

# HACKEN, KRAKEN

Met internet gaat de wereld open, maar dat geldt helaas ook voor de eigen pc. Voor je het weet ben je ongewilt lid van een crimineel robot-net. Gelukkig is er wel wat aan te doen.

DOOR **MARIE-JOSÉ KLAVER**  
FOTOGRAFIE **WIM KLERKX**

Internet heeft veel zegeningen gebracht, maar met de beveiliging van verbindingen en computers is het slecht gesteld. Een onbeschermd pc met Windows die op internet is aangesloten kan binnen enkele minuten gehackt worden. Uit een onderzoek van de *USA Today Show* blijkt dat computerkruikers maar vier minuten nodig hebben om een niet-beveiligde pc te ontdekken. De redactie van het televisieprogramma sloot zes computers met Windows, het meest gebruikte besturingssysteem, aan op internet en wachtte af. Na vier minuten wist de eerste indringer binnen te komen en na een kwartier waren er al drie hackers op de computer bezig. De indringers komen binnen via bekende lekken in Windows en programma's als Internet Explorer.

Behalve hackers loeren ook virusmakers, *spammers*, *spywaremakers* en *phishers* op pc's en

de gegevens op harde schijven. 'Virussen en *spyware* zorgen voor grote problemen bij particuliere internetgebruikers', vertelt Joran Polak van computerbeveiligingsbedrijf Pine Digital Security in Den Haag. 'Wij krijgen regelmatig telefoontjes van radeloze gebruikers die zeggen dat hun computer zo traag is geworden door alle besmettingen met virussen en *spyware* dat hij onbruikbaar is.'

Virusbemettingen zijn de laatste jaren erg gecompliceerd geworden, zegt Polak. 'Van de meeste virussen zijn verschillende varianten in omloop. Virusscanners herkennen meestal niet alle varianten. Vaak is er niet alleen sprake van een virusbesmetting, maar is er ook een indringer actief geweest op de pc en zijn bijvoorbeeld systeembestanden veranderd die ervoor zorgen dat een antivirusprogramma zijn werk niet goed kan doen. Het enige advies is dan: formatteren. Dat betekent dat alle gegevens van de harde schijf gewist moeten worden en dat het besturingssysteem, alle programma's en alle bestanden opnieuw geïnstalleerd moeten worden. Een vervelend en tijdrovend karwei.'

## Slachtoffers

*Phishing* is een relatief nieuwe vorm van internetplichting. Daarbij wordt gebruik gemaakt van bedrieglijk echt lijkende websites van bijvoorbeeld banken en creditcardmaatschappijen. Via een e-mailbericht, dat eruit ziet alsof het van een bank of een ander echt bedrijf afkomstig is, worden slachtoffers uitgenodigd om in te loggen op een website. Vaak staat er in de mail de mededeling dat er een computerstoring bij de bank is geweest en dat de bank nu wil controleren of alle accounts nog bestaan. Voor die controle is het noodzakelijk dat men inlogt. Het doel van de *phishers* is het bemachtigen van inlognamen en wachtwoorden van klanten die internetbankieren. De website

waarop ingelogd moet worden, is meestal een vrijwel exacte kopie van de echte banksite. Zodra het slachtoffer inlogt, vangen de *phishers* zijn inlognaam en wachtwoord op. Met deze gegevens kunnen ze in sommige gevallen zelf geld afschrijven van de bankrekening.

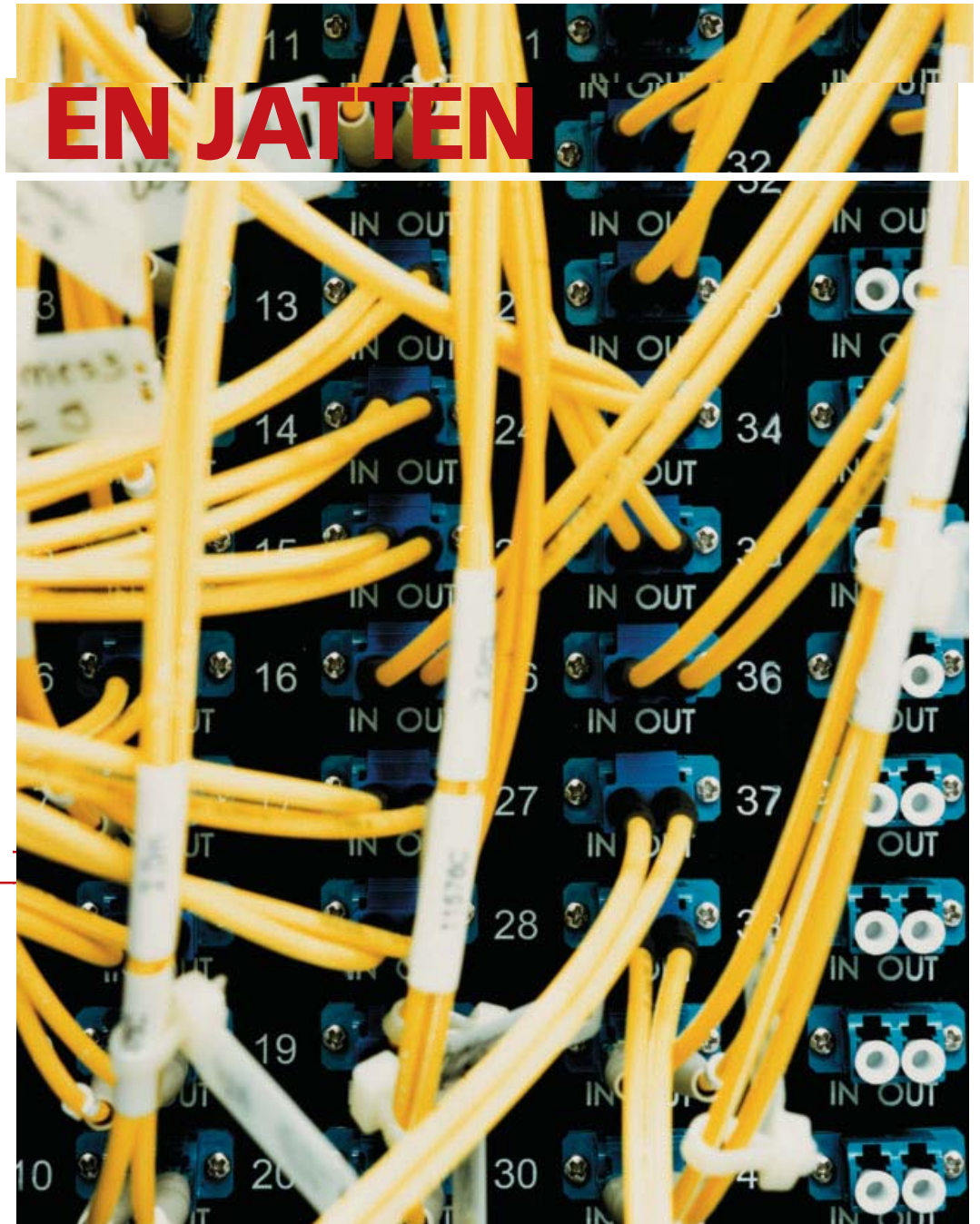
Vooral in de Verenigde Staten en Groot-Brittannië komt *phishing* veel voor. Volgens de Britse Association of Payment Clearing Services, te vergelijken met Interpay in Nederland, is het aantal geregistreerde *phishing*-gevallen in de eerste zes maanden van 2006 verzeventvoudigd. De schade die deze vorm van bankfraude aanrichtte in Groot-Brittannië, bedroeg in die periode bijna 32 miljoen euro. Naar schatting 1 op de 20 Britten die gebruik maakt van internetbankieren is de afgelopen jaren slachtoffer van *phishing* geworden. Volgens onderzoeksbureau Gartner bedroeg de wereldwijde schade door *phishing* in 2006 bijna twee miljard euro.

In Nederland is de Postbank in 2005 twee keer het doelwit van *phishers* geworden. De eerste mail waarmee onbekende criminelen uit het buitenland Postbank-klanten wilden verleiden om op een nepsite in te loggen was in het Engels gesteld en viel daardoor erg op. De tweede *phishing*-poging was in het Nederlands en leek overtuigender. Voor zover bekend zijn er in beide gevallen geen financieel gedupeerden.

Dat in Nederland je bankrekening wordt geplunderd door een hacker die via *phishing* of een inbraak op je pc aan inloggegevens komt, acht internetbeveiliging Polak niet erg aanmerkelijk. 'Diefstal van bankrekeningen en gestolen creditcardnummers is in de Verenigde Staten en Groot-Brittannië wel een groot probleem. In de Verenigde Staten is de gemiddelde schade van digitale bankinbraken 1200 dollar per klant. In Nederland is het internetbankieren net iets beter beveiligd. Je hebt >

# EN JATTEN

Rechts:  
Optische schakelkast voor glasvezelkabels bij het natuurkundig lab CERN in Genève. Door iedere glasvezelkabel kan per seconde 10 Gigabits aan gegevens verzonden worden.



niet genoeg aan een inlognaam en een wachtwoord om geld over te boeken. Hier werken banken met apparaatjes die nog een extra code genereren of met TAN-codes die je van je bank krijgt. Voor elke transactie heb je een unieke code nodig. Zonder die code ben je nergens.'

### Obscuur taaltje

Leon Kuunders van informatiebeveiligingsbedrijf Trusted-Id, dat ook in Den Haag is gevestigd, is het niet helemaal met Polak van Pine eens. 'Het is waar dat er in Nederland weinig concrete gevallen van *phishing* bekend zijn. We hebben het geluk dat Nederlands voor de meeste mensen buiten ons land een obscuur taaltje is. Om mensen in een *phishing*-mail te laten trappen moet je het Nederlands perfect beheersen. Maar in die onbekendheid met het fenomeen schuilt misschien juist het gevaar. Nederlanders zijn er niet alert op. Dus als er een keer iemand met een goede *phishing*-mail komt, is de kans groot dat er slachtoffers vallen.'

Kuunders waarschuwt ook voor *spyware*. 'Er zijn twee soorten *spyware*. De eerste soort is relatief onschuldig en laat alleen ongewenste reclame zien. Daar heb je als gebruiker wel last van omdat je computer erg traag wordt. Van de tweede soort merk je minder, maar die is wel vervelender. Deze *spyware* zorgt ervoor dat je computer een deel wordt van een netwerk van pc's die bijvoorbeeld *spam* versturen of aanvallen uitvoeren op sites – zonder dat je het zelf in de gaten hebt. Zo werk je ongewild en meestal ongemerkt mee aan criminele activiteiten.'

Erik van Veen van Symantec Nederland in Leiden bevestigt dit. 'Er zijn dagelijks 57.000 van dat soort netwerken actief – we noemen ze *botnet*netwerken, dat komt van robot. Die bestaan uit 4,5 miljoen gekraakte pc's van consumenten. Particuliere internetgebruikers zijn een makkelijke prooi omdat hun pc's meestal slecht beveiligd zijn. Op 30 tot 40 procent van de consumenten-pc's is geen enkele vorm van beveiliging aanwezig.'

Ook *phishing* is in Nederland een snelgroeiend probleem, zegt Van Veen. Volgens onderzoek van softwarebedrijf Symantec is het

aantal *phishing*-aanvallen de afgelopen zes maanden met ruim 80 procent toegenomen. 'Er worden 865 nieuwe en unieke *phishing*-mails per dag verstuurd, ook Nederlanders zijn het doelwit.' Financiële schade ten gevolge van *phishing* komt in Nederland ook voor, zegt Van Veen. Wereldwijd gezien wordt volgens Van Veen 2 procent van de *phishing*-aanvallen op Nederland gericht. 'Banken en financiële instellingen zijn daar erg discreet over. Vooral nog betalen de banken zelf de schade en brengen ze zulke gevallen niet naar buiten om hun imago te beschermen.'

Van Veen constateert dat computercriminelen steeds professioneler worden en steeds gericht te werk gaan. 'Het stadium van de student die een virus programmeert om ermee op de voorpagina van de krant te komen zijn we al lang voorbij. We zien dat botnets op een bedrijfsmatige manier gerund worden. De netwerken worden verhuurd aan bijvoorbeeld spambedrijven en *phishers*. Omdat een botnet uit allemaal verschillende computers met een eigen internetverbinding bestaat is het voor politie en justitie moeilijk te achterhalen waar de misdadigers zich bevinden.'

### Zelf doen

Wat kan de eezame pc-gebruiker zelf doen om zijn pc te beschermen tegen *hackers*, virussen, *phishers* en *spam*? Ten eerste is het belangrijk om van belangrijke gegevens een back-up te maken. Uit onderzoek blijkt dat ruim 85 procent van de computergebruikers nooit of slechts zelden een back-up maakt. Dat is vreemd, want 40 procent van de pc-bezitters vindt de informatie op hun harde schijf 'onbetaalbaar'. Een back-up kan op cd-roms of dvd's gemaakt worden of online bij een betrouwbare provider.

Belangrijk is verder verschillende wachtwoorden te kiezen voor je internetaccount (toegang en e-mail) en elektronisch bankieren. Mocht een *hacker* via een internetaccount op een pc binnengekomen zijn, dan kan hij in ieder geval niet direct bij de internet-bankrekening. Een sterk wachtwoord is langer dan acht tekens en is een combinatie van kleine letters,

hoofdletters, cijfers en leestekens. Het is in ieder geval onverstandig de eigen naam of die van een favoriete voetbalclub als wachtwoord te kiezen.

De meeste cyberinbrekers komen niet op een reguliere manier op een pc binnen. Ze maken gebruik van achterdeurtjes en lekken. Vooral het besturingssysteem Windows en de browser Internet Explorer van Microsoft hebben veel last van gaten in de beveiliging. Zodra er een lek ontdekt wordt, worden er door hackers programma's geschreven waarmee misbruik van een lek gemaakt kan worden. Microsoft zorgt regelmatig voor gratis updates via zijn site. Windows kan ook zo ingesteld worden dat de *updates* automatisch gedownload en geïnstalleerd worden.

Verder is installatie van een *firewall* van groot belang. *Firewall* betekent letterlijk brandmuur. Zoals een brandmuur voorkomt dat een brand van de ene kant naar de andere van een gebouw overslaat, zo houdt een *firewall* aanvallen van buitenaf op pc's tegen. In Windows xp met Service Pack 2 zit een *firewall* ingebouwd die standaard aanstaat. De xp-*firewall* biedt een basale bescherming. Wie meer veiligheid wil kan het gratis ZoneAlarm van Zonelabs downloaden of een *firewall* van bijvoorbeeld Symantec of McAfee aanschaffen.

### Heterdaad

Een antivirusprogramma is ook essentieel. De meeste antivirusbedrijven bieden tegenwoordig totaalpakketten aan die niet alleen tegen virussen beschermen, maar ook tegen *spam*, *spyware* en *phishing*. Vaak bevat zo'n pakket ook een *firewall* en een back-up programma. Zulke pakketten zijn erg nuttig, maar ontslaan de pc-gebruiker niet van de plicht om zelf de Windows-updates van Microsoft te downloaden (of dat automatisch te laten doen). Ook de virus-scanner moet minstens een keer per week geupdate worden. Veel providers bieden ook de mogelijkheid tot online virusscannen. Dan wordt de indringer op heterdaad betrapt. **M**

**Marie-José Klaver** is internetjournalist.