Het onderstaande artikel verscheen in het consumenten tijdschrift 'Computer thuis in bedrijf'. Hoewel het artikel geschreven is op 21 februari 1996 zijn de gegeven tips nog steeds bruikbaar.

Computervirussen; een overwonnen probleem?

[Inleiding]

In Computer Thuis en Bedrijf maken we regelmatig melding van computervirussen en de problemen die daardoor kunnen ontstaan. Zo treft u op de bijgevoegde CD-ROM deze/volgende maand een volledige, laatste versie aan van SWEEP; een scanner om uw Windows 95 werkstation op virussen te controleren.

Wellicht hebt u de indruk dat het virusprobleem niet zo urgent (meer) is. Reden om eens te rade te gaan bij een bedrijf dat dagelijks een oplossing voor dit probleem probeert te bieden.

[Dhr. Oud is beveiligingsadviseur bij CRYPSYS Data Security te Gorinchem.]

Een computervirus is een programma dat zichzelf dupliceert zonder dat de computergebruiker daartoe opdracht geeft. Veel computervirussen bevatten naast de instructies die leiden tot duplicatie ook opdrachten die een bijbedoeling (pay-load) hebben. In veel gevallen is die bijbedoeling op zich niet kwaadaardig; het veel voorkomende Form virus liet alleen op bepaalde dagen van het jaar een klikgeluid horen als een toets werd ingedrukt. Veel virussen echter bevatten moedwillig aangebrachte code om data te verminken. Het is mogelijk dat een virus alle data op een vaste schijf wist.

In november 1983 toonde Dr. F. Cohen aan dat computervirussen mogelijk waren als wetenschappelijk experiment. Daarna hebben nog vele wetenschappers zich gebogen over dit onderwerp. Helaas zijn er veel, heel veel, mensen die met minder goede bedoelingen bezig zijn met computervirussen. Vaak wordt vergeten dat het wel degelijk mensen zijn die virussen ontwikkelen (er zijn zelfs mensen die programma's ontwikkelen waarmee anderen virussen kunnen ontwikkelen). Uit onderzoek is gebleken dat het hierbij vooral gaat om enigszins contact gestoorde, hoog-intelligente jonge mannen.

Op dit moment (februari 1996) zijn er ruim 7200 verschillende personal computer virussen en 32 Macintosh virussen. Helaas worden de virussen steeds complexer waardoor maatregelen om het probleem aan te pakken dus ook zwaarder worden.

Is er wat aan te doen en zo ja wat?

Zoals bij biologische virussen ook het geval is, blijft preventie altijd de beste genezing. Belangrijk is om een houding aan te leren waarbij per definitie alle data en programmatuur die u van derden ontvangt, verdacht is. Dus ook software van gerenommeerde firma's en ook dat spel dat u van Internet af haalt. Omgedraaid geldt dus ook; ontvangt u geen software of data van derden dan bent u veilig.

Expliciet wordt hier ook gesproken van data; want gebleken is dat virussen zich al lang niet meer alleen in programma's kunnen bevinden. Jaren geleden is al gewaarschuwd dat macro-virussen, zoals nu opgedoken in MS-Word documenten, mogelijk zijn.

Praktisch iedereen ontvangt data en programmatuur van derden. Dus loopt u risico. Uiteraard kunt u bepaalde bronnen meer vertrouwen dan anderen. Maar wantrouwen is een goede leermeester. Ook firma's waarvan u het niet verwacht hebben virussen verspreid.

U moet u zelf dus beschermen. Dat kan op een aantal manieren. Een aantal maatregelen kosten u niets. Andere gaan u geld kosten. Uw huis of auto is ook verzekerd; dus daarom mag de 'verzekering' van uw kostbare gegevens ook wat kosten.

Veel personal computers hebben de mogelijkheid om opstarten van diskette op een bepaalde manier uit te schakelen. Als u die functie aanschakelt dan kunt u al niet meer gaan behoren tot ruim driekwart van alle meldingen van besmettingen. In meer dan 75% van alle gevallen is namelijk sprake van een besmetting met een virus dat zich verspreidt door de opstartkode op een diskette (de 'bootsector'). Als uw PC deze mogelijkheid biedt gebruikt u hem dan.

U kunt het virusprobleem ook aanpakken door gereedschappen aan te schaffen. U moet daarbij denken aan software die speciaal geschreven is voor dat doel. Dergelijke software is voorhanden in een aantal varianten en ook combinaties van deze varianten komen voor. De eerste variant zijn zogenaamde niet-virusspecifieke produkten. Het betreft hier software waarmee u bijvoorbeeld kunt zeker stellen dat een bestand ten opzichte van een vorige situatie niet veranderd is (en dus niet besmet is met een virus). Ook zijn produkten leverbaar die in achtergrond, dus terwijl u bezig bent met en ander programma, kijken of de PC een kwaadaardige opdracht zoals het wissen van data op de vaste schijf uitvoert en u in dat geval alarmeert.

De tweede variant betreft produkten die virusspecifiek zijn. Het betreft hier programmamakers die kennis van een aantal virussen hebben en proberen in uw programmamakers en bestanden te zoeken of de virussen die het produkt kent er in voorkomen. Met een dergelijk produkt, een scanner, detecteert u dus alleen dat een bepaald programma of databestand besmet is. Hopelijk is dit dan op een diskette die u van plan was te gaan gebruiken en is de besmetting nog niet aanwezig op uw veel grotere vaste schijf. (Of op die enorme stapel diskettes die u hebt!)

Scanners zijn op zichzelf weer in vele varianten op de markt. Uiteraard ook in vele kwaliteiten. In een ideale wereld detecteert een scanner alle virussen 100% zeker en wordt nooit een melding gegeven dat een besmetting aanwezig is zonder dat dat zo is. In een ideale wereld leven we niet, maar er zijn produkten die het bovenstaande vrijwel waarmaken.

Een waarschuwing is op zijn plaats voor de zogenaamde TSR of achtergrond scanners. Het betreft hier programma's die als waakhond in uw werkstation achterblijven en dan elk bestand of programma dat u raadpleegt of opstart, eerst controleert op virussen. Hier zijn twee aandachtspunten; de eerste merkt u direct en de tweede als het te laat is. Eerste aandachtspunt is dat het detecteren van een groot aantal complexe virussen steeds meer capaciteit van uw PC vergt. U zult dus merken dat uw computer traag wordt als u een achtergrond scanner gebruikt. Maar daar kunt u wellicht mee leven.

Het tweede aandachtspunt is ernstiger. Het is onmogelijk een residentie scanner te bouwen die alle virussen detecteert. Veel gebruikers realiseren zich dat niet. Residente scanners detecteren alleen de virussen die door de fabrikant ingebracht zijn. En die fabrikant maakt continue de afweging dat de achtergrond scanner niet te veel geheugen en processortijd in beslag mag nemen. Complexe virussen die moeilijk te detecteren zijn worden dus niet ingebracht. Veel mensen denken beschermd te zijn maar worden toch geconfronteerd met besmetting. Een vals gevoel van veiligheid dus.

Gebruik dus een volledige scanner. Op elke diskette en op elk onbekend bestand.

Er zijn vele scanners op de markt. Regelmatig worden testen gepubliceerd die u een indicatie kunnen geven welk produkt voor u het beste is. Ervaringen van anderen kunnen u ook de weg wijzen. Of vraag advies bij een expert op dit gebied.

Uiteraard staat nu het nieuwe besturingssysteem Windows 95 in de belangstelling, alsmede een belangrijke toepassing voor deze en andere Windows varianten; Microsoft Word. Aan dat laatste produkt wordt deels onterecht (Microsoft is niet verantwoordelijk voor deze virussen) een virusvorm, de macro-virussen, toegeschreven.

Windows 95 wordt niet meer geleverd inclusief een anti-virus produkt. Voorgaande versies kwamen kompleet met Microsoft Anti-Virus (MSAV). Dit produkt kwam met testen altijd op de laatste plaats, maar iets is beter dan niets. Hoewel ook hier dat valse gevoel van veiligheid fataal kon zijn. Het feit dat Windows 95 geen virusprotectie biedt heeft wellicht veel mensen doen denken dat dit besturingssysteem niet kwetsbaar is voor virussen. Niets is minder waar. Windows 95 is niet meer of minder vatbaar dan andere versies van Windows of MSDOS. Bescherming blijft noodzaak.

Onlangs is het eerste Windows 95 specifieke virus ontdekt; het uit Australië afkomstige Boza virus. Dit virus vernielt soms de programma's waarin het zich ophoudt.

De verwachting is dat Boza een uitdaging vormt voor andere virus-ontwikkelaars en dat de komende maanden meer Windows 95 specifieke virussen ontdekt zullen gaan worden.

Virussen zijn programma's. Alle programmeertalen kunnen in principe gebruikt worden om een virus te schrijven. Zonder dat u zich dat realiseert bevatten veel 'normale' programma's, zoals tekstverwerkers, een ingebouwde programmeertaal zoals een mogelijkheid tot het uitvoeren van macro's.

Uiteraard worden deze programmeertalen steeds krachtiger. Een produkt zoals de Microsoft Word tekstverwerker bevat een rijke variant van de BASIC programmeertaal. En juist dit produkt is heel geschikt om een virus mee te ontwikkelen.

Microsoft heeft er voor gekozen om een mogelijkheid te bieden tot het automatisch uitvoeren van programma's binnen Word. Ook is het mogelijk om dit soort automatisch startende programma's op te nemen in de met Word aangemaakte documenten. Opent u dus een met een Word-virus besmet document (officieel heet een dergelijk document dan een sjabloon maar dit onderscheid valt de gebruiker niet op) dan is op dat moment de PC besmet. Elke document dat daarna bewerkt wordt zal door het virus besmet worden. Aangezien documenten veel door gebruikers gedeeld worden kan een dergelijke besmetting zich heel snel verspreiden.

Er zijn nu al vier Word virussen. In potentie kunnen deze virussen zich ook verspreiden naar andere computer architecturen zoals de Macintosh omdat de versie van Word voor die computer dezelfde programmeertaal kent.

De macro-virussen (het is beter de generieke naam te gebruiken want ook andere programma's dan Word zijn als 'host' mogelijk) hebben een groot aantal nieuwe problemen geïntroduceerd.

In het verleden kon u, doordat virussen zich nestelen in programma's, aannemen dat als u programma's controleerde u veilig was. Dus scande u alleen de .exe en .com bestanden. Dat ging snel en hoe het moest was goed bekend. Maar een tekstverwerker staat u toe dat u zelf de naam aan een document geeft en in principe is elke naam toegestaan. Om op zeker te spelen moet u dus nu alle bestanden helemaal controleren. Dat kost helaas meer tijd.

Met de betrokken producenten van software is overleg gaande om bijvoorbeeld duidelijk te maken waar in een document de uitvoerbare code staat zodat alleen deze gecontroleerd hoeft te worden. Een versnelling van het scannen is dan een gevolg.

Wat zijn de ontwikkelingen in de toekomst? Het antwoord is helaas niet makkelijk te geven. Door de intensieve kontakten tussen gebruikers via allerlei media zoals Internet en andere netwerken is de kans op verspreiding van virussen sterk toegenomen. De laatste jaren waren vooral de bootsector virussen (bijvoorbeeld Form) bijzonder succesvol omdat gebruikers veel diskettes uitwisselen en het 'per ongeluk' opstarten van een diskette eenvoudig is.

Communicatie van bestanden via de veel geroemde 'elektronische snelweg' zal een verschuiving naar virussen die zich nestelen in bestanden te weeg brengen.

Virussen worden steeds complexer waardoor de controle steeds moeilijker wordt en steeds meer tijd zal kosten.

Dit alles lijkt op doemdenken. Nog altijd echter zijn de ontwikkelaars van anti-virus produkten in staat het probleem te bolwerken. Op zich is er geen verwachting dat dit in de toekomst anders zal zijn. Advies blijft echter om op uw zaak te letten.
Pas als u merkt dat uw data weg is beseft u hoe waardevol die was en hoe afhankelijk u ervan bent. Virussen; doe er dus wat aan!

Ernst J. Oud Email ernstoud@euronet.nl
WWW http://www.euronet.nl/users/ernstoud/index.html