Op consult bij Dokter Unix

Het antwoord op prangende Unix vragen...

Dr.Unix@nluug.nl

Q: *Beste Dr. Unix,,*

Op diverse platformen speelt de problematiek van virussen. Ik ben al een tijdje actief binnen de Unix-omgeving, maar ik hoor daar eigenlijk weinig over virussen. Ook op het Internet is erg weinig over dit onderwerp te vinden. Speelt dit niet binnen Unix?

-- "FliereFluiter" uit B.

A: Beste "FliereFluiter",

Het is inderdaad het geval dat ik in vergelijking met mijn hooggeleerde confreres die zich specialiseren in Mensen, Dieren en Windows (in volgorde van afnemende intelligentie) mij weinig tot niet bezighoudt met het bestrijden van virii (of, zoals de niet-kenner zegt: "virussen"). In het verleden heb ik wel eens een ernstig geval van wormen aan de hand gehad, maar een paar keer flink naar het toilet en een kuurtje pillen voor de hele familie deed toen wonderen.

Maar, ter zake.

Ik zou wat graag alhier een verhaal ophangen met de strekking dat de superieure architectuur van Unix alsmede de veel hogere praktische, emotionele en sociale intelligentie van de Unix beheerders, programmeurs en gebruikers het virus fenomeen in ons geliefde operating systeem buiten de deur hebben gehouden. Dat zou helaas bezijden de waarheid zijn en, zoals ik tijdens mijn opleiding leerde, je moet nooit jokken tegen patiënten, want dan valt, mocht dit euvele feit aan het licht komen, hun vertrouwensbasis weg. En dat kunnen we als vrije beroepsbeoefenaren in een competetieve markt natuurlijk niet hebben.

Alhoewel er een uitgebreide taxonomie op dit gebied bestaat vat ik voor de eenvoud van het verhaal even alle stukken ongewenste programmatuur die zich tot doel stellen om buiten ons medeweten om dingen te doen die we liever niet gedaan zagen worden samen onder de verzamelnaam "virii". Ik wil eerst even ingaan op wat algemene eigenschappen van virii.

Allereerst moeten de virii de niets-vermoedende gebruiker zover krijgen dat het wordt uitgevoerd. Traditioneel gebeurt dit doordat de virii zichzelf verstoppen in een gastheer, met de gastheer meereizen en op het "moment suprème" worden geactiveerd. Gastheren zijn vaak programma's, waarin de virii zich zodanig innestelen dat ze bij het starten van een geïnfecteerd programma worden uitgevoerd. De laatste tijd zien we echter dat de gastheren steeds vaker databestanden zijn waar de virii zich in verstoppen als attachment of macro. Steeds meer applicaties bevatten krachtige macrotalen met macro's die automatisch kunnen worden uitgevoerd als een bestand met de ene of de andere applicatie wordt geopend. Dergelijke faciliteiten vormen een gehele nieuwe voedingsbodem voor virii. Als een virus wordt gestart probeert het zichzelf meestal eerst in een stuk of wat andere gastheren te kopiëren alvorens het zijn dodelijke missie aanvangt.

Waar virii natuurlijk dol op zijn is op een homogene "*gene pool*". Hoe meer organismen er zijn met dezelfde genetisch opbouw, hoe eenvoudiger het voor een virus is om een geschikte gastheer te vinden. Hoe diverser de genetische samenstelling van een populatie, hoe moeilijker het voor een virus is om zichzelf voort te planten. Gegeven deze eenvoudige biologische feiten is het natuurlijk niet moeilijk om in te zien dat Dos/Windows systemen een ideale populatie zijn voor virii: allemaal systemen met een vrijwel identieke genetische opbouw: processor, besturingssysteem (of wat daar voor doorgaat) en zelfs zeer homogeen op het gebied van applicaties. Vanuit dezelfde feiten geredeneerd is Unix een veel onvriendelijkere omgeving voor virii: allemaal verschillende typen processoren, verschillende besturingssystemen (alhoewel wel sterk op elkaar gelijkend toch niet identiek) en een diversere applicatieomgeving. Een virusuitbraak op een Sun Solaris systeem zal in veel gevallen geen gevolgen hebben voor andere Unix systemen omdat het virus wat is geprogrammeerd voor de Sparc/Solaris DNA structuren niet compatibel is met bijvoorbeeld PA-RISC/HP-UX systemen. Spontane "cross overs" van een virus naar een aanverwante organisme zoals dit bij biologische virii nog wel eens gebeurt (b.v. HIV, wat naar alle waarschijnlijkheid rond 1953 is overgestapt vanuit de aap naar de mens) is bij computervirii erg onwaarschijnlijk. Ik heb daar een erg elegant bewijs voor, maar het paste helaas niet meer in de kantlijn :-)

Als een virus eenmaal losbarst is het ook nog erg belangrijk welke afweermechanismen een organisme allemaal heeft. Hoe effectiever het organisme het virus dwars kan zitten, hoe kleiner de kans is dat een virus zichzelf voort kan planten en zijn destructieve taken kan uitvoeren. DOS en Windows zijn op dit gebied uitermate slecht uitgerust om een virus te weerstaan. Deze besturingssystemen hebben hoegenaam geen beschermende eiwitten aan boord en zijn willoze slachtoffers van ieder virus wat voorbij komt dwalen. Dat die besturingssystemen het toch nog lang hebben volgehouden tijdens de biologische oorlogsvoering eind-jaren tachtig (en het nog steeds volhouden!) zal ons waarschijnlijk tot ver in het volgende millenium bezighouden. Alhoewel diverse onderzoekingen op het gebied van de socio-biologische informatica zich op dit vraagstuk richten moet ik het eerste zinvolle onderzoeksresultaat van die inspanningen nog tegenkomen. Windows NT en Unix zijn aanmerkelijk beter toegerust om de aanvallen van virii te weerstaan. Beide besturingssystemen hebben een diverse beveiligingsmechanismen die ervoor zorgen dat niet iedereen zomaar van alles en nog wat op het systeem kan uitspoken. Dit betekent meestal dat een geactiveerd virus zichzelf meestal niet voort kan planten naar systeemprogramma's of de bootprogrammatuur. Let op, ik zeg hier met nadruk **meestal**, want als het virus het geluk heeft te worden geactiveerd door de systeembeheerder ("root" onder Unix, of een lid van de Administrators local group in Windows NT) dan kan het zich natuurlijk wel succesvol voortplanten naar die systeemprogramma's. Een virus wat door een gewone gebruiker wordt geactiveerd kan alleen "maar" de omgeving van die gebruiker verwoesten. Tamelijk vervelend, maar niet desastreus voor het gehele systeem. Het aangetaste orgaan kan uit het organisme worden verwijderd, en wellicht door transplantie of stimulatie van spontane

regeneratie weer worden hersteld. De grote veronderstelling hier is natuurlijk dat de afweermechanisme van het systeem optimaal zijn geconfigureerd.

Virii die zichzelf eenmaal hebben voortgeplant in een andere gastheer vinden het natuurlijk geweldig als die gastheer regelmatig verhuist van de ene naar de andere habitat. De epidemiologische verspreidingssnelheid van virii wordt hoofdzakelijk bepaald door het aantal en de intensiteit van de contacten tussen besmette dragers van het virus en nog onbesmette organismen. Als een geïnfecteerd programma wordt losgelaten in een nog onbesmet systeem dan heeft het virus daar vrij baan, en zal het zich daar ook voortplanten. De enige manier om dit te voorkomen is hetzij een stricte medische keuring voordat programma's worden toegelaten tot een systeem. Het als beheerder uitvoeren van een programma uit onbekende bron is natuurlijk volledig uit den boze. Ook op het gebied van virusverspreiding heeft Unix het iets gemakkelijker dan bijvoorbeeld Windows. Door de diversiteit van Unix systemen is het vrij uitwisselen van programma's redelijk beperkt. Hierdoor kunnen virii niet eenvoudig van de ene naar de andere habitat overspringen. Als programma's al tussen Unix systemen worden uitgewisseld is dit vaak in source vorm. Voortplanting van virii via source code is wel eens vertoond, maar heeft tot nu toe gelukkig nog niet zo'n grote vlucht genomen. Een potentieel gevaar hier is de toenemende populariteit van Linux. Met de steeds bredere verspreiding van Linux neemt de gemiddelde diversiteit van de Unix gemeenschap af (inteelt?) en wordt het daardoor vatbaarder voor virii. Het feit trouwens dat voortplanting via programma's steeds moeilijker wordt voor virii heeft ertoe geleidt dat steeds meer virii verschijnen die via databestanden of e-mail attachments worden verspreidt. Momenteel wordt in diverse medische labs wereldwijd onderzoek gedaan naar een effectieve behandeling voor dit nieuwe probleem.

Terug naar de originele vraagstelling: tot nu toe is Unix om een aantal redenen verschoond gebleven van virusproblemen. De belangrijkste oorzaken daarvoor zijn een diversere "gene pool", betere afweermechanismem en beter gedrag bij de Unix gebruikers op het gebied van "veilige contacten". Mijn verwachting is echter dat met de toenemende populariteit van Linux (met name ook op de desktop) ons geliefde OS in de toekomst zwaarder onder vuur zal komen te liggen.

Q: *Beste Dr. Unix,,*

In het verleden hebben we regelmatig gezien dat radicale wereldverbeteraars poogden met geweld hun zienswijze aan anderen op te leggen. De Linux gemeenschap lijkt echter wel vrij te zijn van dergelijke terroristen. Hoe zit dit?

-- "Carlos" uit F.

A: Beste "Carlos",

De vreedzaamheid van de Linux gemeenschap is inderdaad overweldigend. Ik heb ergens eens gelezen dat als je Microsoft irriteert je onmiddelijk wordt opgegeten door een troep hongerige wolven, terwijl als je de Linux gemeenschap irriteert je het effect hebt van een kudde vlinders die opfladdert en alle kanten uitzwermt. Linux terrorisme heeft denk ik weinig zin, hoe heilig en waar onze missie ook is. Zoals Lenin namelijk al zei: "het doel van terrorisme is om terreur te zaaien". Diegenen die wij zouden wensen te bekeren doen zichzelf echter al Windows aan.

Wat zouden wij nog kunnen doen om hen te terroriseren? Van de Marquis de Sade heb ik mogen leren dat het geen zin heeft iemand te slaan die dit op prijs stelt. Vandaar.

Zit je ook met een prangende UNIX vraag? Mail het aan Dokter UNIX!