Virussen

Over computervirussen worden de gekste verhalen verteld. Het zouden beestjes zijn die in je computer zitten en de kabels stukbijten. Dat klinkt belachelijk, maar als je aan om het even wie vraagt wat computervirussen eigenlijk zijn, krijg je de meest uiteenlopende, verkeerde antwoorden. In deze tekst wordt de waarheid over virussen onthuld.

Wat is een virus?

Een computervirus is net zo goed een computerprogramma als bv. Microsoft Word. Het is dus een rij van eentjes en nulletjes die zich op een schijf bevindt en op een of andere manier in het RAM geladen wordt.

Zodra de code van een virus zich in het RAM bevindt, wordt het virus actief en voert het drie soorten acties uit. Vooreerst verbergt het zich zo goed mogelijk voor het besturingssysteem. Een virus dat je via Windows Verkenner kunt opsporen, is een slecht virus. Virussen passen soms uiterst ingenieuze technieken toe om zichzelf onzichtbaar te maken. Een tweede actie die een virus onderneemt, is zichzelf vermenigvuldigen. Dat betekent dat het zichzelf kopieert naar andere schijven en/of andere mappen op dezelfde schijf. Hoe meer het zich vermenigvuldigt, des te groter wordt de kans dat het bij een volgende werksessie opnieuw in het RAM terechtkomt. Ten slotte zal het virus ook allerlei beschadigingen aan het computersysteem toebrengen. Dat varieert van het tonen van een pingpongballetje op je scherm tot het formatteren van de harde schijf. Wanneer het die schade toebrengt, kun je niet echt voorspellen: dat kan drie dagen na de besmetting zijn, maar ook pas een jaar later. Het is in ieder geval absoluut noodzakelijk dat je virussen op een georganiseerde manier opspoort, vernietigt en probeert te weren.

Een computervirus kun je in alle opzichten vergelijken met een biologisch virus, zoals een griepje of een verkoudheid. Een biologisch virus dringt ook onopgemerkt zijn gastheer binnen, vermenigvuldigt zich, brengt schade toe en besmet ten slotte andere organismen. Net zoals er onschuldige en gevaarlijke biologische virussen zijn, zijn er onschuldige en gevaarlijke computervirussen.

Het virusmechanisme

Elk computervirus bestaat uit twee delen: een stukje code dat verantwoordelijk is voor het verbergen en het vermenigvuldigen van het virus en een stukje code dat instaat voor de beschadiging van het computersysteem. Virussen kunnen bestanden besmetten, maar ook speciale gebieden op een schijfstation (bv. bootrecords), cd-rw’s of zelfs het BIOS-ROM! De beschadiging die een virus teweegbrengt, gebeurt meestal op een door de software gedefinieerd tijdstip, bv. na drie weken besmetting, op vrijdag de 13de of wanneer de gebruiker voor de twintigste keer Microsoft Word start.

Verspreiding van virussen

Virussen verspreiden zich vooral via het internet. Elk bestand dat je van het internet haalt, kan in principe een virus bevatten. Het is dan ook absoluut noodzakelijk dat je je computersysteem op een efficiënte manier tegen internetvirussen beschermt. Naast het internet kunnen ook diskettes, cd-roms en USB-geheugenkaartjes haarden van virussen zijn. Ten slotte kunnen virussen zich heel gemakkelijk verspreiden via lokale netwerken.

Wie schrijft virussen?

In tegenstelling tot wat heel wat computergebruikers denken, worden virussen door mensen geschreven en ontstaan ze niet uit zichzelf. Het is wel mogelijk dat een virus zonder menselijke tussenkomst verandert (muteert) in een nieuw virus, net zoals dat bij het gewone griepje het geval is. Wie schrijft er nu virussen, denk je? Mensen van allerlei slag, gaande van informaticastudenten tot gefrustreerde programmeurs. Ze vinden het een uitdaging om hun virus zo onzichtbaar en gevaarlijk mogelijk te maken. Virussen verspreiden is een criminele daad die helaas moeilijk op te speuren en te beteugelen is.

Soorten virussen

Als je uitgaat van wat virussen juist besmetten, kun je vier soorten onderscheiden.

Allereerst is er het bestandsvirus. Het nestelt zich voornamelijk in uitvoerbare programma’s, zoals Microsoft Word of Patience. Dat betekent dat de code van het virus (eentjes en nulletjes) zichzelf midden in de code van het uitvoerbare programma plaatst, zodat dat helemaal niet opvalt voor het besturingssysteem. Zodra het uitvoerbare programma gestart wordt en in het RAM geladen wordt, gaat het virus gewoon mee naar het RAM en begint het daar aan zijn driedelige taak. Het zal zichzelf naar andere uitvoerbare programma’s kopiëren zodat de kans dat het in het RAM terechtkomt bij het starten van een programma alsmaar groter wordt.

Een tweede soort virussen zijn de bootsectorvirussen. Die nestelen zich in de bootsector van een harde schijf of een diskette. De bootsector van een schijf wordt door het computersysteem gelezen tijdens het opstarten. De bootsector bewaart vitale informatie voor het opstartproces, onder meer of er op de schijf in kwestie een besturingssysteem geïnstalleerd is waarmee opgestart kan worden. Bootsectorvirussen besmetten het RAM dus tijdens het opstartproces, bv. vanuit een besmette diskette die zich in het diskettestation bevindt of vanuit een besmette cd-rom in het cd-romstation.

Een derde soort virussen zijn macrovirussen. Die nestelen zich in stukjes uitvoerbare code (macro’s) in Microsoft Office-documenten. Zo kan een Word-document een macrovirus bevatten. Als je het Word-document opent, wordt het virus mee in het RAM geladen en begint het van daaruit aan zijn verwoestende taak.

Ten slotte zijn er de ROM-virussen die zichzelf, hoe onvoorstelbaar ook, naar ROM-geheugens kopiëren. Als de BIOS-ROM-chip een virus bevat, wordt dat al direct bij het opstarten actief, want zoals je weet, staat het BIOS-ROM in voor het opstartproces.

Hoe beveilig je het computersysteem tegen virussen?

De enige doeltreffende bescherming tegen virussen is de installatie van antivirussoftware. Een antivirusprogramma bestaat vrijwel altijd uit twee delen: een scanner en een virusschild.

De scanner is een programma dat in staat is om virussen op het computersysteem op te sporen. Elk virus heeft namelijk een stukje code (een patroon) dat uniek is voor dat virus en is daarom ook gemakkelijk herkenbaar. Een virusscanner onderzoekt de bestanden op je computersysteem en gaat na of er in die bestanden bekende viruspatronen voorkomen. Als je weet dat er enerzijds duizenden virussen zijn waarvan de scanner het patroon kent en dat er anderzijds tienduizenden bestanden op het computersysteem aanwezig zijn, besef je wel dat dat een erg intensief en tijdrovend proces is. Als je bovendien weet dat er elke maand tientallen nieuwe virussen verschijnen, is het belangrijk dat je je antivirussoftware up-to-date houdt. Dat gebeurt door via het internet de patronen (virusdefinities) van die nieuwe virussen te downloaden zodat je scanner ook die nieuwe patronen kan gebruiken bij het scanproces.

Anderzijds bevat het antivirusprogramma een virusschild. Dat stukje software wordt bij het opstarten van het besturingssysteem automatisch in het RAM geladen. Het voorkomt dat virussen via het internet, het lokale netwerk, diskettes of cd-roms je systeem binnendringen. Telkens als je een programma start, een bestand opent of gegevens van het internet downloadt, zal het virusschild controleren of de gegevens in kwestie geen viruspatronen bevatten. Het schild gebruikt dezelfde database van viruspatronen als de scanner. Essentieel is dus dat je die database up-to-date houdt door minstens wekelijks via het internet op zoek te gaan naar nieuwe viruspatronen. Beschik je over een breedbandverbinding, dan kun je ervoor zorgen dat je antivirusprogramma constant automatisch geüpdatet wordt.

Tips om virussen te voorkomen

Naast de installatie van goede antivirussoftware, die je bovendien minstens wekelijks vernieuwt, kun je ook andere maatregelen nemen om je computersysteem te beschermen. Laat bv. nooit diskettes of cd-roms in het computersysteem achter als je het uitschakelt. Als je namelijk ’s anderendaags opnieuw opstart en dat schijfje bevat een bootsectorvirus, dan is je systeem besmet! Wees voorzichtig met de informatie die je van het internet haalt. Vooral e-mails met twijfelachtige bijlagen (attachments) vormen een enorm risico. Open nooit een bijlage waarvan je de oorsprong niet kent. Ook gewone webpagina’s van verdachte websites en illegaal gekopieerde software kunnen virussen bevatten.