

Het verschil tussen malware en virussen

Malware is een verzamelnaam voor alle schadelijke software. Als er malware op uw computer aanwezig is, heeft u dit meestal niet door. In dat opzicht is malware ook heel anders dan een virus. Bij een virus merkt u dat uw computer zich anders gedraagt. Deze wordt traag en programma's kunnen soms niet meer geopend worden. Bij malware is dit niet het geval. Tegenwoordig spreken we ook amper meer over een virus. En juist omdat malware zich vaak stil en verborgen houdt, kan dit vervelende gevolgen hebben.

Wat kunt u tegen malware / virussen doen?

- Zorg voor goed en up-to-date antivirus programma
- Verwijder e-mail die u niet vertrouwd, de link in de e-mail kan het virus oproepen of er zit een zip (exe, pdf) bestand bij die het virus bevat. (bel desnoods de afzender, mocht u twijfelen)
- Zorg dat u de extensies (exe, bat, cmd, pdf etc) ziet in de verkenner (een meegestuurde pdf kan bv een factuur.pdf.exe zijn, u ziet als de extensies niet aan staan alleen factuur.pdf)
- Zorg voor een goede back-up
- Zorg ervoor dat de back-up software die u gebruikt geen Windows koppeling heeft (drive letter)
- Zorg ervoor dat Windows (verkenner) geen koppeling heeft (drive letter) met uw back-up device (apparaat)

Mocht u hulp nodig hebben om bovenstaande wijzingen door te voeren, kan PeteSoft u hiermee helpen.

Welke soorten malware zijn er?

Er zijn verschillende soorten malware te onderscheiden. Allemaal zijn het stukjes software die zich via verschillende wegen en met verschillende doelen proberen te nestelen in uw computer.

Trojaanse paarden

Een Trojaans paard zit verstopt in iets dat goedaardige software lijkt. Echter, op de achtergrond wordt er schadelijke software op uw computer geplaatst. Deze schadelijke software opent diverse 'backdoors' van uw computer. Via zo'n achterdeurtje kunnen cybercriminelen uw computer binnenkomen. Vervolgens kunnen zij documenten en gegevens op uw computer inzien en doorsturen.

Rootkits

Een rootkit is schadelijke software die zich diep in de computer weet te plaatsen. De meest vervelende variant is de MBR-rootkit. Hierbij wordt uw 'Master Boot Record' geïnfecteerd, waardoor de schadelijke software al geladen wordt tijdens het opstarten van uw computer. Vaak maken rootkits deel uit van andere malware.

Rogueware

Dit zijn programma's die zich voordoen als 'goede' beveiligingssoftware. Er verschijnen valse meldingen op uw scherm die u vertellen dat er problemen zijn met uw computer. Bijvoorbeeld dat er een virus aanwezig is of dat er problemen zijn met uw harde schijf. Vervolgens moet u dure (nep)software kopen die het probleem zou oplossen, maar daarentegen wordt het probleem juist verergerd. Rogueware is erg moeilijk te verwijderen van uw computer.

Keyloggers

Een keylogger registreert al uw toetsaanslagen, maar maakt ook screenshots van uw scherm. Cybercriminelen kunnen op die manier met u meekijken. Ook wanneer u vertrouwelijke informatie bekijkt of invoert, zoals inloggegevens en bankgegevens.

Browser hijackers

Dit is malware die een deel van uw internetbrowser overneemt. Een browser hijacker zal bijvoorbeeld uw zoekopdrachten omleiden naar kwaadaardige websites. Het belangrijkste doel van zo'n hijacker is dat het internetverkeer naar die site toeneemt. Een browser hijacker installeert vaak een zoekbalk of verandert steeds de startpagina van uw browser. Op de achtergrond wordt vertrouwelijke informatie verzameld en doorgestuurd naar cybercriminelen. Ook worden browser hijackers gebruikt voor klikfraude. Dat is een verschijnsel waarbij de malware expres klikt op online advertenties, zodat cybercriminelen geld verdienen aan de online adverteerders.

Ransomware

Ransomware vergrendelt uw computer en/of uw bestanden, waardoor u deze niet meer kunt gebruiken. De bekendste variant is het 'politievirus'. U krijgt dan een melding te zien, zogenaamd van de politie: u moet een boete betalen voordat u uw computer/bestanden weer kunt gebruiken. Als u getroffen bent door ransomware, betaal dan nooit. Uw geld komt terecht bij cybercriminelen en er is geen garantie dat de boeven na betaling uw computer en bestanden ontsleutelen.

Spyware

Spyware is schadelijke software die wordt geïnstalleerd zonder dat u het weet. Er worden gegevens van u verzameld worden zoals uw surfgedrag. Deze gegevens worden vervolgens gebruikt om verkooptechnieken aan te passen aan uw surfgedrag. Spyware wordt automatisch meegeïnstalleerd met andere software. Dit is meestal dan ook gratis software.

Adware

Dit is eigenlijk de minst gevaarlijke vorm van malware, maar het kan wel vervelend zijn. Tijdens het surfen krijgt u ongewenste reclame, banners en pop-ups te zien. Uw internetbrowser wordt ook traag door adware.