"Code Red" worm virus had erger gekund
Augustus 2001
Henk Jongedijk, vrijdag 22 september 2006 - 00:00:00

De fauna van het Internet wordt dagelijks voorzien van nieuwe bewoners. Wat is nu eigenlijk een worm? Het is een -meestal kwaadaardig- software programma, dat zich van de ene computer naar de andere computer kan verspreiden, zonder eerst bestanden te besmetten. Op het moment dat ik dit schrijf, worden wereldwijd tientallen columns gewijd aan dit onderwerp. Een dankbaar subject: virussen. Het Internet dreigde eind juli 2001 ten onder te gaan aan de eigen populariteit.

Om middernacht op donderdag 19 juli 2001 stopten meer dan 350.000 servers, die besmet waren met het 'Code Red' worm virus, te zoeken naar nog meer nieuw te infecteren servers. In plaats daarvan vielen ze gezamelijk de site van het amerikaanse Witte Huis aan. Ze deden dit door rechtstreeks het IP-adres (198.137.240.91) te benaderen. De hoeveelheden data die over de Internet lijnen werden gepompt namen zulke enorme vormen aan, dat experts vreesden dat delen van het Internet verstopt zouden raken. Dit gebeurde echter net niet. Niet omdat de techniek van het virus faalde, maar wel omdat er een ontwerpfout zat in het zich verspreidende virus zelf. Maar het is natuurlijk wachten op slimmere virusbouwers...

Hoe de systeembeheerders van het Witte Huis de aanval pareerden? Alle data upload naar het IP-adres werd afgevangen, en de inhoud van de site zelf werd geparkeerd op naburig IP-adres (198.137.240.92, let op het laatste verschillende cijfer in het IP-adres). De (onschuldige) bezoekers werden vanaf het oorspronkelijke adres omgeleid. Simpel, maar doeltreffend, want zo voorkwamen ze dat de site wellicht voor dagen uit de lucht ging. Was het maar wel erger geweest, want dan was de wereld wakker geschud omtrent de ernst van de situatie.

Dat namelijk zoveel servers besmet raakten, was niet toevallig. Ze draaiden allemaal Microsoft's Internet Information Server. Naar schatting werken zo'n 6 miljoen Web sites ermee. Maar niet met de allerlaatste versie. Vorige maand was er namelijk een gat in de beveiliging ontdekt (security hole), dat werd opgelost met een software patch. De worm maakte dankbaar gebruik van de "oude" fout. Dat desondanks zoveel besmettingen plaats vonden, lijkt het nogal slecht gesteld te zijn met de alertheid van netwerkbeheerders. Microsoft valt niets te verwijten, de software reus had het lek immers reeds gedicht? Maar ze hadden het gaatje ook zelf gecre Ã «erd, zou men kunnen zeggen. Helaas is software bouwen mensenwerk, is het verweer van Microsoft. Een argument dat zeker hout snijd. En het niet up-to-date houden van al die duizenden servers is natuurlijk geen goede reclame voor het beroep netwerkbeheerder.

Linux beheerders lachen stiekem in hun vuistje. Weer een smet op de blazoen van Microsoft. Maar als Linux wijd genoeg verspreid is, met miljoenen gebruikers, dan zal ook dat platform interessant worden voor virusmakers. En vertrouwt u zelf wel op Microsoft software, schud dan ook uw systeembeheerder even wakker. Goedemorgen!

Naschrift (1 augustus 2001)
Het 'Code Red' worm virus zou in de nacht van 31 juli op 1 augustus toeslaan. Het virus heeft -zeker in Europa- slechts weinig losgemaakt. Kennelijk heeft men in allerijl nog virussen bestreden met de nieuwste patches, of is het bedrijfsleven benauwd om eerlijk voor besmetting uit te komen...