Windows 95 gevoelig voor vele virussen

Anti-virusindustrie moet heil zoeken in expertsystemen om huidige aanwas van virussen de baas te kunnen

Computervirussen zijn al lang het stadium van de balorige studentengrap gepasseerd. Hoe verfijnder de detectietechnieken en hoe minder kansen nieuwe besturingssystemen bieden voor virusbesmetting, hoe sneller het aantal nieuwe virustypen gaat groeien. Het is maar de vraag of de anti-virusindustrie het tempo kan blijven bijbenen, vreest Ernst Oud. Hij benadrukt dat in de bedrijfsstrategie om het virus buiten de deur te houden, de primaire verantwoordelijkheid moet liggen bij de IT-verantwoordelijken en niet, zoals vaak het geval, bij de eindgebruiker.

De onrust van begin jaren '90 rond computervirussen en de schade die ze aanrichten, is verdwenen. In veel gevallen verdrijft het installeren van een virusdetectieprogramma de angst voor gewiste schijven en gecorrumpeerde bestanden. Met de komst van nieuwe PC-besturingssystemen lijkt bovendien de rol van veel oude virustypen uitgespeeld. Maar deze sussende overwegingen zijn onterecht. Eind september werd op de Virus Bulletin Conference het aantal unieke virusvarianten geschat op 6500. Dat aantal groeit met gemiddeld honderd nieuwkomers per maand. Een deel betreft eenvoudige varianten, maar steeds vaker duiken dermate complexe typen op dat het onduidelijk is of de anti-virusindustrie het tempo zal kunnen bijhouden.

In tegenstelling tot wat de fabrikanten beweren, blijken de nieuwe PC-besturingssystemen nog steeds kwetsbaar. Windows NT is, in vergelijking met Windows 3.x, Windows 95 en OS/2, nog het best beschermd tegen virusaanvallen. Een virus probeert altijd buiten het besturingssysteem om toegang te krijgen tot de opslagmedia, zoals diskettes en vaste schijven. Windows NT laat dit niet toe waardoor de reproduktie van virussen onmogelijk wordt.

Maar ook Windows NT is niet veilig. Gebruikers zetten hun computer nogal eens aan terwijl er zich nog een diskette in de schijfeenheid bevindt. De computer kan dan niet opstarten, maar als de diskette besmet is met een virus dat de opstartsector (boot sector) infecteert, kan dit zich wel naar de vaste schijf kopiëren. Is die sector eenmaal besmet, dan krijgt Windows NT de computer niet meer aan de praat. Reparatie is mogelijk maar omslachtig en niet of nauwelijks gedocumenteerd.

Op diskettes of vaste schijven wordt een klein deel gereserveerd voor het bijhouden van informatie over de bestanden. Onder DOS en Windows wordt slechts een klein deel van die gereserveerde ruimte benut: de overige sectoren blijven altijd ongebruikt. Veel virussen beschrijven deze vrije ruimte met bijvoorbeeld extra viruscode. Met Windows NT als besturingssysteem bevatten deze sectoren echter cruciale informatie. Wordt deze informatie overschreven door een DOS-virus dan zal Windows NT niet meer opstarten. Het is belangrijk deze kritieke sectoren van een opstartschijf te beschermen. Daarvoor worden gereedschappen meegeleverd met het besturingssysteem, maar in de praktijk blijkt dat lang niet iedereen deze beschermende actie uitvoert. Bij Windows 95 wordt geen anti-virusprogramma meegeleverd zoals bij Windows 3.x wel het geval was. Dit hulpmiddel was niet van hoge kwaliteit maar bood toch enige bescherming. Bovendien versterkt het ontbreken van een dergelijk programma in Windows 95 het idee dat het virusprobleem met het nieuwe besturingssysteem tot het verleden behoort. Maar niets is minder waar.

Onder Windows 95 kunnen veel virussen zich weliswaar minder makkelijk dupliceren. Een van de redenen daarvoor is dat zij vaak afhankelijk zijn van niet-gedocumenteerde functies in DOS. Bij het ontwerp van de DOS-emulatie in Windows 95 heeft Microsoft deze functies verwijderd.

Het Winword-virus is op 45.000 werkstations van de Amerikaanse defensie aangetroffen

Het besturingssysteem is echter niet in staat te verhinderen dat (DOS-)virussen de hardware rechtstreeks benaderen. Daardoor zijn de virusactiviteiten zoals het wissen van data op de vaste schijf, nog steeds mogelijk.

Sommige virussen onder Windows 95 zorgen er ongemerkt voor dat de 32-bits drivers voor de harde schijf niet worden geladen. Hiervan komt soms geen melding bij het opstarten. Het gevolg is dat de prestaties van het systeem achterblijven. Pas bij het raadplegen van de 'Performance status' van de 'System Properties' geeft Windows 95 aan dat het systeem wellicht besmet is.

Zowel in Windows NT als in Windows 95 bestaat de mogelijkheid oude DOS-programma's te draaien. Daarmee kunnen in principe ook alle 6500 virustypen activiteiten ontplooien onder de nieuwe besturingssystemen. Welke daarvan schade zullen aanrichten, blijft de vraag,

Bij het gebruik van Windows 95 als besturingssysteem is overigens speciale virusdetectieprogrammatuur noodzakelijk. In tegenstelling tot eerder berichten van onder meer Microsoft, zijn anti-virusprodukten, ontworpen voor Windows 3.x of MS-DOS, niet in staat de opstartsector volledig te controleren op infectie. Juist de virussen die deze sector infecteren, komen steeds meer in omloop.

Een voorbeeld van hoe snel een virus schade aan kan richten, is het zogeheten Winword-virus. Inmiddels zijn reeds drie van deze in Microsoft Wordmacro's huizende virussen ontdekt. Een spreker op de Virusconferentie meldde dat het virus op 45.000 werkstations van de Amerikaanse defensie is aangetroffen. Door de 'autoexecute'-functie voor macro's in Winword 6 kan het virus bij het openen van een besmet document overgaan naar de PC.

Elk bestand dat vervolgens wordt geopend of gesloten, wordt dan eveneens besmet. Een adequate remedie voor dit probleem bestaat nog niet. Slechts het voorkomen van besmetting van de PC door alle documenten met een op dit virus toegesneden scanner te controleren, houdt het probleem buiten de deur.

Macro-virussen zijn in principe mogelijk in elke macro-taal en vereisen van de maker relatief weinig kennis. Door het toenemend gebruik van macro's, die ook nog eens automatisch worden uitgevoerd, verwacht de anti-virusindustrie dat dit type virussen een belangrijke bedreiging vormen.

Een nieuw probleem vormt de mogelijkheid in moderne besturingssystemen de bestandsnaam en de extensie van documenten vrij te kiezen. Niet langer zijn slechts de uitvoerbare bestanden met de extensie EXE verdacht. maar kan in feite in elk bestand een potentiële infectiehaard schuil gaan. Virusdetectieprogrammatuur moet daardoor veel meer bestanden controleren dan voorheen. Er ontstaan dan al snel problemen met de verwerkingssnelheid. De toekomstige generatie anti-virusprodukten zullen moeten gaan werken met kennis over de lay-out van documenten. Met zo'n slimmer hulpmiddel hoeven alleen die delen van een bestand gecontroleerd te worden waar een virus actief zou kunnen zijn.

Het inbrengen van kennis over de virusontwikkelingen in software levert de zogenaamde 'heuristic scanners' op. In de ideale situatie zijn dit virusonafhankelijke produkten die niet meer een maandelijkse aanpassing behoeven. In diverse landen wordt onderzoek op dit gebied verricht. De resultaten hebben echter nog niet geleid tot produkten die kunnen concurreren met de traditionele virusdetectiemiddelen. Een probleem is dat heuristische detectieprogrammatuur altijd ook onschuldige bestanden als verdacht zal blijven aangeven. De keuze of het bestand werkelijk besmet is, wordt dan neergelegd bij de gebruiker. Die weet in veel gevallen niet wat hij met de verdachtmaking aan moet, negeert de melding en werkt verder.

Het ontbreken van een virusscanner in Windows 95 versterkt het idee dat het virusprobleem tot het verleden behoort

Een belangrijke bron van virusverspreiding is Internet. Het weren van ongewenste programmatuur en dus ook virussen via dit kanaal is nauwelijks tegen te gaan. Door het niet-hiërarchisch karakter van het netwerk valt of staat de veiligheid met de persoonlijke inspanningen van vele tienduizenden systeembeheerders. Niemand kan verzekeren dat zij alle aangeboden bestanden op virussen controleren. Soms is detectie zelfs praktisch onmogelijk: Bijvoorbeeld het opsporen van een PC-virus in een bestand dat op een Macintosh Workgroup Internet Server is opgeslagen, is geen sinecure. PC-virussen kunnen meestal alleen worden gedetecteerd met scanners die op het PC platform draaien. Een Internet-systeembeheerder kan die scanners dus simpelweg niet gebruiken op zijn Unix-systeem.

Nog lastiger wordt het als er binnenkort aan World Wide Web-pagina's kleine programmaatjes (objecten) kunnen worden gekoppeld om bij de gebruiker lokaal taken uit te voeren. Onder meer Hot Java van Sun maakt gebruik van deze mogelijkheid. Maar niemand weet wat zo'n object ongevraagd nog meer uitvoert op de PC van de gebruiker. De beste filosofie blijft er van uit te gaan dat de gehele stroom informatie uit het Internet pen definitie verdacht is,

Ruwweg vallen de maatregelen om virussen uit te bannen uiteen in twee categorieën; oplossingen voor losstaande werkstations en netwerkoplossingen.

Op losse werkstations staat in praktijk veelal een programma dat onbekende diskettes en bestanden detecteert en deze realtime op virussen controleert (de zogenaamde residentie scanner). Veel werkstations bezitten een beperkt geheugen en relatief trage verwerkingscapaciteit. Door de teruglopende prestaties is een residentie scanner vaak minder wenselijk.

Bovendien bezit geen enkele residentie virusscanner de kwaliteit van een volledig virusdetectieprogramma. Zo herkent geen enkele residentie scanner virussen die zich muteren bij het dupliceren - de zogenaamde polymorfische virussen - wanneer deze zich op een schijf bevindt. Een enkele residentie scanner is wel in staat dit type virus te herkennen in het geheugen, maar dan is de PC dus al besmet.

Het gebruik van residentie scanners leidt dus tot een vals gevoel van veiligheid. Het blijft noodzakelijk regelmatig een volledige controle van harde schijven en diskettes uit te voeren nadat is zeker gesteld dat er geen virussen in het werkstation actief zijn. Dat kan door de PC op te starten met een schone systeemdiskette.

Steeds vaker maken werkstations onderdeel uit van een netwerk. Dat maakt het mogelijk de virusdetectie op een centrale plaats te installeren. Dit komt het beheer ten goede en is een oplossing voor de geschetste problemen. Scanning vindt dan niet meer plaats op het werkstation, De geavanceerde detectieprogrammatuur op de server berekent voortdurend lokale controlegetallen ('local checksums') voor de werkstationdocumenten. De controleren worden berekend met een mathematische formule die garandeert dat elke wijziging aan een document, legaal of niet, een afwijkend getal oplevert. Het veranderde document wordt vervolgens automatisch getest op de aanwezigheid van een virus. Door de virusdetectie te scheiden van het controleurs wordt een veiliger en sneller systeem mogelijk. De detectie kan met de grotere machine grondig gebeuren en kent dus niet de problemen van de resident scanners.

Belangrijk is dat gecentraliseerde viruscontrole de verantwoordelijkheid wegneemt bij de gebruiker die de zwakste schakel in een doelmatige veiligheidsstrategie vormt. Die verantwoordelijkheid komt te liggen waar hij hoort; bij de systeembeheerder.

Ernst Oud

De heer E.J. Oud is als beveiligingsadviseur werkzaam bij Crypsys Data Security in Gorinchem.
E-mail: ernstoud@euronet.nl