

Inhoudsopgave

Cursus Onderhoud & Beveiliging.....	1
Installatie en Partioneren.....	1
Waarom partitioneren?.....	1
Hoe partitioneren?.....	1
Vensters: Windows XP met beperkte rechten	3
Hoe installeert u nu een nieuw programma of update?.....	6
Uitvoeren als.../Runas.....	7
Werken met beperkte rechten.....	7
Schijfbeheer.....	9
Schijfdefragmentatie.....	11
EHBO.....	13
Zien we alles?.....	13
Ontvlooiën.....	14
Virusscanner.....	15
veilige modus.....	15
HitmanPro.....	16
Sites.....	17
Firewall.....	17
Autostarters.....	24

Cursus Onderhoud & Beveiliging

Klantvriendelijkheid betekent voor leveranciers van hard- en software dat het na installatie werkt. Dat is hun belang. Hun belang is ook zoveel mogelijk te besparen op productiekosten. Handleidingen en de vertalingen daarvan zullen zo kort mogelijk zijn. Dat spaart ruimte, papier en vertaalkosten. Ze willen voorkomen dat de helpdesk moet worden geraadpleegd of dat ze overspoeld worden met emails. Dat doen ze door u iets te leveren dat het weliswaar doet, maar waarmee meestal geen of weinig rekening wordt gehouden met uw belangen. Belangen als veiligheid of onderhoudsgemak bij de klant spelen nauwelijks een rol.

Installatie en Partioneren

Waarom partitioneren?

Omdat het binnen Windows XP wel mogelijk is de map 'Mijn documenten' makkelijk naar een andere partitie te verleggen. In het geval er dan iets mis gaat met windows en we moeten herinstalleren, blijft deze belangrijke map, in tact. We zijn onze foto's, films, documenten etc. niet kwijt.

Ook is het onverstandig back-up bestanden of images op te slaan op dezelfde partitie.

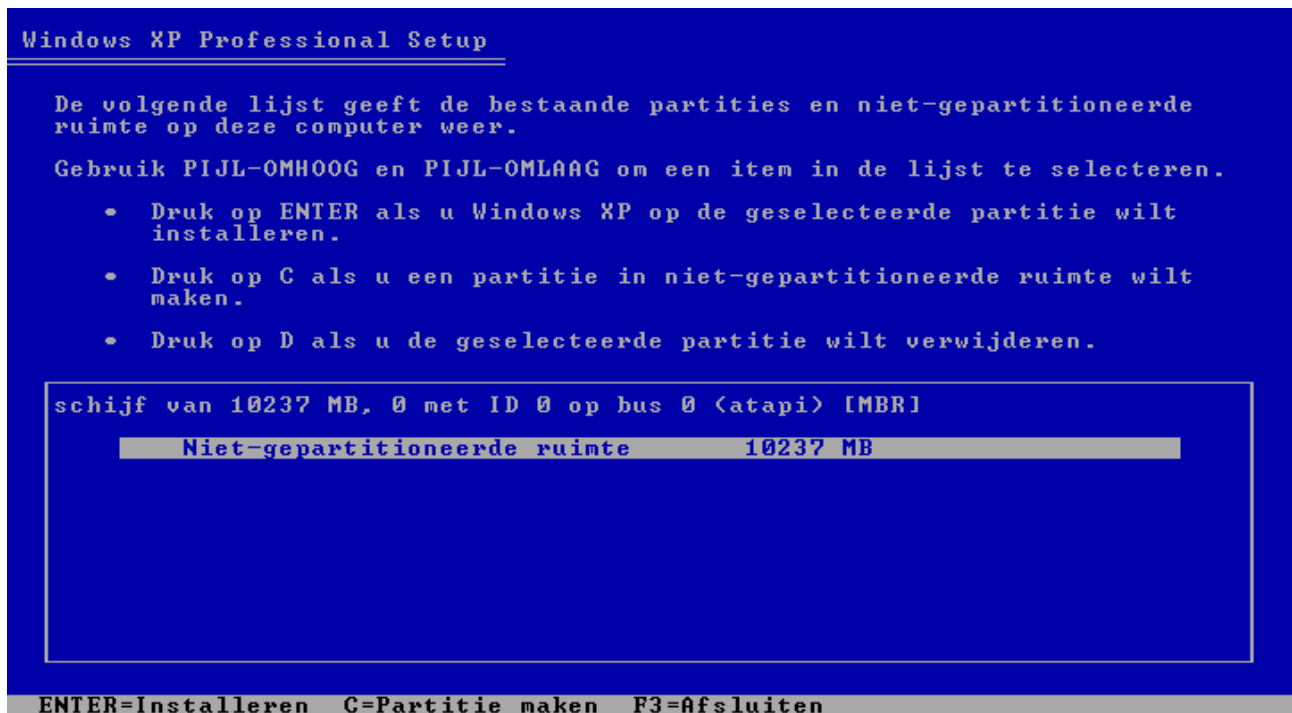
Hoe partitioneren?

Het is helaas niet mogelijk om met een geïnstalleerde Windows XP de partities nog aan te passen. We kunnen dus niet een reeds bestaande partitie vanuit winxp vergroten of verkleinen of verplaatsen. Alleen in vrije ongepartitioneerde ruimte kan winxp nog iets zinnigs doen.

Wel kan tijdens de (her-)installatie van Windows XP gepartitioneerd worden. Vrij vroeg in het installatieproces komt XP met de vraag waar geïnstalleerd moet

worden.

Bestaande partities kunnen gewist worden en nieuwe gemaakt. In de afbeelding hieronder moet eerst in ongepartitioneerde ruimte een partitie gemaakt worden. Door de grootte van de gewenste partitie in te typen (in MB!) kunnen we straks, binnen de dan geïnstalleerde Windows, nog andere partities maken.

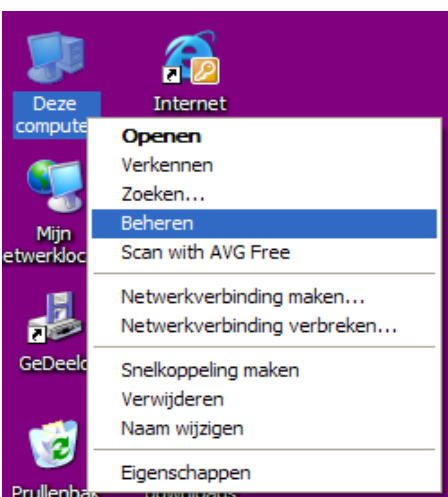


Een Windows XP partitie is minimaal 10 GB groot. Liever nog iets groter, bijv. 15 GB. Door alle servicepacks en updates zal de schijf snel vollopen. Er moet ook rekening worden gehouden met de 1,5 GB voor het interne geheugen, de slaap- of hibernate-file en de benodigde ruimte voor systeemherstel. Windows XP maakt voor zichzelf een Primaire Partitie en zet ook de vlag voor die partitie op Actief.

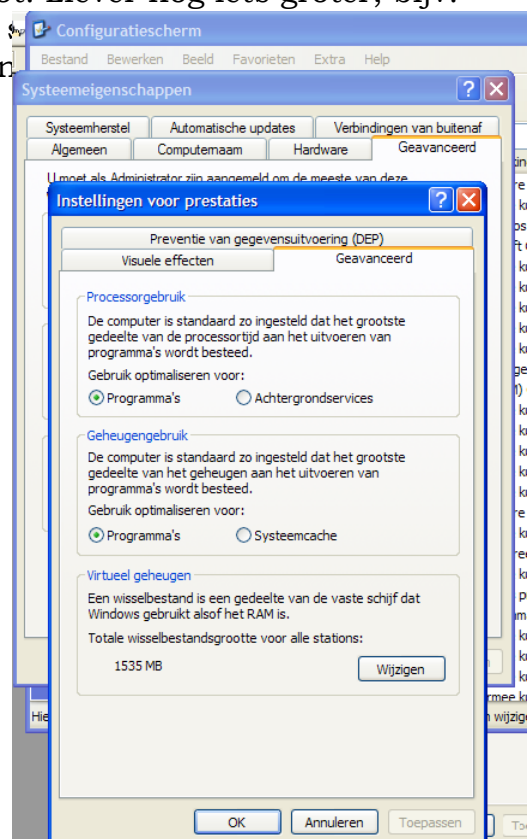
Eenmaal geïnstalleerd kunnen we met Computerbeheer de schijf of schijven beheren.

Bestand	Grootte	Type
NTDETECT.COM	47 kB	MS-DOS-toepassing
ntldr	246 kB	Systeembestand
pagefile.sys	1.572.072 kB	Systeembestand

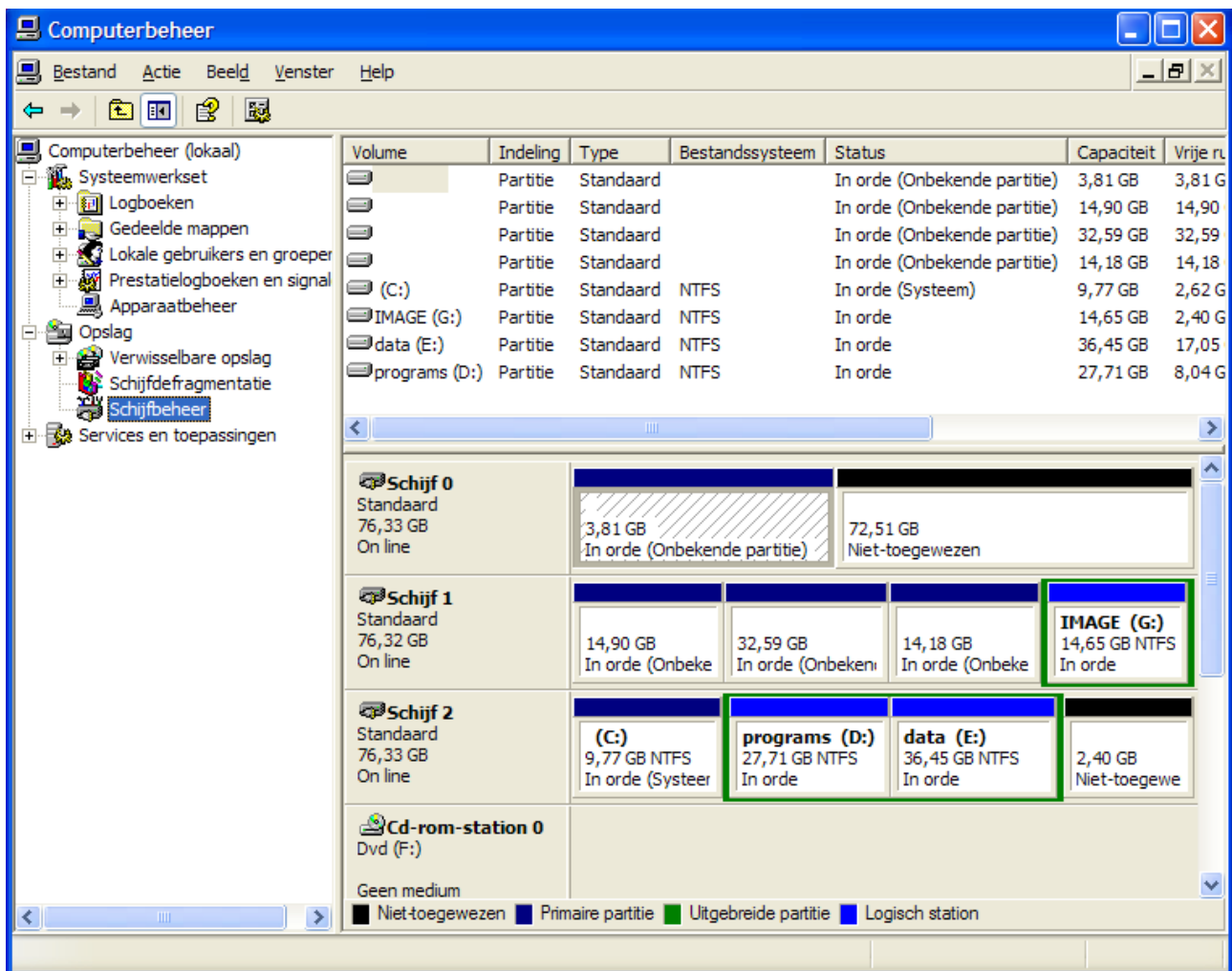
Pagefile.sys; het bestand voor het virtuele geheugen



Computerbeheer



Instelling voor het Virtuele Geheugen



Op Schijf 2 zien we de belangrijkste windowspartities. Schijf 0 en 1 zijn voor verschillende Linuxen.

Als u werkelijk omhoog zit en niet opnieuw wilt installeren, dan kunt u met de OpenSource opstart-CD van Gparted, ook windowspartities aanpassen.

Hier - <http://gparted-livecd.tuxfamily.org/> - kunt u het Iso-bestand van de LiveCD downloaden. Brand daarna dit iso-image met DeepBurner of Nero op een CD. Leg de CD na het branden in de lade, start de machine opnieuw op en u krijgt een grafisch mini-Linux-systeem met de mogelijkheid om partities te beheren. Er zijn nog tal van andere mogelijkheden die Gparted biedt.

Vensters: Windows XP met beperkte rechten

Bij de installatie van het populaire Windows XP krijgen standaard alle aangemaakte gebruikers *beheerderrechten*. Dat wil zeggen dat ze alles mogen doen. En als zodanig dus ook de systeeminstellingen aanpassen.

Inmiddels is de roemruchte firma er ook achter gekomen dat dat geen zorgvuldige manier van werken is en zijn er in de nieuwe versie Vista tal van aanpassingen op dit vlak gekomen. Ze moeten tenslotte wat doen als ze roepen dat ze veiligheid hoog in hun vaandel hebben staan. Dat pakt in Vista nu zo uit, dat voor iedere toegang tot iets dat potentieel het systeem zou kunnen bedreigen, de gebruiker wordt geattendeerd en toestemming moet verlenen.

De XP-gebruikers kunnen zelf maatregelen nemen door de gebruikers de

beheerrechten te ontnemen. Dat betekent voor de doorsnee gebruiker in de praktijk weinig belemmering op een eenmaal geïnstalleerd systeem. Op elk systeem moet altijd minimaal één gebruiker met beheerderrechten aanwezig zijn. En om ook een achterdeur te hebben is het verstandig te zorgen voor twee accounts met beheerderrechten!

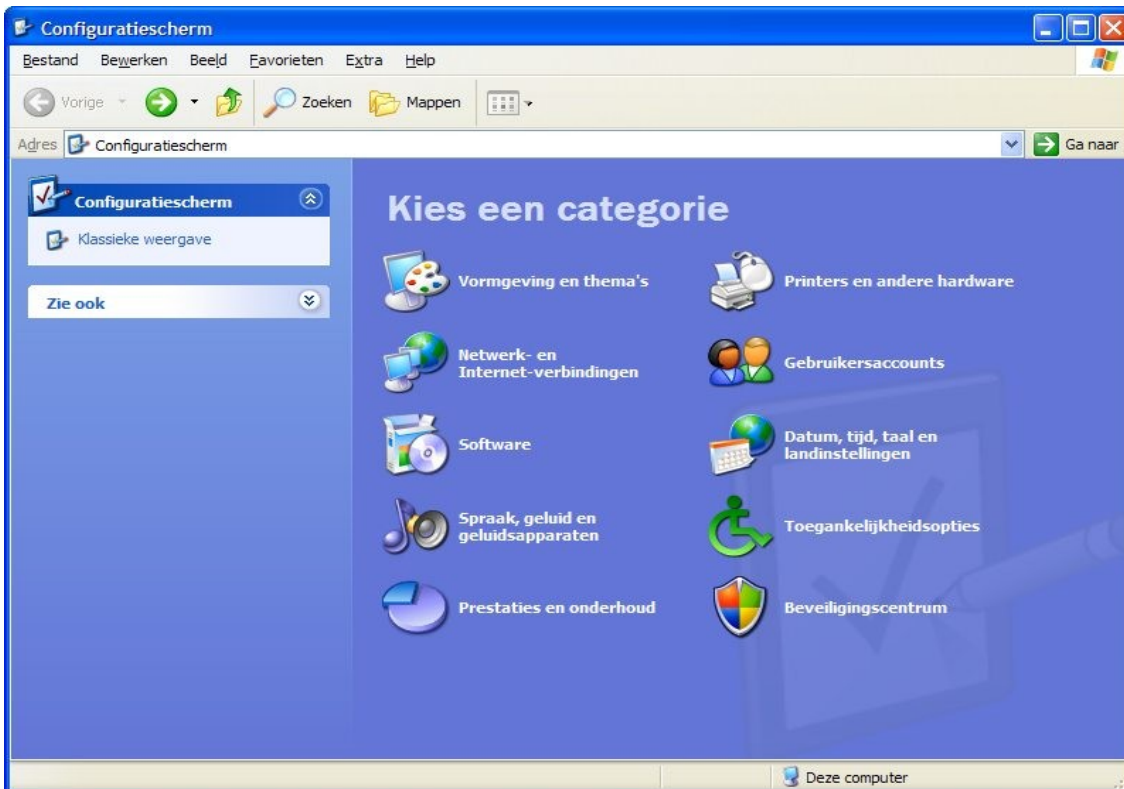
Als deze horde eenmaal genomen is, is de volgende stap om de accounts ook van een wachtwoord te voorzien alleen maar een uitbreiding en verbetering van de beoogde veilige omgeving.

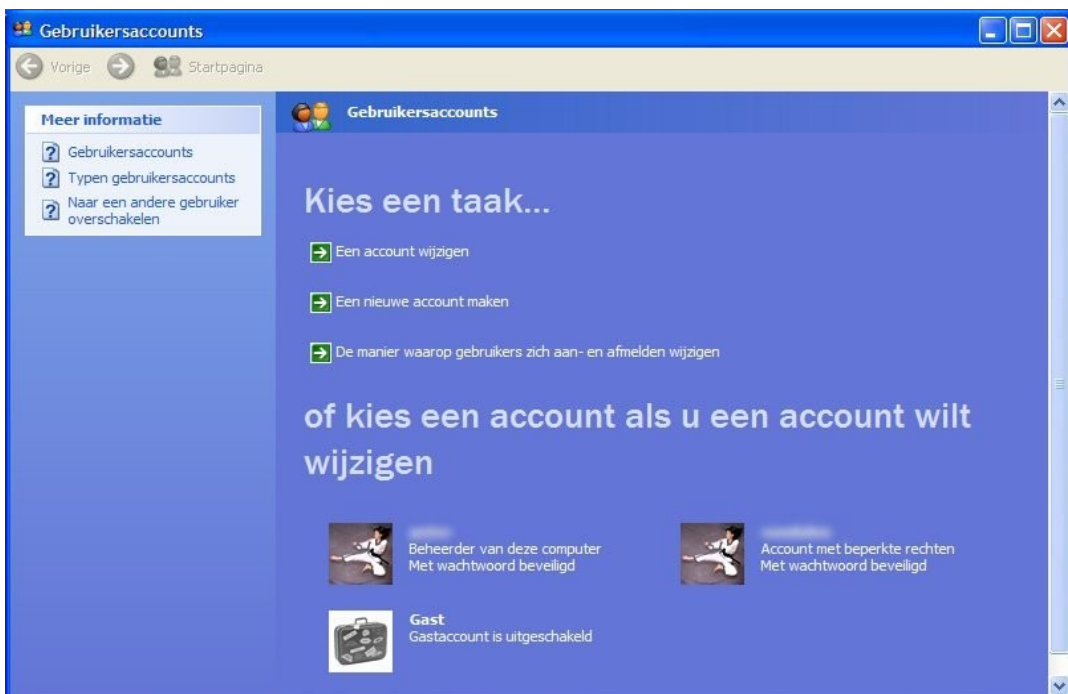
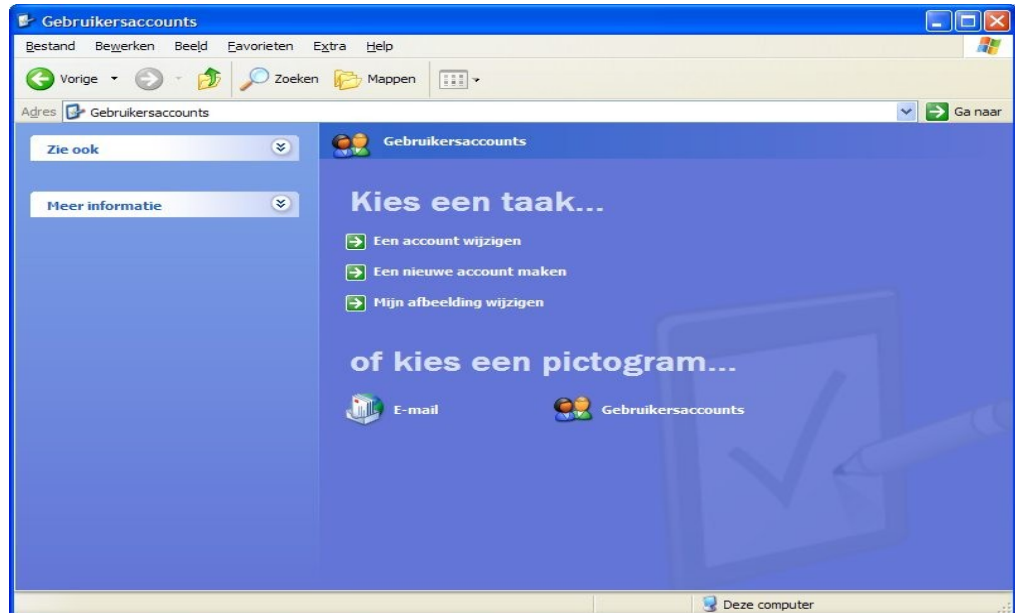
Deze maatregelen brengen met zich mee dat de zogenaamde snelle gebruikerswisseling uitgeschakeld dient te worden. Dit is dus een duidelijk voorbeeld van het feit dat gemak of klantvriendelijkheid niet strookt met veiligheid!

Hoe gaan we nu te werk?

De standaard aanwezige administrator-gebruiker is vooralsnog voor ons onzichtbaar.

Aangenomen dat de gewone account al beheerderrechten heeft nemen we een kijkje in het Configuratiescherm onder Gebruikersaccounts.





Hier kunt u accounts aanmaken en wijzigen. Bedenk dat uw 'normale' account een gebruiker met beperkte rechten moet worden. Dat betekent dat u begint met tenminste één gebruiker met beheerderrechten aan te maken. In aanmerking komen gebruikersnamen als beheerder, admin, sjefke, manager, baas, president, koning, keizer, admiraal, darth vader etc.

En een goed en makkelijk te typen wachtwoord bestaat uit minimaal 8 tekens, met daarin zowel cijfers, als letters en andere leestekens. Het is zeker verstandig aantekeningen te maken van de paren accountnaam en wachtwoord!! Voorzie alle accounts van een behoorlijk wachtwoord.

Twee of meer gebruikers mogen best hetzelfde wachtwoord hebben, maar dit wordt – juist uit veiligheidsoverwegingen – ten zeerste afgeraden.

Gebruikersnamen (accountnamen) zijn onder Windows niet hoofdlettergevoelig.

WaChTWOoRden Wel!

Pas dan schakelen we over naar (een nieuw aangemaakte) account met beheerrechten en ontnemen we de beheerrechten van de (oude) standaard-gebruiker(s).

Op enig moment zal u gevraagd worden of ook de snelle gebruikerswisseling uitgeschakeld moet worden. Dat is inderdaad in onze opzet noodzakelijk.

Het gevolg van dit alles is dat een 'normale' gebruiker niet langer een programma kan installeren. Dat lijkt heel vervelend maar heeft als voordeel dat een kwaadaardig programma (een virus of aanverwante) ook niet geïnstalleerd kan worden. Ook andere ingrepen in het systeem worden op deze wijze voorkomen.

Terzijde: Een gebruikersaccount is onzichtbaar gekoppeld aan een zogenaamd UserID. De UserID is een uniek getal. U kunt een gewiste gebruiker/account **niet** herstellen door opnieuw een account aan te maken met dezelfde naam en wachtwoord. Dat zal echt niet lukken.

U hebt nu een belangrijke stap gezet bij het beveiligen van uw computer!


Hoe installeert u nu een nieuw programma of update?

Hebt u het advies van Microsoft gevolgd om automatische updates te activeren dan is dat geen enkel probleem. Die worden gewoon gedownload en geïnstalleerd.

Andere automatische updates van geïnstalleerde programma's hebben wellicht een account met beheerrechten nodig. Als 'normale' gebruiker krijgt u bij het gebruik van een programma meestal wel een melding dat er updates beschikbaar zijn. Het heeft dan geen zin die al te downloaden want u hebt het recht niet ze te installeren.

Dus zo af en toe inloggen met beheerrechten. Dan diezelfde programma's starten en controleren op beschikbare downloads geeft ook het recht ze daadwerkelijk te mogen installeren.

Een andere weg loopt als volgt: U downloadt een programma in het standaardmapje dat u hebt gereserveerd voor de downloads. U gaat naar die map en zoekt het zoeven opgehaalde bestand. Meestal is dit een uitvoerbaar bestand en heeft het als extensie *.exe*. Uitvoerbare programma's kunt u rechtsklikken en dan kiezen voor Uitvoeren als...

	<p>In het onderste deel van het dialoogvenster kiest u dan voor een accountnaam met beheerrechten en geeft het bijbehorende wachtwoord.</p>
---	---

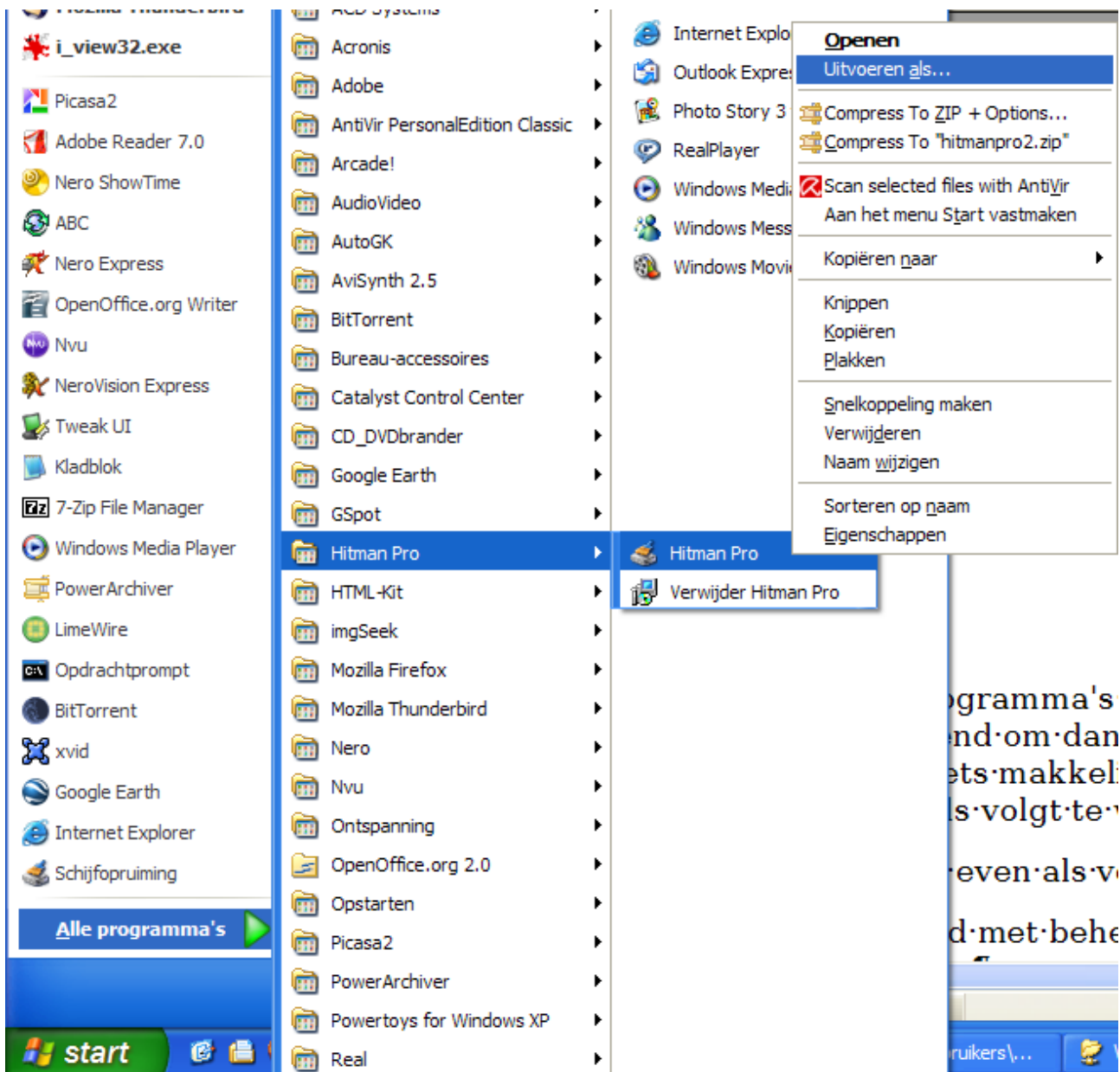
Uitvoeren als.../Runas

Werken met beperkte rechten.

Sommige belangrijke programma's hebben om goed hun werk te doen beheerdersrechten nodig. HitmanPro is zo'n programma.

Om te zorgen dat ook een gebruiker met beperkte rechten dit uit kan voeren, kan die het volgende doen:

- Klik de startknop
- Klik op alle programma's
- Ga naar de ingang met het gezochte programma
- Rechtsklik het programma
- Klik bovenaan op Uitvoeren als...
- Kies onderin voor een gebruiker met beheerdersrechten (tijdelijk, baasTijdelijk) en voer het wachtwoord voor die gebruiker in.



Een andere mogelijkheid is om het programma op te zoeken in de installatiemap voor programma's. Meestal is dit de map \Program Files.

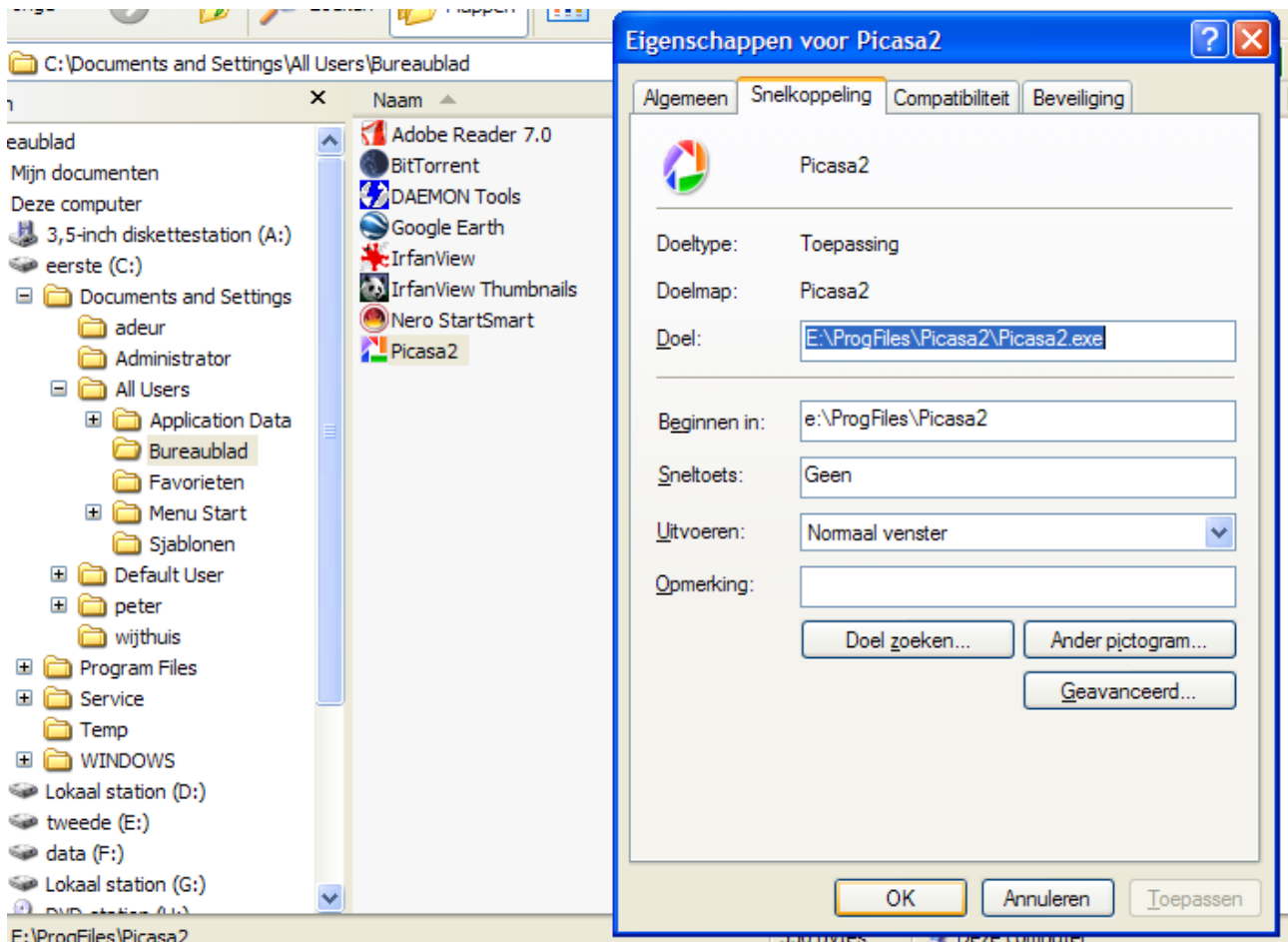
Rechtsklik het programma, kies weer voor uitvoeren als... etc.

Sommige oudere of slecht geschreven programma's moeten altijd met beheerdersrechten starten. Het is vervelend om dan steeds te moeten rechtsklikken etc. Om het (de kinderen) iets makkelijk te maken met zo'n programma, als BearShare¹ bijv., kun je als volgt te werk gaan.

Ik heb geen BearShare en gebruik Picasa even als voorbeeld.

Je logt op de pc (van het kind) aan als iemand met beheerdersrechten, dus als **baasTijdelijk**, **koning** of **administrator**.

Zoek de map 'Documents and Settings' op (of DocSet) en ga op zoek naar Alle gebruikers (all users), of de gebruikersnaam. Zoek daar verder naar de map Bureaublad. Klik het icoon van het gewenste programma met de rechtermuisknop aan en kies onderaan voor eigenschappen.



In het vak doel typ je vóór de naam van het programma:

runas /user:tijdelijk² <de programmaam>

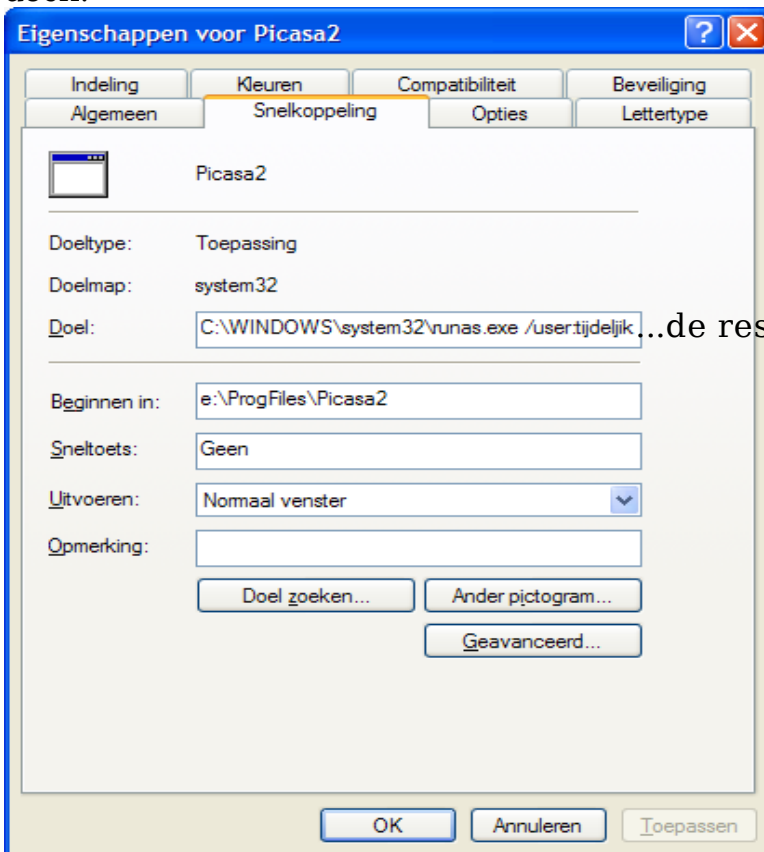
Je klikt op OK en bent klaar.

Wanneer ze nu het programma-icoon op het bureaublad dubbelklikken om het

1 Ik adviseer BearShare zeker niet, ik gebruik het alleen maar als voorbeeld

2 Of een andere naam van een gebruiker met beheerrechten

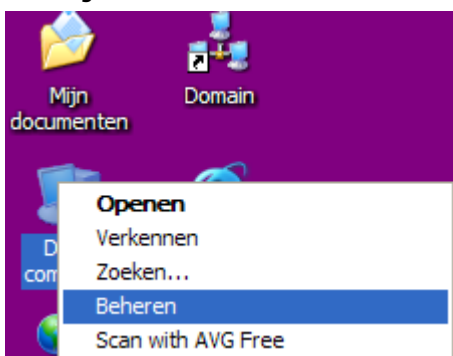
programma te starten moeten ze alleen nog het wachtwoord voor de gebruiker tijdelijk intypen. Dat typen van het wachtwoord zien ze niet. Je moet het gewoon doen!



Dan ziet het er zo ongeveer uit als hierboven. Runas wordt automatisch vervangen door het volledige pad.

Het kan zijn dat je nog even het pictogram/icoon opnieuw op moet geven. Dat kan ook vanuit het eigenschappenvenster dat je nog open hebt.

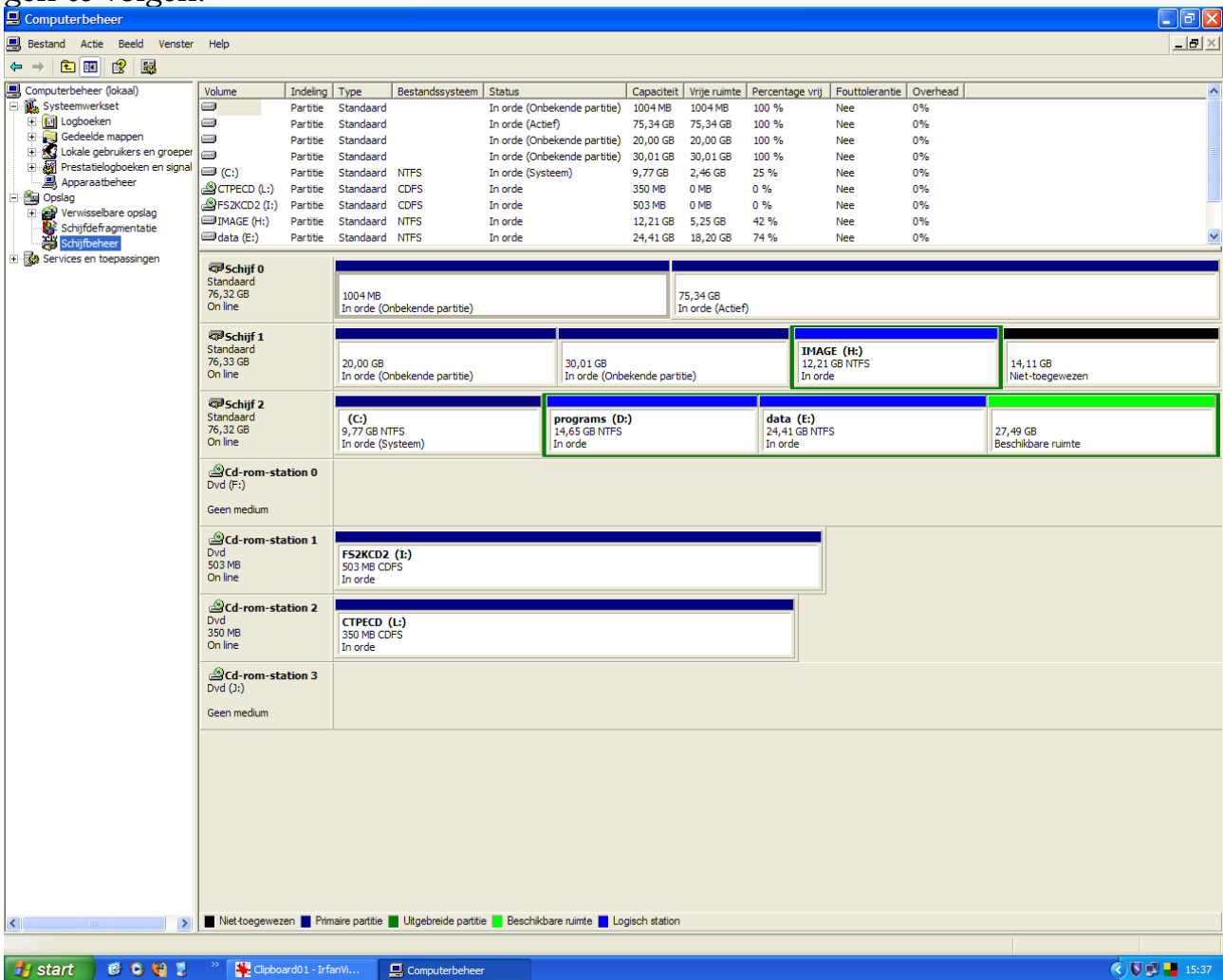
Schijfbeheer



Rechtsklik het pictogram 'Deze computer' en kies voor Beheren. Indien u voldoende rechten hebt kunt u in het Computerbeheervenster, bijna onderaan in het linkerdeelvenster kiezen voor schijfbeheer. Als dat nog nooit eerder gebeurt is, dan kan het even duren voordat u wat ziet, want alle gegevens moeten eerst verzameld worden.

U kunt hier door in het detailvenster een schijf of partitie aan te klikken opnieuw een schijf indelen door partities aan te maken en te formatteren. Maar doet u dat met een reeds benutte schijf of partitie dan zal **alle** informatie vernietigd worden. Voor het beheren van reeds gebruikte schijven of partities is geen meegeleverd Windows gereedschap beschikbaar. U zult uw toevlucht moeten nemen tot Acronis Disk Director of PartitionMagic om een paar namen te noemen. (Acronis software komt regelmatig op de Nederlandse markt onder de naam Easy Computing) U kunt alleen **tijdens** de installatie van Windows iets aan de partitionering van de harde schijf doen. En dat is een kwestie van heel goed lezen wat er staat en de

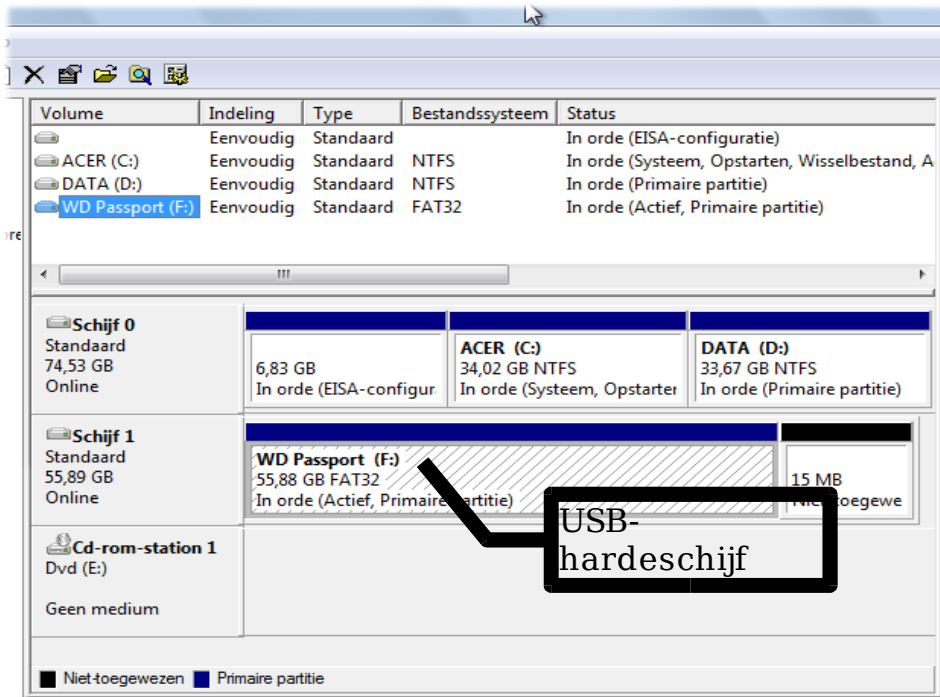
aanwijzingen nauwkeurig volgen. Zolang u niet tevreden bent, omdat u bijv. 1500 MB opgaf i.p.v. 15000 kunt u partities weer wissen etc. door strikt de aanwijzingen te volgen!



Wanneer is er nu wel nut voor het Windows schijfbeheer? U kunt zien hoe Windows uw bestanden opslaat. In de afbeelding hierboven ziet u NTFS staan. Dat is goed. Staat er bijv. FAT of FAT32, dan is het verstandig die schijven te converteren naar NTFS. Dat kan Windows wel met het meegeleverde programma 'convert'. Let op, dit is éénrichtingverkeer; met behoud van de bestanden. Terug kan niet!

Een ander mogelijk nut is het partitioneren en herformatteren van een externe (USB-)harde schijf. Tot op heden worden die, vanwege het gebruiksgemak - en dus niet uit beveiligingsoverwegingen - vaak als FAT32-geformatteerd afgeleverd. Wil ik mijn data ook beveiligd, aan een gebruiker gekoppeld, op de externe harde schijf hebben dan is daar minimaal NTFS-formattering voor nodig. Maar om dat goed te regelen hebt u gedegen kennis van het rechtensysteem van NTFS nodig en dat bevordert de verkoop van externe harde schijven niet.

Een willekeurige FAT32-harde schijf kan iedereen meenemen en uitlezen. Tenzij u gebruik maakt van encryptie van de gegevens. En daarvoor is weer extra (aan te schaffen) software nodig.



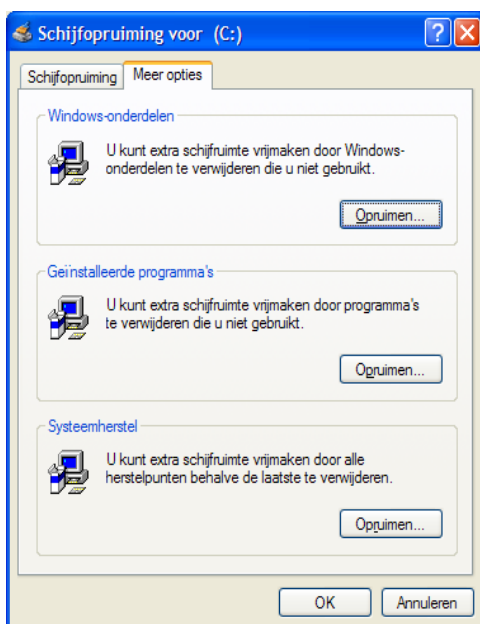
Schijfdefragmentatie

De defragmentatie van Windows deugt. Daarvoor een ander pakket gebruiken of aanschaffen is niet nodig.

Het kan voorkomen dat u defragmentatie wilt uitvoeren en een melding krijgt dat er te weinig ruimte is. U kunt doorzetten, maar de defragmentatie zal nog langer dan normaal gaan duren.

Verstandiger is het eerst ruimte te maken. Defragmentatie heeft volgens eigen zeggen minimaal 15% schijfruimte nodig. Overigens moet u bij minder dan 10% vrije ruimte op de systeemschijf rekening gaan houden met problemen met Windows zelf.

Hoe maakt u ruimte? Door rotzooi en/of prullaria op te ruimen!

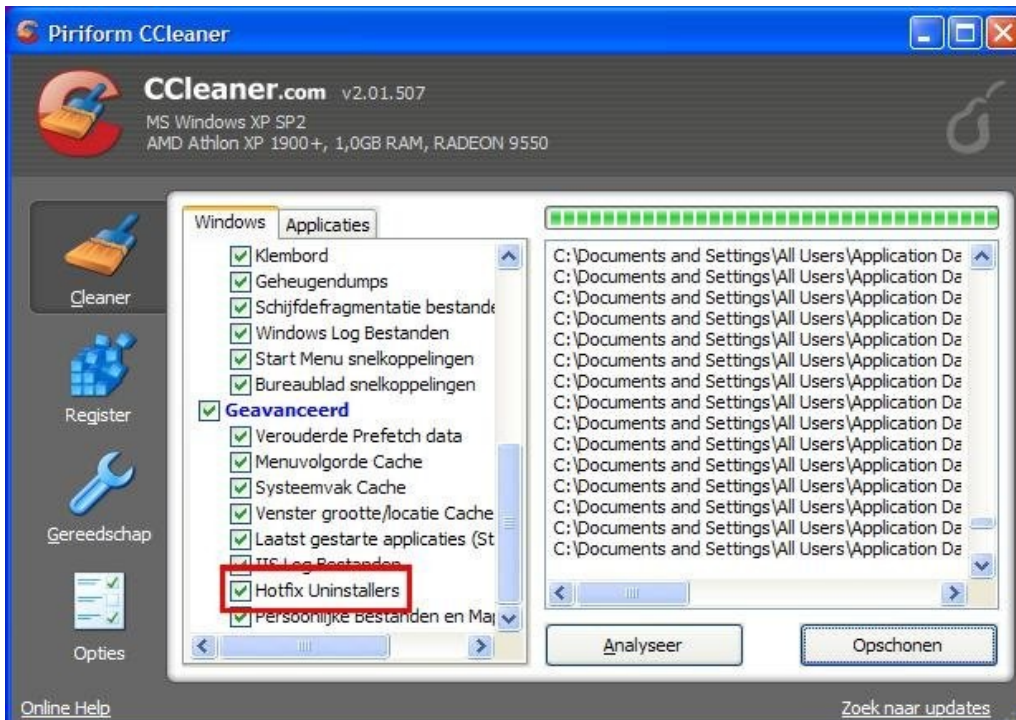


Begin eerst met weg te gooien wat u niet nodig hebt. Dat kan dus ook de Hibernat.fil zijn die een gevolg is van de slaapstand van Windows. Dan gaan we *schijfopruiming* doen met windows. Onder start – all programma's – bureau-accessoires – Systeemwerkset vindt u Schijfopruiming. Die heeft nog een tweede tabblad *Meer opties* waar u onderaan kunt kiezen voor het opruimen van alle oude *stelsystemherstelpunten*, behalve de laatste. Stelsysteemherstel gebruikt flink wat ruimte op de harde schijf, dus dat is een mooie optie om ruimte vrij te maken.

Dan kunnen de *Prullenbak* eens bekijken en die legen indien nodig. Maar ook kunnen we de gereserveerde ruimte voor de prullenbak aanpassen. Rechtsklik de prullenbak, kies voor eigenschappen en pas de grootte aan.

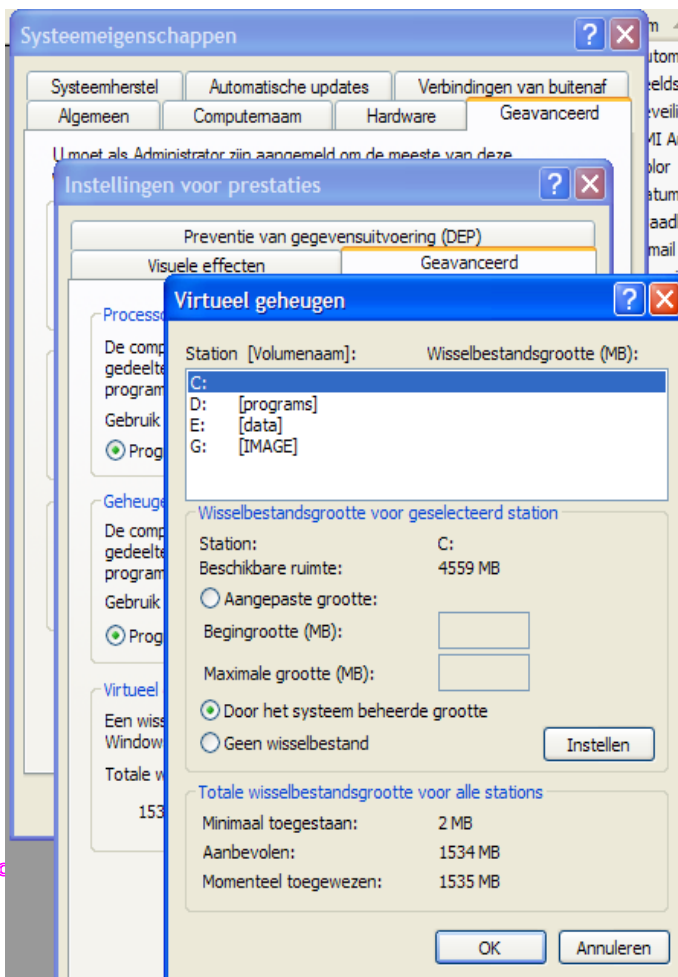
Dan wordt het tijd om Ccleaner (www.filehippo.com) aan te roepen. In de

geavanceerde sectie vinden we een interessante optie:



Hoewel in het voorbeeld hierboven alle geavanceerde opties zijn aangevinkt, raad ik dat niemand in eerste instantie aan. Behalve de optie met het rode vak omlind! Na een eerste opruiming kan het geen kwaad meteen een tweede te doen om te zien of er nog iets is blijven hangen.

Indien we nog steeds te weinig ruimte hebben om te defragmenteren, kunnen we ook nog de grootte van het virtuele geheugen (pagefile.sys), ook wel wisselbestand genoemd, verkleinen. Desnoods helemaal verwijderen; maar dan wordt de defragmentatie wel erg traag.



Verkleinen gaat als volgt:

Start – Configuratiescherm –
Systeem – Geavanceerd – Prestaties –
Instellingen ... - Geavanceerd –
onderste sectie: virtueel geheugen.

Hier zien we opnieuw een voordeel van meerdere partities. We hoeven niet per se het wisselbestand op de systeemschijf te hebben. Ook zien we dat we zonder wisselbestand ook nog kunnen werken. Geen wisselbestand maakt windows wel trager. Als we de ruimte echt nodig hebben zetten we het wisselbestand geheel uit.

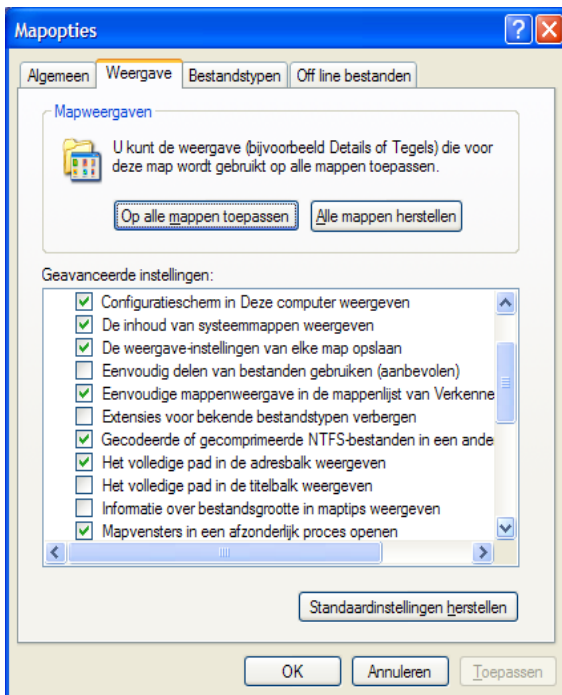
Andere opties die nog open staan om ruimte te maken is het deïnstalleren van software die nauwelijks gebruikt wordt of makkelijk opnieuw van internet kan worden gehaald, zoals, Adobe Reader, OpenOffice,

HitmanPro etc. Nog een mogelijkheid is zoeken naar gecomprimeerde-, tekst- en internetbestanden (.zip; .txt; .htm; .html). Kies in het zoekresultaatvenster voor de detailweergave en sorteer op Mapnaam. Honderden zo niet duizenden bestanden zullen gevonden worden. Nadeel is dat die tekst- en internetbestanden i.h.a. klein zijn. Maar wie het kleine niet eert ...

Vee; tekstbestanden kunnen gewist worden. Kijk in eerste instantie naar de programmamappen. Veel geïnstalleerde programma's worden weggeschreven met allerlei mogelijke talen. Bijv. Picasa. U zult zien dat er in 12 of meer talen tekst- en htmlbestanden zijn. Die kunnen gewist worden, behalve natuurlijk van de taal die u gebruikt. Ook kunnen alle Eula.txt-bestanden gewist worden. Maar meestal moet u wat kunstgrepen uithalen om het recht te krijgen om ze mogen wissen. Alles dat deel uit lijkt te maken van overeenkomsten, helpbestanden, gebruikershandleidingen etc. kan evt. gewist worden. Let op: wat gewist wordt, komt weer in de prullenbak terecht!

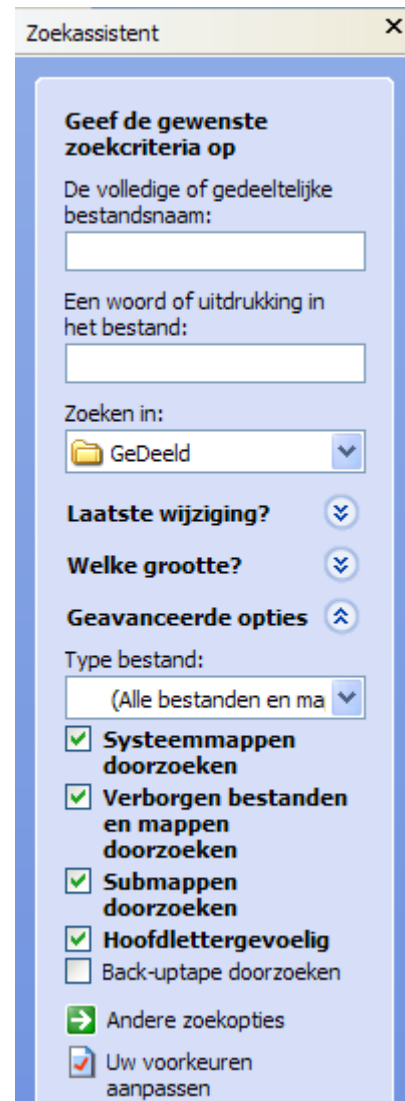
EHBO

Zien we alles?



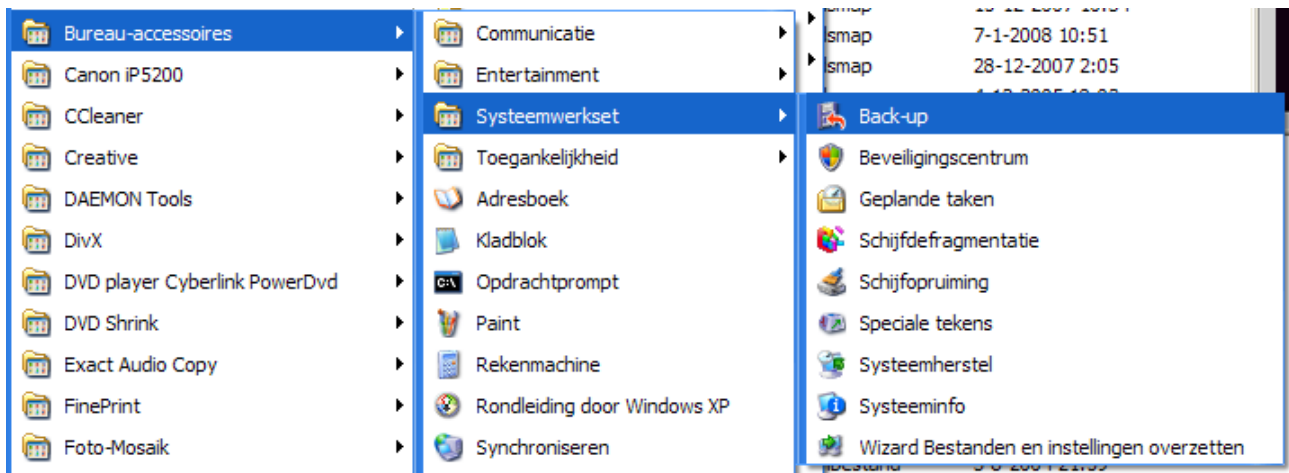
Wanneer we ons systeem willen beheren is het van belang dat we alles zien. Echter, om de gebruiker niet lastig te vallen met allerlei moeilijke zaken is dat meestal standaard uitgeschakeld.

Om te zorgen dat we alles zien gaan we als volgt te werk. We openen een verkennervenster en gaan daarin naar het menu Extra en kiezen onderaan voor *mapopties*, tabblad Weergave, bijna helemaal onder-aan moet je een vinkje zetten bij Verborgen mappen en bestanden zetten. Als dat vinkje niet aan staat, zal een zoekactie ook geen verborgen bestanden vinden, ook al staat de optie zoeken naar verborgen bestanden wel aan.



Ontvlooiën

Vooraf: het ontvlooiën van een pc kost tijd, veel tijd. Maar soms hebt u geluk en valt het mee. In het algemeen kost het minder tijd om Windows opnieuw te installeren. Of nog minder tijd wanneer u een *image* terug kunt zetten. Met dien verstande dat alle belangrijke gegevens als wachtwoorden voor de ADSL-verbinding en emaildiensten bekend zijn, alsmede alle noodzakelijke en recente drivers voor de aangesloten hardware. Staat alles op één grote partitie dan loopt u een groot risico dat u al uw brieven, mails, foto's, muziek etc. kwijtraakt! Tenzij u een backup maakt van alles dat u niet kwijt wilt raken.



Het kan geen kwaad om met het eigen Back-up-programma van windows reservekopieën te maken. Als u geen extra geld uit wilt geven is het de enige optie, maar zeker niet de handigste of prettigste.

In een test van het computerblad Computer!Totaal van februari 2008 zijn Back-up pakketten onder de loep genomen. De aanbeveling 'Best Getest' krijgt het pakket: True Image Home 11 van Easy Computing (alias: Acronis). Het maakt images die als back-up gebruikt kunnen worden. En omdat het een imager is kunnen die images ook gebruikt worden bij computerherstel of na het vergroten van een steempartitie.

Vermoedt u een besmetting van het een of ander dan kunt u een aantal dingen doen.

Neem in kijkje in taakbeheer, door Ctrl+Alt+Del te drukken en te kiezen voor taakbeheer; tabblad Prestaties. Wacht even en kijk hoeveel procent activiteit er is. Is dat meer dan pakweg 10% dan is er wel een reden om uit te zoeken waar al die activiteit dan aan besteed wordt.

Daarvoor schakelen we over naar het tabblad Processen om de lijst met processen eens kritisch te bekijken.

Door daar op de knop CPU te klikken kunnen we de lijst zodanig sorteren dat we snel zicht krijgen op welke processen vaak activiteit vertonen. Houd het even in de gaten en noteer de namen van de actieve processen.

Het venster taakbeheer kan nu evt. gesloten worden. We openen een venster op de harde schijf waar Windows geïnstalleerd is (meestal C:). We klikken op de knop zoeken, zorgen dat er ook in verborgen mappen en submappen gezocht kan worden en voeren in het bovenste zoekvak de naam van het gezochte proces in.

Wordt er niets gevonden, dan controleren we de naam nog eens goed. Was die

juist, dan gaan de alarmbellen rinkelen, want hier is een proces dat zich erg goed weet te verstoppert. Weten we dat nu al zeker? Nee, want het kan nog op een andere schijf, in een andere map zitten.

Wel gevonden, dan gaan we de eigenschappen van het bestand nader bekijken. Komt het van een 'vertrouwde' firma, dan laten we het even voor wat het is en richten onze aandacht op het volgende bestand.

Bij twijfel over de betrouwbaarheid gaan we de rest van de wereld maar eens raadplegen met een zoekactie op internet. Dus start uw internet browser en geef in een zoekvenster de naam van het verdachte programma.

Is het een virus, dan zullen in de lijst met gevonden *sites* de namen van bekende antivirussoftware leveranciers opduiken. U kunt ook eens zoeken bij:

www.waarschuwingsdienst.nl

www.virusalert.nl

www.antispywareoffensief.nl (stel je vragen in het forum; hier kun je ook hulp vragen voor de uitvoer van HijackThis)

www.seniorweb.nl

www.hijackthis.nl

Is het een recente besmetting probeer dan via Systeemherstel terug te gaan naar een vroegere datum toen het systeem nog probleemloos werkte. U vindt systeemherstel onder Bureau-accessoires – Systeemwerkset.

Virusscanner

Hebt u een virusscanner besef dan dat het automatisch ontvangen van de nieuwe virusdefinities niet hetzelfde is als het automatisch ongedaan maken van virussen. Virusscanners kunnen in het algemeen ingesteld worden om met regelmaat een complete scan te doen. Raadpleeg daarvoor de handleiding. In geval van een verdenking moet u de scan handmatig starten in zijn scherpste instellingen. Ziet u in de configuratie van de scanner iets staan met Heuristic of Heuristiek, vink dat dan aan. Veel automatische scans kijken oppervlakkig naar een bestand, terwijl een (handmatige) nauwkeuriger analyse soms tot andere bevindingen komt. Maar zo'n nauwkeuriger kijk kost aanmerkelijk meer tijd dan een snelle scan. De oppervlakkige instelling is gekozen door de fabrikant omdat de PC anders veel te traag wordt.

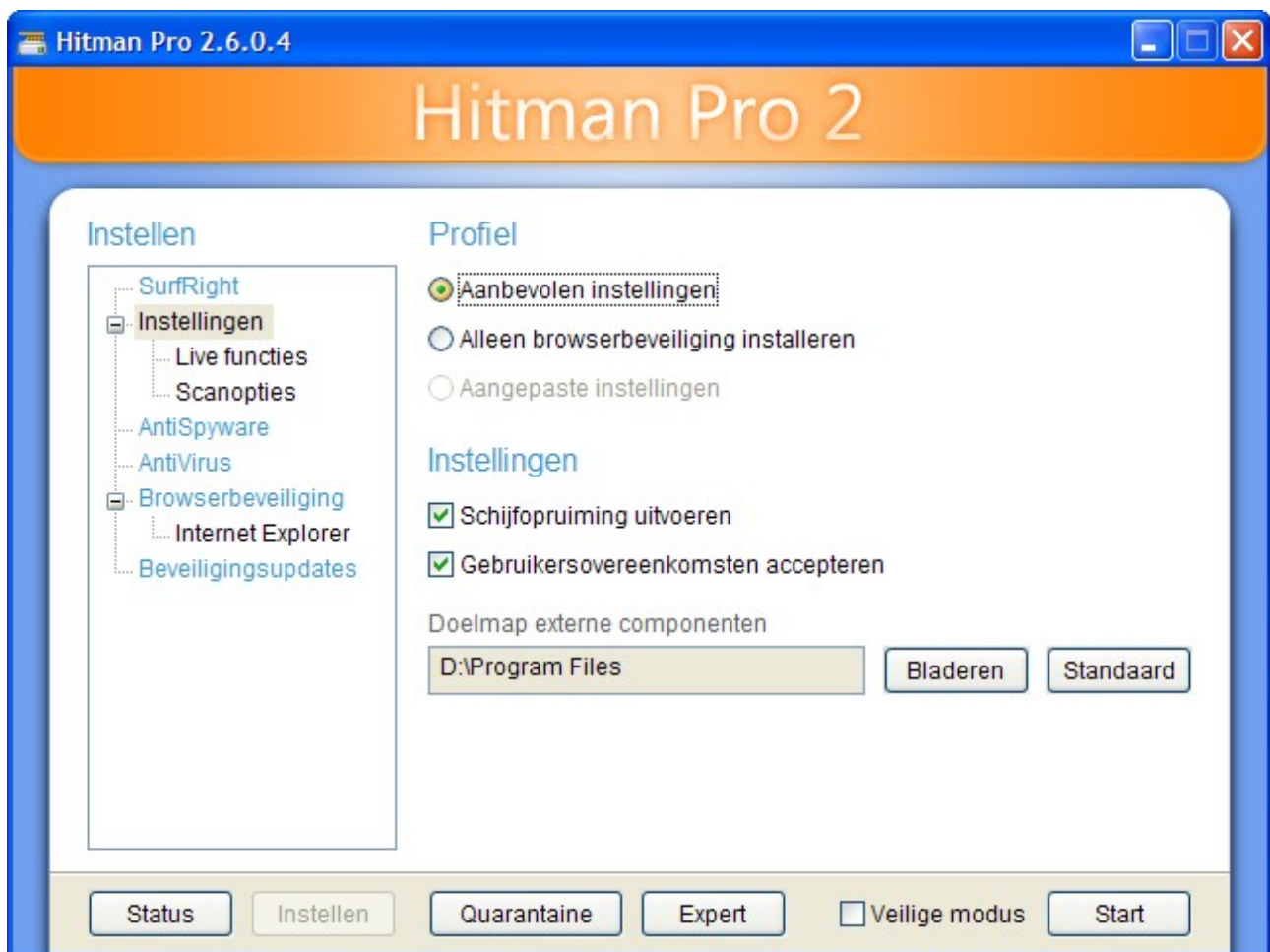
De scan moet het liefst worden uitgevoerd met zo min mogelijk lopende processen. Daarom doet u er goed aan de PC opnieuw op te starten en tijdens het opstarten een aantal keren op functietoets F8 te drukken. Windows komt dan naar voren in de veilige modus, met een zwart scherm met witte letters. Bijna bovenaan ziet u veilige modus met netwerk staan. Kies die optie, zodat u nog steeds kunt browsen op internet of programma's kunt downloaden. Eenmaal opgestart start u de virusscanner in zijn strengste variant. U kunt nu gaan afwassen, boodschappen doen, de krant lezen etc. Werp af en toe een blik op het scherm om te zien of er een melding is. Lees die nauwkeurig en volg evt. aanwijzingen op. Is er een aanbod om een verdacht item in quarantaine te plaatsen, kies daar dan voor. Sommige bestanden kunnen niet in quarantaine geplaatst worden. U kunt overwegen het dan te wissen. Wissen is echter ons 'laatste redmiddel'. Maar bedenk dan dat het wel eens om een onmisbaar

onderdeel van windows kan gaan. Noteer alleen de naam van het bestand. Klik (nog) niet op uitvoeren of Ok of accepteren. Doe eerst een normale zoekactie naar het bestand. Worden er meerdere versies op verschillende plaatsen gevonden kijk dan nauwkeurig naar de datum en de grootte. De oudere versies kunnen meestal wel gemist worden. Is dit de versie die gemeld wordt, dan kunt u het bestand (enigszins) gerust wissen. Maar liever kiezen we voor quarantaine. Hernoemen van de bestandsnaam kan ook een optie zijn. Ik hernoem een bestand altijd naar naam.ext(ensie).vals. Dat zoekt makkelijk.

Daarna zoekt u een online virusscanner op, bijvoorbeeld HouseCall van de firma TrendMicro. Er zijn meer gratis te gebruiken online virusscanners. Zie bijv. www.virusalert.nl. Met de online virusscanner doet u nog eens een scan van het hele systeem. Overtuig u ervan dat de online scanner niet alleen de problemen noteert, maar ook ongedaan maakt.

De volgende en laatste oplossing kan ook gebruikt worden als u nog geen virusscanner hebt. Download en installeer het programma HitmanPro van www.hitmanpro.nl.

Stel ook meteen het SurfRight gebruik in. Dit voorkomt dat u met beheerderrechten surft en emailt. HitmanPro (HP) biedt o.a. het tijdelijk gebruik van de virusscanner NOD32 aan. U bent dus eventjes gered en de scanner is van goede kwaliteit.



Er is bij de instellingen van HP een vinkvakje om alle gebruiksrechtsovereenkomsten te accepteren. Vink dat aan en u kunt weglopen terwijl HP zijn werk doet. HP kent zelfs de mogelijkheid om na het scannen de computer automatisch uit te

schakelen. Ideaal voor de vrijdagavond om voor het naar bed gaan de scan te beginnen en rustig te kunnen gaan slapen. De volgende morgen is het scanrapport te vinden in de programmamap van HP.

HitmanPro is een schil om een aantal bekende programma's heen. Elk met hun eigen specialiteit. Enkele van die programma's mogen tijdelijk gebruikt worden. Andere laten alleen een probleem zien (herkenning) maar verwijderen het niet. Webroot SpySweeper bijvoorbeeld.

HP wordt goed onderhouden en komt regelmatig met nieuwe voorzieningen. U mag HP gratis gebruiken, maar als u er goed mee geholpen bent neem dan de kleine moeite een bedrag(je) aan de maker over te maken. Daarmee helpt u uzelf (en anderen) ook weer in de toekomst.

Sites

McAfee SiteAdvisor	http://www.siteadvisor.com
Gratis Virusscanners	http://www.gratisvirusscanners.nl/
Antivir	http://www.free-av.com
AVG	http://free.grisoft.com/doc/1
HouseCall	http://housecall.trendmicro.com/
HitmanPro	http://www.hitmanpro.nl
CrapCleaner	http://www.ccleaner.com
Andere Software	http://www.filehippo.com

Digitale Klusjesman www.exeit.com

Firewall

De FireWall (FW) voorkomt problemen met indringers. Waar een virusscanner de indringers te lijf gaat probeert de FireWall juist indringers buiten de deur te houden.

Dat is geen makkelijke taak want gebruikers gebruiken niet allemaal dezelfde programma's. Veel producenten proberen de klant enthousiast te maken en te houden voor hun programma's door ze op de hoogte te houden van verbeteringen en volgende versies. Maar daarvoor moet wel er een verbinding zijn. Sommige producenten gaan zover dat ze op de hoogte gehouden willen worden van elk bestand dat door hun product geproduceerd werd/wordt.

Zodra bijvoorbeeld een Word-bestand geopend wordt wordt er gekeken of er een verbinding mogelijk is met één van de vele servers van Microsoft.

Bovenstaande ging – in het gunstigste geval – over verbindingen van binnen naar buiten. Maar er zijn ook lieden die heel nieuwsgierig zijn en gewoon willen kijken of ze van buiten naar binnen kunnen kijken. En zonder firewall is dat helemaal niet zo moeilijk.

In algemene zin krijgen we te maken met de protocollen (talen) die gebruikt worden voor het *contact* tussen computers – lokaal en via internet – en voor het contact tussen programma's en bestanden.

Van de 64-duizend poorten (deuren) die de gemiddelde PC heeft zijn pakweg de eerst duizend gaanstaat, zal een zoekactie ook geen verborgen bestanden vinden, ook al staat de optie zoeken naar verborgen bestanden wel aan. oed gedefinieerd. Goed gedefinieerd in die zin dat er goede afspraken zijn gemaakt over door wie, wanneer en hoe die deuren gebruikt moeten worden. Het grootste deel van de andere poorten is voor nieuwe software en het staat een ieder vrij daar gebruik van te maken.

Zo worden de poorten 25 en 110 vaak voor de emaildiensten gebruikt; de poorten 137 -139 en 441 worden voor de Bestands- en printerdeling van Microsoft Windows gebruikt. In een thuisnetwerk bijvoorbeeld.

Poort 80 zou iedereen moeten kennen als de standaarddeur voor internetbrowsers. Om te kunnen surfen op internet moet u dus verkeer via deze poort toestaan! En voor veilig internetbankieren is poort 443 nodig want die wordt voor HTTPS gebruikt.

Met het gebruik van een goede firewall wordt het mogelijk om het verkeer van binnen naar buiten te volgen en te regelen. Dat wil zeggen dat alles dat van binnen naar buiten wil bekeken wordt. Dat lijkt nutteloos en overbodig. Maar is er eenmaal iets kwaadaardigs binnen, dan wil dat vaak de gevonden resultaten versturen. *De bedoeling van de firewall is nu juist dat verkeer te betrappen en te verhinderen.*

Een firewall die vrij is voor persoonlijk gebruik is de Sunbelt Kerio Personal Firewall (voorheen gewoon Kerio PF), te vinden op www.sunbelt-software.com. Een andere is ZoneAlarm van www.zonelabs.com.

In het vervolg houden we ons bezig met de Sunbelt Kerio PF.

Met de zoektermen "Sunbelt Kerio kpf firewall" in Google doken er meerdere pagina's op, waarvan de tweede me het meest voor de hand leek te liggen vanwege de naam aan de onderkant "Kerio-Download.cfm".



Het Internet

Tip: [Alleen in het Nederlands zoeken](#). U kunt uw zoektaal bepalen in [Voorkeuren](#)

[Free Firewall Download - Kerio Firewall Replacement](#) ✓

Sunbelt Personal Firewall 4 is called the best **personal firewall** security ... If you're looking for the free **Kerio Firewall** or a replacement for the Sygate ...

www.sunbelt-software.com/Kerio.cfm - 26k - [In cache](#) - [Gelijkwaardige pagina's](#)

[Free Firewall Download - Kerio Firewall Replacement](#) ✓

Sunbelt Kerio Personal Firewall 4 can run in a free mode vs. a full (paid) mode. Install it now, and for the first 30 days it will run in 'full' mode. ...

www.sunbelt-software.com/Kerio-Download.cfm - 24k - [In cache](#) - [Gelijkwaardige pagina's](#)

[[Meer resultaten van www.sunbelt-software.com](#)]

Download Sunbelt Personal Firewall™

Top-Rated PC Firewall - Rock-Bottom Price

Keep the bad guys out of your PC with the Sunbelt Personal Firewall.

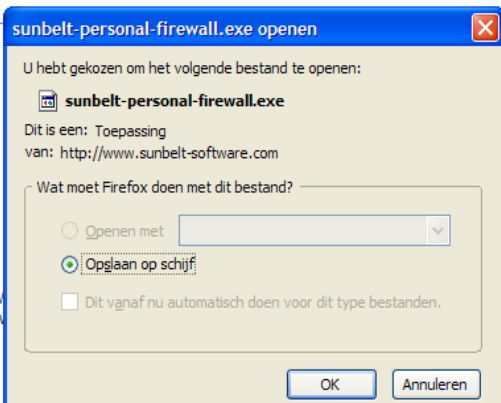
Why do you need a firewall? Together with antivirus and antispyware, it is an absolute must to protect your PC. And the Windows Firewall in WinXP isn't checking any outgoing traffic from your PC!

Free 30 day full featured evaluation

For Windows - 2000 Professional (desktop version) - XP Home - XP Professional - XP Media Center Edition	Download Sunbelt Personal Firewall (6.48MB)
---	--

Sunbelt Kerio Personal Firewall 4 can run in a free mode vs. a full (paid) mode. Install it now, and for the first 30 days it will run in 'full' mode. After that, it shuts down selected features, but will continue to run in 'free' mode".

Note: Do not "Run", select "Save". Download to your desktop and then double-click to install.



De goede verstaander leest hier dat de eerste 30 dagen de firewall in zijn volledige versie met allerlei extraatjes zal lopen. Na die dertig dagen blijft de vrije versie aanwezig en die beperkt zich puur tot de firewall. Voor ons doel dus prima.

Ze adviseren zelf om te downloaden en niet te 'runnen'. Adviezen zijn er niet om in de wind te slaan en dus volgen we gehoorzaam de aanwijzingen.

Na het downloaden kijken we even onder "support" en zien daar een vraag staan over de volledige *Stealth modus*. Stealth maakt de PC onzichtbaar voor de buitenwereld. De aanpassing hiervoor staat in de volgende afbeelding, i.c. de geselecteerde regel.

Omschrijving	Vertrouwd		Internet		Log	Waarsc...
	Inkomend	Uitgaand	Inkomend	Uitgaand		
c:\windows\system32\lsass.exe	vraag	sta toe	verbied	vraag	-	-
c:\windows\system32\winlogon.exe	vraag	sta toe	verbied	vraag	-	-
c:\windows\system32\userinit.exe	vraag	sta toe	verbied	vraag	-	-
c:\windows\system32\svchost.exe	sta toe	sta toe	verbied	sta toe	-	-
netbios	sta toe	sta toe	verbied	verbied	-	-
c:\windows\system32\logagent.exe	sta toe	sta toe	verbied	sta toe	-	-
c:\program files\realvnc\vnc4\winvnc4.exe	sta toe	sta toe	verbied	verbied	-	!
c:\windows\system32\rdpclip.exe	sta toe	sta toe	verbied	verbied	-	-
d:\program files\mozilla firefox\firefox.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\avg\avg\avginet.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\avg\free\avgemc.exe	sta toe	sta toe	verbied	sta toe	-	-
c:\program files\outlook express\msimn.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\veset\nod32km.exe	sta toe	sta toe	verbied	verbied	-	-
c:\program files\windows media player\wmplayer.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\hitman pro\hitmanpro2.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\musicmatch\musicmatch jukebox\mmbj.exe	sta toe	sta toe	vraag	vraag	-	-
c:\windows\system32\vmnat.exe	sta toe	sta toe	verbied	sta toe	-	-
c:\windows\pchealth\helpctr\binaries\helphost.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\spyware doctor\swdoctor.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\spyware doctor\update.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\avg\anti-spyware 7.5\avgas.exe	sta toe	sta toe	verbied	sta toe	-	-
c:\program files\google\google earth\googleearth.exe	sta toe	sta toe	verbied	sta toe	-	-
d:\program files\microsoft file transfer manager\transfermgr.exe	sta toe	sta toe	verbied	sta toe	-	-
Elke andere applicatie	verbied	sta toe	verbied	vraag	-	-

Van belang is hier dat zowel in de sectie Vertrouwd als onder het kopje Internet de instelling **verbied** staat onder Inkomend. Klikken voor de juiste instelling

Om te zien of de stealth-modus werkelijk doet wat 'ie moet doen gaan we naar de site <http://grc.com> waar een schatkamer aan informatie op het gebied van veiligheid te vinden is. We gaan het programmaatje LeakTest downloaden en gebruiken.



In de afbeelding zien we ook meteen dat de KerioPF begint te brullen als we LeakTest starten. LeakTest wil namelijk van binnen naar buiten toe.

Voor de test is het van belang dat bij het aanslaan van de firewall steeds met Nees geantwoord wordt.

Zeggen we consequent dat de FW geen verbinding naar buiten toe moet staan en alle andere instellingen deugen ook, dan krijgen we de volgende gunstige mededeling te zien.

Het log-bestand dat hieronder is afgebeeld laat zien dat de verbindingen met grc.com inderdaad niet zijn toegelaten.

De 'punten op afstand:631' (poort 631) is voor de netwerkprinter en die moet wel doorgelaten worden anders wordt de printer niet gevonden en kan er niets geprint worden.



Lijn	Aan...	Datum	Omschrijving	Applicatie	Richting	Lokaal punt	Punt op afstand	Protocol	Actie
8975	1	16/Apr/2007 14:48:36	Unopened port	n/a	in	10.0.0.6:1531	www.grc.com:https	TCP	denied
8976	1	16/Apr/2007 14:48:40	Unopened port	n/a	in	10.0.0.6:1531	www.grc.com:https	TCP	denied
8977	1	16/Apr/2007 14:48:54	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
8978	1	16/Apr/2007 14:49:03	Unopened port	n/a	in	10.0.0.6:1537	www.grc.com:https	TCP	denied
8979	1	16/Apr/2007 14:49:04	Unopened port	n/a	in	10.0.0.6:1538	grtech.com:https	TCP	denied
8980	1	16/Apr/2007 14:49:04	Unopened port	n/a	in	10.0.0.6:1539	www.grc.com:https	TCP	denied
8981	1	16/Apr/2007 14:49:05	Unopened port	n/a	in	10.0.0.6:1540	grtech.com:https	TCP	denied
8982	1	16/Apr/2007 14:49:08	Unopened port	n/a	in	10.0.0.6:1533	www.grc.com:https	TCP	denied
8983	1	16/Apr/2007 14:49:24	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
8984	1	16/Apr/2007 14:49:55	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
8985	1	16/Apr/2007 14:50:26	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
8986	1	16/Apr/2007 14:50:39	Unopened port	n/a	in	10.0.0.6:1542	www.grc.com:https	TCP	denied
8987	1	16/Apr/2007 14:50:40	Unopened port	n/a	in	10.0.0.6:1543	www.grc.com:https	TCP	denied
8988	1	16/Apr/2007 14:50:40	Unopened port	n/a	in	10.0.0.6:1545	grtech.com:https	TCP	denied
8989	1	16/Apr/2007 14:50:41	Unopened port	n/a	in	10.0.0.6:1546	www.grc.com:https	TCP	denied
8990	1	16/Apr/2007 14:50:42	Unopened port	n/a	in	10.0.0.6:1547	grtech.com:https	TCP	denied
8991	1	16/Apr/2007 14:50:58	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
8992	1	16/Apr/2007 14:51:29	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
8993	1	16/Apr/2007 14:52:00	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
8994	1	16/Apr/2007 14:52:19	Unopened port	n/a	in	10.0.0.6:1548	www.grc.com:https	TCP	denied
8995	1	16/Apr/2007 14:52:20	Unopened port	n/a	in	10.0.0.6:1549	www.grc.com:https	TCP	denied
8996	1	16/Apr/2007 14:52:20	Unopened port	n/a	in	10.0.0.6:1551	grtech.com:https	TCP	denied
8997	1	16/Apr/2007 14:52:21	Unopened port	n/a	in	10.0.0.6:1552	www.grc.com:https	TCP	denied
8998	1	16/Apr/2007 14:52:22	Unopened port	n/a	in	10.0.0.6:1553	grtech.com:https	TCP	denied
8999	1	16/Apr/2007 14:52:32	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9000	1	16/Apr/2007 14:52:43	Unopened port	n/a	in	10.0.0.6:1554	www.grc.com:https	TCP	denied
9001	1	16/Apr/2007 14:52:43	Unopened port	n/a	in	10.0.0.6:1555	www.grc.com:https	TCP	denied
9002	1	16/Apr/2007 14:52:44	Unopened port	n/a	in	10.0.0.6:1557	grtech.com:https	TCP	denied
9003	1	16/Apr/2007 14:52:45	Unopened port	n/a	in	10.0.0.6:1558	www.grc.com:https	TCP	denied
9004	1	16/Apr/2007 14:52:46	Unopened port	n/a	in	10.0.0.6:1559	grtech.com:https	TCP	denied
9005	1	16/Apr/2007 14:53:04	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9006	1	16/Apr/2007 14:53:35	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9007	1	16/Apr/2007 14:54:07	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9008	1	16/Apr/2007 14:54:38	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9009	1	16/Apr/2007 14:55:09	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9010	1	16/Apr/2007 14:55:40	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9011	1	16/Apr/2007 14:56:10	Unopened port	n/a	in	10.0.0.255:netbios-dgm	klusjesman.exeit.com:netbios-dgm	UDP	permitted
9012	1	16/Apr/2007 14:56:10	Unopened port	n/a	in	10.0.0.255:netbios-dgm	klusjesman.exeit.com:netbios-dgm	UDP	permitted
9013	1	16/Apr/2007 14:56:12	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9014	1	16/Apr/2007 14:56:43	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9015	1	16/Apr/2007 14:57:14	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9016	1	16/Apr/2007 14:57:46	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9017	1	16/Apr/2007 14:58:17	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9018	1	16/Apr/2007 14:58:48	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted
9019	1	16/Apr/2007 14:59:20	Unopened port	n/a	in	10.0.0.255:631	klusjesman.exeit.com:631	UDP	permitted

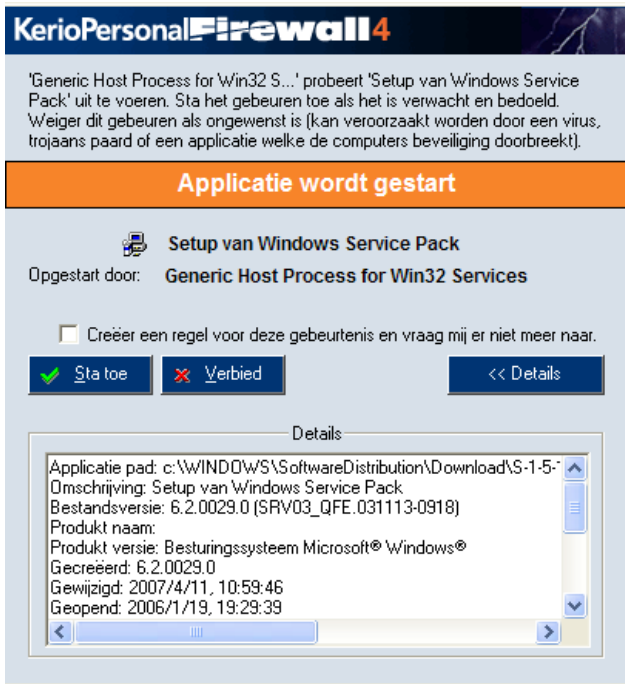
En de printer mag erdoorheen omdat we onder het tabblad Vertrouwd van de Netwerkbeveiliging hebben ingesteld dat dat IP-adres behoort tot het vertrouwde domein.

Vertrou...	Omschrijving	Adres / inbelnummer	Adapter
<input checked="" type="checkbox"/>	Loopback	127.0.0.1	... nvt ...
<input checked="" type="checkbox"/>	lokale netwerk	10.0.0.0 / 255.255.255.0	LAN-verbinding
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input checked="" type="checkbox"/>	Virtuele Echte Windows 166	10.0.0.166 / 255.255.255.0	... alle ...
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>	VMWAREtoestand	192.168.0.0 / 255.255.0.0	VMware Network Adapter VMnet1 VMware Network Adapter VMnet8
<input type="checkbox"/>			
<input type="checkbox"/>			
<input checked="" type="checkbox"/>	canon printer lokaal netwerk	10.0.0.177	... alle ...

De vermelding 'canon printer lokaal netwerk' is in feite overbodig en hier alleen voor de duidelijkheid aangebracht. 'Lokale netwerk' met het bereik 10.0.0.0/255.255.255.0 is voldoende om alle netwerkdonderdelen in het netwerk 10.0.0.x tot de vertrouwde zone te rekenen.



Voorbeeldafbeeldingen van de Kerio PF die aanslaat staan hieronder:



De FW reageert op het setup-proces van de Windows Updates die pakweg iedere week op woensdag binnenkomen. Aangezien dit een regelmatig terugkerende vraag is wordt hier een regel van gemaakt door een vinkje te zetten in het vakje bij "Creëer een regel voor deze gebeurtenis en vraag mij er niet meer naar." En dan op de [Sta toe](#)-knop te klikken.

Lees de hele tekst in het dialoogvenster van boven naar beneden!



Deze afbeelding staat ook hierboven in het plaatje van blz. 15 onderaan. De FW slaat alarm omdat de LeakTest-toepassing gestart wordt. Dit is een onbekend programma voor de FW en komt niet in zijn lijst van toepassingen/applicaties voor, want het is net gedownload en geïnstalleerd.

Dit is vermoedelijk éénmalig en dus wordt er alleen op de [Sta toe](#)-knop geklikt. Er wordt géén regel voor gemaakt omdat er geen vinkje bij de regel "Creëer een regel voor deze gebeurtenis en vraag mij er niet meer naar." wordt gezet.

Voor een soortgelijk verhaal over

ZoneAlarm verwijst ik naar:

<http://home.hccnet.nl/p.a.blok/veiligheid/zonelabs-firewall.pdf>

En voor andere onderdelen op het gebied van veiligheid

<http://home.hccnet.nl/p.a.blok/veiligheid/beveilig.html>

N.B. <http://home.hccnet.nl/p.a.blok/veiligheid/beveilig.html> was niet meer dan een lijst van punten die tijdens een soortgelijke cursus aan de orde kwamen, maar bevat wel interessante links.

Autostarters

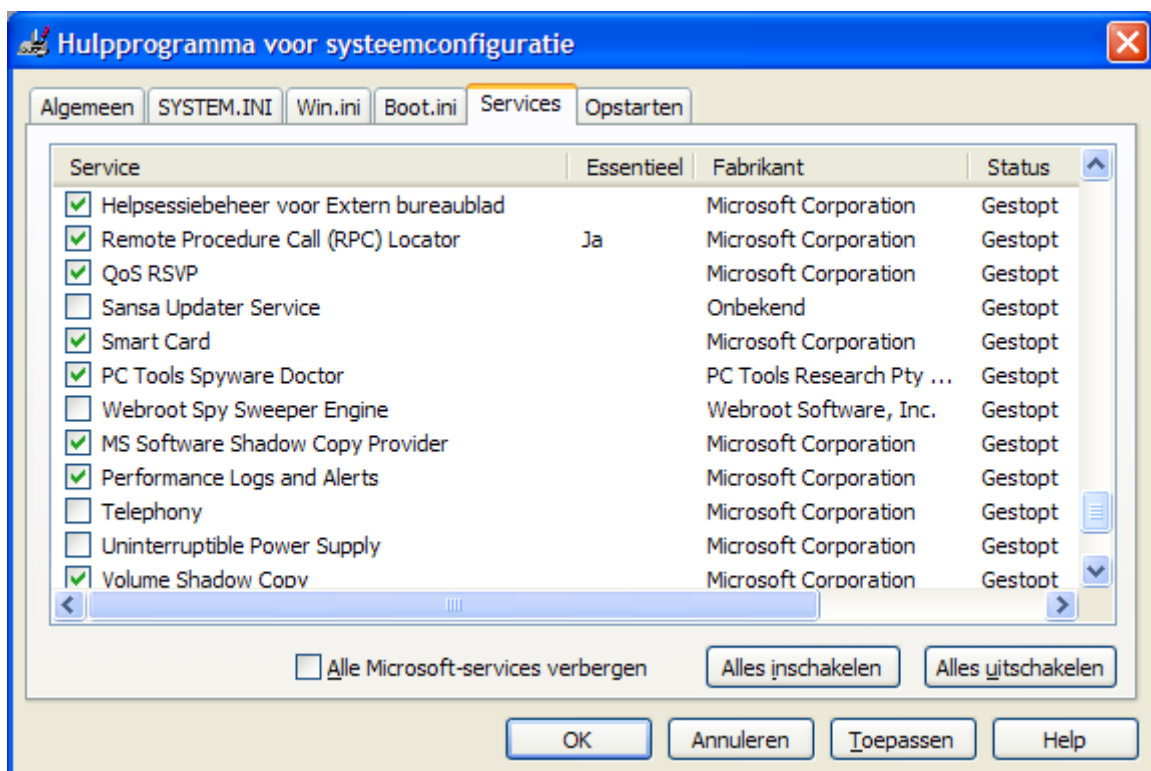
Autostarters zijn in het algemeen kleine programmaatjes die bij het starten van de PC ook gestart worden en dus in het geheugen geladen worden en processortijd in beslag nemen.

U zult begrijpen dat kwaadaardige programma's gebaat zijn bij een dergelijke autostart.

Maar de Virusscanner en de Firewall en allerlei andere noodzakelijke diensten moeten ook – liefst automatisch – gestart worden. Om enig zicht te krijgen op de autostarters kunnen we eens kijken naar het hulpprogramma “msconfig”.

Daarvoor gaan we naar de Startknop en kiezen in het menu voor Uitvoeren....

In de ruimte achter 'Openen:' typen we msconfig en geven een Enter. Msconfig zal gestart worden (wanneer de firewall alarm slaat het eenmalig toestaan). We klikken op het tabblad *Services*.



In de afbeelding is gesorteerd op Status; met een klik op de status-knop. Als het vertrouwen in Microsoft groot is kan men ervoor kiezen om alle Microsoft-services te verbergen. Dit suggereert dat alleen derden services leveren die in aanmerking komen om uitgeschakeld te worden. Met de knoppen naast het aanvinkvakje kan met één klik Alles ingeschakeld of Alles uitgeschakeld worden. Dit is meestal niet aan de orde.

In de afbeelding is gekozen om een aantal services uit te schakelen omdat ze

nutteloos zijn. In geval van problemen kunnen deze diensten weer gewoon ingeschakeld worden!

De Webroot SpySweeper-service is een restant dat door HitmanPro is meegekomen. Na 30 dagen vervalt de spysweeper dienst maar wordt dus nog steeds automatisch gestart. Overbodig, dus uitzetten.

Telephony-service lijkt overbodig want ik gebruik geen telefoonmodem of faxtoepassing meer.

Helaas heb ik geen uninterruptable power supply en een service op dat gebied kan ik dus wel ontberen. Ook werk ik niet met smart cards (soms bij draadloze netwerken als beveiliging gebruikt) en dan moet ik dus ook zonder die dienst wel kunnen computeren. Wel heb ik een Sansa mediaplayer maar ik wil absoluut niet dat dat kreng – Sansa updater service - om de haverklap naar zijn thuisbasis wil om te zien of er een nieuwere versie is – terwijl ik weet dat de leverancier van dit goede product ongelooflijk laks is op dat vlak. Iets dat deugt kan niet snel beter. Dus schakel ik deze dienst ook uit.

Hoewel er verhalen gaan dat de indexing service van Microsoft best uitgeschakeld kan worden en dat daarmee snelheidswinst geboekt kan worden, waarschuw ik tegen het uitschakelen van deze dienst.

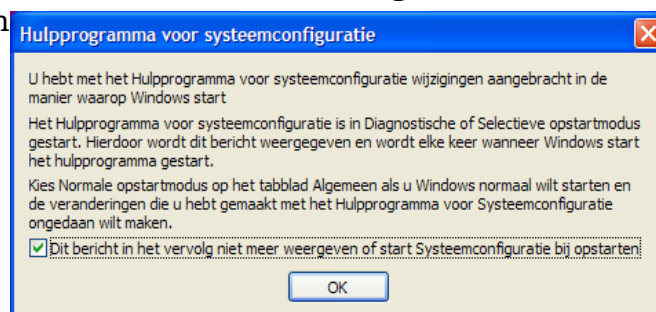
Houdt u alleen bezig met duidelijk herkenbare diensten. Zo is het niet slim om de Google updater service uit te schakelen als u bijvoorbeeld met Picasa of Google Earth werkt.

Daarentegen kunnen sommige diensten van grafische kaarten als ATI en NVIDIA na installatie van de kaart best uitgeschakeld worden. Het is echt niet nodig dat die toepassingen voor de configuratie van die kaarten iedere keer opnieuw in het geheugen geladen worden om hun diensten permanent aan u beschikbaar te maken.



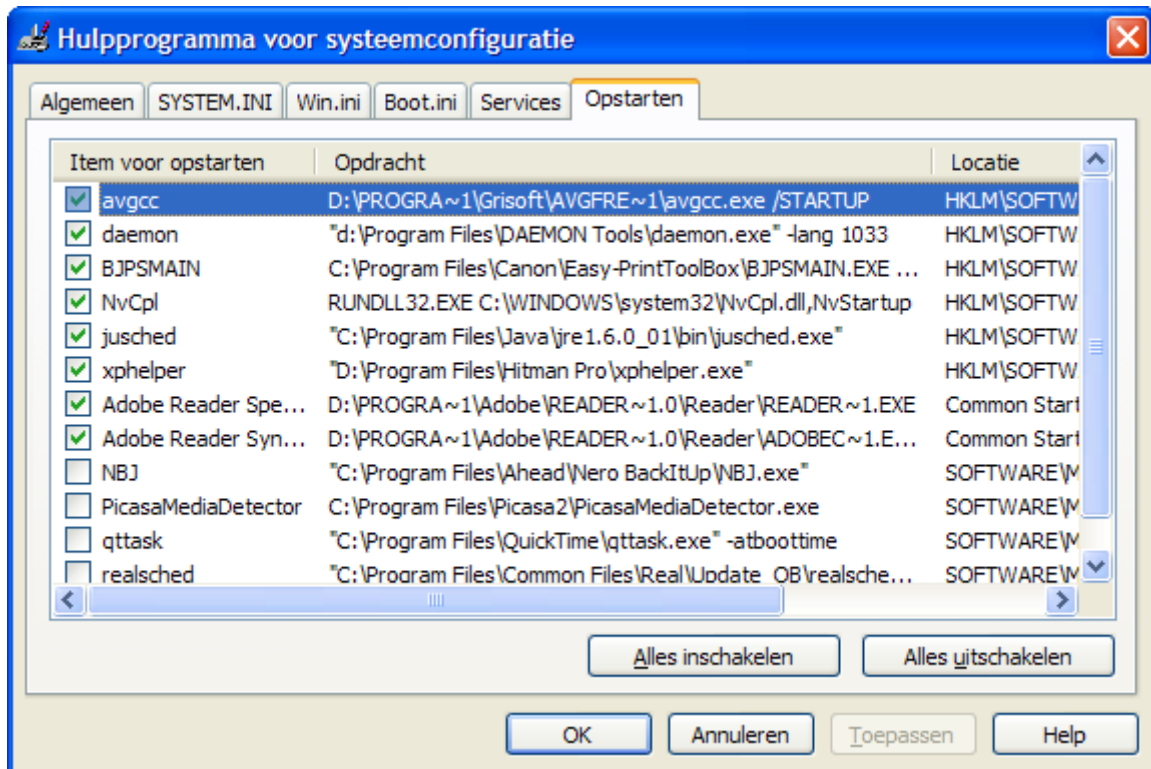
Bij twijfel slechts één item veranderen opnieuw opstarten. Gebeuren er rare dingen dan de zaak terugdraaien.

Na het opnieuw opstarten moeten we dan nog vertellen dat de PC voortaan met de wijzigingen voortaan gewoontje mag starten. Dat doen we door een vinkje onderaan in het dialoogvenster te zetten.



Wat we nog niet gezien hebben is het laatste tabblad van msconfig genaamd Opstarten. Ook daar staan nog wat autostarters die we met een gerust hart uit kunnen zetten. Daarbij valt te denken aan de PicasaMediaDetector en de 'handigheidjes' van Real Media, Apple iTunes,

Apple Quick Time etc.



Omdat de locatie niet zo belangrijk is, is de kolomrand van de kolom Opdracht verder opgeschoven zodat men beter kan zien over welk programma het gaat. De NBJ, of Nero BackItUp is een kleine treiteraar waarvan ik slechts op deze manier kan ontkomen. Wilt u het NBJ programma gebruiken dan moet u het beslist aan laten staan.

Picasa vertel ik zelf wel wanneer ik een CD of DVD met foto's inleg. Qttask en realsched zijn ronduit vervelend en dienen mij niet (genoeg). Zou u dagelijks gebruik maken van de toepassingen dan is er een reden ze te gebruiken. Ik doe dat slechts sporadisch. Uit dus die handel.

In het lijstje staat een Canon Printertoepassing die ik wel wil gebruiken. Maar ik kan me voorstellen dat een gebruiker er geen gebruik van wil maken en dan scheelt het toch weer om hem uit te zetten.

Jusched is de java update scheduler. U kunt deze uitschakelen. Gebruikt u OpenOffice als kantoorpakket, dan zou ik deze aan laten staan omdat OOo gebruik maakt van Java.

Adobe Reader componenten zou ik niet uitschakelen als u dagelijks PDF-bestanden bekijkt. Komt het af en toe voor dat u dat doet, dan kunnen ze m.i. wel uit. Het duurt dan iets langer om de Reader te starten. Omdat het bovendien een belachelijk lompe en grote toepassing is, zou ik hem vervangen door de Foxit Reader (o.a. te vinden op www.filehippo.com)

Wie meer wil zien dan met msconfig kan hier terecht voor een download van het klassieke AutoRuns:

<http://technet.microsoft.com/en-us/sysinternals/bb963902.aspx>