ESB
Economisch Statistische Berichten

De vuurmuur

Auteur(s):
Koning, R.H.
Ruud H. Koning (ruud@rhkoning.com) is internet-hobbyist en verbonden aan de Faculteit der Economische Wetenschappen, Rijksuniversiteit Groningen.

Verschenen in:
ESB, 86e jaargang, nr. 4298, pagina 219, 9 maart 2001

Rubriek:
Prikkel

Trefwoord(en):

Op het moment dat dit wordt geschreven is het Valentijnsdag en zucht de wereld onder het Kournikova-virus. Dit computervirus van Nederlandse makelij verspreidt zich via e-mail en richt gelukkig geen blijvende schade aan. Om die reden is het eigenlijk een worm en geen virus. Hoe verspreidt dit 'virus' zich? Een nietsvermoedende internetter krijgt een e-mail van iemand die hij waarschijnlijk wel kent en bij deze e-mail is een bijlage gevoegd: ogenschijnlijk een plaatje van de tennis pin-up Anna Kournikova. Slechts een kleine minderheid van het heterosexuele mannelijk deel van de bevolking kan dan de verleiding weerstaan om het plaatje van mooie Anna te bekijken door er even op te klikken en het kwaad is geschied. Het bestand dat een plaatje lijkt is geen plaatje, maar een klein programmaatje. Het programmaatje doet niet zo vreselijk veel, behalve het versturen van hetzelfde 'plaatje' naar de mensen in het adresboek van het emailprogramma. Daar waar genoemde internetter normaal gesproken slechts een paar e-mails per dag verstuurt, stuurt hij nu een e-mail aan iedereen in zijn adresboek. Een internetprovider die veel van dit soort klanten heeft zal plots te maken krijgen met een sterke toename in de belasting van de computers die de e-mail versturen, en dat kan leiden tot verminderde of afwezige dienstverlening aan klanten die reguliere e-mail willen versturen. Dit zijn de belangrijkste kosten die door het virus worden veroorzaakt, samen met de extra telefoontikken die worden gegenereerd bij het verzenden en ontvangen van deze stortvloed aan e-mail. Deze kosten zijn niet geïnternaliseerd bij de computergebruiker, die het virus al dan niet onwetend verstuurt. Ze zouden kunnen worden voorkomen door voorzichtig computergebruik, aanschaf van een anti-virusprogramma, of door een besturingssysteem te gebruiken dat niet zomaar e-mailbestanden programma's laat uitvoeren.

Het bovenstaande is slechts een recent voorbeeld van de gevaren die loeren op het internet. Recent bezweken de computers van Microsoft nog onder een grote toevloed van internetverkeer, en vorig jaar waren aanvallen op de diensten van Amazon, eBay en Datek voorpaginanieuws. In de meeste van deze gevallen werden computers die een permanente verbinding met het internet hebben, misbruikt door een cracker die indirect de besturing van deze computers overnam. Het is buitengewoon lastig om de man of vrouw die iets dergelijks doet, te vinden. In het recente geval bleek het een Canadees te zijn, die tegen de lamp liep door eigen grootspraak, niet door goed speurwerk van internettechnici. De schade bedroeg ettelijke miljoenen guldens.

Technisch gezien is het niet al te moeilijk om een computer die permanent aan het internet is verbonden enigszins van de buitenwereld af te schermen door een 'firewall' te installeren. Dit is met name van belang voor het sterk groeiend aantal computers dat permanent via de kabel of via ADSL met het internet is verbonden.

Wat zegt een econoom nu over al deze risico's? Op dit ogenblik zijn de externe effecten van het beschermen van een computer tegen misbruik door derden niet geïnternaliseerd. In een wereld zonder transactiekosten zal uiteindelijk een efficiënte beveiliging van het internet tot stand komen [1]. Echter, hoe komen bedrijven in gesprek met particuliere internetgebruikers? Bovendien zijn tot op heden geen particuliere internetgebruikers aangeklaagd voor misbruik van hun computer door derden. Zij hebben dus weinig prikkels om de beveiliging van hun computer ter hand te nemen. Internetproviders die de verbinding leveren aan de particulieren verkeren in een moeilijke positie: aan de ene kant kunnen zij misschien uitgaand en binnenkomend internetverkeer controleren op virussen en pogingen om andere computers aan te vallen, aan de andere kant verhoudt zich dat erg slecht met hun standpunt dat zij niet verantwoordelijk zijn voor wat hun klanten doen op het internet. Van hun kant is dan ook niet direct een veiliger internet te verwachten.

Een interessant idee is naar voren gebracht door Hal Varian. Hij zegt in een column in de *New York Times*, dat een eerste oplossing van (ongewild) computermisbruik kan worden gevonden in het toewijzen van aansprakelijkheid aan de partij die het risico van misbruik het best kan beïnvloeden. Op dit ogenblik slikken de bedrijven die worden getroffen door aanvallen van andere computers in het algemeen hun verlies. In het licht van het bovenstaande zou dat dus betekenen dat ook particulieren van wie een computer is misbruikt, aansprakelijk gesteld zouden moeten worden voor dit misbruik: zij kunnen hun computer die permanent met het internet is verbonden eenvoudig beveiligen met een anti-virusprogramma, en met een firewall [2]. Per slot van rekening doet men de voordeur ook op slot als men weg gaat, zodat er geen ongenode gasten binnenkomen. Waarom zou onverantwoordelijk gedrag wel toelaatbaar zijn voor een computerbezitter die zijn computer niet fatsoenlijk afsluit voor de buitenwereld

---

1 Er zijn verschillende firewalls voor MS-Windowscomputers gratis beschikbaar op het internet.

2 Internetaanbieder Xs4all biedt al haar klanten gratis antivirus- en firewallsoftware aan, zodat de klanten zelf gedeeltelijk kunnen zorgen

voor de veiligheid van hun verbinding met het internet.