Beveiliging en Privacy

Tips en Trucs voor veilig computer gebruik

Gino Damen
12 juni 2001
Versie 1.2

Inhoudsopgave

Inleiding

De beveiliging van de PC is iets waar de meeste mensen niet zo bij stil staan. Echter de PC vormt een steeds belangrijker onderdeel van onze dagelijkse werkzaamheden. Zo hebben regelen steeds meer mensen hun geldzaken via de PC en ook bij de belastingaangifte is de PC vaak een dankbaar hulpmiddel.

Ook zaken als correspondentie (sollicitaties, adresbestanden enz) en muziek bestanden zijn echter steeds vaker het beschermen waard. Ik persoonlijk zou er niet aan moeten denken om de vele documenten die ik ondertussen geschreven heb te verliezen door een beveiligingsprobleempje.

In dit document ga ik in op de mogelijke manieren waarop zaken te beveiligen en te beschermen zijn. Hierbij komen allerlei zaken aanbod, zowel op het vlak van hardware als ook software. Het aspect Internet en het feit dat steeds meer mensen er een constante verbinding mee hebben maakt het nog complexer.

Bij dit document hoort ook het bestandje: RESTRICTED.INF. Het meest recente exemplaar is te downloaden van mijn website. Lees voor installatie van dit bestandje wel eerst dit document even door!

De meest recente versie van dit document is altijd beschikbaar onder Downloads bij:

http://www.damen.cjb.net

Revisies

Versie	Omschrijving
1.0	Initiële document
1.1	Correctie van de installatie bestanden i.v.m. niet correcte de-installatie
1.2	Uitgebreid naar een meer generiek beveiligingsdocument

Disclaimer

Introductie

De kreet "beveiligen van de PC" roept bij de meeste mensen direct visioenen op van onhandige wachtwoorden met rare tekens die je telkens weer vergeet en die zodra je ze wel kent weer moet veranderen.

Dit is echter vaak alleen het geval bij bedrijven en daar spelen hele andere belangen en motieven om naar dit soort paardenmiddelen te grijpen. Voor de thuisgebruiker van een PC zijn andere zaken van belang zodra we het over beveiliging hebben.

De meeste mensen zitten er niet op te wachten dat al hun, met vaak veel moeite, verzamelde muziekbestanden, plaatjes en documenten verloren gaan omdat ze door een virus getroffen worden. Ook zitten de meeste mensen er niet echt op te wachten dat hun bankgegevens door een of andere onverlaat via hun internetverbinding kunnen worden gestolen.

Gelukkig kan je deze problemen voorkomen, en dus een goede beveiliging van je persoonlijke gegevens hebben, zonder dat je naar zware maatregelen hoeft te grijpen die bedrijven toepassen.

Informatie bewaren

Voordat we naar mogelijke beveiligen gaan kijken is het eerst zaak om te zorgen dat de persoonlijke informatie überhaupt ergens bewaard wordt. Dit wordt vaak een back-up genoemd. Het hebben van een back--up heeft dus als voordeel dat er bij problemen in ieder geval niet alle persoonlijke informatie verloren driegt te gaan. Ook is het hiermee mogelijk om in het geval van problemen de persoonlijke informatie eenvoudig terug te halen. Dit betekent echter wel dat we dus, met enige regelmaat, onze persoonlijke informatie ergens anders dan op de PC zelf zullen moeten bewaren. Het bewaren van de informatie in een andere map op de harde schijf zelf is dus niet een oplossing. Ook daar is de informatie namelijk te kwetsbaar bij mogelijke problemen. De informatie moet dus buiten de PC zelf worden bewaard.

Als bewaarmedium is de diskette het eerste wat in je opkomt. Maar met de huidige bestandsgroottes is dat niet meer een realistische optie, behalve als je erg van diskjockey spelen houdt. Een alternatief is echter de CD schrijver. Steeds meer nieuwe Pc's worden standaard hiervan voorzien en ook in bestaande Pc's wordt hij steeds als uitbreiding geplaatst. Echter omdat Windows standaard (nog) geen ondersteuning kent voor het direct beschrijven van Cd's moet er speciale software geïnstalleerd worden (zoals DirectCD). Hiermee wordt het wel mogelijk om een CD te gebruiken als een soort van super diskette. Een ander voordeel van de CD schrijver is dat de lege CD-R's relatief goedkoop zijn.

Een andere alternatief, waar ik zelf voor gekozen heb, is de Iomega ZIP drive. Vooral voor het dagelijkse gebruik is dit een uitkomst. De USB-ZIP drive is het summum van gebruiksgemak. Het is een kwestie van de stekker in een vrije USB poort steken waarna Windows (98, ME en 2000) hem direct herkent en de ZIP als een nieuwe schijf letter in de verkenner zichtbaar wordt. Het gebruik is daarna exact hetzelfde zoals bij een diskette, alleen veel sneller en een stuk groter. Van ZIP's zijn er twee varianten, de 100 MB en de 250MB versie. De nieuwste 250MB USB versie is ideaal omdat dat deze geen losse voeding meer nodig heeft. Hij haalt zijn voeding direct uit de USB aansluiting.

Het grootste nadeel van de ZIP drives is helaas hun prijs. Een 100 MB USB ZIP kit kost ongeveer 300 gulden en de 250 MB USB ZIP drive kost zelfs bijna 600 gulden. De losse schijfjes kosten per stuk ook nog eens 25 (100 MB) tot 40 (250MB) gulden. Het is gebleken dat zodra je meer dan 600 MB aan informatie wilt gaan bewaren de CD schrijver goedkoper in het gebruik is dan een ZIP drive. Het is natuurlijk ook mogelijk om beide te gebruiken en zo het gemak van beide oplossingen tot je beschikking te hebben.

Hardware beveiliging

De BIOS beveiliging

De eerste beveiliging die je ook nog eens eenvoudig kunt aanbrengen zit in het BIOS van elke PC ingebakken, namelijk het BIOS wachtwoord. Indien de PC voorzien is van zo'n wachtwoord dan wordt er, zodra de PC aanzet wordt, om een wachtwoord gevraagd. Na drie foutieve pogingen zal de PC zichzelf weer uitzetten. Dit kan echter wel zo vaak herhaald worden totdat het wachtwoord geraden is.

Deze beveiliging is met wat kennis (en durf) relatief makkelijk te omzeilen. Hiervoor moet eerst de PC worden open gemaakt. Zodra de PC geopend is moeten er twee pennetjes (vaak vlakbij de BIOS chip zelf) op het moederbord worden kortgesloten. Dit kan met een schroevendraaier, maar ook een muntje of wat aluminiumfolie kan hiervoor gebruikt worden, zolang het maar elektriciteit geleidt. Het resultaat is dat alle BIOS instellingen gewist worden, waaronder het wachtwoord. Bij de volgende start van de PC zal het BIOS vervolgens de standaard instellingen gebruiken en dat is altijd zonder wachtwoord!

Nu lijkt dit een slechte zaak, maar bedenk je wel dat als je zelf je wachtwoord vergeten hebt het wel erg fijn is om toch nog een uitweg tot je beschikking te hebben. Het alternatief zou namelijk zijn dat je dus een nieuw moederbord moet kopen en (laten) installeren.

Het is dus ook zaak om er voor te zorgen dat de PC zelf niet eenvoudig te openen is, zodra er als beveiliging gekozen wordt voor een BIOS wachtwoord. Bepaalde PC kasten zijn eenvoudig met een hangslotje te beveiliging omdat ze voorzien zijn van een oogje aan zowel de kast zelf als de omhullende deksel. Is dit niet het geval dan is het ook mogelijk om een speciale schroef te koop met een ingebouwd slotje. Deze gebruik je dan in plaats van een van de standaard schroeven. De "gelegenheidsinbrekers" zoals de kinderen of huisgenoten worden zo effectief tegengehouden. Echt kwaadwillende zullen zich echter tegen laten houden door deze fysieke beveiliging. Zij zetten desnoods een boor, beton schaar of blik schaar in om de kast te forceren.

LET OP: Bij een laptop / notebook is het BIOS wachtwoord een stuk moeilijker te omzeilen. Vaak moet voor het deactiveren van het BIOS wachtwoord zelfs de hulp van de fabrikant worden ingeroepen. Dit heeft weer alles te maken met de diefstalgevoeligheid van deze categorie van machines.

Het beveiligen van Windows

Gebruik je Windows 3.1, 95, 98 of ME dan is het standaard niet mogelijk om Windows eenvoudig te beveiligen. Met de nodige kennis en het hulpprogramma Group Policy (onderdeel van de Resource Kit voor Windows) is Windows 9x/ME redelijk veilig in te richten voor meerdere gebruikers.

Bij Windows NT/2000/XP is beveiliging juist een integraal onderdeel. Deze versies van Windows zijn juist berekend op het feit dat er meerdere mensen met dezelfde PC zullen gaan werken. Vooral in Windows XP, maar ook in 2000 is dit ook voor de beginner eenvoudig goed te regelen.

Beveiligen van Windows 98, 98SE en ME

Een kenmerk van Windows 98, 98SE en ME is dat iedereen standaard dezelfde instellingen krijgt. Dit is vaak echter helemaal niet de bedoeling want wat de ene persoon lekker vindt werken is voor de ander onmogelijk.

Het is echter mogelijk om Windows zo is ingesteld dat ieder gebruiker zijn eigen omgeving krijgt waarmee we al halverwege zijn. Daarnaast is het ook mogelijk om het systeem beter te beschermen tegen al dan niet opzettelijke veranderingen. Het resultaat is dan ook een voor elke gebruiker prettiger bruikbare pc met menu's voor iedereen en wat meer beveiliging tegen al te makkelijk gemaakte blunders?

Zoals al gezegd is het niet mogelijk om Windows 9x zo bomvrij te maken als Windows 2000 / XP, maar je zal zien dat er toch veel mogelijk is.

Veilig werken met meerder gebruikers op één PC

Opmerking: Degenen die met Windows 95 werken zullen hier en daar merken dat soms wat moeten worden gezocht omdat het nét even anders is aangegeven, maar ook daarin kan onderstaande gerealiseerd worden.

Het volgende zal het uitgangspunt zijn van de geschetste aanpak. Er komt één beheerder en de andere gebruikers zullen beperkt worden in hun vrijheden. Zo zal een normale gebruiker bijvoorbeeld geen programma's mogen kunnen installeren en ook geen directe toegang mogen krijgen tot de instellingen van Windows zelf. Elke gebruiker zal de beschikking krijgen over een eigen bureaublad en startmenu. Ook komt er een oplossing voor het probleem van het omzeilen van het Windows wachtwoord met een druk op de ESC.

De strategie

Er zijn twee manieren waarop we het einddoel kunnen bereiken:

1. We zorgen voor een compleet geïnstalleerde pc met daarop alle software en snelkoppelingen die iedereen nodig zal hebben. Vervolgens wordt, na het aanmaken van de gebruikers, per gebruiker de mogelijkheden beperkt;
2. We zorgen voor een pc waar zo goed als niets op staat behalve Windows, maken de gebruikers aan, en installeren daarna per gebruiker de programma's, programmagroepen en snelkoppelingen.

In de praktijk werkt strategie 1 het eenvoudigst en daar wordt verder dan ook vanuit gegaan. Verder moet er ook een redelijk goed beeld zijn van wat elke gebruiker nu wel en niet mag. Maak desnoods even een checklijstje. Denk hierbij aan zaken als: Mag men wel/niet op 't internet? Of naar de Dos-prompt? Of wel al die tierelantijnen zien? Per gebruiker een eigen achtergrondje. Is er soms een harddisk waar iemand niet op mag? Mag er te zien zijn aan het startmenu -> documenten welk bestand het laatst is gebruikt? (Of wil je zelf niet zien wat een ander zoal heeft gestart in het verleden). Kortom, denk hier eerst even over na.

Installatie Poledit en TweakUi

Poledit is de Policy-Editor (systeembeleidseditor). Een programma om het Windows register per computer en/of gebruiker aan te passen. Het is een behoorlijk krachtige programma, waarmee het dus uitkijken geblazen is. Voor je het weet heb je zoveel rechten beperkt, dat het moeilijk is ze weer terug te zetten. Dit omdat je Poledit niet meer kan starten. Kijk er dus goed mee uit.

Met Poledit zijn o.a. de volgende zaken te regelen:

- Beperken van het recht van personen om programma's te starten (je kan er zelfs mee instellen dat alleen door jou aangegeven programma's gestart mogen worden)
- Voorkomen van de toegang tot de dos-prompt
- Onbereikbaar maken van een aantal 'gevaarlijke' onderdelen zoals het configuratiescherm, printerinstellingen, netwerkomgeving, de mogelijkheid om via start -> uitvoeren iets te installeren, toegang tot de beeldscherm instellingen (screensavers, bureaublad achtergrond) beperken enz.
- Ieder zijn eigen Start-menu en programma mappen geven
- Per gebruiker al dan niet voorkomen dat aanpassingen van de instellingen worden opgeslagen.

Poledit staat op de Windows98 cd-rom en is op de volgende manier te installeren. Open het configuratiescherm en vervolgens Software. Selecteer het tabblad Windows setup en klik vervolgens op Diskette en kies voor Bladeren. Open nu op de Windows 98 cd-rom de map \Tools\Reskit\Netadmin\Poledit. Kies vervolgens voor OK en zet een vinkje in het vakje voor de optie Systeembeleidseditor en kies daarna voor installeren. In de groep systeemwerkset zal nu de optie systeembeleidseditor erbij verschijnen.

TweakUi is een handige utility waarmee je Windows wat meer naar je hand kan zetten. TweakUI is via mijn website eenvoudig te downloaden. Met TweakUi zijn o.a. de volgende zaken te regelen:

- de snelheid waarmee en de wijze waarop menu's reageren instellen
- de weergave van snelkoppelingen instellen (met of zonder pijl etc.)
- de Active Desktop uitschakelen
- het toestaan van uitloggen aan- of uitzetten
- de menukeuzes documenten en favorieten uit het startmenu weghalen
- de prullenbak en de netwerkomgeving van het bureaublad verwijderen
- drives onzichtbaar maken in 'deze computer'
- het Windows98 opstartscherm verwijderen, de functietoetsen (F8!) uitschakelen bij het opstarten
- het automatisch starten van data en/of audio cd's uitschakelen

- het 'onthouden' van logon namen, laatst gestarte documenten en programma's uitschakelen.

TweakUi wordt op de volgende manier geïnstalleerd: Klik met de rechter muisknop op Tweakui.inf (setup-informatie) en kies voor installeren. TweakUi wordt nu in het Configuratiescherm geplaatst, van waaruit je het kan starten.

Installatie Multi-User ondersteuning

In het configuratiescherm zijn de volgende twee icoontjes beschikbaar: Beveiliging en Gebruikers. We beginnen met 'Beveiliging'. Open deze en selecteer daar het tabblad gebruikersprofielen en selecteer de optie 'Gebruikers kunnen hun voorkeuren ...' . Zet vervolgens een vinkje in beide instellingen van het gebruikersprofiel. Herstart de pc nog even niet. Open nu 'Gebruikers' uit het configuratiescherm en geef de gebruikersnamen op en de bijbehorende wachtwoorden. Herstart vervolgens de pc.

Tip: moet er een erg jong iemand gebruik maken van de pc, maak dan alleen een naam aan, en laat het wachtwoord leeg. Straks beperken we de rechten van deze gebruiker tot het minimale, en bij het inloggen hoeft alleen maar de naam gekozen te worden.

Wat gebeurt er nu allemaal na het installeren van die multi-User omgeving? Er wordt per gebruiker een eigen sub-register aangemaakt, en er wordt per gebruiker onder de directory C:\windows\Profiles een hele structuur van het startmenu en de programma mappen zoals deze in de pc bestonden gekopieerd. Per gebruiker worden déze structuren gebruikt in plaats van de structuren onder C:\windows\startmenu. In deze structuren per gebruiker kan je vervolgens naar hartelust verwijderen en overlaten wat per gebruiker gewenst is.

Bij het starten van Windows komt nu een menu in beeld, waarin de namen van de aangemaakte gebruikers staan. De truc met de Escape toets wordt straks nog aangepakt.

Inrichten van het systeem per gebruiker

Er zijn -zoals altijd onder Windows- meerdere wegen die naar Rome leiden. Je kan inloggen als een bepaalde gebruiker en vervolgens die snelkoppelingen en menu's verwijderen die ongewenst zijn. Vervolgens zou je het systeem zó in kunnen richten dat er een paar snelkoppelingen overblijven op het bureaublad, waarop direct geklikt kan worden voor de betreffende programma's. Er blijven natuurlijk een aantal zaken over in het menu Start en in 'deze computer' die we er liever niet zien, dat pakken we straks aan.

Een tweede manier is om in te loggen als de beheerder en m.b.v. de Verkenner in de map profiles\{gebruiker} weg te halen wat we er niet wensen. Merk op, dat je ook de map Programma's en Opstarten bij de betreffende gebruiker nu wel gewoon kan verwijderen als je dat wenst.

Controleer ook goed of alles wel blijft werken per gebruiker zoals je dat wenst. Een snelkoppeling op het bureaublad van de beheerder naar de map policies is natuurlijk erg handig. Zo kan de als beheerder makkelijk bij de mappen en instellingen komen van de andere gebruikers, en daar wijzigingen in aanbrengen.

Beperken van rechten per gebruiker

Met Poledit kan je vervolgens per gebruiker rechten afnemen. Log eerst in als de beheerder gebruiker van deze gebruiker beperken we dus de rechten bij voorkeur niet. Vanaf nu geldt dat de veranderingen die nu worden aangebracht bij de lokale gebruiker in Poledit alleen gelden voor de gebruiker onder wiens naam men nu bezig is.

Log in als de eerste normale gebruiker waarvan de mogelijkheden moeten worden beperkt. Start vervolgens Poledit en kies bestand, register openen, lokale gebruiker. Dit zijn dus de instellingen voor de **huidige** gebruiker. Loop alle opties af en beperk datgene wat beperkt moet worden. Sluit vervolgens Poledit af sla de wijzigingen op. Het vinden van de juiste instellingen kan even zoeken zijn maar het is gelukkig niet nodig om telkens Windows opnieuw te herstarten. Uitloggen en opnieuw inloggen onder dezelfde naam is voldoende om het resultaat te zien van de wijzigingen.

In Poledit is er naast Lokale gebruiker ook nog een keuze Lokale Computer maar daar hoeft en mag niks gewijzigd worden!

Merk op, dat iedere gebruiker een eigen bureaublad achtergrond kan worden geven en een eigen kleurenschema. Ook eventuele instellingen van het beeldscherm (b.v. 800*600 voor de bijziende gebruiker en 1024*768 voor spreadsheetfanaat). Ook geluiden bij opstarten enz. worden per gebruiker onthouden.

Laat vooralsnog even de vinkjes nog weg bij de optie Shell -> beperkingen -> de opdracht Uitvoeren verwijderen. Anders wordt het opstarten van Poledit straks wat moeizaam ;-) . Ook de vinkjes bij 'mappen uit instellingen uit het menu Start...' en 'Instellingen niet opslaan bij afsluiten' kunnen in het begin beter nog niet uit worden gezet. Doe dit pas als alles volledig naar de zin is, en ná het gebruik van TweakUi.

Opmerking: 'Mappen uit instellingen uit het menu Start verwijderen' verwijdert niet alleen de keuze instellingen bij het menu Start, maar ook het complete configuratiescherm uit 'Deze Computer'. Het starten van TweakUi wordt dan wat problematisch

Met TweakUi kan tenslotte voor het hele systeem of per gebruiker (sommige instellingen gelden voor de computer en andere weer alleen per gebruiker) dicht worden getimmerd wat verder nog (on)gewenst is. Ook de prullenbak valt zelfs van het bureaublad te verwijderen indien nodig. De beheerder kan deze in het geval van nood altijd nog benaderen met de verkenner (C:\recycled en met rechtsklikken een verwijderd item terugplaatsen).

Let er wel op dat het beperken niet doorslaat. Wat voorbeelden: Het automatisch starten van Cd-rom's kan worden uitgezet met TweakUi, dat geldt dan voor iedereen (het is een zogenaamde systeem brede instelling). Wordt met TweakUi vervolgens ook de driveletter van de Cd-rom weg gehaald, en de opdracht uitvoeren uit het startmenu verwijderd, dan wordt het wel erg lastig om een cd-rom te starten. Wordt de Dos-prompt uit geschakeld met Poledit, dan kan er ook geen Wp5.1 meer worden starten, want dat werkt onder de dos-prompt. Wordt aangegeven dat alle items op het bureaublad verborgen moeten worden, dan kan er ook niets meer, zelfs geen nieuwe snelkoppeling, op geplaatst worden. Alleen via het menu Start zijn de programma's dan nog te bereiken.

Niemand ingelogd, en tóch toegang..

Wordt er ingelogd in Windows en er wordt om een naam en wachtwoord gevraagd dan dit worden omzeild via een druk op Esc. Men komt er dan toch gewoon in. Eigenlijk komt men dan in de standaardconfiguratie van Windows terecht. Is die Standaardconfiguratie voorzien van allerlei mogelijkheden om toch het systeem te kunnen wijzigen dan zijn we dus nog niks opgeschoten met alle wijzigen. De truc is dan ook om deze standaardinstelling van Windows zó ernstig te beperken dat er niks mee te bereiken is.

Een waarschuwing is hier wel op zijn plaats. Vóór dat de standaard configuratie beperkt wordt moet wel duidelijk zijn dat de beheerdergebruiker alles mag doen en overal bij kan. Test dit dus eerst! Werkt dit naar tevredenheid dan pas kan met Poledit en TweakUi de 'Escape' gebruiker zó worden beperken dat niks meer kan , behalve afsluiten...

Let er bij TweakUi op, dat sommige instellingen per gebruiker zijn en sommige voor de gehele pc gelden. Bij twijfel kan je rechts klikken op een optie en vervolgens op 'What's this' klikken. Je krijgt dan uitleg over die optie. Onder meer wordt verteld of dit een 'system wide' setting of een 'per user' setting is.

Overige beveiligingsvoorzieningen:

Zet in het bios van de computer opstarten van floppy uit. Dit is niet alleen een probaat middel tegen bootsector virussen, maar voorkomt ook dat programma's van A: worden geladen. Mocht het BIOS wachtwoord nog niet geactiveerd zijn, doe dit dan alsnog!

Zet met TweakUi vervolgens de functietoetsenondersteuning uit. Dit voorkomt dat m.b.v. F8 mensen in de Dos-prompt of in de veilige mode kunnen komen. Ook als men Windows afsluit komt er in het keuzemenu de optie "Herstarten in Dos-mode" voor. Dit is op een van de volgende manieren te ondervangen:

Verwijder m.b.v. Poledit de mogelijkheid tot afsluiten van de pc (shell,beperkingen) en maak op iedere desktop een snelkoppeling "Deze computer afsluiten" met de volgende inhoud achter pad

```
C:\WINDOWS\RUNDLL.EXE user.exe,exitwindows
```

Let op de komma, spaties en punten!
Wijzig, of maak met Notepad in de directory C:\Windows Dosstart.bat en voer daar bijvoorbeeld in:

```
@echo off
cls
Echo U kunt de computer nu uitzetten...
:loop
goto loop
```

Een zeer snelle lus die eeuwig bezig blijft tussen :loop en goto loop. Dit voorkomt vrijwel altijd dat met Ctrl-C of Ctrl-Break zo'n batch bestand kan worden afgebroken. Desnoods wordt er tussen :loop en goto loop ook nog "echo ^G" (^G betekend CTRL+G) geplaatst , waarmee een aanhoudende pieptoon blijft klinken, zodat men de pc echt wel uitzet. Dosstart.bat wordt namelijk altijd uitgevoerd als er gekozen wordt voor 'Opnieuw opstarten in Dos-mode' (tenminste, als het in de directory Windows staat).

Omzeilen van de aangebrachte beveiligingen

Het is altijd mogelijk om deze beveiligingen te omzeilen. Daarvoor is Windows namelijk domweg niet waterdicht genoeg voor. Maar voor de gemiddelde gebruiker en ook de gemiddelde kwaadwillende is het wel erg moeilijk geworden om dingen (on)opzettelijk de vernieling in te helpen en dat is waar het allemaal om ging.

Voor de échte beveiliging moeten we uitwijken naar besturingssystemen als de Linux-achtigen of Windows NT/2000/XP. De laatste zullen we hierna bespreken.

Beveiligen van Windows NT, 2000 en XP

{nog te doen}

Het beveiliging van het Internet gebruik

Voorkomen is beter dan genezen dat geld ook voor de PC en zeker in combinatie met het gebruik van het medium internet. Daarom zou elke PC minimaal voorzien moeten zijn van een recent antivirus programma en een goede firewall.

Antivirus software

Antivirus software is er van vele fabrikanten en allemaal hebben ze wel hun zwakke en sterke punten. Ikzelf gebruik AntiVir van H+BEDV (Duits bedrijf). Maar Norton Antivirus of McAffee is ook een goede keuze. Alle antivirus programma's hebben de mogelijkheid om een monitor (vaak ook guard genoemd) te installeren. Dit is een onderdeel van de virusscanner die constant controleert wat er op de computer gebeurd. Vooral handig als je veel download en/of de kinderen hun gang wilt kunnen laten gaan met de PC.

Een belangrijk punt bij antivirus software is dat deze regelmatig voorzien moet worden van de nieuwste virushandtekeningen. Doe je dit niet dan zal op den duur de software niet meer instaat zijn om de nieuwste virussen te herkennen! Alle nieuwe antivirus programma's kunnen eenvoudig zelf de nieuwste virusinformatie ophalen. Het beste kan je het programma dit elke week of in ieder geval één keer per maand laten doen.

Firewall's

Een ander belangrijk programma bij het internetten is een firewall. Een firewall is een soort van portier die er voorzorgt dat alle kwade invloeden van het internet buiten de computer worden gehouden. Ook beschermt hij uw gegevens door te voorkomen dat ongewenste programma's (zoals SpyWare en Trojanen) toegang tot het internet kunnen krijgen. Momenteel zijn er helaas niet zoveel goede en gratis firewall's beschikbaar. De beste zijn op dit moment ZoneLabs ZoneAlarm en Tiny Personal Firewall.

Trojanen

Een Trojaan is een speciaal soort virus en daarom krijgt hij hier ook even een speciale vermelding. De naam "Trojaan" is ontleend aan de Griekse historie en verwijst naar manier waarop de Grieken de stad Troje hebben kunnen veroveren. De Grieken hadden namelijk als probleem dat Troje een hele sterke stadsmuur had die zelfs na een tiental jaren van oorlog voeren onneembaar bleek. Hierop verzonnen de Grieken de volgende list.

Ze deden net alsof ze het beleg opgaven waarbij ze een "kado" voor de mensen van Troje achterlieten bij hun stadspoorten en wel in de vorm van een heel groot houten paard. Wat de mensen van Troje echter niet besefte was dat het paard hol was en dat daarin Griekse soldaten zaten. Zij openden dus hun stadspoorten en haalden het paard naar binnen. In de nacht die daarop volgden klommen de Grieken uit het paard en openden de stadspoorten waarop Troje dus veroverd werd door de Grieken.

Een Trojaan in het geval van een computer is dus een stukje software, screensavers en spelletjes zijn favoriet, waarin dus nog iets anders is verborgen. De screensaver is dus in dat geval het paard. Het stukje software is vaak bedoeld om op afstand, zodra er een internetverbinding is, je PC te kunnen benaderen en daarmee van alles uit te kunnen halen. Dit kan lopen van het zoeken naar je creditcard nummer tot het aanvallen van andere computers.

Tegen Trojanen helpt alleen maar voorzichtigheid, een goed antivirus programma en een goede firewall!

SpyWare

Het is de nieuwste trend van de 21ste eeuw: spyware. Kleine programma's die zonder je medeweten 'gratis' bij echte software worden geleverd, met als enige doel je bewegingen op het internet te volgen. Want dat is lekker makkelijk voor de adverteerder. Die kan er op deze manier namelijk voor zorgen dat je op maat gesneden reclameboodschappen te zien krijgt.

Stel je het volgende eens voor. Op de deurmat valt een superaanbieding van een meubelfabrikant. Die biedt je een bankstel aan dat onbeperkt gebruikt mag worden, zonder dat er maar één gulden voor hoeft te worden betaald. En om het helemaal af te maken wordt het meubilair bij je in de woonkamer afgeleverd. Wederom zonder extra kosten. Klinkt goed, nietwaar? Wat je echter niet weet is dat de bank is uitgerust met meerdere camera's en microfoons, die elke beweging en ieder geluid opnemen en automatisch versturen naar een speciale instantie. Alles wat leeft en beweegt in de huiskamer is dus bekend bij die organisatie.

Uniek nummer Windows

Het klinkt wel heel erg als een ver-van-je-bed-show? Dat is het niet. Grote kans dat je je al in een vergelijkbare situatie bevindt: op je pc! Twee jaar geleden werd bekend dat de naam van Windows 98-bezitters gekoppeld was aan een uniek nummer, de Global Unique Identifier. Wie het product online registreerde voorzag Microsoft niet alleen van de ingevulde persoonsgegevens, maar ook van dat unieke nummer. En datzelfde nummer werd onder meer opgeslagen in Officedocumenten en cookies.

Onder druk van de publieke opinie werd de Global Unique IDentifier (GUID) vaarwel gezegd. Althans, Microsoft hield niet meer bij wie wat gebruikt. De reus uit Redmond verkocht de gegevens niet aan derden, maar parkeerde de klantgegevens 'slechts' in de eigen database. Het kan ook anders: de gegevens worden verkocht.

Spyware is jargon voor Advertising Supported-software (adware) en wordt gebruikt als alternatieve inkomstenbron voor softwareontwikkelaars. In plaats van betaling voor een programma verschijnt een advertentie-banner in beeld. De adverteerder betaalt dus voor de vele uren programmeerwerk van de maker. Tot zover geen probleem, je hebt er louter voordeel van. Maar er is meer. In het programma zit een aparte applicatie verstopt, bijvoorbeeld in de vorm van een DLL-bestand dat precies bijhoudt wie je bent en wat je online doet. De gegevens worden verstuurd naar de leverancier of een speciaal bedrijf dat de logbestanden verzamelt want klantgegevens zijn goud waard!

De software lijkt dus free- of shareware te zijn, terwijl de leverancier intussen dik geld aan je verdient. Zonder je medeweten of controle worden persoonlijke gegevens (naam, e-mailadres, naam van de computer, het unieke nummer van uw netwerkkaart, enzovoort) en/of surfgedrag over het internet verstuurd. Het gevolg is dat je op maat gesneden advertentie-banners of e-mail krijgt.

Adware

Het is echter te kort door de bocht om alle software met banners (adware) dan maar als spyware te bestempelen. Want lang niet iedere softwareleverancier maakt zich schuldig aan deze slinkse manier van geld verdienen. Het kan ook goed zijn dat u alleen banners in beeld krijgt zonder dat uw persoonlijke gegevens bekend zijn, een goede voorbeeld hiervan is de webbrowser Opera. Er wordt net als bij spyware wel data naar de leverancier verstuurd, maar alleen over de getoonde banners, zodat de adverteerder de rekening kan worden gepresenteerd. De advertentie is zoveel duizendmaal getoond, daarvoor moet dus worden betaald.

Andersom geldt ook dat spyware niet perse adware hoeft te zijn. Een programma zonder banners kan evengoed stiekem data verzenden via het internet. Eén ding is wel zeker: de scheidslijn tussen adware en spyware is flinterdun. Helemaal zeker weet u nooit wat naar de leverancier wordt verstuurd.

Het gaat bij spyware niet om de minste programma's. Enkele grote spelers in softwareland kunnen de verleiding niet weerstaan om een gedetailleerd beeld van de klantenkring te krijgen. Zo kwam RealNetworks begin 2000 in opspraak. De stuwende kracht achter de populaire Real-Player hield actief het luister- en kopieergedrag van zijn klanten bij via het gratis programma RealJukebox, een muziekspeler voor cd's, MP3-bestanden en andere muziekformaten. De geheime 'feature' werd ontdekt en zorgde voor een enorme rel.

Elke dag stuurde RealJukebox namelijk een rapportje naar RealNetworks, waarin onder meer stond welke cd's een gebruiker had gedraaid, hoeveel MP3's hij had afgespeeld en welk merk MP3-speler werd gebruikt. RealNetworks betuigde spijt en beloofde beterschap. Intussen had het Amerikaanse bedrijf wel een database vol gegevens van maar liefst twaalf miljoen klanten.

Spyware opsporen, verwijderen en voorkomen

Grote kans dat je computer inmiddels is vervuild met spyware. Want veel populaire software maakt gebruik van modules zoals Aureate. Voorbeelden hiervan zijn het populaire ftp-programma Cute FTP en de nog populairdere downloadmanagers GoZilla en GetRight. Simpelweg het programma verwijderen helpt niet. De applicatie verdwijnt wel van de harde schijf, maar de spyware bestanden blijven achter in de systeemmap van Windows!

Gelukkig is het tegenwoordig eenvoudig om te achterhalen wat er zoal is achtergebleven. Het makkelijkst gaat dit met Ad-Aware (http://www.lavasoftuse.com). Ad-Aware doorzoekt je computer (geheugen, register en de harde schijf) op verdachte bestanden en verwijzigen en toont deze vervolgens. Met eenvoudig aanvinken zijn dan de gevonden piraten eenvoudig te verwijderen. Laat Ad-Aware wel even een backup van deze bestanden maken want de kans dat je systeem instabiel wordt is altijd aanwezig. Reageert na het verwijderen (en een nieuwe herstart) de computer naar behoren, dan kan je de bestanden alsnog laten verwijderen.

Cookies en privacy

Naast spyware zijn er nog andere manieren waarop de adverteerders je over het internet kunnen volgen, namelijk via een cookie. Hiermee volgen ze je van site naar site waarbij ze telkens bijhouden wat je allemaal te zien krijgt (vooral de advertenties, want die verkopen zij).

Zodra je een keertje op zo'n advertentie klikt zit je aan ze vast. Dit omdat je voor het kopen van het betreffende artikel toch echt minimaal je naam, adres en woonplaats (en vaak nog veel meer) moet invullen, wat weer in het cookie gestopt wordt. Na zo'n koop actie begint dus het spelletje van het presenteren van de "juiste" advertenties met als doel dat je dus nog meer koopt waardoor ze nog beter de "juiste" advertenties kunnen bepalen enz. Naast steeds gerichtere advertenties zal het ook steeds vaker voorkomen dat er allerlei reclame e-mail in je postbus terecht komt.

Gelukkig is ook dit alles met wat kennis en kunde eenvoudig te stoppen. Bedenk wel dat een reeds aanwezig profiel helaas niet eenvoudig te verwijderen is. Aan de andere kant is het echter wel weer zo dat hoe langer het geleden is dat ze je profiel hebben kunnen bij werken hoe minder waard hij wordt. Uiteindelijk wordt het profiel vanzelf verwijderd omdat hij commercieel niet meer interessant is.

Wat zijn cookies

Cookies zijn kleine bestandjes die je browser lokaal op de harde schijf bewaart en die door sites worden gebruikt om bij terugkomst te achterhalen of je al een keer de site hebt bezocht. Nu is het zo dat deze techniek ontwikkeld is met een positieve gedacht in het achterhoofd. Via zijn cookie kan de site dus achterhalen wie je bent zodat hij de juiste instellingen kan ophalen. Hierdoor hoef je deze niet elke hoeft in te vullen. Verder worden er in cookies ook vaak wachtwoorden opgeslagen. Niet echt veilig, maar wel handig. Het is wel zo dat een website alleen maar zijn **eigen** cookie kan ophalen en niet een willekeurige andere cookie van een andere website.

Een voorbeeld van een site die cookies op deze manier gebruikt is Amazon.com. Zij kunnen dankzij het cookie op je machine je een leuke aanbieding laten zien. Op zich dus een zeer handig iets. Totdat iemand anders achter je machine gaat zitten, naar Amazon.com surft om dan te zien dat ze de nieuwste playboy video aanraden!?.....

Het voorbeeld van Amazon is echter niet helemaal willekeurig. Dit is namelijk ook de manier waarop bedrijven als DoubleClick te werk gaan. Maar hoe komt dan dat cookie op je machine? De meeste mensen surfen echt niet uit zich zelf naar de site van een bedrijf zoals DoubleClick en toch hebben ze er een cookie van gekregen! De oplossing is dat de advertenties via een link zijn op genomen in de pagina's die je bekijkt. De browser haalt dus de advertentie fysiek van de DoubleClick site en wordt daarvoor "beloond" met een cookie. Deze cookie wordt vervolgens bij elk volgend bezoek (voor het ophalen van een volgende advertentie dus!) weer uitgelezen waarop ze weer je profiel kunnen bijwerken.

Cookie categorieën

Het zal nu wel duidelijk zijn dat er verschillende soorten cookies zijn. Globaal zijn ze in een drietal groepen in te delen; namelijk cookies van de Goeden, de Slechten en de Lastigen.

Om een cookie te kunnen indelen zal je ze stuk voor stuk moeten nalopen. Dit gaat het eenvoudigst op de volgende manier. Ga naar de Eigenschappen van de Internet Explorer (via Extra -> Internet-opties...) Klik bij de Tijdelijke Internet Bestanden op de knop Instellingen... en noteer de huidige locatie zoals die staat in het venstertje dat verschijnt. Sluit dit vensterje weer en klik op de Wissen bestanden... knop om de tijdelijke Internet bestanden op te ruimen. Start nu de Windows Verkenner en ga naar de net genoteerde directory die dus normaal de tijdelijke internet bestanden bevat.

Opmerking: Cookies zijn eenvoudiger te bekijken en te verwijderen via het programma Cookie Viewer van Karen Kenworthy (www.karenware.com).

Als het goed is staan er alleen nog maar cookies (dat zijn dus die tekst documenten die allemaal met het woordje Cookie beginnen). Dit is tevens de reden dat de tijdelijke internet bestanden verwijderd moesten worden.

Zoals je nu wel begrepen hebt is het nalopen van al die cookies een nogal langdurig werkje. Gelukkig hoef je dit niet meer te doen want dat heb ik reeds gedaan bij het schrijven van dit stukje.

Bekende slechte sites

Hieronder vind je het lijstje van websites die bij mij nu in de "Websites met beperkte toegang" zone staan.

*.about.com
*.accendo.com
*.adbureau.net
*.adflight.com
*.adforce.com
*.adknowledge.com
*.admaximize.com
*.admonitor.net
*.adsmart.net
*.adsoftware.com
*.advertising.com
*.adwisdom.com
*.affina.com
*.ap-adcenter.net
*.aureate-im.com
*.aureate.com
*.avenuea.com
*.bankads.com
*.beseen.com
*.bfast.com
*.bnex.com
*.broadcast.com
*.burstnet.com
*.centrport.net
*.cimedia.com
*.ads.cimedia.com
*.click2net.com
*.clickagents.com
*.cometsystems.com
*.commission-junction.com
*.coremetrics.com
*.datais.com
*.doubleclick.com
*.doubleclick.net
*.e-media.com
*.eads.com
*.engage.com
*.engageaudience.net
*.engageaudiencenet.com
*.enliven.com
*.eu-adcenter.net
*.euroclix.nl
*.flycast.com
*.focalink.com
*.futurenet.com
*.fxweb.com
*.hearme.com
*.hitbox.com
*.hitslink.com
*.home.net
*.ads.home.net
*.hyperbanner.net
*.iadnet.com
*.imgis.com
*.klikklik.nl
*.klsoft.com
*.link4ads.com
*.linkexchange.com
*.linksynergy.com
*.livestat.com

*.maximumpcads.com
*.maximumpcads.net
*.mediaplex.com
*.mediasynergy.com
*.monster.com
*.adserver.monster.com
*.mycomputer.com
*.narrowcastmedia.com
*.netbanner.com
*.nethit-free.nl
*.netpoll.nl
*.networkedbanners.com
*.ngadcenter.com
*.ngadcenter.net
*.nordby.com
*.pagecount.com
*.preferences.com
*.radiate.com
*.realmedia.com
*.realtracker.com
*.realtrackernl.com
*.registration-server.com
*.sabela.com
*.shopnow.com
*.smartage.com
*.spylog.com
*.superstats.com
*.targetnet.com
*.teknosurf.com
*.thecounter.com
*.track-star.com
*.track4.com
*.utopiad.com
*.valueclick.com
*.voila.com
*.webconnect.net
*.webtrends.com
*.webtrends.net
*.webtrendslive.com
*.worldbannerexchange.com
*.xxxcounter.com
*.zdnet.com
*.ads1.zdnet.com
*.ads2.zdnet.com
*.ads3.zdnet.com
*.ads4.zdnet.com

Dit is een hele waslijst zoals je ziet, maar dat is dan ook het resultaat van het nodige spitwerk op een aantal machines die door een groot aantal mensen gebruikt wordt om er mee te internetten. Dit zijn dus stuk voor stuk de sites van bedrijven wiens broodwinning het is om ons in kaart te brengen zonder dat ze het ons vertellen.

Omdat het dus een ongelofelijke hoeveelheid werk is om deze lijst in te voeren waarbij er ook nog een grote kans op typefouten aanwezig is, is deze lijst ook via een los programmaatje te installeren. Dit programmaatje (RESTRICTED.INF) zit standaard bij dit document en is via een klik met de rechtermuisknop en vervolgens de optie "Installeren" eenvoudig te gebruiken.

Let op: RESTRICTED is alleen bedoeld voor gebruikers van Windows 9x, NT en 2000 die minimaal Internet Explorer 4.0 of hoger gebruiken.

RESTRICTED zal er dus voorzorgen dat al de hierboven genoemde sites in de "Websites met beperkte toegang" van Internet Explorer worden opgenomen. Na installatie zijn de wijzigingen direct actief.

De toevoegingen zijn te bewonderen door in Internet Explorer te kiezen voor Extra -> Internet-opties... Klik vervolgens op het tabblad Beveiliging. Hier vind je de vier standaard zones terug die IE kent, namelijk: Internet, Lokaal intranet, Vertrouwde websites (Trusted Sites) en Websites met beperkte toegang (Restricted Sites). Kies voor de laatste, want daaraan zijn de hierboven genoemde sites toegevoegd. IE geeft zelf al als omschrijving dat hierin sites staan die potentieel gevaarlijk zijn voor je computer en of je gegevens. Iets wat dus precies is waarvan we de ingevulde sites van verdenken c.q. beschuldigen.

De inhoud kan je eenvoudig controleren (en zo nodig aanvullen of verwijderen) via de knop Websites... In het venstertje wat hierna verschijnt staan stuk voor stuk alle websites die we wilden beperken. Wil je zelf een website toevoegen dan moet deze op de volgende manier worden ingevoerd:

*.doubleclick.com

Het resultaat

Het effect van het opnemen van al deze websites onder "Websites met beperkte toegang" is dat we er een aparte set van regels op los kunnen laten. Eén kenmerk van de instellingen voor "Websites met beperkte toegang " is dat er geen cookies van worden geaccepteerd. Om hiervan zeker te zijn moet wel het beveiligingsniveau (dat schuifje) op Hoog staan. Staat hier echter Aangepast (Custom), klik dan op de knop Standaardniveau (Default level). Hierdoor wordt het beveiligingsniveau standaard op Hoog gezet. Indien je ook nog sites bij "Vertrouwde websites" hebt ingevuld dan moet ook deze nog worden gewijzigd. Klik hier ook op de Standaardniveau knop en wijzig daarna het niveau van Zeer Laag naar Gemiddeld. Hierdoor kunnen ze nog wel een cookie plaatsen zonder dat ze het je telkens vragen, maar verder kunnen er geen rare dingen gebeuren.

Voor alle andere websites die dus niet in de Vertrouwde of Beperkte toegang zones staan kunnen we ook nog wat instellen. Namelijk dat ze wel een tijdelijk cookie mogen plaatsen zonder dat te vragen, maar dat ze voor een permanent cookie wél toestemming moeten vragen. Om dit te bereiken moeten we de instellingen van de Internet zone op de volgende manier wijzigen.

Klik op de mini aardbol, hierdoor is de Internet zone actief geworden. Zet deze nu eerst op medium via de Standaardniveau knop als dit nog niet het geval is. Klik vervolgens op de knop "Aangepast niveau...". Scroll in het venster dat nu verschijnt naar de Cookies sectie en wijzig de optie "Cookies toestaan die op de computer zijn opgeslagen" van "Ingeschakeld" in "Vragen" en bevestigen de wijziging. Vanaf dit moment zullen alle andere websites die een permanent cookie willen plaatsen dit moeten vragen en heb je de keuze om dit wel of niet toe te staan.

Internet Explorer 6.x

Veel van wat hierboven staat is onder IE6 niet meer nodig of eenvoudiger te bereiken. Dit omdat IE6 voorzien is van uitgebreide privacy functionaliteit. Omdat IE6 nog in beta is, is het te vroeg om nu al diep hierop in te gaan. Wat ik al wel kan zeggen is dat het heel goed werkt en dat er meer gestopt wordt dan dat ik had verwacht!

Reclame filters

We hebben nu de spyware gestopt en ook het gebruik van cookies in de hand. Maar nog steeds zien we al die advertenties op de webpagina's en dat kost alleen maar downloadtijd en vertraagd het surfen onnodig. Maar ook hiervoor is door creatieve mensen een handige oplossing bedacht en wel de advertentie filters.

De twee meest gebruikte reclame filters zijn WebWasher en Proximitron. WebWasher is het eenvoudigst in het gebruik en zeker aan te raden voor een ieder die zich niet al te druk maakt over het feit dat er soms nog wel eens een advertentie er doorheen glipt. Ook de installatie van WebWasher is releatief eenvoudig en WebWasher is ook nog eens gratis voor persoonlijk gebruik.

Overzicht beveiligingssoftware

Dit overzichtje is meer een soort van service dan echt van toepassing op het voorgaande stuk. De software die hieronder genoemd wordt onderscheidt zich doordat het in principe freeware of goedkope shareware is en dat ze een duidelijk en strak gedefinieerd doel dient. Het laatste omdat specifieke software vaak uitblinkt in precies datgene wat het moet doen, terwijl duizendpoten vaak van alles een beetje kunnen en dat is dus te weinig als we het over beveiliging hebben.

Opmerking: De programma's met een * gebruik ik zelf naar persoonlijke tevredenheid

Anti-virus

AntiVir*	http://www.free-av.com
E-Trust	http://my-etrust.com
F-Prot	http://www.complex.is/f-prot

Cookie Management

Cookie Viewer*	http://www.karenware.com

FTP programma's zonder advertenties:

WS_FPT LE	http://www.ipswitch.com

Persoonlijke Firewalls

ZoneAlarm*	http://www.zonelabs.com
Tiny Personal Firewall	http://www.tinysoftware.com

Privacy en Encryption

Pretty Good Privacy (PGP)	http://www.pgpi.org

Reclame filters

WebWasher*	http://www.webwasher.com
Proxomitron	http://members.tripod.com/Proxomitron

Spyware

Ad-aware*	http://www.lavasoftusa.com

Trojanen

The Cleaner - van MooSoft	http://www.moosoft.com/cleaner.html