

Tien antivirustips

Het is een heel verhaal, maar lees het toch, want als uw computer besmet raakt, kan dit veel problemen opleveren voor uzelf en anderen.

Leg de vliegenmepper binnen handbereik

Tien praktische tips om het ongedierte buiten de deur (lees: computer) te houden.

Een computervirus is een stukje software, dat geschreven is om gegevensbestanden of programma's op de computer te wijzigen of iets toe te voegen. Een virus wordt gemaakt om zichzelf naar zoveel mogelijk bestanden te kopiëren. Ondertussen is de stamboom uitgebreid met wormen en Trojaanse paarden. Wormen willen zoveel mogelijk computers (in plaats van bestanden) aantasten. Ze doen dat typisch via e-mail of chatprogramma's. Een Trojaans paard camoufleert zich als iets leuks, een "cool spelletje dat je zeker moet proberen", maar is dat niet. De meest gehoorde voorbeelden zijn Trojaanse paarden die ongemerkt de veiligheidsinstellingen van uw computer veranderen en zo een achterpoortje openzetten voor inbrekers. Maar een Trojaans paard reproduceert zich niet zoals een virus of worm. Wel bestaan er ondertussen ook al virussen die deels ook worm en/of Trojaans paard zijn.

Om het eenvoudig te houden, gooien we alle termen op een hoop onder de naam virus. Vroeger verspreidden ze zichzelf vooral via diskettes. Maar met de opkomst van het Internet zijn de voornaamste bronnen van besmetting e-mail en downloads geworden. Slechts tien tot twintig procent van de virussen is echt schadelijk. Maar die schade kan aanzienlijk zijn en soms niet te herstellen. Stel u voor dat u morgen een virus binnenhaalt en plotsklaps alle bestanden in Word, Excel en PowerPoint verliest. Hoelang zal het duren voordat u weer verder kunt?

Als u geïnfecteerd bent en dit doorgeeft aan anderen, kan het nog erger worden. Uw familie en vrienden zouden het niet leuk vinden door u besmet te worden.



Preventie is dus geen luxe. 1. Installeer antivirussoftware

Een antiviruspakket heeft u al voor minder dan 50 euro per licentie. De software scant uw harde schijf en probeert te voorkomen dat een virus actief wordt. Als er een virus binnengedrongen is, zal de virusscanner de schade aan het bestand in kwestie proberen te repareren of het bestand vernietigen. Een antiviruspakket herkent uiteraard enkel virussen die in zijn databank zitten. Aangezien er elke dag nieuwe virussen bijkomen, is het belangrijk om regelmatig een update te installeren. Die update van virusdefinities kunt u gratis downloaden van de site van de fabrikant. Niet enkel de lijst met virussen moet pakweg wekelijks nagekeken worden. Ook de scan engine, de zoekmachine van de antivirussoftware, moet af en toe bijgewerkt worden.

Ook daarvoor vindt u on line updates. Op de websites van de fabrikanten van antivirussoftware vindt u zelfs gratis on line scanners. Bijvoorbeeld bij het Symantec AntiVirus Research Center of bij Thunderstore voor Kaspersky Anti Virus. Zo kunt u uw systeem via internet laten testen op de allernieuwste virussen. Dat is echter geen vervanging van geïnstalleerde pakketten. Het is slechts een momentopname en virussen via diskettes of e-mail ontsnappen aan deze on line controle.

U moet ook opletten welke programma's er gescand worden door een antiviruspakket. Ze scannen niet allemaal elk mogelijk e-mailprogramma of webbased e-mail, zoals Hotmail. Uw e-mailadres op het werk zal hoogstwaarschijnlijk wel gescand worden. Maar als u op het werk ook uw privé, e-mail via Hotmail opent, en een bijgevoegd bestand wil lezen, kunt u dat best nog eens apart scannen.

2. Installeer antivirussoftware overal

Als u op verschillende locaties werkt, is het belangrijk overal antivirussoftware te hebben. Ook elke desktop en elke laptop moet individueel gescand worden, en dit zowel op het werk als thuis.



3. Haal de bugs uit andere software

Schrijvers van virussen inspireren zich dikwijls op de bugs of programmeerfouten, in veel gebruikte software. Vooral van e-mailprogramma's zoals Outlook. Uiteraard schieten de producenten, bijvoorbeeld Microsoft, dan ook in actie. Zij geven regelmatig patches vrij, lapmiddel-tjes om de mazen in het net te dichten. Vandaar dat u niet alleen uw virus-scanner up to date moet houden, maar ook uw andere software.

4. Gebruik de juiste instellingen

Uw virusscanner moet ingesteld zijn voor alle mogelijke bronnen van besmetting: bestanden, macro's (kleine zelf toe te voegen programmatuur voor routine handelingen), attacheert (toegevoegde bestanden) en alles via het Web (e-mailen, chatten, downloaden). Stel in uw e-mailprogramma verder geen preview pane in, het kadertje onderaan waarin u het eerste stuk van een e-mail kan bekijken. Het staat gelijk met de e-mail openen en dat kan soms al fataal zijn. U moet goed uitkijken met de extensies van toegevoegde bestanden.

Dat zijn de twee of drie lettertjes na de punt, zoals bijvoorbeeld doc voor een Word-document. Probleem is dat door een standaardinstelling in Windows die extensies niet meer zichtbaar zijn.

Maar u kunt dat ongedaan maken. In "Verkenner" of "Explorer" kiest u "Extra" of "Tools", dan "Mapopties" of "Folder Options" en vervolgens "Weergave" of "View". Het kruisje bij "Bestandsextensies verbergen voor gekende bestandstypes" of "Hide file extensions for known file types" vinkt u weg.

5. Wantrouw toegevoegde bestanden

Als u een attachment ontvangt via e-mail, moet u wel oppassen. Bewaar en scan het bestand eerst op de harde schijf vooraleer het te openen. Enkel oppassen met e-mails van vreemden is niet voldoende. De recentste virussen verspreiden zich immers door zichzelf verder te sturen naar het adressenbestand binnen het e-mailprogramma. Dat zijn dus juist de collega's, vrienden en familie. Gebruik uw gezond verstand. Als uw baas u een liefdesbrief in attachment toestuurt, mag uw nieuwsgierigheid wel gewekt zijn. Maar geef toe, de kans is klein dat dit echt is. En uw beste vriend begint ook niet plotseling met u te corresponderen in het Engels of het Spaans, tot nu toe de talen waarin zo'n virusmails meestal geschreven worden. Een onderwerplijn met flarden tekst die op niets slaan is ook een indicatie. Controleer eerst bij de afzender of hij wel echt iets naar u gestuurd heeft.

Het is niet te verwonderen dat Word, Excel en PowerPoint de meest getroffen bestanden zijn. Virusschrijvers weten ook wel wat meest gebruikt wordt. Scan dus zeker documenten met de extensies doc, xls en ppt. Helemaal verboden zijn extensies die duiden op programma's die zichzelf installeren. De zwarte lijst van extensies is: bat, com, exe, js, pif, reg, scr, vba en vbs. Dubbele extensies, zoals loveletter.txt.vbs, zijn zo goed als zeker een virus.

6. Download voorzichtig

Als u programma's begint te downloaden van het Net, doe dat dan enkel van betrouwbare instellingen. Nadat de download op een diskette of de harde schijf staat, test u het best eerst met de virusscanner voordat u het opent en installeert.

7. Bij twijfel, haal hulp

Begin niet zelf te experimenteren als u twijfelt of iets besmet is of niet. Haal uw informaticadienst erbij. Als dat niet mogelijk is, kunt u on line ook terecht bij de fabrikanten van antivirussoftware.

8. Verspreid geen nepvirussen

Om het helemaal ingewikkeld te maken, zijn er ook nog grappenmakers die graag een HOAX, een vals alarm over een zeer gevaarlijk virus, de wereld insturen. De boodschap gaat dan als volgt: Een zeer belangrijke bron, zoals een nieuwzender of een software-fabrikant, waarschuwt voor een gevaarlijk virus. U wordt dringend verzocht de boodschap door te sturen naar al de mensen die u kent. Geloof niet zomaar alles. Stuur het bericht niet rond. Van dit soort kettingbrieven wordt niemand beter, dus in de prullenmand ermee.

9. MAAK REGELMATIG EEN BACKUP

Als een virus schade toebrengt, is het niet zeker dat de aangetaste bestanden gerepareerd kunnen worden. Maak dus regelmatig een back-up. Doe dit na een viruscontrole, zodat de back-up virusvrij is. Maak op diskette of op een beschrijfbare

cd-rom een back-up van zowel uw systeem (om uw computer later weer opgestart te krijgen), als van uw data (om uw verloren gegevensbestanden te recuperen)

10. VOLG HET LAATSTE NIEUWS OVER VIRUSSEN

Laat u niet verrassen door het allerlaatste virus waartegen de virusscanners nog niet gewapend zijn. Als er een echt ernstig virus opduikt, worden er door verschillende antivirusbedrijven en instanties waarschuwingen verspreid. Ook op IT-nieuwssites zoals www.zdnet.nl of de sites van de fabrikanten zelf vindt u informatie.

Symptomen

Symptomen herkennen is zeer moeilijk. Van een goed geschreven virus merk je immers niets. De volgende gebeurtenissen kunnen verdacht zijn:

- U dubbelklikt op een toegevoegd bestand in een e-mail. Het bestand gaat open en vliegensvlug weer dicht.
- U dubbelklikt en krijgt een foutmelding.
- Uw computer begint veel trager te werken dan normaal, zonder dat u extra software hebt geïnstalleerd.
- Tijdens een chatsessie ziet u antwoorden verschijnen die u helemaal niet geschreven hebt.
- Tijdens het chatten begint uw harde schijf hard te draaien. Alles wat ongebruikelijk is, berichtjes of geluidjes, plots verdwenen of aangemaakte bestanden, mag een alarmbelletje doen rinkelen.

Te laat! Wat nu?

- Verbreek onmiddellijk de verbinding met internet en schakel uw eigen netwerk uit als u dat hebt. Zo voorkomt u de verspreiding naar andere computers.
- Laat de computer gewoon open staan. Een aantal virussen wordt pas echt actief als de computer opnieuw opstart.
- Haal uw systeembeheerder erbij, of andere professionele hulp. Vertel hen eerlijk wat er gebeurd is. Als u dubbelklikte op een toegevoegd bestand met de naam "mooi_kontje", dan komt men daar toch achter.
- Neem contact op met de mensen met wie u recent nog gegevens uitwisselde (bestanden of e-mail). Als u weet van wie het virus kwam, laat die persoon het dan zo snel mogelijk weten.

Bron: ZD Smart Business

