1. Uw computer beveiligen

Voor computers die verbinding maken met internet is goede beveiliging essentieel. Een goed beveiligingssysteem verkleint het risico op *malware* (virussen of andere schadelijke software) op uw computer.

Een met virussen besmette computer kan erg frustrerend zijn. Niet alleen voor u, maar ook voor anderen. Als uw computer besmet is, kan deze ook andere computers infecteren. Dit gebeurt ongemerkt, bijvoorbeeld wanneer u een e-mail verzendt of als u bestanden deelt.

Als computergebruiker bent u verantwoordelijk voor de beveiliging van uw eigen pc. In de eerste plaats is het belangrijk dat u *Windows* en gewone programma's regelmatig *update*. Dit houdt in dat een nieuwe, verbeterde versie van een programma wordt geïnstalleerd. Hiermee worden onder andere recent ontdekte veiligheidsproblemen opgelost.

Windows 8.1 helpt bij beschermen tegen malware met *Windows Defender*. *Windows 7* gebruikt hiervoor *Microsoft Security Essentials*. Een ander beveiligingshulpmiddel van *Windows* is het *Onderhoudscentrum*. In het *Onderhoudscentrum* kunt u de beveiligingsinstellingen voor *Windows* controleren op uw computer en, indien nodig, aanpassen. U ziet dan ook of *Windows Firewall*, de bescherming tegen ongewenste toegang, is ingeschakeld.

Ook is het belangrijk dat de beveiligingsopties van internetbrowsers als *Internet Explorer* ingeschakeld zijn. Hiermee voorkomt u onder andere dat u het slachtoffer wordt van *phishingwebsites*. Dit zijn websites waarop met behulp van valse informatie wordt geprobeerd belangrijke gegevens, zoals uw toegangscodes voor internetbankieren, te stelen.

Invoegtoepassingen, ofwel *plugins* of *add-ons*, voegen extra functies toe aan een internetbrowser. Meestal functioneren ze goed, maar soms kunnen ze problemen geven. Daarom is het handig als u ze zelf weet te beheren.

In dit hoofdstuk leert u:

- wat malware is;
- *Windows* updaten;
- andere software updaten;
- over antivirussoftware;
- werken met het *Onderhoudscentrum*;
- werken met *Windows Defender* in *Windows 8*;

- werken met *Microsoft Security Essentials* in *Windows 7*;
- *Windows Firewall* gebruiken;
- kennismaken met phishing;
- anti-phishing opties aanzetten in een internetbrowser;
- andere beveiligingsopties aanzetten in een internetbrowser;
- werken met invoegtoepassingen of plugins in internetbrowsers.

Let op!

Windows 8.1 wordt in dit boek aangeduid als *Windows 8*. *Windows 8.1* is namelijk een update van *Windows 8*.

1.1 Wat is malware?

De term *malware* is een samentrekking van *malicious software*, ofwel kwaadaardige of schadelijke software. Het is een verzamelnaam voor software die schade kan aanrichten op uw computer.
Voor een deel worden deze programma's gemaakt door personen die het leuk vinden om in te breken in computers (ook wel *hacken* genoemd) of vervelende programma's te verspreiden. Maar vooral professionele criminelen houden zich tegenwoordig bezig met deze lucratieve vorm van misdaad. Met computercriminaliteit of cybercrime zijn namelijk miljoenen te verdienen.

Malware is onder te verdelen in verschillende soorten:

- *Virus* is een verzamelnaam voor kleine programma's die zelfstandig kunnen functioneren, maar meeliften in een ander programma. Als het besmette programma wordt geopend, wordt automatisch het virus geactiveerd. Sommige virussen richten weinig schade aan. Ze laten bijvoorbeeld een bepaalde boodschap op uw beeldscherm zien op een bepaalde datum, maar doen niet meer dan dat. Andere, meer agressieve, virussen nemen steeds meer ruimte in op uw harde schijf en besmetten steeds meer programma's, zodat u op een gegeven moment niet meer kunt werken op uw computer. Een belangrijke eigenschap van virussen is dat ze zich makkelijk kunnen vermenigvuldigen en zichzelf zelfstandig kunnen verspreiden, bijvoorbeeld door zichzelf te versturen via e-mails aan mensen in uw adresboek.

- *Wormen* en *Trojaanse paarden* zijn varianten op virussen. Ook dit zijn programma's die net zo schadelijk kunnen zijn als virussen, maar los van andere programma's functioneren. Ze worden vaak gebruikt door hackers (computerinbrekers) om uw computer over te nemen voor criminele activiteiten, zoals voor het inbreken op grote bedrijfswebsites.

- *Spyware* is geen virus, maar schadelijke software die stiekem op uw computer wordt geplaatst wanneer u een besmet programma installeert of een schadelijke website bezoekt. Spyware wordt gebruikt om uw computer te bespioneren en uw gegevens via internet door te geven aan malafide organisaties en criminelen. Die gebruiken uw gegevens bijvoorbeeld om u ongewenste reclamemails (spam) te sturen.

- *Adware* plaatst tijdens het surfen advertenties in uw venster of een apart venster. Adware verschijnt vaak nadat u een gratis programma heeft geïnstalleerd.

- De laatste jaren is de zogenaamde *ransomware* (gijzelvirus) in opkomst. Hierbij wordt met malware uw computer lamgelegd. U krijgt de mededeling dat u door geld te storten uw computer weer 'terugkrijgt'. Een variant hierop is een valse mededeling van ransomware dat u zogenaamd illegale activiteiten met uw computer heeft uitgevoerd en dat u door geld te storten, arrestatie door de politie kunt voorkomen. U moet nooit op dit soort afpersing ingaan en aangifte doen bij de politie.

1.2 Windows updaten

Windows wordt continu aangepast, uitgebreid en verder beveiligd. De toevoegingen en verbeteringen worden door Microsoft in de vorm van *software updates* verspreid. Er zijn kleine updates met enkele toevoegingen voor *Windows* of de programma's. Maar ook grotere updates, *Service Packs* genoemd.
Het is belangrijk dat *Windows* zo snel mogelijk van de laatste updates wordt voorzien. Zo voorkomt u dat ontdekte beveiligingsfouten kunnen worden misbruikt.

De updates van *Windows* worden verzorgd door *Windows Update*. Dit is een systeem dat controleert of u de meest recente versie van *Windows* gebruikt. *Windows Update* staat standaard ingesteld op automatisch updaten, maar het is verstandig dit te controleren.

Ook is het soms nodig om zelf handmatig *Windows* te updaten in plaats van te wachten tot de automatische update zijn werk doet. Bijvoorbeeld als u merkt dat *Windows* niet goed werkt. Soms kan een update dan helpen de problemen op te lossen.

Let op!

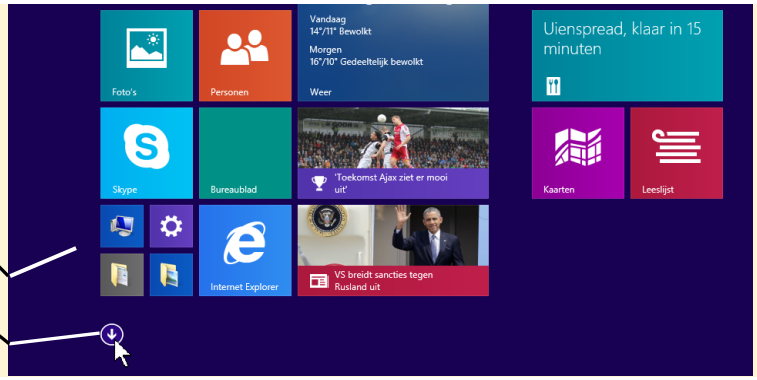
Microsoft verstuurt nooit software updates per e-mail. Als u een e-mail ontvangt waarin staat dat de bijlage Microsoft-software of een *Windows*-update bevat, open dan nooit de bijlage. Verwijder de e-mail onmiddellijk en vergeet niet deze ook uit de map *Verwijderd* te verwijderen. Dergelijke e-mails worden door criminelen verstuurd die proberen schadelijke software op uw computer te installeren.

U opent *Windows Update* via het *Configuratiescherm*.

In *Windows 8*, vanuit het startscherm:

Plaats de aanwijzer onder in het startscherm

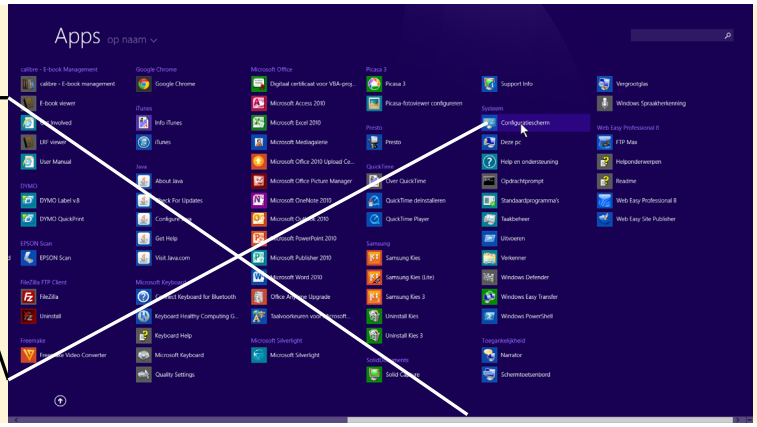
Klik op 



U ziet de apps op uw computer:

Sleep, indien nodig, het schuifblok naar rechts

Klik bij Systeem **op** Configuratiescher...



Tip

Configuratiescherm in Windows 8

U kunt het *Configuratiescherm* in *Windows 8* snel openen door te rechtsklikken op de startknop in de taakbalk. Klik daarna op Configuratiescherm.
Ook kunt u in het startscherm 'Configuratiescherm' typen.

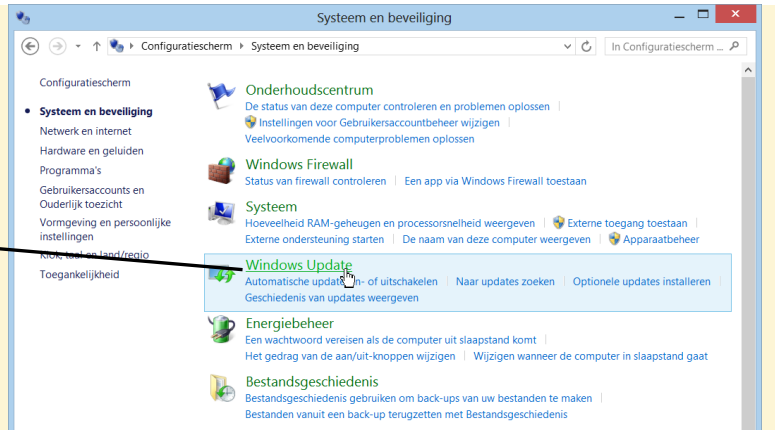
In *Windows 7*:

Klik op , Configuratiescherm

Vervolgens in beide versies:

Klik op Systeem en beveiliging

Klik op
Windows Update

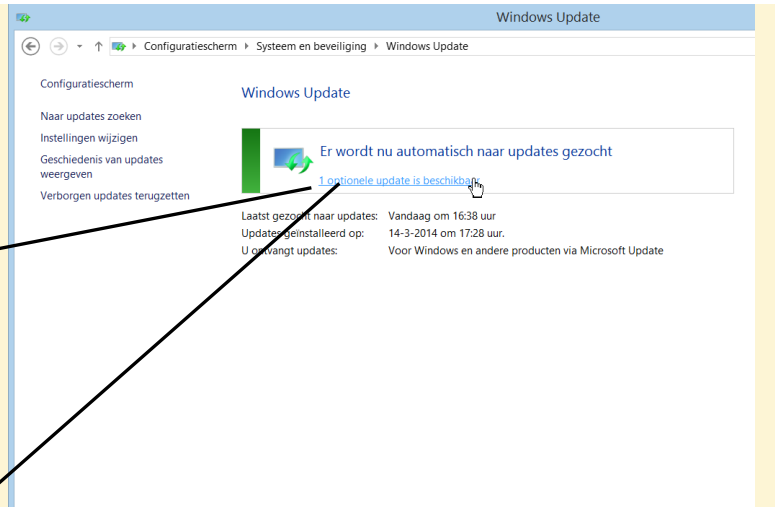


U ziet het venster *Windows Update*:

In dit voorbeeld staat een update klaar om geïnstalleerd te worden:

Om deze te bekijken en eventueel te installeren:

Klik op
update is beschikbaar



U ziet de updates die geïnstalleerd kunnen worden. Om een update te installeren:

Klik een vinkje ☑ bij de gewenste update

In *Windows 8*:

Klik op Installeren

In *Windows 7:*

Klik op OK