



Hackers hebben hun onschuld verloren

Cyber crime

Het digitale dievengilde gaat het allang niet meer om het voor iedereen gratis toegankelijk maken van software. Idealisme heeft in veel gevallen plaats gemaakt voor ordinair materialisme: hackers zijn crackers geworden. Kan een eenvoudige pc-gebruiker zich nog wel tegen ongewenste aanvallen beschermen? 'Het is niet verstandig om zomaar elke link te volgen.'



ILLUSTRATIE JOHANNES ROEBERINK

HONING VOOR HACKERS

Om een beeld te krijgen van de meest voorkomende aanvallen op pc's thuis, initieerde de redactie van *De Ingenieur* dit jaar een onderzoek. Walter Bergers van beveiligingsbedrijf Madison Gurkha nam de opzet en uitvoering van de test op zich. Hans van de Looy van hetzelfde bedrijf analyseerde achteraf de ruim 24 MB verkregen ruwe data. Madison Gurkha maakte voor de test gebruik van een *honeypot*, een computersysteem dat er van buiten aantrekkelijk uitziet voor een hacker, maar waarbij of waarmee hij weinig kwaad kan aanrichten. Een *honeypot* is te gebruiken om een hacker af te leiden van een gevoeliger systeem maar ook, zoals in dit geval, om de acties van de inbreker te registreren.

'De *honeypot* werd zodanig geconfigureerd dat het van buitenaf leek alsof er in totaal dertien systemen actief waren die vanaf internet als eenvoudige Windows XP Professional server zou worden geïdentificeerd', zegt Van de Looy. 'Binnen anderhalf uur ontving de *honeypot* de eerste geautomatiseerde aanval. In een periode van 48 dagen onderschepte het detectiesysteem 77 238 inbraakwaarschuwingen. Dit zijn ruim 1600 meldingen per dag.' Volgens Van de Looy is bij alle aanvallen gebruik gemaakt van geautomatiseerde scripts. 'In totaal zijn er 13 607 IP-adressen vastgelegd van waaruit de systemen zijn aangevallen. De adressen bevinden

| KENGETALLEN TEST | |
|----------------------------|----------|
| TESTDUUR | 48 dagen |
| TOTAAL AANTAL AANVALLEN | 77 238 |
| AANVALLENDE IP-ADRESSEN | 13 607 |

zich verspreid over de hele wereld. Uit Nederland kwamen 786 aanvallen.' De aan meest voorkomende aanvallen waaraan ieders pc bloot kan staan, hebben we op een rijtje gezet.

1. Barebyte unicode encoding (15 356 meldingen) Op internet is het de afspraak om normaliter alleen zogenaamde ASCII-karakters te gebruiken in URL-adressen. Met de zogenoemde Unicode zijn afwijkende karakters te vormen door een % teken te combineren met een ASCII-teken. Dit is legaal. Het is echter ook mogelijk codes te sturen, waarbij het % teken gecombineerd is met niet-ASCII-teken. Met deze codes is het mogelijk om van buitenaf een (verouder-

de) IIS-webserver commando's te geven en zo bijvoorbeeld een webroot directory traversal (zie 6) te maken.

2. Oversize request-uri directory (13 009) Een link naar een webserver overschrijdt de maximale limiet van het aantal karakters. Dit kan leiden tot een *buffer overflow*. Het teveel aan karakters overschrijft hierbij andere delen van de software. In het ergste geval kan een cracker op deze manier de controle overnemen.

3. Double decoding attack (11 743) Net als bij 1 een coderingstruc. Het verschil is dat deze codering niet één filter, maar twee filters probeert te omzeilen. Met behulp van bepaalde

codes kan de hacker zien wat voor data er buiten de openbare pagina's op de webserver staan.

4. Non-RFC HTTP delimiter (10 433) Met een delimiter wordt een scheidingsteken bedoeld. Door gebruik van een niet-standaardscheidingsteken is het mogelijk de software op de webserver in de war te schoppen. Inbraak, ongewenste gegevensverspreiding en of een crash kan het gevolg zijn.

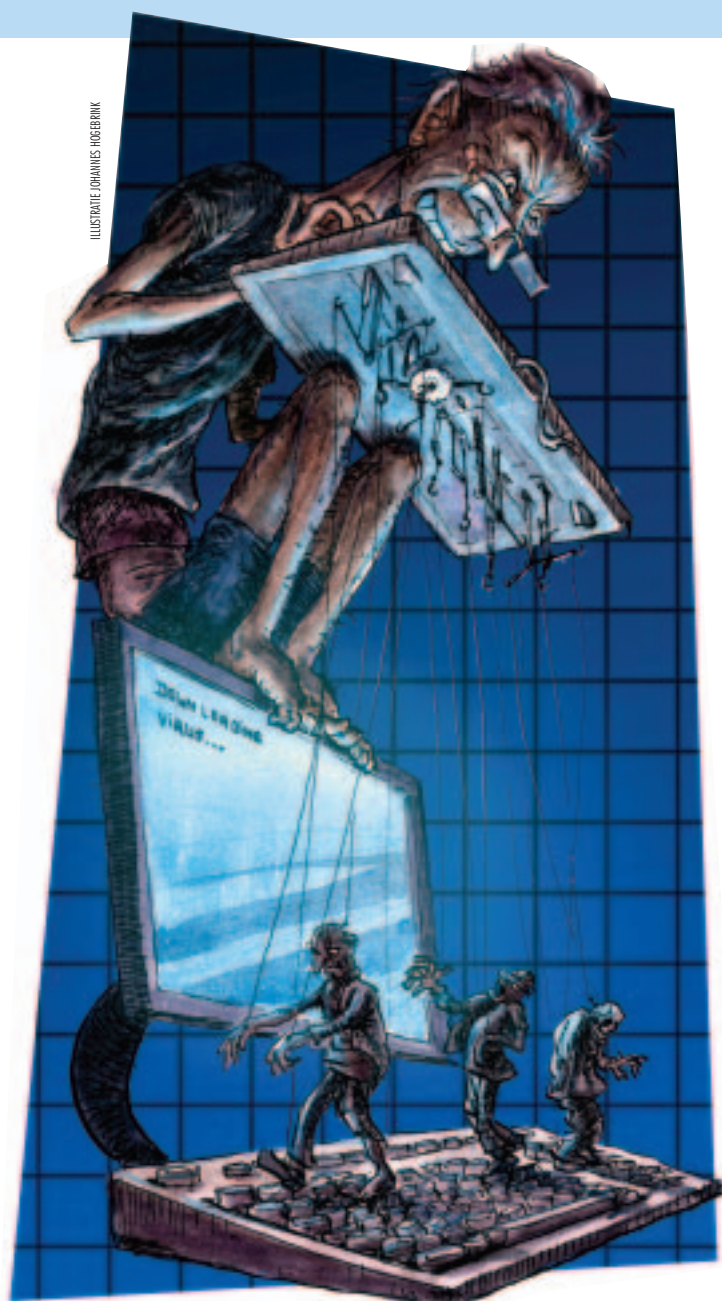
5. ICMP PING NMAP (9641) Met NMAP is het mogelijk een netwerk te verkennen. Hiermee kan een hacker inzicht krijgen in de beschikbare diensten en gebruikte systemen.

6. Webroot directory traversal (4483) Op

een webserver staan behalve publieke webpagina's ook vaak bestanden die niet openbaar zijn en zodoende in een aparte map op de server staan. Met een truc is het bij bijvoorbeeld een fout in de software van de webserver mogelijk om de publieke folder met de website te verlaten en toegang te krijgen tot andere data op de server.

7. MS-SQL overflow attempt (3546) MS-SQL is een databasesysteem. Net als bij 2 is het hiermee mogelijk een Buffer Overflow te creëren.

8. MS-SQL worm propagation attempt (3515) Van buitenaf probeert iemand met een worm binnen te dringen bij de MS-SQL server.



ILLUSTRATIE: JOHANNES HEEBINK

geen weg meer terug. Je begeeft je op het pad naar perfectie en laat de rest achter je.'

Dit citaat lijkt afkomstig van een initiatieritueel van een of andere sekte, maar staat in een korte handleiding voor beginnende hackers. En hoewel zij niet specifiek religieus zijn, is het fenomeen hacker voor een *404* (iemand die met betrekking tot computers dom of onwetend is, zie woordenlijst) minstens zo mysterieus als een sektelid. Een ingewijde in de kunst van het hacken begeeft zich dan ook regelmatig tussen legers van zombies, muren van vuur, Trojaanse paarden, geniepige wormen en allesvernietigende virussen die allemaal tot leven zijn gewekt met ingewikkelde toverspreuken in een vreemde taal. In deze onderwereld speelt zich een sprookjesachtige strijd af tussen de *blackhats* en *whitehats*. Welkom in *cyberspace*.

EERLIJK DELEN

Hacker was een predikaat voor iemand die zo goed met een (computer)systeem om kon gaan dat hij de grenzen ervan wist te omzeilen of verleggen. In die zin waren de eerste hackers *phonephreaks*. Zij hielden zich vooral bezig met telefoonnetwerken (zie 'Kraker met kinderfluit'). De eerste computerhackers waren over het algemeen programmeurs die zochten naar fouten in software, zodat ze in staat waren programma's te verbeteren en systeembeheerders konden waarschuwen voor mogelijk misbruik. Het sportelement was hierbij ook van groot belang.

Aangezien computers in die periode schaars waren, speelden deze taferelen zich vooral af op technische universiteiten, zoals het Artificial Intelligence Lab van het Massachusetts Institute of Technology. Deze *old school hackers* (hackers van de oude stempel) vonden het belangrijk dat informatie voor iedereen vrij toegankelijk was en zagen het als hun ethische plicht om hun expertise te delen door gratis software te schrijven en waar mogelijk informatie en computers vrij toegankelijk te maken. Deze denkwijze is onder andere terug te vinden bij het besturingsprogramma Linux, dat in tegenstelling tot Windows gewoon beschikbaar is en gratis van internet is te halen. Minder bekende programma's als FreeBSD en OpenBSD gaan zelfs nog verder dan Linux. Ook Wikipedia, een online encyclopedie waarvoor iedereen een eigen lemma kan kiezen en beschrijven, is op dit uitgangspunt gebaseerd.

Dit zijn relatief bekende voorbeelden, maar hackers delen meer informatie, zoals wachtwoorden voor websites op www.bugmenot.com. Een meer omstrede overtuiging van



Een honeypot ziet er van buiten aantrekkelijk uit, maar een hacker kan er weinig kwaad aanrichten.

| KENGEGEVENS HONEYPOT | |
|-------------------------|--|
| SOFTWARE | Windows XP Professional (met Service Pack 1) Honey D Snort |
| SERVICES | IIS/5.0 SSH (open SSH 3.5p1) |
| ROUTER | Cisco 1601R met IOS12.1 (5) met toegang tot telnet |

veel hackers is dat het ethisch acceptabel is een systeem voor de lol of voor een studie te kraken zolang de inbreker maar niks steelt, kapotmaakt of geheime informatie naar buiten brengt. Deze denkwijze heeft echter ook veel niet-kwaadwillende hackers in problemen gebracht. Inbreken is nou eenmaal verboden bij de wet, ongeacht het motief.

ROBIN HOOD

Hackers die van de basisregels afwijken en op het dievenpad terecht komen heten geen hacker meer, maar worden *crackers* of *blackhats* genoemd. De grens is echter soms moeilijk te trekken. Sommige hackers vinden dat alle software gratis moet

zijn, dus ook software die bedrijven willen verkopen. Daarom kraken ze deze programma's om ze vervolgens op internet te zetten waar iedereen ze kan downloaden. Volgens de wet is dit diefstal. Maar hackers identificeren zich graag met Robin Hood: het is niet eerlijk dat software alleen beschikbaar is voor

mensen met geld. Andere voorbeelden van *hacks* zijn bijvoorbeeld het zodanig aanpassen van een Ipod Shuffle of – in Nederland nog niet verkrijgbaar – Play Station Portable dat de ingebouwde restricties van de fabrikant worden omzeild.

Over het algemeen steken hackers hun overtuigingen niet onder stoelen of banken. Websites die tegen hun moraal indruisen, lopen kans dat ze worden platgelegd of verminkt.

VISSEN NAAR GELD

Eén van de grootste trends onder internetcriminel is waarschijnlijk *phishing*. Bij deze methode maken de zwendelaars gebruik van zowel hacker-vaardigheden als *social engineering*. Via de computer doen ze zich voor als een bedrijf, persoon of instantie om informatie los te krijgen waarmee ze hun slag kunnen slaan.

Een recent voorbeeld zijn de vervalste e-mails die zogenaamd van PayPal, een bedrijf dat zakelijke transacties via internet mogelijk maakt, komen (ook wel *spoofing* genoemd). Onlangs werden er in Nederland vergelijkbare

e-mails gesignaleerd die van de Postbank kwamen. In de nepbrief probeerden de oplichters te suggereren dat er vanaf een buitenlands IP-adres één of meerdere pogingen zijn ondernomen om in te breken op rekeningen bij PayPal. Om de gegevens te controleren verzochten ze de Postbank-klant vriendelijk om binnen een bepaalde termijn en via de meegestuurde link in te loggen bij PayPal. Wie uit voorzorg op deze link klikte en inlogde liep kans op een geplunderde rekening. Alleen al door te klikken was het mogelijk een *keylog* te installeren die vervolgens alle aanslagen van de gedupeerde op het toetsenbord vastlegt voor de zwende-

laars. Als hij ook nog inlogt op de link hebben de criminelen niet eens een *keylogger* nodig: het slachtoffer tikt zijn inlognaam en wachtwoord dan zelf in op hun website. Hoewel lang niet iedereen in deze val trapt, kunnen deze praktijken zeer lucratief zijn. Als er 1 % reageert op een miljoen verstuurd mails, hebben de criminelen toegang tot 10 000 bankrekeningen. Maar *phishing* blijft niet beperkt tot nepmails. Met een *gespoofde* website hebben crackers geen *keylogger* nodig. Zonder dat het slachtoffer er erg in heeft, tikt hij zijn wachtwoord in op een onbeschermd website. Maar op het

werk kan een telefoontje van een systeembeheerder ook verdacht zijn. Iemand kan zich voordoen als beheerder om achter een wachtwoord te komen.

Rob van Dalen, teamleider bij de digitale recherche, benadrukt dat een foutje snel is gemaakt.

'Nieuw aangenomen mensen proberen we wel eens uit door ons voor te doen als de systeembeheerder. Het komt wel voor dat we zo wachtwoorden weten te ontfutselen. Het voordeel van deze test is dat ze daarna minder goed van vertrouwen zijn.'

Volgens de Anti-phishing Workgroup, een organisatie die deze vorm van criminaliteit

bestrijdt, liep het aantal actieve, gerapporteerde nepsites van oktober 2004 tot mei 2005 op van 1142 per maand tot 3326. Gezien de korte levensduur van dit soort sites, is het niet onwaarschijnlijk dat er honderden nepsites per dag bij komen.

Zo onderging de Nederlandse website van de B.I.G.-campagne (Ban Illegale Games en software) in februari een *defacement*. Behalve de nodige aanpassingen van het logo met daarvoorheen de kreet 'HACKED!', plaatsten de inbrekers ook leuzen op de website: 'Eerlijk zullen we alles delen' en 'Jongeren worden al genoeg uitgebuit'. Zover bekend heeft misdaadverslaggever Peter R. de Vries, die het boegbeeld van B.I.G. is, de daders nog niet weten te traceren.

Dit soort acties is uit idealistisch oogpunt nog wel te billijken. Helaas zijn deze nobele *sporthackers* tegenwoordig sterk in de minderheid. Steeds meer inbrekers willen vooral geld zien en vormen een nieuwe vorm van georganiseerde misdaad. Zo probeerde een groep crackers eerder dit jaar een Londense vestiging van de Japanse bank Sumitomo Mitsui te beroven van 220 miljoen pond. De daders konden rekeningnummers, wachtwoorden en andere gevoelige informatie achterhalen. De politie in Londen wist de overval, die één van de grootste uit de geschiedenis zou zijn geweest, te voorkomen. In Israël is een

verdachte van de roof aangehouden die probeerde 13,9 miljoen pond over te schrijven op een Israëlische rekening.

Een ander recent voorbeeld is de roof van de gegevens van veertig miljoen creditcards van MasterCard International. Een computervirus bij CardSystems, een Amerikaanse onderneming die betalingstransacties verwerkt, zou de diefstal hebben ingeleid. Ook een aantal Nederlandse creditcardhouders kreeg uit voorzorg een nieuwe pas. Het is duidelijk dat *cyber crime* groeit, en met onze toenemende afhankelijkheid van computersystemen neemt onze kwetsbaarheid voor computercriminelen toe.

WERKWIJZE

Hoe gaat een hacker eigenlijk te werk? 'Bij een aanval begint een hacker altijd met het verzamelen van informatie over het slachtoffer. Dit kan een bedrijf, instantie of een enkel persoon zijn', zegt Job de Haas, 'een professionele hacker'. Als directeur van IT-beveiligingsbedrijf ITSX breekt hij regelmatig in bij bedrijven om de beveiliging te testen. 'De informatie die van belang is voor de aanvallers bestaat uit IP-adressen, bij bedrijven de namen en telefoonnummers van de medewerkers en een overzicht van de aangeboden netwerkdiensten, zoals een web-, mail- of FTP-server.' Over het algemeen is het inwinnen van deze informatie geen probleem. 'IP-adressen zijn niet geheim en daardoor over het algemeen makkelijk te vinden in zoge-

noemde WHOIS-databases op internet. Namen en telefoonnummers van medewerkers staan vaak op internet en zijn anders met een simpel telefoontje naar het bedrijf te achterhalen. Een overzicht van de aangeboden netwerkdiensten is te verkrijgen door een *poortscan* uit te voeren. Simpel gezegd ziet de hacker met zo'n scan welke poorten (softwarematige sluisen waardoor informatie kan worden uitgewisseld) open staan en welk soort informatie de poort doorsluis. Zo'n scan is bijvoorbeeld uit te voeren met het gratis te downloaden programma NMAP.

'Vervolgens is het zaak er achter te komen wat de zwakke plekken zijn in het systeem. Draait er verouderde software? Welke webserver gebruikt het slachtoffer? Als je dat eenmaal weet, is het een koud kunstje om de zwakke plekken in één van de vele databases op internet op te zoeken en welke mogelijkheden tot misbruik (*exploits*) hierbij horen.' Dit lijkt voor de gemiddelde gebruiker moeilijk te achterhalen, maar dit komt vooral omdat we met Windows niet meer zien wat er achter de schermen gebeurt. Dit was bij een besturingsprogramma als DOS veel duidelijker. Hackers maken daarom onder andere gebruik van een speciale *proxy server* (bijvoorbeeld Burp proxie van Portswigger), een soort station tussen de browser op de computer en de webserver waarmee hij contact maakt. Met dit gereedschap kan de hacker al het passerende verkeer onderscheppen, inspecteren en aanpassen. De manier waarop de proxy de informatie weergeeft, is vergelijkbaar met het 'onderwaterscherm' van het tekstverwerkingsprogramma WordPerfect dat tegenwoordig voor het grootste deel door Word is verdrongen.

ACHTERDEUR

De handelingen tot nu toe zijn nog legaal. De eigenlijke inbraak kan nu beginnen. Sommige hackers maken gebruik van bestaande gereedschappen die op internet zijn te vinden. Een goede hacker is ook in staat zelf programma's te schrijven en bestaande programma's aan te passen.

Wanneer hij eenmaal binnen is, kan de hacker het hele systeem overnemen door de aanwezige software te herprogrammeren en nieuwe programmatuur toe te voegen. Zo kan hij bijvoorbeeld een 'achterdeur' creëren om op een later tijdstip makkelijk binnen te dringen, de firewall en virusscanner uit te schakelen, spam te versturen, het toetsenbord af te luisteren, geheime informatie te kopiëren en vanaf de betreffende pc andere systemen aan te vallen. En dit alles kan

gebeuren zonder dat de gebruiker iets merkt. Maar natuurlijk kan de hacker een computer ook platleggen.

Om een beeld te krijgen van de meest voorkomende aanvallen voor een pc-gebruiker heeft *De Ingenieur* beveiligingsbedrijf Madison Gurkha gevraagd te helpen bij een onderzoek. Medewerkers van Madison Gurkha hielden ruim een maand alle aanvallen op een speciaal ingerichte *honeypot* bij. Dit is een systeem dat speciaal voor dit doel is geconfigureerd (zie 'Honing voor hackers').

LEGER

Een cracker zal overigens niet snel een directe, gerichte aanval op een thuisgebruiker openen. Dat kost hem veel te veel tijd om wat te verdienen. Toch is het belangrijk voor de cybercrimineel om macht te hebben over veel verschillende computers. Hiermee kan hij namelijk een leger 'zombies' of *bots* vormen, ook wel zombienet of botnet genoemd. Deze netwerken worden onderling zelfs verhandeld. Zodra een geïnfecteerde computer contact maakt met internet, kan hij als zombie communiceren met de cracker via bijvoorbeeld een chatroom. Vanaf deze plek geeft de cracker commando's aan zijn leger en kan hij grootschalige aanvallen doen op bijvoorbeeld een specifieke webserver. Zonder dat we het weten besturen criminelen hierbij als poppenspelers onze computers. Door met soms wel duizenden zombies tegelijk informa-

tie op te vragen raakt de server overbelast en is hij onbruikbaar. Dit noemen hackers een Distributed Denial Of Service (DDOS). Door te dreigen een server plat te leggen met behulp van een DDOS kan een cracker een bedrijf dat afhankelijk is van internet, zoals een webwinkel of een bank waarbij het mogelijk is om te internetbankieren, gemakkelijk chanteren. Vaak doen dit soort bedrijven geen aangifte van deze vorm van afpersing. Als bekend wordt dat hun site is gekraakt, bestaat de kans dat ze klanten kwijtraken.

Om een groot botnet bij elkaar te krijgen hoeft de hacker niet één voor één systemen te penetreren. De meeste van deze aanvallen zijn geautomatiseerd. 'De bekendste manier is het per e-mail versturen van een virus via een zombie', zegt beveiligingsexpert Tomislav Pavlovic van Symantec, een van de grootste antivirussoftware-aanbieders ter wereld. 'Maar ook door een website te bezoeken kan een gebruiker automatisch, zonder het te weten, ongewenste programmatuur downloaden. Een andere bekende truc is het gebruik van een Trojan Horse. Een document dat iemand willens en wetens downloadt - een digitale wenskaart of een screensaver - functioneert dan als een paard van Troje, omdat er bijvoorbeeld een virus in verborgen is. Via *peer-to-peer*-programma's, zoals het bekende muziekuitwisselingsprogramma Kazaa, en chatprogramma's is het ook mak-

'Van alle virussen verspreidt zich 95% nog steeds via e-mail'



'Het belangrijkste wapen is een goede firewall en virusscanner'

KRAKER MET KINDERFLUIT

Veel hackers van het eerste uur zijn ooit begonnen met *phonephreaking*, het manipuleren van het telefoonnetwerk om bijvoorbeeld gratis te kunnen bellen. De bekendste *phreak* is waarschijnlijk John 'Captain Crunch' Draper. Hij ontdekte begin jaren zeventig dat hij met een gratis fluitje, dat bij een pak graanontbijt (Captain Crunch) voor kinderen zat, interlokaal kon bellen. Het geluid van het door John aangepaste fluitje was namelijk exact gelijk aan de 2600 Hertz toon, die het telefoonsysteem opdracht gaf een lijn te openen. Later ontwikkelde Draper de *blue box*, een apparaat dat ook andere tonen kon voortbrengen die telefoonmaatschappij AT&T gebruikte. Hiermee was het ineens erg makkelijk om in te breken op het telefoonnetwerk. Whizzkids Steve Jobs en Steve Wozniak, de latere grondleggers van Apple, bouwden op aanwijzingen van Draper zelfs hun eigen *blue boxes* die ze verkochten.

lijkelijk om *malicious code* (ongewenste programmatuur, red.) te verspreiden.'

Een andere aanvalsmethode heet *phishing*. Bij deze combinatie van hackertechnieken en *social engineering* hopen de criminelen iemand geld afhandig te maken door zich via de computer anders voor te doen dan ze in werkelijkheid zijn. Bij een bekende *phishing*-zwendel deden de criminelen zich voor als het bedrijf PayPal, dat veel van het betalingsverkeer via internet regelt (zie 'Vissen naar geld').

Weer een stap verder is cyberterrorisme. Een handige hacker kan een telefoon- of stroomnetwerk lamleggen of het netwerk van een bank of luchtvaartcontrolesysteem.

GEDRAG

Wat kan een onwetende computergebruiker doen tegen *cyber crime*? 'Het belangrijkste wapen ligt voor de hand: een goede firewall en virusscanner die *up to date* is', zegt Pavlovic. 'Van alle virussen verspreidt zich 95 % nog steeds via e-mail. Met goede software zijn veel infecties te voorkomen.' Maar volledige veiligheid is niet haalbaar. De beschikbare systeem-aanpassingen lopen altijd iets achter en nieuwe virussen, wormen en andere ongewenste programmatuur komen over het algemeen dus ongedetecteerd door de firewall. Volgens Pavlovic is een goed geconfigureerde *personal firewall* wel vaak in staat om het verspreiden van een infectie tegen te houden.

'Daarnaast is het belangrijk dat een gebruiker zich realiseert dat niet alles zonder gevaar is en zijn gedrag op internet aan dit besef aanpast. Het is bijvoorbeeld niet verstandig om zomaar elke link te volgen.' Links die via spam binnenkomen, zijn potentieel sowieso gevaarlijk. 'Zelfs van een betrouwbare persoon of instantie. De link die zichtbaar is op het scherm, kan wel eens een andere zijn dan die wordt aangeklikt. Bij belangrijke zaken kan iemand het beste zelf het webadres intikken.'

Ook het openen van toegestuurde bijlagen kan gevaarlijk zijn. Mail van onbekenden is altijd verdacht, zeker als de bijlage een vreemde extensie heeft (.pif of .exe) of een dubbele extensie (.doc.pif). Een andere belangrijke gebruikersregel is nooit vertrouwelijke gegevens versturen per e-mail, want het is niet duidelijk wie er meeluistert. Tot slot is het verstandig goed back-ups bij te houden van de dingen die belangrijk zijn.

Zich aan deze regels houden betekent echter geen garantie voor veilig computergebruik. Het maken van een fout in een

Ondertussen is het systeem dat het Amerikaanse telefoonnet gebruikt, allang aangepast door aparte circuits te gebruiken voor het versturen van signalen en gesprekken. De Captain Crunch-fluitjes zijn tegenwoordig niet meer dan collectors items. Maar dat hackers hun interesse in telefoonnetwerken niet hebben verloren, bleek in februari. Hackers hadden ingebroken in het computersysteem van telefoongigant T-mobile. Paris Hilton van het Hilton-hotel had hier foto's, berichten en contactinformatie van veel beroemde personen uit haar vriendenkring opgeslagen die vervolgens verschenen op internet. De hackers maakten hierbij gebruik van een beveiligingsfout op de website.

En John Draper? Die heeft inmiddels een eigen computerbeveiligingsbedrijf. Met zijn Captain Crunch-ontdekking verwierf hij een plaats in de Hackers Hall of Fame. Een bekend tijdschrift voor hackers (*2600: The Hacker Quarterly*) is naar de frequentie van het fluitje vernoemd.



Een originele blue box in het Computer History Museum te Californië.

adres kan naar een website leiden waar de computer automatisch gevaarlijke programmatuur downloadt, zoals de onlangs ontdekte www.google.com. De letter 'k' zit op het toetsenbord direct naast de 'l', waardoor deze tikfout veel voor kan komen bij een wereldwijd bekende website als Google. Uiteraard is het niet aan te bevelen Google uit nieuwsgierigheid te bezoeken. Gelukkig blijven dit soort websites vaak kort in de lucht om ontmaskering te voorkomen.

Tegenwoordig zijn er ook steeds meer organisaties die proberen computercriminaliteit tegen te gaan zoals de *anti-phishing workgroup*, *hackerwatch*, *the honeynet project* en *hitmanpro*.

BESTRIJDING

Het aantal arrestaties in Nederland met betrekking tot computercriminaliteit kan in de toekomst wel eens stijgen als het wetsvoorstel Computercriminaliteit II wordt aangenomen. Dit is een voortvloeisel van het internationale Cybercrime-verdrag dat in 2001 is gesloten. Onderdeel van het voorstel is de plicht voor providers al het internet- en e-mailverkeer te bewaren.

Bits Of Freedom (BOF), een Nederlandse organisatie die opkomt voor digitale burgerrechten, heeft echter ernstige kritiek op het nieuwe wetsvoorstel. 'Tot nu toe was het binnendringen in een computer alleen strafbaar als de beveiliging werd gekraakt of omzeild. Maar iemands pc bezoeken mag straks ook niet meer, terwijl het met de huidige praktijk op internet heel gewoon is om andermans systeem binnen te

HACKERS WOORDENLIJST

404 Iemand die met betrekking tot computers dom of onwetend is. De term refereert aan de melding '404, URL Not Found', die op het scherm verschijnt wanneer een opgegeven website onvindbaar is. Ook wel aangeduid met *Noob*.

Adware Programma's die het mogelijk maken om reclameboodschappen te laten verschijnen in vensters op de computer. Deze scripts verzamelen soms ook informatie over iemands computergedrag. Vaak stemt een gebruiker hier (zonder het te weten) mee in door een *License Agreement* te accepteren.

Blackhat Een kwaadwillende hacker.

Blended threat Een script dat meerdere vormen van *malicious code* combineert.

Bot/zombie Een systeem waarover een hacker van buitenaf controle heeft of een programma waarmee hij dit voor elkaar kan krijgen.

Buffer overflow Een situatie waarbij een programma, meestal door een programmeerfout, data wegschrijft die de grenzen van de hiervoor gereserveerde ruimte overschrijft. Het kan zichzelf dan deels overschrijven. Hackers kunnen hiervan gebruik maken om software te veranderen.

Cracker Zie *blackhat*.

Cyberspace Een virtuele realiteit die bestaat tussen computers en computernetwerken over de hele wereld. Tegenwoordig wordt met deze term vooral internet bedoeld.

Defacement Het tegen de wil van de eigenaar veranderen van een website. Meestal al met een politiek doel of voor naamsbekendheid.

Distributed Denial Of Service (DDOS) Het platleggen van een website door de server te overbelasten. Dit kan door met veel verschillende systemen (meestal *bots*) tegelijk informatie op te vragen.

Exploit Script of mogelijkheid om een programmeerfout te misbruiken.

Firewall Dit is een belangrijk onderdeel van de totale beveiliging op de computer.

Hiermee wordt geregeld welk dataverkeer naar binnen en naar buiten mag.

Hacker Iemand die zo goed met een (computer)systeem om kan gaan dat hij de grenzen ervan weet te omzeilen of verleggen. Tegenwoordig vooral in negatieve zin gebruikt. Een hacker is dan een computercrimineel.

Honeybot Een computersysteem dat er van buiten aantrekkelijk uitziet voor een hacker, maar waarbij of waarmee hij weinig kwaad kan aanrichten. Een *honeypot* is te gebruiken om een hacker af te leiden van een gevoeliger systeem en om de acties van een hacker te registreren.

IP-adres Een IP-adres is een uniek nummer van een computer die verbinding heeft met internet. De computers weten hierdoor waar ze de uit te wisselen informatie naartoe moeten sturen.

Keyboard logger Een programma dat, zonder dat de gebruiker het weet, alle aanlagen op het toetsenbord vastlegt en doorsluist naar derden.

Malicious code Hieronder valt elke vorm van ongewenste programmatuur.

Newbee Iemand die wil leren hacken, maar nog onervaren is.

Phishing Vorm van zwendel waarbij een crimineel gebruikmaakt van hackervaardigheden en social engineering.

Poort Softwarematige aansluitingen waarmee data tussen twee computers kunnen worden doorgesluist.

Poortscan Het onderzoeken of een poort van de computer openstaat en welke diensten er via deze poort worden aangeboden.

Proxy server Een tussenstation tussen de browser op de computer en de webserver waarmee hij contact maakt. Dit gereedschap is bedoeld om sneller over internet te surfen. Met een speciale proxy kan de hacker echter al het passerende

verkeer onderscheppen, inspecteren en aanpassen.

Script kiddie Iemand die probeert te hacken, maar eigenlijk geen verstand van zaken heeft. Meestal maken *script kiddies* alleen gebruik van programma's die ze downloaden, omdat ze zelf niet kunnen programmeren.

Social engineering Posing vertrouwelijke informatie te krijgen door computergebruikers te manipuleren. Dit gebeurt meestal via internet of per telefoon.

Spoofing Het vervalsen van e-mail en websites. Meestal met de bedoeling het slachtoffer geheime informatie te ontfutselen.

Spyware Programma's die stiekem informatie verzamelen en doorsluizen over iemands computeractiviteiten. Denk hierbij aan wachtwoorden, inlognamen, rekeningnummers en andere persoonlijke informatie.

Tiger team Een team hackers dat inbreekt op een computersysteem om eventuele zwakheden bloot te leggen.

Trojan horse Software, zoals een digitale wenskaart of screensaver, waar *malicious code* in zit. Bij het downloaden van de software komt er ook kwaadaardige programmatuur binnen.

Virus Een kwaadaardig programma dat na activering (door aanklikken) zichzelf kan vermenigvuldigen en andere programma's kan aantasten en de werking ervan kan verstoren.

Vulnerability Fout in de programmatuur die misbruikt kan worden

Whitehat Een hacker die geen kwaad in de zin heeft.

Whois Een database met IP-adressen en domeinnamen.

Worm Virus dat zich kan kopiëren en verplaatsen (bijvoorbeeld via e-mail) over het netwerk zonder dat de gebruiker dat activeert. De worm kan schade aanrichten of de beveiliging aantasten.

dringen.' Hierbij doelt BOF onder andere op uitwisselingssoftware als Kazaa. 'Uiteraard vindt er ook misbruik plaats, maar hierbij gaat het vaak om slecht beveiligde systemen. Wie niet wil dat er wordt ingebroken, moet gewoon de deur dicht doen met behulp van goede beveiliging.'

BOF meent tevens dat met de bewaarplicht van alle verkeersgegevens, die niet alleen bij het opsporen van cybercriminelen handig kan zijn voor de politie, de privacy van de gebruikers in het geding komt. 'Er is dan geen sprake meer van gerichte opsporing, maar van algemeen toezicht op alle burgers. Door invoering van de bewaarplicht zullen burgers zich bij elk telefoontje, bij elke muisklik en bij het intypen van elk zoekwoord in Google moeten afvragen of deze informatie ooit tegen ze kan worden gebruikt. Daarnaast is de enorme hoeveelheid gevoelige en persoonlijke gegevens van burgers, die bij de internetaanbieders ontstaat, kwetsbaar voor interne en externe fraude.'

TRANSACTIONEN

Natuurlijk heeft de politie een belangrijke taak bij het bestrijden van deze nieuwe criminaliteit. 'Maar we hebben niet de tijd en de mensen om iedereen die op internet de wet overtreedt te achterhalen en te arresteren', zegt Rob van Dalen, teamleider bij de digitale recherche van het Korps Landelijke Politie Diensten. Volgens Van Dalen kan iemand die heel gedisciplineerd is lang

doorgaan met zijn criminele praktijken zonder gepakt te worden. 'Als een hacker bij grote hoeveelheden transacties telkens een paar cent achterover drukt, kan dat een prima inkomen opleveren. En enkele centen minder op een rekening mist eigenlijk niemand aan het eind van de maand. Pas als hackers een grote slag slaan, vallen ze op en lopen ze de kans op arrestatie. De beste hackers zijn dus onzichtbaar.'

In Nederland is dit jaar voor het eerst een computerkraker veroordeeld tot een onvoorwaardelijke gevangenisstraf van 38 dagen en 240 uur werkstraf. Hij was de hoofdverdachte van een groep krakers die in oktober 2004 de websites regering.nl en overheid.nl met DDOS-aanvallen een week lang platlegden. In Amerika treedt de overheid al jaren keihard op tegen hackers, zoals tegen de inmiddels beroemde hacker Kevin Mitnick.

Volgens Van Dalen zijn de meeste computercriminelen echter geen tophackers. 'Ik schat dat ongeveer 70 % van de DDOS-aanvallen wordt gedaan door *script kiddies*, handige gastjes die met behulp van op internet beschikbaar gereedschap een zombienet opzetten. Slechts 30 % weet echt waarmee hij bezig is.' Volgens Van Dalen wordt na aangifte maar liefst 90 % van de gevallen opgelost. Uiteraard raadt hij iedereen dan ook aan bij chantage met DDOS aangifte te doen. 'Zelf zien wij op het moment vooral *phishing* als een groeiend probleem. Een ander hot item blijft cyberterrorisme.' ●

INTERNETBRONNEN

www.hackaday.com

www.infowar.com

www.portswigger.net

www.securiteam.com/exploits

www.madirish.net

www.insecure.org

Forums, gereedschappen, exploits, tutorials en overige informatie voor en over hackers in de breedste zin.

www.ripe.net

Whois-database met IP-adressen voor Nederland.

www.wardrivemap.nl

Hier is te zien waar je gratis gebruik kan maken van onbeveiligde draadloze internetaansluitingen in Nederland.

www.itsx.com

www.madison-gurkha.com

www.symantec.nl

Beveiligingsbedrijven.

www.hackerwatch.org

www.antonline.com

www.antiphishing.org

www.security.nl

www.honeynet.org

Organisaties die cyber crime bestrijden.

www.bof.nl

Bits Of Freedom komt op voor digitale burgerrechten

www.whatthehack.org

Hackerfestival in Nederland van 28 t/m 31 juli 2005.

www.linux.org

Hier is het besturingsprogramma Linux gratis te downloaden.

www.bugmenot.com

Wachtwoord nodig voor een site? Wellicht vindt u die hier.

GEbruik OP EIGEN RISICO!

www.wikipedia.com

Deze online encyclopedie is geschreven voor en door de gebruikers.

www.hitmanpro.nl

Gratis te downloaden anti-spyware.

<http://tlc.discovery.com/convergence/hackers/hackers.html>

Hacker's hall of fame

www.hackerwatch.org/probe/

Mogelijkheid om een online poortscan van de eigen pc maken.

<http://www.watismijnip.nl>

Wat weet een webserver die een gebruiker bezoekt van zijn systeem?

e-woordenboek.solcon.nl

Woordenboek voor computer en internetgebruikers in de breedste zin.

Het Dossier
TOETSENBOORDEN
CRIMINALITEIT
Pas op voor
digitale dieven!