd zijn wordt er gevraagd of we windows willen installeren of een bestaand systeem **repareren**!
   Kiezen we voor reparatie dan wordt er gezocht naar een bestaande installatie en wanneer die gevonden wordt moeten we het bijbehorende keuzecijfer van de bestaande windows intypen. Daarna wordt ons gevraagd het administratorwachtwoord in te voeren. Is het een geldig wachtwoord dan krijgen we toegang tot een beperkte set commando's waarmee we herstel van het systeem kunnen proberen. De set van beschikbare commando's wordt getoond door *help* in te typen op de commandoprompt.

Herstelconsole - overzicht

(gekopieerd uit de Help van WinXP)
Als de veilige modus en de andere opstartopties niet werken, kunt u overwegen de herstelconsole te gebruiken. Deze methode wordt alleen aanbevolen voor ervaren gebruikers die overweg kunnen met de basisopdrachten voor de identificatie en het

opsporen van stuurprogramma's en bestanden die problemen veroorzaken. Bovendien moet u een beheerder zijn om de herstelconsole te kunnen gebruiken.

Met de herstelconsole kunt u services inschakelen en uitschakelen, stations formatteren, gegevens lezen en schrijven op een lokaal station (ook op stations met een NTFS-bestandssysteemindeling) en vele andere beheertaken uitvoeren. De herstelconsole is vooral handig als u het systeem wilt repareren door een bestand van een diskette of een cd-rom naar de vaste schijf te kopiëren of als u een service opnieuw wilt configureren wanneer uw computer niet correct kan opstarten vanwege deze service.

U kunt de herstelconsole op twee manieren starten:

- Als uw computer niet start, kunt u de herstelconsole uitvoeren vanaf de Setup-cd-rom.

- U kunt de herstelconsole ook op uw computer installeren zodat deze beschikbaar is wanneer u Windows niet opnieuw kunt starten. U kunt vervolgens de herstelconsole selecteren in de lijst met beschikbare besturingssystemen bij het opstarten.

Nadat u de herstelconsole hebt gestart, moet u opgeven op welke installatie u zich wilt aanmelden (als u over een dual-boot- of multiboot-systeem beschikt) en moet u zich aanmelden met behulp van uw beheerderswachtwoord.

De console bevat opdrachten voor eenvoudige bewerkingen, zoals het kiezen van een andere map of het bekijken van een map, en krachtiger bewerkingen, zoals het herstellen van de opstartsector op de vaste schijf. U krijgt toegang tot de Help voor de opdrachten in de herstelconsole door achter de opdrachtprompt van de herstelconsole **help** te typen.

Zie 'Verwante onderwerpen' voor meer informatie over het starten en gebruiken van de herstelconsole.

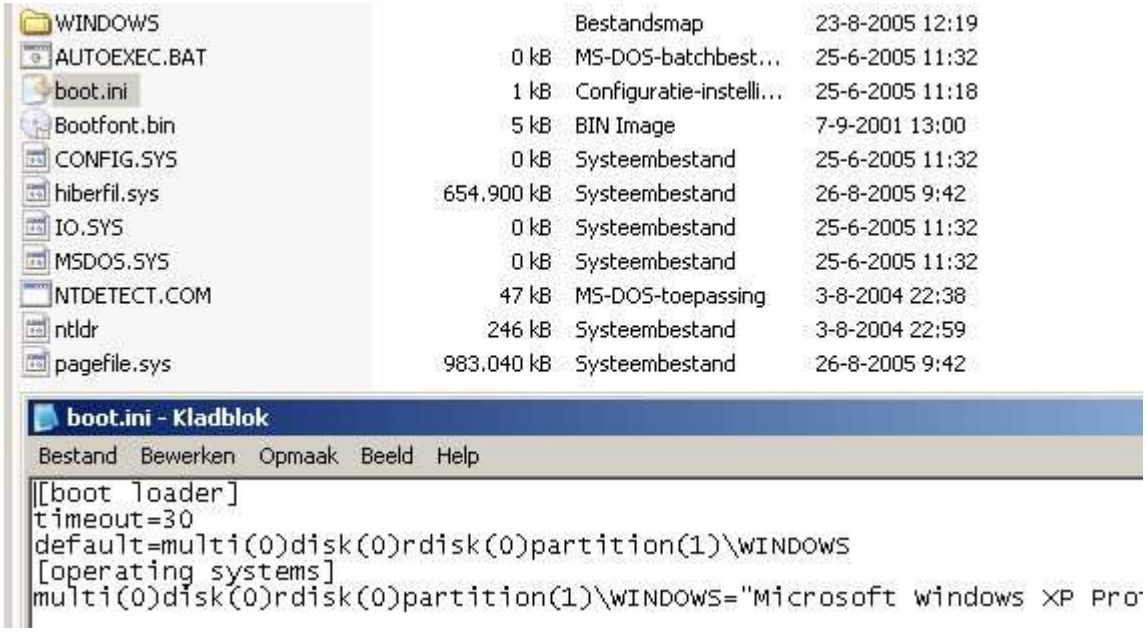
Zodra de herstelconsole is gestart, kunt u Help weergeven over de beschikbare opdrachten door **help** te typen bij de opdrachtprompt

4. Systeemherstel gebruiken
   U vindt Systeemherstel onder de Bureau-accessoires in de submap Systeemherstel maakt een ‘snapshot’ (afbeelding) van kritische systeembestanden en een aantal programmabestanden en slaat die informatie op in een herstelpunt.
5. Automatisch Systeemherstel (ASR). Geldt alleen voor Windows XP Professional. Wordt hier niet verder behandeld.

Boot disk

Voor die gevallen waarin Windows XP niet zijn goede installatiepunt kan vinden is het altijd verstandig om een boot-disk bij de hand te hebben.
Het maken van een boot-disk op opstartflop bestaat uit:

- het formatteren van een diskette m.b.v. Windows (xp).
- Op de floppy worden dan de bestanden Ntldr en Ntdetect.com van de juiste versie (bijv. SP2) gekopieerd. Dit zult u overigens wel als beheerder van de PC moeten doen!
- het maken of kopieren van een boot.ini-bestand om te vertellen waar windows zijn bestanden moet zoeken. De boot.ini file heeft een nogal bijzondere en lastige manier om dat aan te geven!



- Probeer vooral na het maken van de opstartdisk eens of die wel werkt.

Extern

Gereedschap voor schijven

Om een schijf te kunnen gebruiken moet de schijf geformatteerd worden. Formatteren maakt de schijf geschikt voor opslag. Men kan dit vergelijken met het aanbrengen van stellages om spullen in op te bergen in een loze ruimte. De soort stellages die we gebruiken wordt dan het bestandssysteem of file system genoemd.

Voor de latere versies van Windows, NT en later heeft het NTFS-bestands-systeem de voorkeur. Een reden is dat deze Windows i.s.m. NTFS vrij nauwkeurig de toegang tot mappen en bestanden kunnen bepalen. Dus ook wat een bepaalde gebruiker ziet en kan doen met een bestand. Een andere reden is dat in toenemende mate enorme bestanden 'nodig' zijn (zoals video-bestanden) die met NTFS een grote kunnen hebben van 4GB.

partitionering

Tijdens de installatie van Windows XP kunnen we nauwkeurig de indeling van de harde schijven bepalen. We kunnen ook oude indeling en formatteringen verwijderen. Mogelijke bestandssystemen zijn FAT32 en NTFS.

Fdisk.exe is het programma waarmee de indeling van een schijf onder Windows wordt bestuurd.

Later kan binnen Windows een NTFS-partitie nog wel aan de rechterkant uitgebreid worden, maar dan moet er aan die kant wel ongeformatteerde ruimte te vinden zijn. Dat wil zeggen dat in eerste instantie niet de hele harde schijf gebruikt werd.

Ook kan achteraf met *convert.exe* een FAT32-partitie worden omgezet in een NTFS-partitie. Omgekeerd kan dat niet.

Maar wie uitgebreid achteraf een andere indeling van de schijf/schijven wil bewerkstelligen **en** de bestaande bestanden wil bewaren is aangewezen op gespecialiseerde software. Bekende programma's zijn Partition Magic en Acronis Partition Expert.

Via andere besturingssystemen kan soms ook wel de grootte van de schijf of partitie worden aangepast.

> Linux kent een verzameling programma's onder de naam *ntfsprogs* waarmee op dit vlak het een en ander gedaan kan worden. Deze set hulpmiddelen wordt door een groep vrijwilligers goed onderhouden en wint bijna maandelijks aan functionaliteit. Het is zelfs mogelijk om met behulp van twee Linux Live-CDs via een netwerk een ISO-image van een systeem te maken en op het andere systeem op te slaan.

Om te conroleren of een schijf/partitie nog in orde is en om eventuele fouten te herstellen kan prima het programma *testdisk* van de fransman Grenier op http://cgsecurity.org gebruikt worden

imaging

Een image is een sectorgewijze afbeelding van een partitie. Dat wil zeggen dat het niet alleen de inhoud van een datadrager bevat maar ook de struktuur ervan. Een image wordt opgeslagen als een bestand.

Slimme imagers slaan de loze ruimte op een partitie over en comprimeren de bestanden. M.a.w. domme imagers maken een image dat net zo groot is als de partitie. Slimme imagers maken een image dat veel kleiner is. Een bekende imager is Ghost. Een goede 'kostenloze' imager is het Duitse Acronis True Image waarvan een oudere versie vrij te gebruiken is. Alleen de netwerkfunctionaliteit ontbreekt in de 'vrije' versie. Maar je kunt de image gewoon op CD of DVD wegschrijven of op een andere harde schijf of zelfs via het netwerk op een ander systeem opslaan.

Vragen die je bij een imager kunt stellen zijn:

- is er netwerkfunctionaliteit?
- werkt het alleen met windows?
- kan ik een enkel bestand uit de image terugzetten?

Een andere term die we in dit verband vaak tegenkomen is de ISO image.

De ISO image is een losse aanduiding voor een image van een ISO 9660 datadrager, d.i. een optisch apparaat als een CD.

Antivirus

Een goed antivirusprogramma hoort tegenwoordig helaas tot de normale voorzieningen op een PC.

Maar ook al hebt u dat, of denkt u dat te hebben, houd dan goed in de gaten wanneer de licentie verloopt en u weer moet gaan betalen.

Maar ook als uw licentie niet verlopen is moet u nog wat doen. Zorg dat de nieuwste definities of handtekeningen van virussen **regelmatig** of beter nog automatisch worden opgehaald!

Moet er altijd betaald worden? Er zijn heel behoorlijke 'gratis' virusscanners als Grisofts AVG, Avast, Bitdefender e.a.

Grotere namen zijn: Norton, McAfee, Symantec, Kaspersky, Panda, Sophos, Trend, om er een aantal te noemen.

Tegen een nieuw virus is nu eenmaal geen bescherming. Die bescherming moet eerst gemaakt worden en dan gedistrubueerd. Eigenlijk is een goede virusscanner een scanner die snel met een tegengif komt. De ervaring heeft geleerd dat het regelmatig niet de grote namen zijn die het snelst met een oplossing komen.

Zelf vind ik AVG een prettige oplossing.

Het verdient aanbeveling om een getroffen systeem met meerdere virusscanners te lijf te gaan. Ze zijn namelijk niet allemaal even goed in het herkennen van de infectie en hebben verschillende specialiteiten.

Een onafhankelijke bron over virussen en alles dat ermee samenhangt is www.virusalert.nl die ook een nieuwsbrief uitgeven. Ook hebben ze een online security check. Ook bij andere virusscanbedrijven kunt u terecht voor online kontrole van uw systeem (bijv. Trends Housecall en Panda).

Wat meestal wel kan is bij de grotere bedrijven een 30-dagen versie downloaden en die gebruiken. Doe dat dan voor 3 scanners. Gebruik de een, deïnstalleer die weer en gebruik dan de ander en dat dan nog een keer.

Treft u een specifiek virus dan zijn er bij de verschillende bedrijven vaak kosteloos kleine programma's te downloaden die die ene variant en haar familieleden vernietigen.

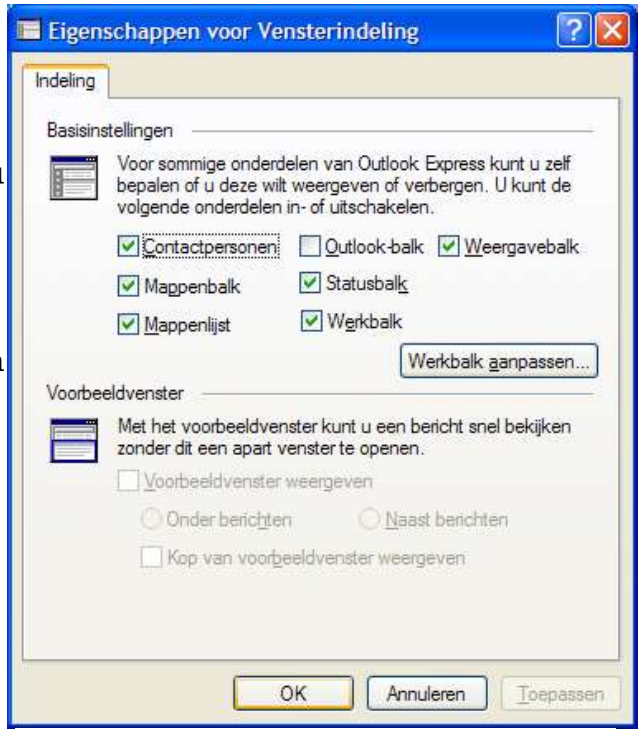
Iets meer krijgt u wanneer u in staat bent om bij McAfee *Stinger.exe* te downloaden. Die gaat op zoek naar een beperkte set van recente en kwaadaardige virussen.

EMAIL

Veel virussen worden verspreid via email. Al enige jaren kunt u het advies lezen om geen email van onbekenden of onverwachte email van bekenden klakkeloos te openen.

Mocht u, nog voordat u op welke wijze dan ook het bericht geopend hebt, twijfel hebben over een bericht sla het dan - indien mogelijk - op als gewoon tekstbestand (d.w.z. met de extensie .txt). Dit gaat meestal wel via het menu Bestand gevolgd door Opslaan als….En bekijk het dan in een teksverwerker als Kladblok/Notepad waarin geen macro's af kunnen spelen.

Een andere maatregel die u zeker moet nemen is het voorbeeldvenster van de emailtoepassing uit te zetten! Bij Outlook Express vind u dat onder het menu Beeld, Indeling. Zou u het voorbeeldvenster aan laten staan dan is bij het aanklikken van een bericht een eventueel virus ook meteen geactiveerd omdat het bijbehorende bericht immers meteen geopend wordt.



Outlook Express: Beeld, Indeling, Voorbeeldvenster UIT!

Maar u kunt ook heel goed overwegen om afstand te doen van Outlook Express. Probeer echter niet het programma te verwijderen! Gebruik gewoon iets anders als het Open Source programma Mozilla Thunderbird. Andere mogelijkheden zijn Pegasus of Eudora.

Naast het opslaan als tekstbestand kan het uiterst zinnig zijn een blik te werpen op het pad dat de post af heeft moeten leggen om onze brievenbus te bereiken. Daarvoor moet wel nauwkeurig worden gekeken en niet alleen wat er in de kop staat bij een normale blik. Met een rechter klik op de mail krijgen we vaak de mogelijkheid om de opties of de eigenschappen of details te bekijken.

Hieronder een voorbeeld:

```
Return-Path: <info@ngn.nl>
Received: from fallback10.hccnet.nl by deliver10.hccnet.nl
      via fallback10.hccnet.nl [62.251.0.46] with ESMTP
      id j7Q3aHtJ026494 (8.13.2/2.05); Fri, 26 Aug 2005 05:36:17 +0200 (MEST)
Received: from master.ngn.nl by fallback10.hccnet.nl
      via master.ngn.nl [80.253.112.206] with ESMTP
      id j7Q3VjkX007307 (8.13.2/2.03); Fri, 26 Aug 2005 05:32:33 +0200 (MEST)
X-RelayHost: 80.253.112.206
Received: from master.ngn.nl (master.ngn.nl [127.0.0.1])
 by master.ngn.nl (sendmail/GZ) with ESMTP id j7Q10CSi018978;
 Fri, 26 Aug 2005 03:00:12 +0200
Received: from localhost (apache@localhost)
 by master.ngn.nl (sendmail/Submit) with SMTP id j7Q10CZb018975;
 Fri, 26 Aug 2005 03:00:12 +0200
Date: Fri, 26 Aug 2005 03:00:12 +0200
Received: by master.ngn.nl (bulk_mailer v1.14); Fri, 26 Aug 2005 02:56:32 +0200
MIME-Version: 1.0
From: "NGN Verenigingsbureau" <info@ngn.nl>
Sender: info@ngn.nl
Reply-To: info@ngn.nl
Mail-Reply-To: info@ngn.nl
Subject: LanVision Nieuwsbrief v.8.63
Content-Type: multipart/related;
 boundary="=_d9f7017e74ef18a9ed622dc732088c9b"
Message-ID: <ilt1a8.5yu31o@master.ngn.nl:4712>
To: nieuwsbrief@ngn.nl
Precedence: bulk
X-HenZ-MailScanner-Information: Scanned at host master.ngn.nl
X-HenZ-MailScanner: Found to be clean
X-MailScanner-From: info@ngn.nl
```

Een werkelijk doortrapte mail is moeilijk te herkennen, maar het kan geen kwaad om een blik te werpen op de [ip-adressen] tussen de [ ] achter de servernamen van de verzender(s). Staan daar getallen in groter dan 255? Zo ja, dan zijn die vals. Zijn er meer of minder dan 4 groepen getallen? Dan deugt het niet. Is de tijdzone van de mail heel erg anders dan die waar u zich bevindt? Dat kan een aanwijzing zijn dat er iets ‘raars’ mee is. Net als de verstreken tijd tussen de ontvangsten op de tussenliggende mailservers. Is de Mail-Reply-To anders dan de Return-Path bovenin? En als laatste, maar zeker niet de minste: Komt de Reply-to (bovenaan) overeen met de From (verderop)?

Spam

Spam is zoveel als ongewenste email. U hebt geen sticker op de brievenbus en dus ontvangt u alles dat mensen u sturen. Daar zit ook veel bij dat u misschien helemaal niet wilt weten. Enerzijds omdat u het toch eerst moet binnenhalen, anderzijds omdat u het toch moet gaan bekijken om tot de conclusie te komen dat u het niet wilt lezen. Of nog erger omdat het iets ongewenst met zich meebrengt als een virus.

Ik adviseer u naast uw standaard email adres nog een ander (web)emailadres te nemen bij hotmail, yahoo, gmail e.d. Dit is dan het adres dat u opgeeft wanneer u eens aan het surfen bent en u iets wilt bekijken waarbij u zich eerst aan moet melden en naar uw emailadres wordt gevraagd. Alle reclame die u wordt gestuurd gaat dan naar dit adres toe.
Een andere aanbeveling is uw emailadres niet als leesbare tekst op uw website te zetten. Speciale robots schuimen het internet af op zoek naar emailadressen. Die adressen worden per miljoenen tegelijk verkocht aan bedrijven die om aandacht voor hun produkt schreeuwen.
Zet uw emailadres liever in een plaatje op uw website. Of schrijf het zodat robots er niet zo snel iets van kunnen bakken. Bijvoorbeeld: *Eiberhof bij/at gmail punt com, of grijpskerkgaatdigitaal$hotmail,com (vervang de $ door een apenstaart en de komma door een punt).* Het is even wennen en niet zo heel vriendelijk, maar het voorkomt veel post!

> Het apenstaartje @ betekent zoveel als voor en werd in de negentiende eeuw al gebruikt om een prijs aan te geven.

Steeds meer emailprogramma's hebben de mogelijkheid om spam te filteren. Veel spam wordt van dezelfde bron verstuurd. Daarop kan gefilterd worden. Andere kunnen getraind worden op afzenders of berichtinhoud.

Andere waar

Met andere waar bedoelen we hier programma's die worden aangeduid als spy-ware en mal-ware. Strikt genomen zijn het geen virussen maar vaker een bedreiging van uw privacy. Er wordt wel degelijk iets geïnstalleerd waarvan u zich in veel gevallen niet eens bewust bent. U installeert een programma en neemt zoals gewoonlijk niet de moeite om de licentieovereenkomst te lezen waarin staat dat er wel degelijk iets geïnstalleerd wordt en u impliciet toestemming geeft tot het verzamelen van de gewenste gegevens en het overzenden daarvan via uw internetverbinding. En daarmee wordt er een dienst of toepassing op de achtergrond geïnstalleerd die uw dure bronnen als processortijd en geheugenruimte gebruiken zonder dat u dat beseft.
Gelukkig zijn er een aantal gereedschappen waarmee u zich kunt wapenen tegen dit soort gedrag van nieuwsgierige aagjes. We noemen voor de XP gebruiker *HitmanPro* van Nederlandse hand. HitmanPro is een schil om een aantal andere voortreffelijke toepassingen die achtereenvolgens gedownload en geïnstalleerd worden. Andere namen zijn Ad-Aware, Search & Destroy, HijackThis. Een uitmuntende website op dit gebied is www.castlecops.com .
Er bestaan sterke vermoedens dat een aantal omstreden sites waar films en/of muziek wordt uitgewisseld middels peer-to-peer protocollen door de audiovisuele industrie bewust worden "vervuild". Waar gaat u klagen wanneer u zelf een strafbaar feit hebt gepleegd?

Phishing

Is het vissen naar persoonlijke informatie die misbruikt kan worden. U wordt ver- of misleid door een perfect nagebouwde website of email. Om nu toch echt uw bankrekeningnummer met wachtwoord even door te geven zodat die prijs kan worden overgemaakt, of zodat de problemen die er met uw rekening/account zijn verholpen kunnen worden.

Kijk wanneer u bankiert via het Internet vooral naar het soort verbinding dat u hebt. Voor een veilige verbinding is het niet langer het standaard http-protocol maar http**s**! Ziet u het slotje in de statusbalk van de webclient?
Bij zo'n verleidelijk mailtje is het zaak die eens nauwkeurig te bekijken door het eerst eens als tekstbestand op te slaan en te bekijken. Vraag eventueel hulp bij het betreffende bedrijf, de bank, eBay, PayPal etc, voordat u antwoordt.

Firewall

De firewall (vert.: brandgang) houdt het kontakt tussen de lokale PC en de andere computers (buitenwereld en/of LAN) in de gaten. Een goed ingestelde firewall voorkomt dus dat er vanuit de buitenwereld iets kwaadaardigs naar binnen kan (worden geduwd).
De PC is een huis met ruim 64-duizend deuren waarachter gepopeld wordt om open te doen zodra er aan die deur geklopt wordt. Via al die deuren kan dus ingebroken worden. Een paar deuren staan regelmatig open. Voor het ophalen en verzenden van post moeten deur 25 en 110 vaak open. Voor het surfen op Internet is het bijv. deur 80.
In feite kontroleert de Firewall het verkeer dat naar buiten of naar binnen wil. Sommige programma's mogen naar buiten, sommige naar binnen. Maar het meeste verkeer moeten we liever buiten houden.

Voorbeeld

Als interessant voorbeeld ziet u hieronder een afbeelding van de logfile van

Logs | Instellingen

	Omschrijving	Applicatie	Richting	Lokaal punt	Punt op afstand	Protocol	Actie
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1702	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1702	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1703	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1703	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1704	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1704	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1705	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1705	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1706	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1706	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1707	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1707	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1708	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1708	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1709	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1709	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1710	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1710	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1711	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1711	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1712	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1712	UDP	permitted
15:03:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1713	UDP	permitted
15:03:49	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1713	UDP	permitted
15:09:35	Unopened port	n/a	in	exeit6.klusjesman.xx:1175	http-unix.lb.network.bit.nl:http	TCP	denied
15:10:51	Microsoft File and ...	Microsoft File an...	out	exeit6.klusjesman.xx:netbios-ns	exeit2.klusjesman.xx:netbios-ns	UDP	permitted
15:10:51	Microsoft File and ...	Microsoft File an...	in	exeit6.klusjesman.xx:netbios-ssn	exeit2.klusjesman.xx:1042	TCP	permitted
15:33:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1714	UDP	permitted
15:33:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1714	UDP	permitted
15:33:43	Unopened port	n/a	in	239.255.255.250:1900	SpeedTouch.klusjesman.xx:1715	UDP	permitted

de firewall. Hierin is te zien dat de Speedtouchrouter in een enkele seconde tig-keer probeert om kontakt te maken met een duister IP-adres als

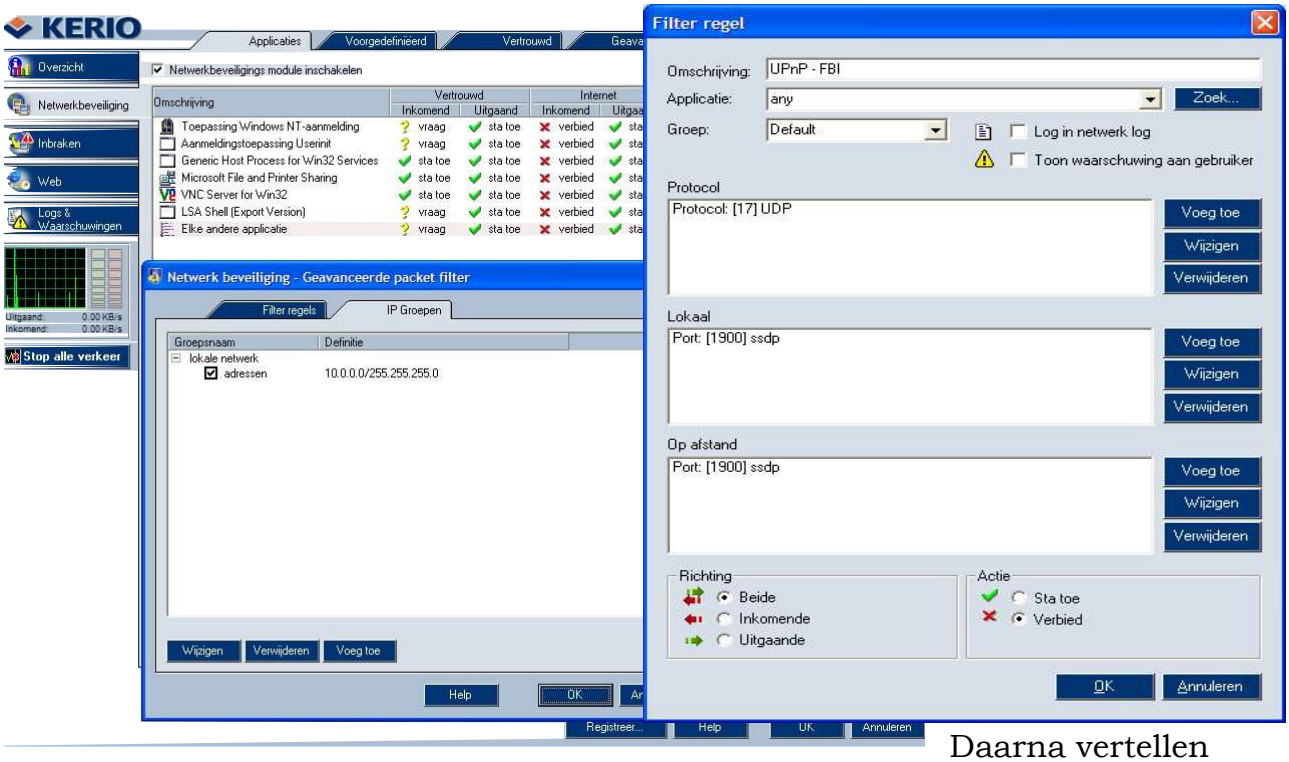
239.255.255.250 als lokaal punt op poort 1900. Onderzoek op internet leert dat dit IP-adres toebehoort aan een SSDP-service van Windows. Nog verder zoeken leert dat SSDP staat voor Simple Service Discovery Protocol, dat veelal gebruikt wordt om zogenaamde UPnP-apparaten te bedienen of te installeren. Zonder dat u zich dat goed bewust bent draait er dus een UPnP-server met een eigen IP-adres die om zich heen staat te roepen of er iets wil antwoorden. En al die poorten op de speedtouchrouter – blijkbaar zo'n UPnP-apparaat - melden zich keurig aan.

Dit drukke netwerkverkeer zou wel eens geheel overbodig kunnen zijn.

Om het te beperken kunnen we de firewall opdracht geven dit geblèr niet langer door te laten en zo beslag te leggen op processortijd en/of bandbreedte en geen antwoord meer te geven.

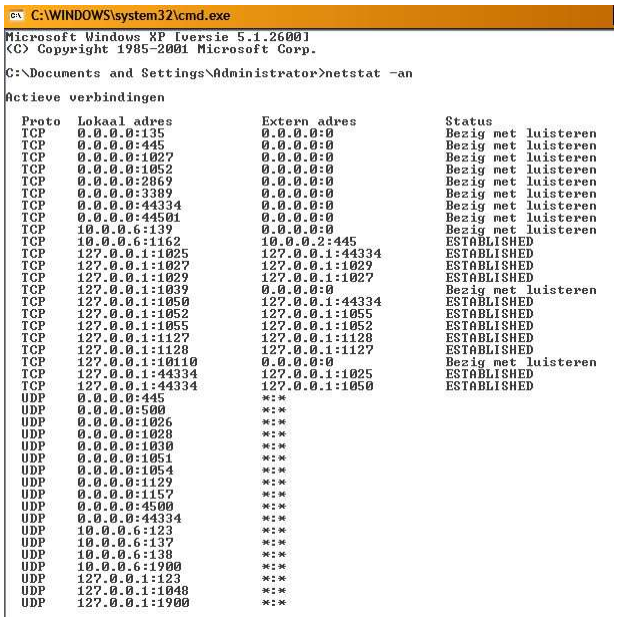
In dit voorbeeld wordt gebruik gemaakt van de Kerio Personal Firewall v. 4.2.

Daarvoor openen we eerst het tabblad Netwerkbeveiliging en Applicaties/-toepassingen. Daarin zit een knop Packet filter… die we aanklikken. In het dialoogvenster geven we dan eerst een groepsnaam en naam op via welke we de herkenbaarheid van de filterregels kunnen bevorderen.



Daarna vertellen we over welk soort protocol we het hebben. In ons geval is dat het UDP-protocol en welke poort aan de buitenkant en welke poort aan de binnenkant we willen filteren.

We moeten een beetje schipperen met de mogelijkheden van het punt op afstand. Omdat het vermoedelijk de lokale ssdp-server is die op poort 1900 staat te kijken wat er elders reageert volstaan we lokaal en op afstand met die poort.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [versie 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -an

Actieve verbindingen

  Proto  Lokaal adres          Extern adres        Status
  TCP    0.0.0.0:135           0.0.0.0:0           Bezig met luisteren
  TCP    0.0.0.0:445           0.0.0.0:0           Bezig met luisteren
  TCP    0.0.0.0:1027          0.0.0.0:0           Bezig met luisteren
  TCP    0.0.0.0:1052          0.0.0.0:0           Bezig met luisteren
  TCP    0.0.0.0:2869          0.0.0.0:0           Bezig met luisteren
  TCP    0.0.0.0:3389          0.0.0.0:0           Bezig met luisteren
  TCP    0.0.0.0:44334         0.0.0.0:0           Bezig met luisteren
  TCP    0.0.0.0:44501         0.0.0.0:0           Bezig met luisteren
  TCP    10.0.0.6:139          0.0.0.0:0           Bezig met luisteren
  TCP    10.0.0.6:1162         10.0.0.2:445        ESTABLISHED
  TCP    127.0.0.1:1025        127.0.0.1:44334     ESTABLISHED
  TCP    127.0.0.1:1027        127.0.0.1:1029      ESTABLISHED
  TCP    127.0.0.1:1029        127.0.0.1:1027      ESTABLISHED
  TCP    127.0.0.1:1039        0.0.0.0:0           Bezig met luisteren
  TCP    127.0.0.1:1050        127.0.0.1:44334     ESTABLISHED
  TCP    127.0.0.1:1052        127.0.0.1:1055      ESTABLISHED
  TCP    127.0.0.1:1055        127.0.0.1:1052      ESTABLISHED
  TCP    127.0.0.1:1127        127.0.0.1:1128      ESTABLISHED
  TCP    127.0.0.1:1128        127.0.0.1:1127      ESTABLISHED
  TCP    127.0.0.1:10110       0.0.0.0:0           Bezig met luisteren
  TCP    127.0.0.1:44334       127.0.0.1:1025      ESTABLISHED
  TCP    127.0.0.1:44334       127.0.0.1:1050      ESTABLISHED
  UDP    0.0.0.0:445           *:*
  UDP    0.0.0.0:500           *:*
  UDP    0.0.0.0:1026          *:*
  UDP    0.0.0.0:1028          *:*
  UDP    0.0.0.0:1030          *:*
  UDP    0.0.0.0:1051          *:*
  UDP    0.0.0.0:1054          *:*
  UDP    0.0.0.0:1129          *:*
  UDP    0.0.0.0:1157          *:*
  UDP    0.0.0.0:4500          *:*
  UDP    0.0.0.0:44334         *:*
  UDP    10.0.0.6:123          *:*
  UDP    10.0.0.6:137          *:*
  UDP    10.0.0.6:138          *:*
  UDP    10.0.0.6:1900         *:*
  UDP    127.0.0.1:123         *:*
  UDP    127.0.0.1:1048        *:*
  UDP    127.0.0.1:1900        *:*
```

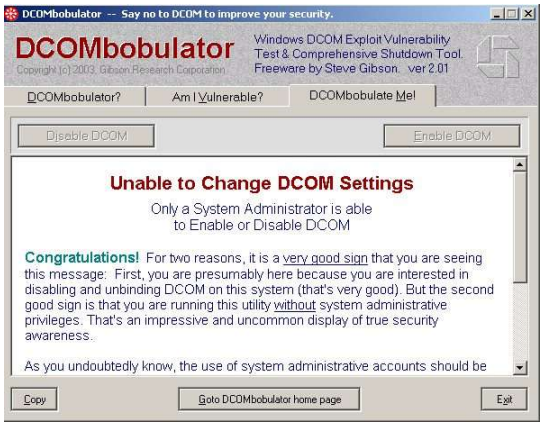
In de afbeelding hiernaast is met de *netstat*-opdracht nog eens in kaart gebracht op welke ip-adressen welke poorten aktief waren op een bepaald tijdstip.

Wat we met de filterregel bereikt hebben is dat er geen onnodig verkeer meer over het netwerk gaat.

Helaas is dit voorbeeld nog uit een ander beveiligingsoogpunt van belang.

De al eerder genoemde site http:\\grc.com van Steve Gibson Research heeft nog andere schokkende verhalen over SSDP en UPnP te melden. Ik zal hier niet een complete vertaling van die webpagina geven maar het samenvatten met de mededeling dat zelfs de FBI op enig moment vond dat het aanbeveling verdiende de SSDP-service uit te zetten. Het hele verhaal is lang maar uiterst interessant en ik raad iedereen aan het te lezen als u het engels voldoende machtig bent. Enerzijds omdat het weer eens laat zien wat voor machtig marketingapparaat de firma Microsoft feitelijk is en anderzijds hoe onder het motto 'klantvriendelijk en op de toekomst voorbereid', u zaken krijgt toegeschoven die potentieel een bedreiging vormen.

Gelukkig heeft GRC een tooltje voor ons waarmee we snel en einde kunnen maken aan die SSDP-service. En het eventueel ook snel weer aan kunnen zetten indien we het toch nodig blijken te hebben. U kunt het van zijn website downloaden. Net als de andere twee tools die DCOM en Windows Messenger uit kunnen zetten.



Welke?

Op het vlak van de 'gratis' firewalls ken ik Kerio Personal Firewall en ZoneAlarm. Zelf gebruik ik Kerio, ook al omdat het samenwerkt met AVG.

Maar laten we de belangrijke bijdrage van Microsoft op dit gebied niet vergeten. Sinds Service Pack 2 van Windows XP bevat Windows een aardige,

zij het rudimentaire, firewall. Deze firewall is vooral nuttig wanneer je een systeem aan het inrichten bent en je tijdens de installatie je netwerk configureert en Windows je meteen aanbiedt de laatste updates en patches te downloaden.

Nota Bene

Bedenk dat virussen zich willen verspreiden. Wil uw PC niet netjes afsluiten dan is een virusbesmetting zeker iets waar u aan moet denken. Immers, zolang windows aktief is kunnen virussen hun werk blijven doen. Overigens kan een andere reden dat Windows niet netjes af wil sluiten een verkeerde driver zijn. Met Systeemherstel kunt u snel terug naar een vorige versie.

Maar wat nu wanneer er helemaal geen Windows meer is? Dan zult u moeten kijken of u een virusscanner op basis van een ander besturingssysteem kunt vinden, zoals DOS of Linux.

Veel virusscanners hebben de mogelijkheid om zogenaamde Rescue Disks te maken, die u in zo'n geval kunt gebruiken.

Alwils Avast kostenloze antivirus versie kent die mogelijkheid bijvoorbeeld niet, maar biedt wel de mogelijkheid om een DOS-versie te downloaden. Daarmee moet dan een opstartbare CD-ROM gemaakt worden. Maar, dan is er een nieuw probleem. Namelijk hoe een NTFS-bestandssysteem te scannen met behulp van DOS?? Dat werkt standaard niet!!

Nu zou dit probleem nog op te lossen zijn, maar Avast komt zelf natuurlijk met een betaalde oplossing: de Avast Bart CD.

AVG kan daarentegen wel Rescue Disks maken tijdens de installatie van het programma.

Index

Index