3 1 Virussen

Auteur	Bètapartners
Team	Wikiwijs Maken Auteurs
Laatst gewijzigd	29 oktober 2014
Licentie	CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie
Webadres	https://maken.wikiwijs.nl/45972/

Inhoudsopgave

1 Virussen

Een virus is een computerprogramma dat zich op je computer kan bevinden, vaak zonder dat jij daar weet van hebt. Alhoewel dit soms weinig kwaad kan, worden computervirussen in het algemeen als schadelijk beschouwd. In ieder geval nemen ze schijfruimte en computertijd in beslag. In ernstige gevallen kunnen ze in de computer meer schade aanrichten: bijvoorbeeld het verwijderen van belangrijke bestanden of het verspreiden van gevoelige informatie.

Virussen zijn gemaakt om zichzelf te dupliceren en te verspreiden. Op die manier besmetten ze zoveel mogelijk computers. Net als organische virussen (het griepvirus bijvoorbeeld) kunnen sommige computervirussen niet apart bestaan. Dan zijn het stukjes code die aan een ander programma vastgeplakt zitten.

Virussen verspreiden zich door van het ene (besturings)systeem naar het andere over te gaan, door van het ene bestand naar het andere overgebracht te worden en van een digitaal transportmedium naar het andere vervoerd te worden. Veel virussen hebben een "gastheer" nodig: een bestand waar het gebruik van kan maken, of waar het zich aan kan hechten. Zo'n bestand is meestal een *executable*, een programma dat je in werking kunt stellen, bijvoorbeeld een spelletje dat je wilt spelen.

De schade die een virus kan aanbrengen, varieert van geen tot heel veel. Geen schade brengt het aan als het bijvoorbeeld alleen bijvoorbeeld een pop-up laat zien met een boodschap die je een beetje in verwarring kan brengen. Een onverwacht bericht "*Uw printer kan nu niet meer gebruikt worden*" terwijl het apparaat uitstekend functioneert, kan storend werken maar het richt geen schade aan. In het begin werden vooral virussen met een wat pesterig karakter verspreid. Sommige virussen zorgden voor de aantasting van het normale computerbeeld door op willekeurige plekken pixelkleuren te veranderen of die zwart te maken, waardoor het leek alsof ze uitgevallen waren. Serieuzer wordt het als het virus allerlei onzinpagina's op je printer laat afdrukken, want dat kost je papier en inkt of toner. En erg kwalijk is het als een virus bestanden gaat verwijderen, zodat je na herstart van je pc niet meer (goed) kunt werken.

Er bestaan verschillende soorten virussen. De belangrijkste typen zijn:

- **Bestandsvirus** : Een bestandsvirus hecht zichzelf aan een programmabestand. Programmabestanden zijn de bestanden die je uit kunt voeren; je kunt ze herkennen aan de extensies .EXE of .COM (onder extensie verstaan we de letters achter de punt in een bestandsnaam). Zodra een besmet programmabestand geopend wordt, wordt het virus actief.
- **Macrovirus** : Macrovirussen komen voor in Word- of Excel-documenten. Ze worden actief als het document gestart wordt. Macrovirussen komen bijna niet meer voor, de laatste grote uitbraak was in 1999.
- **Bootsectorvirus** : Bootsectorvirussen richten schade aan in de bestanden die nodig zijn om een computer op te starten. Een bootsectorvirus kan er voor zorgen dat een computer niet meer kan worden opgestart.
- **Polymorf virus** : Een polymorf virus verandert steeds van verschijningsvorm als het zich verspreidt.
- **Tijdbom virussen** : Tijdbom virussen zijn geprogrammeerd om op een bepaalde datum of tijd in actie te komen. Voor die tijd doen ze niets.
- **Mobielvirus** : Een mobielvirus richt zich niet op computers, maar op mobiele telefoons of PDA's. Het virus kan zich verplaatsen van de ene mobiele telefoon naar de andere.

1.1 Wormen

Wormen zijn stukjes programmacode die zich in een computer nestelen.

Belangrijke eigenschappen van een worm zijn:

- de worm verspreidt zich via netwerkpoorten, waarbij hij zelfstandig op zoek gaat naar computers op het netwerk (Internet of een ander netwerk)
- de worm werkt op zichzelf en niet via een ander programma;
- hij gaat van systeem naar systeem en infecteert geen bestanden, maar systemen.

Een wormvirus zoekt bijvoorbeeld slecht beveiligde computers op waar hij op kan binnendringen. Van daaruit verspreidt hij zich weer verder. Zoals gezegd verspreiden wormen zich zelfstandig, ze hoeven niet mee te liften met een e-mail of een of ander programma.

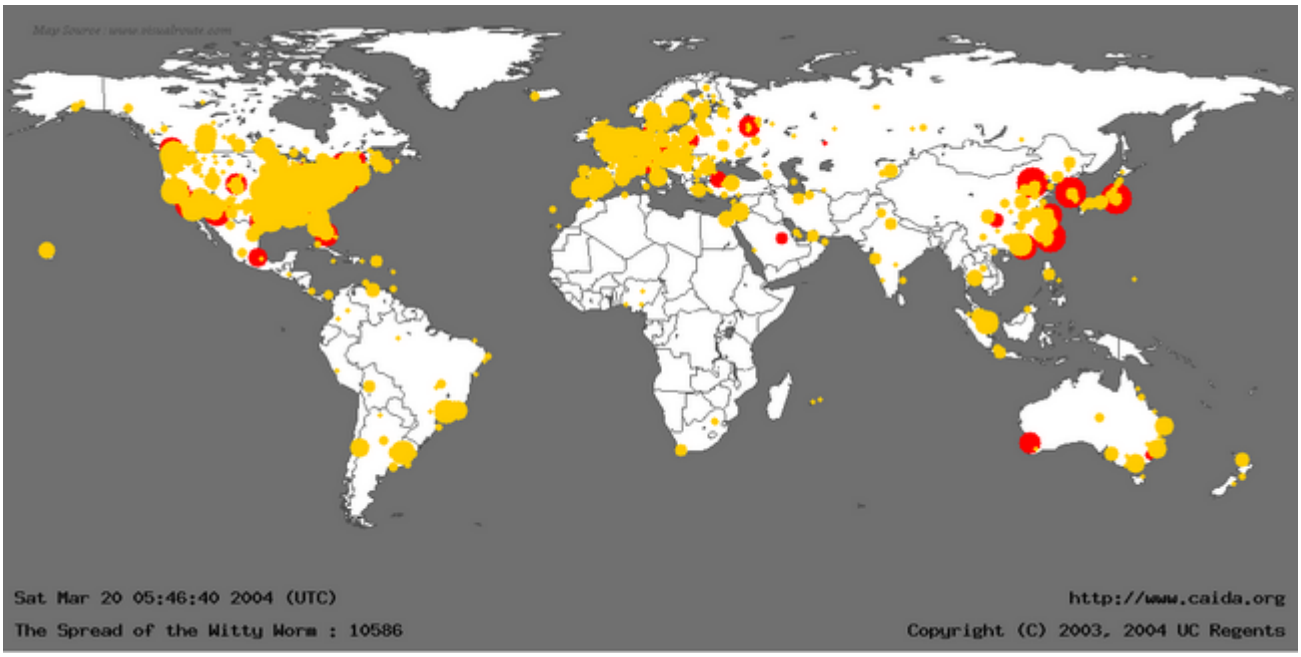
Wormen kunnen allerlei nare effecten hebben. In het eenvoudigste geval benadelen ze het netwerkgebruik door zelf bandbreedte te gebruiken, waardoor je computer heel traag wordt. Ze kunnen echter ook de geïnfecteerde computer schade toebrengen door bestanden te vernielen. Sommige wormen versturen *spam* vanaf de computers die ze infecteren, of ze laten aanvallen uitvoeren op andere computers op Internet.

Belangrijk is te weten dat een worm een pc kan omvormen tot een zogenaamde *zombie* (afgeleid van het woord robot).

De eerste worm op het internet werd gemaakt door Robert Tappan Morris jr in 1988. De worm heette daardoor ook de Morris Worm.

In 2004 verspreidde zich de W32/Amus-A worm via e-mail. Als een gebruiker het meegestuurde bestand opende, dan werd er een boodschap voorgelezen. Deze pratende worm maakte gebruik van de Microsoft speech engine in Windows.

Omdat wormen zich zelfstandig verspreiden gaat dit veel sneller dan bij virussen. In de animatie hieronder is te zien hoe de worm Witty zich in 2004 binnen 2 uur over de hele wereld kon verspreiden



Opdracht

Maak nu de opdracht "Wormen" uit het menu-onderdeel "Opdrachten en Toetsen".

1.2 Logic Bomb

Een *logic bomb* is een soort digitale tijdbom die onder bepaalde voorwaarden afgaat. Je pc zal er niet door ontploffen, maar een logic bomb kan alles uithalen wat ook door malware (schadelijke software) kan gebeuren. Iemand die weet hoe hij zo'n logic bomb kan programmeren, kan er voor zorgen dat het ding afgaat als bijvoorbeeld niet aan zijn wensen wordt voldaan. Denk aan een ict-beheerder die ontslagen dreigt te worden en dan met behulp van zijn logische bom het netwerk zodanig kan ontregelen dat hij de enige is die het systeem kan herstellen. Je vraagt je dan natuurlijk wel af of zo iemand weer in dienst genomen wordt ...
De meeste logic bombs worden gemaakt met kwaadaardige doeleinden. Ook gewone virussen kunnen logic bombs zijn, als ze op een bepaalde dag of een bepaalde tijd hun kwalijke werk gaan verrichten. Vrijdag de 13e is zo'n beruchte dag.

Celstraf voor systeembeheerder wegens digitale tijdbom

Een voormalig systeembeheerder van Medco Health Solutions heeft een gevangenisstraf van dertig maanden en een boete van tachtigduizend dollar gekregen wegens sabotage van computersystemen. De straf die de ex-systeembeheerder Yung-Hsun Lin in het vonnis kreeg opgelegd was uitzonderlijk hoog, aangezien de gegevens die de man probeerde te wissen, zeer gevoelig waren. De voormalige werkgever Lin verwerkte farmaceutische gegevens van particulieren. Aangezien artsen de Medco-database raadplegen bij het voorschrijven van medicatie, werd voor de hoge straf gekozen.
Yung-Hsun Lin probeerde in oktober 2003 een zogenaamde logic bomb te plaatsen bij zijn toenmalige werkgever. Doel was om de gegevens op ruim zeventig HP-Unix servers te wissen, omdat hij verwachtte dat hij op korte termijn ontslagen zou worden. De 'bom' zou op zijn verjaardag, 23 april 2004 moeten afgaan, maar weigerde door een programmeerfout tot actie over te gaan. Hoewel hij zijn baan op dat moment nog niet kwijt was, herprogrammeerde Lin zijn software zodat die een jaar later af zou gaan. Een paar maanden voor die datum ontdekte een collega-systeembeheerder de software echter waarna de bom ontmanteld werd.

Naar: Willem de Moor, Tweakers.net, 9 januari 2008

1.3 Trojaanse paarden

Een Trojaans paard is een programma dat nuttig lijkt maar heel vervelende eigenschappen heeft. Je downloadt het programma omdat je denkt dat het nuttig is, maar nadat je het programma hebt gestart blijkt vaak dat het programma de beveiliging op je PC heeft lekgeprikt.

Een Trojaans paard vermenigvuldigt zichzelf niet zoals wormen en sommige andere virussen dit doen, maar zorgt ervoor dat gebruikers zelf de code binnenhalen. Het programma komt meestal in de vorm van een handig hulpprogramma, een leuke screensaver of als zogenaamde upgrade. Of misschien als gratis fotobewerkingsprogramma, omdat de legale varianten daarvan best wel wat kosten. Wil je zo'n hebbedingetje dan op je pc hebben staan, dan download je het bestand en besmet je zo je eigen computer. Vooral in peer-to-peer netwerken zijn veel trojans actief. Peer-to-peer netwerken zijn min of meer directe verbindingen tussen diverse computers op Internet, die rechtstreeks van elkaar bestanden kunnen downloaden of uploaden.

Zo'n "aantrekkelijk" programmaatje heeft bijvoorbeeld de bestandsnaam *Christina_Aguilera_bloot_in_bad.exe*. Mensen die Christina Aguilera leuk vinden, downloaden het bestand en klikken erop. Het lijkt of er niks gebeurt, maar in feite wordt de computer dan onzichtbaar besmet en verandert het systeem in een *zombie* (een computer die op afstand bestuurbaar is door degenen die de trojan hebben gemaakt). Trojans hoeven niet meteen aan de slag te gaan, dus je merkt er soms de eerste tijd niks van dat je het Trojaanse paard in huis gehaald hebt. Maar na een tijdje begint de trojan zijn kwalijke activiteiten en kan hij bijvoorbeeld wachtwoorden stelen, bestanden verwijderen, of poorten op je pc openzetten.

Een voorbeeld hiervan is een Trojaans paard dat zich voordeed als een gratis programma tegen de Blasterworm. Maar wie het programmaatje installeerde zette zijn computer open voor hackers.

De naam Trojaans paard heeft te maken met een verhaal over de Trojaanse Oorlog.

De Trojaanse oorlog (rond 1180 voor Christus):
Al tien jaar vochten de Grieken tegen de Trojanen. Het lukte de Grieken maar niet om de stad Troje in te nemen. Daarom bedacht de Griek Odysseus een list.
De Grieken bouwden een reusachtig houten paard. Soldaten verstopten zich in de buik van het paard. Dit paard werd 's avonds voor de poort van Troje achtergelaten. De Grieken verzonnen een list zodat de Trojanen dachten dat het paard van Pallas Athena kwam en de stad zou beschermen. De Trojanen trapten in de list en haalden het paard met veel moeite de stad binnen. Ze dachten dat ze gewonnen hadden en vierden de hele avond feest om de overwinning te vieren. Toen 's nachts alle Trojanen sliepen, verlieten de Grieken het paard en openden de poorten zodat de Grieken die nog buiten waren, naar binnen konden. De Trojanen waren te moe en te dronken om de stad nu nog te verdedigen. De Grieken staken alles in brand en binnen korte tijd was er niets meer van Troje over.

1.4 Botnets

Een bot is een programma dat zelfstandig geautomatiseerde taken kan uitvoeren. Zo worden bots vaak gebruikt om zaken te doen die bijna onmogelijk zijn voor mensen.

Het woord bot komt van robot. Als een hacker op duizenden pc's tegelijk een virus loslaat, die de duizenden pc's tot botnet omtovert, dan kan de hacker dit botnet op afstand beheersen. Al de machines in een botnet zijn in de macht van de hacker die ze kan gebruiken om spam te versturen, wachtwoorden en creditcardgegevens te verzamelen en nog veel meer. Een botnet van enkele duizenden computers wordt overigens beschouwd als een kleine jongen. De echt zware jongens tellen honderdduizenden tot miljoenen computers. Een bot van een botnet draait meestal op de achtergrond zodat hij niet opvalt op de computer. Vaak heeft de (kwaadwillende) beheerder van een botnet de beschikking over een aantal hulpmiddelen om firewalls en buffers op andere computers te omzeilen. Heel slimme bots kunnen vaak zelf zwakke punten in een computer opzoeken. Met de worm en bot zijn we al een heel eind verwijderd van de oorspronkelijke virus.

Een bot kan heel onschuldig en zelfs handig zijn, maar ook heel vervelend. Een computer die besmet is met een bot wordt ook wel een zombie genoemd. Een botnet is een netwerk van een groot aantal willoze zombies die allemaal besmet zijn met dezelfde bot. Vanuit één centraal punt kan een kwaadwillend persoon alle zombies in het netwerk opdracht geven dezelfde taak uit te voeren.

Opdracht

Maak nu de opdracht "Bots" uit het menu-onderdeel "Opdrachten en Toetsen".

1.5 Meelifters

1.5a Spyware

Spyware is de naam voor computerprogramma's (of delen daarvan) die informatie vergaren over een computergebruiker en deze doorsturen naar een derde partij. Het doel van spyware is meestal geld verdienen. De term is een samentrekking van het Engelse woord *spy* van spion en *ware*, dat aangeeft dat het om software gaat.
De opkomst van spyware is onder andere het gevolg van het illegaal kopiëren van software. De programmamakers zoeken, nu ze minder inkomsten uit verkopen halen, naar andere manieren om geld te verdienen. Het toevoegen van spyware aan een programma is een manier om dat te bereiken. Zo zijn er twee versies van het peer-to-peerprogramma Kazaa: de ene kost geld, de andere bevat spyware. Naast deze commerciële vorm van spyware bestaat er ook een vorm met meer criminele doeleinden.

Meestal hebben gebruikers geen weet van de spywarefunctie van een programma. Er zijn echter varianten waarbij gebruikers wel over de spywarefunctionaliteiten ingelicht worden. Vaak vindt dit dan op een listige wijze in de algemene voorwaarden plaats.

Voorbeelden van het aftappen van gegevens zijn bezochte internetpagina's inclusief de tijdsduur van het bezoek, e-mailadressen, gebruikte en geïnstalleerde programma's. Deze informatie wordt voornamelijk gebruikt voor reclamedoeleinden, het belangrijkste doel is dan ook geld verdienen.

Spyware is de verzamelnaam voor de volgende types software:

- **Trackingcookies** : Een cookie is een klein bestandje met informatie dat op je computer terecht komt na het bezoeken van een website. Vaak zijn cookies nuttig: ze onthouden bijvoorbeeld je instellingen of loginnaam voor een bepaalde site. Trackingcookies zijn minder onschuldig, ze volgen je surfgedrag (dus welke websites je bezoekt) en sturen dat door naar de site dat het trackingcookie heeft geplaatst. Zo is het voor bedrijven mogelijk om met trackingcookies je surfgedrag te volgen.
- **Reclame banners** : Een reclame banner is een pop-up venster met reclame. Naast de pop-up schermpjes bestaan er ook pop-under vensters. De verbergen zich onder de openstaande vensters. Je ziet het pop-under scherm dus pas later als je de openstaande vensters wegklikt. Reclame banners zijn niet gevaarlijk, maar kunnen wel irritant zijn.
- **Browser hijackers** : Browser hijackers zorgen ervoor dat bepaalde aspecten van de browser aangepast worden. Hierbij is te denken aan het aanpassen van startpagina's, zoekpagina's of favorieten zonder dat je dat zelf wilt.
- **Keyloggers** : Keyloggers zijn programma's die elke toets die jij op je toetsenbord intikt registreren. De zo verkregen gegevens kunnen verstuurd worden naar een centrale computer, waardoor wachtwoorden te achterhalen zijn. Er bestaan ook hardware keyloggers (zie het plaatje hiernaast). Key logging wordt dan gerealiseerd door een apparaatje te gebruiken waarin de toetsenbordkabel ingeplugd wordt. Vervolgens wordt dit apparaat aan de pc gekoppeld en onthoudt het in zijn flashgeheugen welke toetsen zijn ingedrukt. De hardware keylogger kan niet gevonden worden door een virusscanner, de softwareversie vaak wel.

- **Adware**: Adware staat voor *advertising supported software.* Het staat voor elk soort software die automatisch advertenties toont of downloadt op de pc waar de adware op is geïnstalleerd of dat zelfs doet tijdens het gebruik van de adware. Sommige vormen van adware kunnen *spyware* zijn en mogen dus gezien worden als privacy aantastende software. In de volgende paragraaf

lees je hier meer over.

1.5b Adware

Adware staat voor *advertising supported software.* Het staat voor elk soort software die automatisch advertenties toont of downloadt op de pc waar de adware op is geïnstalleerd of dat zelfs doet tijdens het gebruik van de adware. Sommige vormen van adware kunnen spyware zijn en mogen dus gezien worden als privacy aantastende software.

Adware wordt vaak gebruikt bij freeware-programma's (gratis software) waarbij je die advertenties voor lief moet nemen. Gebruik je zulke freeware programma's zonder betaling, hetgeen meestal toegestaan wordt, dan word je telkens lastig gevallen met de pop-ups die je aanzetten tot officiële betaling en registratie van het programma. De adware wijst je op de grote voordelen van het gebruik van een geregistreerde en vaak uitgebreidere versie van het programma. De betaalde versie bevat de adware dan niet meer.

Omdat adware je tot kopen wil aanzetten, zou je kunnen denken dat het niet de bedoeling is dat adware iets op je pc uitspookt dat je niet wenst. Dat is helaas niet altijd het geval. Adware kan je browse-gedrag, je uitgaven en je netwerk-activiteiten nagaan. En dat kan weer aanzetten tot andere reclame-uitingen die daar specifiek op zijn gericht.

1.5c Cookies

Een cookie is een link tussen je pc en de webserver die de cookie gestuurd heeft, zodat deze link na de eerste keer het contact met de webserver vergemakkelijkt. De cookie wordt op je pc opgeslagen in een aparte cookie-map die meestal te vinden is onder de Windows-map. Op deze wijze word je herkend als iemand die al eens eerder de site op de webserver bezocht heeft, zodat de communicatie gemakkelijker kan verlopen. Dit hoeft niet altijd verkeerd te zijn. Het kan zelfs heel gemakkelijk zijn.

voorbeeld

Een cookie kan er als volgt uitzien als je het in een tekstprogramma opent. In dit geval is er een Google cookie aangemaakt.

SNID
13=6pA57EAFsZQdg-dltNtE3x85msasws_RCDoPqC2G=eps3y4VB5Ltb6mv-C
google.com/verify
1536
3088610304
30096276
3333325200
29949425
*

Je ziet dat in codevorm gegevens vastgelegd worden.

Cookies kunnen gebruikt worden voor

- het onthouden van een login-naam of instellingen;
- het vergaren van surfinformatie (de zgn. *profiling*);
- het koppelen van een browser aan tijdelijke variabelen op de server (*session cookie*).

Dit lijkt allemaal heel onschuldig, maar we noemen de cookies niet voor niks in deze module. Het tweede aandachtspunt dat je hiervoor ziet (profiling) is namelijk een punt dat ook misbruikt kan worden door de cookie-aanvrager. In 1997 kwam er een voorstel dat browsermakers aanmoedigde om het gebruik van cookies inzichtelijker te maken voor de gebruiker. Het gevolg hiervan was dat de gebruiker vanaf toen kon instellen in welke mate cookies geaccepteerd mogen worden en of aan de gebruiker gevraagd moet worden of een cookie geaccepteerd mag worden. Dit was om het eerder genoemde profiling tegen te gaan want als gebruikers de cookies van een Internet-advertentiebureau niet accepteren, kan dit advertentiebureau geen profile samenstellen.

Cookies kwamen pas echt in opspraak toen DoubleClick, een Internet-advertentiebureau, een bedrijf

overnam met een grote klantendatabase. DoubleClick wilde de naamsgegevens koppelen aan de profiles van surfers en was van plan deze gegevens te verkopen. Deze combinatie van een naamsgegevens en profile is heel aantrekkelijk voor marketingbedrijven, want zij kunnen hiermee advertenties gericht naar iemand sturen. De reclame wordt dan gerichter verspreid, waardoor er meer geld voor een advertentie gevraagd kan worden. Onder druk van verschillende privacy-organisaties heeft DoubleClick de gegevens niet verkocht.

In 2002 is de eerste *P3P-recommendation* gepubliceerd door de *W3C*. Browsers die zich aan deze specificatie houden, accepteren standaard veel minder cookies. De gebruiker kan desgewenst de instellingen van de browser aanpassen. Zo worden bijvoorbeeld cookies in een frame van een ander domein niet meer automatisch geaccepteerd door zo'n browser, tenzij de server een statement opstuurt dat de cookies niet gebruikt worden om privacygevoelige informatie op te slaan.

1.6 Mailvirus

Een mailvirus is een 'ouderwets' virus dat zichzelf als bijlage verspreidt via e-mail. Tijdens een besmetting kan er automatisch een mailserver geïnstalleerd worden, zodat er geen gebruik gemaakt hoeft te worden van een e-mailprogramma op de geïnfecteerde computer. Ook de mailserver van de internetprovider waarmee de besmette computer verbonden is, hoeft niet te worden gebruikt. Internetproviders controleren streng op dit soort virussen, waardoor de kans groot is dat de verdachte berichten er direct uitgefilterd zouden worden als ze via de provider verstuurd worden.

Mailvirussen vervalsen het afzenderadres, vaak door adressen te gebruiken uit het adressenboek op de computer. Zo'n adressenboek heb je bijvoorbeeld staan in je Outlook-programma. Daardoor kan het gebeuren dat je een e-mail krijgt van het adres van je vriendin Marja, terwijl het bericht eigenlijk verstuurd is vanaf de computer van Carolien. Het virus doet dat zodat je Marja gaat lastigvallen in plaats van Carolien. Dat vergroot de chaos. Veel mailvirussen hebben namelijk als enige doel troep te maken en chaos te veroorzaken. Daardoor kunnen ze mailservers verstoppen, mailprogramma's onbruikbaar maken en daardoor e-mailverkeer ernstig bemoeilijken.

Wat heel belangrijk is: installeer een goede virusscanner die altijd up-to-date blijft. De meeste internetproviders filteren de virusmails er gelukkig al uit. Bij sommige providers moet daarvoor wel extra betaald worden.

 Opdracht

Maak nu de opdracht "Virussen " uit het menu-onderdeel "Opdrachten en Toetsen".

Over dit lesmateriaal

Colofon

Auteurs	Bètapartners
Team	Wikiwijs Maken Auteurs
Laatst gewijzigd	29 oktober 2014 om 13:12
Licentie	De Nederlandse Creative Commons 3.0 licentie waarbij de gebruiker het werk mag kopiëren, verspreiden en doorgeven en afgeleide werken mag maken onder de voorwaarden: Naamsvermelding en Gelijk Delen, zie http://creativecommons.org/licenses/by-sa/3.0/nl/. Meer informatie over de CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie licentie.

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Leerniveaus	VVE, HAVO 4, Praktijkonderwijs, VWO 4
Leerinhoud en doelen	Informatica
Eindgebruiker	leerling/student
Trefwoorden	a1 wetenschap en technologie, a2 maatschappij, e-klassen rearrangeerbaar