

## Weren hackers van internet moet prioriteit krijgen

*Informatiebeveiliging heeft nog steeds een lage prioriteit voor providers, omdat groei als het hoogste doel wordt beschouwd. J.A. van der Wel meent dat een proefproces, juridisch lastig maar niet kansloos, tegen een nalatige provider van groot belang is voor de toekomst van het internet.*

RECENT onderzoek van de Consumentenbond heeft laten zien dat e-business achterblijft bij de verwachtingen. Het publiek vertrouwt het internet nog niet en dat is niet zo vreemd. Hacks halen geregeld de krant en laatst verscheen een handig knulletje op tv met een hack op de software van een bank, hét instituut waarop wij moeten kunnen vertrouwen. De amusementswaarde is hoog, het is tenslotte leuk om David Goliat te zien verslaan.

Toch is er meer aan de hand dan amusement, het criminele circuit raakt ook betrokken. De creditcard-sector lijdt nu al 50% van zijn schade door internettransacties, terwijl slechts 10% van de omzet op het internet wordt behaald. Hoe lang houdt deze sector dat nog vol?

Dat het probleem serieus is, blijkt ook als we kijken naar de belagers. Daaronder zijn de echte hackers, virtuozen die uit liefde voor het vak internetsites onderzoeken en hacks melden aan de beheerder. Echte hackers willen niets te maken hebben met de Internethooligans.

In deze groep wil de één niet onderdoen voor de ander, waardoor wedstrijdsjes digitaal vér pissen ontstaan. Echte hackers en internethooligans doen hun kennis op via internet. Daar publiceren de *oldies* de laatste ontwikkelingen om vervolgens het handwerk aan anderen over te laten. Een bekende is 'Mixer'. Met een programma van hem legde een jongen van 17 de grootste en best beveiligde internetsites van de wereld plat, waaronder zelfs de FBI-site. De hackersscene groeit en bloeit. Niet voor niets gaan veel ondernemingen omzichtig te werk om het gladder ijs van de e-business te betreden. Weliswaar ontwikkelt de techniek nieuwe verdedigingsvormen,

ook tegen de aanval van 'Mixer', maar deze wapenwedloop doet de kosten exorbitant toenemen. De veiligheid van internet is zwak en de beveiligingskosten zijn hoog.

Er wordt wel verzucht dat effectieve bestrijding van hackers onmogelijk zou zijn doordat hackers vanaf iedere plek op de wereld kunnen toeslaan. Veel aanvallen vinden evenwel binnen de landsgrenzen plaats. Een Belg toonde enige tijd geleden een beveiligingslek aan in de site van de Generale Bank. Nederlandse hackers toonden tekortkomingen aan in het wachtwoordbeheer van de sites van Nederlandse verzekeringsmaatschappijen.

Effectieve beveiliging vereist een bijdrage van alle betrokken partijen en daár schort het aan. Organisaties die

e-commerce bedrijven zijn meest belanghebbend en zij investeren wel in beveiliging. Ook overheden zijn actief. Binnen Europa en de Verenigde Staten is de strafwet al behoorlijk op orde en recent zijn Internet Service Providers zelfs verplicht om handelingen van hun internetters te registreren. Landen die hiaten in de wet ontdekken, repareren die snel. De Filipino van het 'I love you virus' ging toen nog vrijuit, nu is bestrafing wel mogelijk.

Het grote probleem is de handhaving van de strafwet, het lijkt op dweilen met de kraan open door het grote aantal kwaadwillenden. Providers kunnen veel doen om hackers te weren, de kwaliteitsorganisaties onder hen doen dat ook. Anderen doen dat niet. Bancaire internetdiensten zijn rond de klok en alle dagen van de week open maar tal van providers bestrijden hackers alleen op werkdagen. De Telegraaf van 11 december jl. meldde dat iemand van 350 sites de wachtwoorden had gekraakt. Uit het bericht bleek dat men dagen achtereen had kunnen proberen, zonder dat de Provider ingreep.

Aanbieders van internetdienstverlening beperken zich gewoonlijk tot passieve verdediging, zoals het blokkeren van aanvallers met technische middelen. Het is een werkwijze met nadelige bijwerkingen, die bovendien

veel alertheid vereist. Een nadelige bijwerking is het risico van gebloekte klanten en omdat bekende sites vaak meerdere keren per dag worden uitgeprobeerd, leidt het kleinste foutje vrijwel onmiddellijk tot feest bij de hackers.

Aanbieders hebben een alternatief, de juridische tegenaanval. Deze aanpak bestaat uit een schadeclaim bij de provider die eenvoudige aanvallen toelaat. Ik ken een organisatie waarvan de directie direct reageert op een aanval door

## Zakelijke prikkels voor providers ontbreken

onmiddellijk tegenmaatregelen te verlangen van de directie van de provider waar de aanval van afkomstig is. Dit dreigen met juridische stappen is nog ongebruikelijk maar wel effectief.

Door het achterwege blijven van serieuze claims, bestrijden providers hackers eigenlijk alleen maar vanuit een moreel besef van wat goed en slecht is. Wat ontbreekt is een zakelijke prikkel. Zoals al gezegd, springen tal van providers ook zonder die zakelijke prikkel serieus om met de beveiliging van internet. Voor tal van service providers is groei evenwel het hoogste doel met als gevolg dat zij alle zeilen moeten bijzetten om hun service in de lucht te houden en het weren van hackers een lage prioriteit krijgt.

De providers staan juridisch niet sterk. De rechter zal in aanmerking nemen dat zij veel kunnen doen zoals alert reageren op klachten en vreemd gedrag onderscheppen. Argumenten dat dit allemaal teveel zou kosten, zijn nauwelijks geloofwaardig in deze tijd van gigahertzcomputers voor consumentenprijzen. Eveneens onzin is het argument dat privacywetgeving een actief beleid van providers in de weg staat. Alsof de privacy van mede-internetters niet beschermd zou moeten worden. Als providers het aantal hackers terugbrengen, kan de overheid op haar beurt de dreiging van de strafwet vergroten met verhoogde pakkans. Een proefproces tegen een nalatige provider, juridisch lastig maar niet kansloos, is van groot belang voor de toekomst van het internet.