Hoofdstuk 2

Geschiedenis van hacking en digitale criminaliteit

Een hacker is niet per se een crimineel en iemand die zich schuldig maakt aan een digitale misdaad is niet per se een hacker, maar de geschiedenis van beide is flink met elkaar vermengd. Dat komt niet in de laatste plaats doordat ingenieuze hackerdaden die niet bedoeld zijn voor financieel gewin, soms toch illegaal waren of dat door wetswijzigingen zijn geworden. Daar tegenover staat dat sommige hackerpraktijken zo succesvol zijn gebleken, dat ze zelfs door opsporingsinstanties zijn overgenomen.

U leert in dit hoofdstuk:

Wat computercriminaliteit is

Waar de eerste computermisdaad (vermoedelijk) plaatsvond

Hoe computercriminaliteit in de twintigste eeuw snel aan belang won

Welke rol Nederland hierin speelde

"In 1971 when I joined the staff of the MIT Artificial Intelligence Lab, all of us who helped develop the operating system software, we called ourselves hackers."

Richard Stallman

"Being a social outcast helps you stay concentrated on the really important things, like thinking and hacking."

Eric Raymond

Definitie van computercriminaliteit

Voordat de geschiedenis van computercriminaliteit aan bod kan komen, is het noodzakelijk vast te stellen wat we precies bedoelen met deze term. Hoewel er meer en ingewikkelder definities circuleren, hanteert dit boek een zo eenvoudig mogelijke: computercriminaliteit omvat alle misdrijven die zijn verwezenlijkt met behulp van specialistische computerkennis, -hardware of -software. De diefstal van een computer is dus geen computercriminaliteit. Een crimineel die zijn gecompliceerde plannen enkel met behulp van een computer en een spreadsheet kon uitwerken, pleegt ook geen computercriminaliteit. Voor het bedienen van een spreadsheet is immers geen specialistische kennis vereist. Maar een scriptkiddie is wel degelijk een computercrimineel. Als hij een virus maakt met behulp van een programma dat hem daarbij helpt, heeft de scriptkiddie zelf niet al te veel kennis nodig. Het virusprogramma echter is een typisch voorbeeld van specialistische software.

De eerste computermisdaad

Daarover kunnen we kort zijn: hier is weinig over bekend. Wel is duidelijk dat een verre voorloper van de computer al zo'n tweeduizend jaar geleden mogelijkheden gaf om te frauderen. Het gaat dan om de abacus, oftewel het telraam. Het leidt geen twijfel dat er slimmeriken zijn geweest die hun vaardigheid met de abacus gebruikten om anderen te belazeren. Het apparaat was in gebruik bij de Chinezen, maar heeft ook dienst gedaan bij onder meer de Babyloniërs, de Japanners, de Russen en in het Romeinse rijk.

Afbeelding 2.1 *Een authentiek Romeins telraam (zonder Romein).*

Computercriminaliteit die alweer wat meer lijkt op zoals we die nu kennen, begon in de vroege negentiende eeuw. De Fransman Joseph Marie Jacquard bedacht weefgetouwen die werden aangestuurd met behulp van een primitief ponskaartensysteem. Ponskaarten zijn de voorlopers van moderne computerprogramma's. Zijdewevers waren niet zo blij met deze aantasting van hun werkgelegenheid en saboteerden daarom nogal eens Jacquards vindingen. Dit vroege verzet tegen automatisering kan worden gezien als een voorloper van de acties van black-hathackers van tegenwoordig.

Luddieten

Ook in het Groot-Brittannië van de vroege negentiende eeuw werden regelmatig machines gesaboteerd. De daders waren arbeiders die vreesden voor het verlies van hun baan. Deze vernielzuchtige types heetten Luddieten, een naam die ze te danken hadden aan hun vermeende leider, ene Ned Ludd. Tegenwoordig staat de term 'Luddiet' gelijk aan iemand die uit sociale of culturele overwegingen niets moet hebben van technologische vooruitgang. In tegenstelling tot vroeger staat hier echter niet meer de doodstraf op. De Britten executeerden destijds nogal wat werknemers wegens 'machine breaking'.

Computercriminaliteit en hacking in de twintigste en eenentwintigse eeuw

Vroege computercriminaliteit

Hoewel de Brit Charles Babbage al in de negentiende eeuw een voorloper van de computer had ontworpen onder de naam 'Analytical Engine', zou het tot de jaren veertig van de twintigste eeuw duren voordat computers enigszins begonnen te lijken op de apparaten die we tegenwoordig onder die naam kennen. Een van de eerste volledig elektronische computers was de ENIAC, wat staat voor Electronic Numerical Integrator And Computer. ENIAC werd in 1946 in gebruik genomen. Het ding woog 30 ton en vulde een grote ruimte. Tegenwoordig kan een minuscule chip precies hetzelfde.

Deze eerste computers werden gebruikt voor uiterst serieuze en hoogst specialistische zaken. In het geval van ENIAC was dat het berekenen van ballistische banen voor projectielen, ten bate van het Amerikaanse leger. Aan het afschieten van projectielen viel voor een crimineel weinig eer te behalen. Bovendien zou het misbruik van een computer met de complexiteit van ENIAC zo veel kennis van een crimineel vergen, dat deze vermoedelijk al op een andere manier rijk was geworden. Hoewel ENIAC naar moderne standaarden bijzonder dom is, was er een klein leger aan programmeurs voor nodig om het ding te voeden met instructies. Het spreekwoordelijke stelen van het goud uit Fort Knox zou vermoedelijk aantrekkelijker zijn geweest dan het verzinnen van een manier om met ENIAC geld te verdienen.

Pas ongeveer twintig jaar na ENIAC waren computers alomtegenwoordig en gebruiksvriendelijk genoeg om misbruik van te kunnen maken. In hoofdstuk 1 is al aan de orde geweest hoe hackers van het Massachusetts Institute of Technology (MIT) in de jaren zestig een universiteitscomputer aan het werk

Afbeelding 2.2 *Size does matter. Want waarom trok ENIAC wél de aandacht van deze twee legerbabes en lukt dat met een laptop nooit?*

zetten voor allerlei taken waar het apparaat nooit voor was bedoeld. De MIT-hackers waren relatief onschuldig bezig, maar dat gold niet voor iedereen die in die tijd de mogelijkheden van de computer onderkende. In 1966 vond de eerste computermisdaad plaats die tot een vervolging leidde. Een programmeur die werkte voor een bank in de Amerikaanse stad Minneapolis voegde aan de banksoftware wat extra computercode toe. Dankzij dit staaltje huisvlijt kon de programmeur niet meer rood komen te staan.

Computercriminaliteit richtte zich in de jaren zestig en zeventig vrijwel exclusief op de grote computersystemen van bedrijven en instellingen. Hoewel de eerste massageproduceerde computer voor thuisgebruik in 1975 op de markt kwam, de MITS Altair, zou een doorbraak van de personal computer tot in de jaren tachtig op zich laten wachten. Grote computersystemen waren dus de enige reële doelen voor kwaadwillenden. Het duurde niet lang of juist het massale karakter van deze systemen bleek een kwetsbaarheid. De salami-aanval (salami attack) was geboren.

De salami-aanval behelst geen aanval met de producten van de eerbiedwaardige worstenfabrikant Stegeman, maar een slimme manier om geld te stelen zonder dat dit (althans in eerste instantie) wordt opgemerkt. Bij de salami-aanval steelt een dief niet één keer een groot bedrag van één persoon of instelling, maar vele duizenden of zelfs miljoenen malen een klein bedrag van verschillende personen. Een salami-aanval kan bijvoorbeeld bestaan uit een computerprogramma dat steeds een paar centen van een bankoverschrijving verwijdert of zelfs fracties van centen, en die stort op de rekening van de crimineel. Het gezegde 'Wie het kleine niet eert, is het grote niet weerd' krijgt zo in het computertijdperk een geheel nieuwe betekenis.

Al in 1975 zou de salami-aanval in het wild zijn gesignaleerd en toen 380.000 dollar hebben opgeleverd. Maar ook tegenwoordig zijn er genoeg criminelen die heil zien in deze methode. De Amerikaan Willis Robinson

werd in 1997 tot tien jaar cel veroordeeld omdat hij de kassa van een vestiging van de fastfoodketen Taco Bell had geherprogrammeerd. Voor iedere snack van 2,99 dollar ontving Taco Bell slechts één cent. De overige 2,98 dollar verdween richting Robinson. Erg rijk is hij er overigens niet mee geworden. De winst bedroeg slechts 3600 dollar.

Dan waren vier leidinggevenden van een autoverhuurfirma uit Florida succesvoller. Zij slaagden erin om tussen 1988 en 1991 zo'n 47.000 klanten op te lichten. Iedere klant die zijn huurauto terugbracht zonder deze vol te hebben getankt, kreeg een rekening voor five *gallons* (ongeveer 19 liter) extra benzine dan gerechtvaardigd was. De buit bedroeg tussen de 2 en 15 dollar per klant. In 1993 werden ze voor de rechter gesleept.

Het gevaarlijke aan salami-aanvallen is dat ze uiterst moeilijk te detecteren zijn. In de voorbeelden heeft de gulzigheid van de daders zeker meegespeeld bij hun ontmaskering. Het is daarom bepaald niet uit te sluiten dat slimmere criminelen met meer geduld er nog steeds in slagen hun pensioengat aardig aan te vullen met deze computermisdaad.

White-hat- en grey-hathackers in opkomst

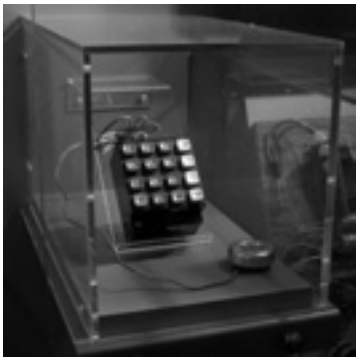
Het Amerikaanse telefoonnet lag eind jaren zestig en begin jaren zeventig onder vuur van *phreakers,* hackers die zich specialiseren in telefonie. Een van de beroemdste phreakers is Vietnam-veteraan John Draper. Hij krijgt het voor elkaar om met een fluitje uit een doos Cap'n Crunch, een soort graanontbijt, de telefooncentrale voor de gek te houden. Draper kan gratis het hele land doorbellen en krijgt al snel de bijnaam Cap'n Crunch, naar het ontbijt dat hem indirect zijn ontdekking bezorgde. Het aangepaste fluitje maakt tonen van 2600 hertz (trillingen per seconde), en het beroemde hackerblad '2600: The Hacker Quarterly' (**www.2600.com**) werd er dan ook naar vernoemd. Ook de persoonlijke site van Draper draagt nog altijd verwijzingen naar zijn fluitende verleden: die heet namelijk **www.webcrunchers.com**.

Joybubbles

Joe Engressia, ook bekend als Joybubbles, is een van de eerste phreakers. Engressia is uniek. In tegenstelling tot 'Cap'n Crunch' heeft hij geen fluitje nodig. De blinde Joybubbles kan de benodigde toon van 2600 hertz met zijn eigen mond produceren.

Het fluitje raakte al snel in onbruik. Draper ontwikkelde samen met Steve Wozniak een zogeheten *blue box,* een elektronisch kastje dat dezelfde geluiden kon produceren. Later zou Wozniak met Steve Jobs het computerbedrijf Apple oprichten. Het 'Think Different' zat er blijkbaar al vroeg in bij de

heren, want geïnspireerd door Jobs verkocht Wozniak *blue boxes* aan wie ze maar wilde hebben, ongetwijfeld tot grote irritatie van telefoniebedrijf AT&T. De verbondenheid van Apple met de geschiedenis van de *phreakers,* zoals hackers die zich op telefoons richten ook wel heten, houdt daar niet op. Draper schreef later ook nog EasyWriter, de eerste tekstverwerker voor Apple. Zonder smetten is het verleden van Draper overigens niet. Zowel in 1972 als in 1976 werd hij gearresteerd wegens zijn 'telefoonhobby'.



Afbeelding 2.3 *De voormalige blue box van Steve Wozniak.*

Phreakers

Hackers die hun technologische vernuft op de telefoon loslaten, heten ook wel phreakers.

De jaren zeventig zijn ook de tijd waarin Bulletin Board Systems (BBS'en) hun opwachting maken. Hoewel internet al in 1969 werd geboren, duurde het tot eind jaren tachtig voordat de eerste nerds er mee konden spelen, en in veel gevallen zelfs tot in de jaren negentig. Lange tijd bleef de toegang tot internet een voorrecht van universiteiten, grote bedrijven en het Amerikaanse leger. BBS'en boden, op een veel beperktere schaal dan internet, de computerfreaks van de jaren zeventig en tachtig toch een communicatiemogelijkheid.

Computerclub

Steve Wozniak, John Draper en Steve Jobs ontmoetten elkaar in de fameuze Homebrew Computer Club. In Nederland is nog altijd een organisatie actief met bijna dezelfde naam: de HCC, wat een afkorting is van Hobby Computer Club.

In 1978 gaat het eerste BBS de lucht in, een bedenksel van Ward Christensen en Randy Seuss. Dit 'Computerized Bulletin Board System' wordt later herdoopt in 'Bulletin Board System': een soortnaam is geboren. Zoals de naam al zegt, is een BBS niets meer dan een digitaal prikbord, te bereiken met een telefoonaansluiting, een computer en een ouderwetse modem. De hackers van weleer laten er berichten, maar ook software voor elkaar achter. Net zoals tegenwoordig websites als **www.fok.nl** en **www.geenstijl.nl** een vaste schare liefhebbers aan zich hebben weten te binden, hebben veel BBS'en hun eigen fans. Verschillende hackergroepjes vinden elkaar op BBS'en met welluidende, soms nogal ronkende namen als 'Demon Roach Underground' en 'Sherwood Forest'. (Nog veel meer voorbeelden staan op **http://bbslist.textfiles.com**.)

Het Hackermanifest en de Grote Hackeroorlog

In 1986 publiceert hacker 'The Mentor', ook bekend als Loyd Blankenship, het 'Hacker Manifesto'. Blankenship is dan eenentwintig. Hoewel hier en daar wat bombastisch, geeft het Hacker Manifesto nog altijd een goed inzicht in wat white-hat- en grey-hathackers drijft. Het uit 1986 daterende stuk is onder zijn oorspronkelijke naam, 'The Conscience of a Hacker', na te lezen op **http://cybercrimes.net/Property/Hacking/Hacker%20Manifesto/HackerManifesto.html**. Een citaat:

'We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.'

Dat hackers zelf echter ook niet heilig zijn, blijkt vier jaar later, bij het uitbreken van de Grote Hackeroorlog. Twee rivaliserende groepen, het Legion of Doom (LOD) en Masters of Deception (MOD), houden tussen 1990 en 1992 een flink uit de hand gelopen wedstrijdje 'wie kan het beste treiteren'. De oorlog begon met het overstappen van de talentvolle hacker Mark Abene van LOD naar MOD. Inbraken (en pogingen daartoe) in elkaars computers, gerommel met telefoonlijnen en nog veel meer digitale pesterijen waren het resultaat. Uiteindelijk grijpen de Amerikaanse autoriteiten in. In 1992 krijgen verschillende hackers, waaronder Abene, gevangenisstraffen opgelegd.

Dat de hackergemeenschap alleen nieuwsgierige jongeren van goede wil aantrekt, valt inmiddels niet meer vol te houden, ook al niet vanwege een groot spionageschandaal dat kort daarvoor aan het licht komt.

Hackers als spionnen

Dr. Clifford Stoll, een astronoom, krijgt in 1986 een baantje als systeembeheerder in het Lawrence Berkeley Laboratory. Al snel ontdekt hij een op het eerste gezicht onbetekenend probleem. Op de gebruiksrekening voor de universiteitscomputer staat een bedrag van 75 dollarcent dat hij niet kan thuisbrengen. Stoll onderzoekt de rekening en komt erachter dat een gebruiker met de naam 'Hunter' de kosten heeft veroorzaakt. Dat is nog vreemder, want in het laboratorium werkt helemaal niemand met die gebruikersnaam.

In samenwerking met de Amerikaanse federale politie FBI gaat Stoll op speurtocht. 'Hunter' wordt tien maanden gevolgd en blijkt in die tijd de laboratoriumcomputer te gebruiken als springplank voor bezoekjes aan ruim 450 computers, waarvan hij er ruim dertig weet binnen te dringen. Onder de doelen zijn onder meer computers van het Amerikaanse ministerie van Defensie en ruimtevaartorganisatie NASA. In 1987 wordt 'Hunter' getraceerd. Stoll legt hiervoor een val die later bekend zal worden onder de naam 'honeypot', een digitale variant van een wespenval (zie voor meer over honeypots hoofdstuk 6). Deze specifieke 'honeypot' bevat zogenaamd informatie over het Strategic Defense Initiative (SDI). SDI is beter bekend als 'Star Wars' of het raketschild van Ronald Reagan, tot 1989 president van de Verenigde Staten.

'Hunter' kan geen weerstand bieden en duikt verlekkerd op de buit. De dader blijkt de Duitse student Markus Hess uit Hannover te zijn. Hess, ook bekend onder het alias 'Mathias Speer' of Stolls bijnaam 'the Wily Hacker', hackt omdat hij Amerikaanse militaire informatie door wil verkopen aan de KGB, de geheime dienst van de Sovjet-Unie. Op 29 juni 1987 doet de Duitse politie een inval in de woning van Hess. Maar omdat Hess op dat moment niet thuis aan het hacken is, kan hij niet op heterdaad worden betrapt en er volgt vrijspraak.

In 1989 krijgt de Duitse justitie een herkansing. Dan worden op 2 maart behalve Hess nog vier andere hackers in staat van beschuldiging gesteld: Karl Koch ('Hagbard Celine'), Dirk-Otto Brzezinski ('DOB'), Peter Carl en Hans Huebner ('Pengo'). Huebner weet het op een akkoordje te gooien met het Openbaar Ministerie. Koch, een stevige druggebruiker, overlijdt op 23 mei 1989, vermoedelijk door zelfverbranding. Op internet waart nog altijd een samenzweringstheorie rond dat Koch vermoord zou zijn (zie **www.hagbard-celine.de** en **www.schaechl.de/kk**).

Boek

Stoll schreef een boek over zijn speurtocht, *The Cuckoo's Egg* (ISBN 0743411463).


Karl Koch
(hogbard)

Afbeelding 2.4 *'KGB-hacker' Karl Koch: vermoord of zelfmoord?*


Selbstmord oder Hinrichtung?
CDU-Fahrer aus Hannover war KGB-Spion – im Wald verbrannt
Viele Passwörter sind zu einfach
Gelangweilter US-Student legte 6000 Forschungs-Rechner lahm
in Datenkrimi – die uchenach dem SDI-Hacker
So gingen die Hacker aus Hannover dem
Astronomen ins Datennetz
Die KGB-Hacker: Geständnis am Bahnhof
Haftbefehl gegen Computer-Spion aus Hannover

Afbeelding 2.5 *Nabestaanden gaven Duitse media...*


Erst War Games in den USA, dann Spionage für die UdSSR
„Er konnte an jedem Ort der Welt sitzen"
Computer-Spionage: So wurde der größte Skandal aller Zeiten aufgedeckt
Sergej vom KGB – der Boß der Hacker-Bande
Kurz vorm Verschwinden redete Spion wie von Außerirdischen
KGB-Hacker: Er war Bote für die CDU
Toter KGB-Hacker
SPD schaltet Landtag ein
Hannover
KGB-Hacker auf Feldweg verbrannt
Der mysteriöse Tod des KGB-Hackers Koch wirft immer neue Fragen auf
„Alle großen Anarchisten starben am 23."
Zu Gast in Hannover: Der Hacker-Jäger

Afbeelding 2.6 *...de schuld van dood Koch.*

In 1990 krijgen Brzezinski, Carl en Hess gevangenisstraffen en boetes opgelegd. Hoewel geen van de 'KGB-hackers' ook daadwerkelijk de cel in hoeft, betekenen de arrestaties wel degelijk een klap voor het imago van de hackergemeenschap. De 'KGB-hackers' hebben namelijk banden met de Chaos Computer Club (**www.ccc.de**), een organisatie met licht-anarchistische inslag die zich tegenwoordig vooral profileert als een typische white-hatclub vol nieuwsgierige hobbyisten. Een staartje volgt in 1998. Dan komt de film *23* uit, een semi-documentaire over het leven van Koch en diens geloof in samenzweringstheorieën (**www.dreiundzwanzig.de**).

Ondertussen is men in de Verenigde Staten black-hathackers goed zat. Dat komt met name omdat in 1991 twee grote hackergroeperingen besluiten om digitaal indiaantje te gaan spelen.

Kevin en Kevin, twee beroemde black hats

Kevin Mitnick en Kevin Poulsen: over weinig hackers zijn de meningen zo verdeeld als over deze twee computerexperts. Met name Kevin Mitnick heeft, ook in bepaalde white-hatkringen, een cultstatus. Hackerblad 2600 stampte zelfs een heuse protestactie uit de grond onder de naam 'Free Kevin'. De bijbehorende website is nog altijd online op **www.freekevin.com**. Mitnick is echter geen lieverdje. Hij brak in bij de computers van minstens 35 grote bedrijven en organisaties. Nieuwszender CBS schat de schade die Mitnick heeft veroorzaakt op 300 miljoen dollar, al heeft Mitnick dat zelf altijd ontkend. Vanaf 1981 werd Mitnick diverse malen gearresteerd, de laatste keer op 15 februari 1995. Toen moest hij tot 1999 wachten op zijn proces, een feit dat zijn medestanders graag aangrijpen om Mitnick als slachtoffer af te schilderen. Dat is niet helemaal terecht. Mitnicks advocaat heeft zelf meermalen om uitstel van het proces gevraagd. Op 21 januari 2000

Afbeelding 2.7 *Mitnick werd lang gezocht door de Amerikaanse autoriteiten.*

Afbeelding 2.8 *De website van het Mitnick-bevrijdingsfront. Onder aan de pagina staat een verwijzing naar LabMistress.com, de site van Kevins vriendin.*

kwam Mitnick vrij. Hij kreeg onder meer een verbod opgelegd om drie jaar lang een computers aan te raken, tenzij hij daarvoor speciaal toestemming aanvroeg bij zijn reclasseringsambtenaar. Inmiddels heeft Mitnick zijn eigen beveiligingsbedrijf (**www.mitnicksecurity.com**) en geeft hij lezingen over hoe bedrijven zich kunnen weren tegen mensen zoals hijzelf.

Sociaal hacken

Mitnick is een expert in het met een vlotte babbel manipuleren van anderen, het zogeheten *social engineeren*. Meer hierover leest u in hoofdstuk 6.

Twee kanten

Wilt u het verhaal van de kant van Mitnicks medestanders horen? Bezoek dan **www.freekevin.com** en **www.freedomdowntime.com**. Meer geïnteresseerd in een ouderwets boevenverhaal? Ga dan naar **www.takedown.com**, de site van computerexpert Tsutomu Shimomura en New York Times-verslaggever John Markoff. Shimomura speelde een belangrijke rol bij het opsporen van Mitnick in 1995.

Veel artikelen over het proces van Mitnick werden ironisch genoeg geschreven door Kevin Poulsen. Tegenwoordig presenteert Poulsen zich als journalist, maar hij heeft een verleden als black hat onder de bijnaam 'Dark Dante'. Die slechte reputatie is enigszins verdiend. Poulsen verwierf faam door een

telefoonspelletje van een radiostation uit Los Angeles te kraken zodat hij de honderdtweede en winnende beller werd. Het leverde Poulsen een Porsche 944 S2 op. Poulsen had ook minder grappige activiteiten. In 1991 gaat hij de gevangenis in vanwege diverse telefoonkraken. In 1996 wordt hij vrijgelaten en zegt hij tot inkeer te zijn gekomen. Hij kiest voor een carrière in de journalistiek. Zijn stukken zijn tegenwoordig met regelmaat te lezen op **www.securityfocus.com**.

Overal scriptkiddies

De opkomst van internet maakt het ook voor technisch minder goed onderlegde personen eenvoudig om digitale misdrijven te plegen. Voor het maken van virussen of het plegen van computerkraken komen kant-en-klare programma's in omloop. Een berucht voorbeeld is het programma Back Orifice, in 1998 uitgebracht door de beroemde hackergroep Cult of the Dead Cow (cDc). Met een minimum aan kennis en een goedgelovig slachtoffer is met Back Orifice (tegenwoordig BO2K geheten en te downloaden op **www.bo2k.com**) het computer van een slachtoffer volledig over te nemen. De naam van het programma is overigens een nogal ranzige woordspeling op het bij bedrijven populaire programma BackOffice Server van Microsoft. cDc zegt het programma vrij te geven om duidelijk te maken hoe kwetsbaar het Microsoft-besturingssysteem Windows is. Die denkwijze heet ook wel *'full disclosure'* en komt uitgebreid aan de orde in hoofdstuk 3.

Computercriminaliteit in Nederland

Het overgrote deel van de hackergeschiedenis speelt zich af in de Verenigde Staten. Maar Nederland heeft zijn eigen coryfeeën, schurken en helden.

Hacken in de lage landen

Nederlands eerste grote hack is er eentje om hard om te lachen. Onno Tijdgat en Tom de Regt weten in augustus 1985 de computer met telefoonnummers van de toenmalige PTT binnen te dringen. Deze zogeheten 008-database, naar het inlichtingennummer van die tijd, blijkt voorzien van een uiterst beroerde beveiliging. Het wachtwoord is namelijk 008.

Net als in de Verenigde Staten organiseren hackers zich aanvankelijk rond een BBS. Op NEABBS, Nederlands Eerste Algemene Bulletin Board System dat werd gerund door Max Keijzer, ontmoeten de vaderlandse computerfreaks elkaar. Rop Gonggrijp, hacker van het eerste uur, leert er Paul Dinnissen kennen. Ze gaan samenwerken en produceren het 'techno-anarchistische' tijdschrift Hack-Tic, waarvan het eerste nummer in 1989 verschijnt.

Afbeelding 2.9 *Chique automatiseerders konden niet op veel respect rekenen van Hack-Tic…*

Afbeelding 2.10 *…net zomin als de Postbank of de toenmalige PTT. Overigens schijnt de voormalige telefoonmonopolist aardig in paniek te zijn geraakt van de oproep aan de onderkant van deze afbeelding.*

Kosten: vier gulden, oftewel ongeveer 1,82 euro. De inhoud van Hack-Tic kan het best worden omschreven als 'oud-Hollands autoriteiten jennen'. Hack-Tic haalde meermalen het nieuws, onder meer door het op de markt brengen van een apparaatje waarmee semafoonverkeer kon worden afgeluisterd. Een semafoon, voor lezers jonger dan twintig, is een apparaatje waarmee SMS-achtige berichten kunnen worden ontvangen. Ook deed Hack-Tic

Afbeelding 2.11 *Hack-Tic bevond zich, zoals veel hackergroepen, aan de linkerkant van het politieke spectrum.*

zijn lezers een methode aan de hand om gratis te bellen. Hack-Tic had het, niet verwonderlijk, dan ook regelmatig aan de stok met de toenmalige PTT (tegenwoordig KPN Telecom). Wat niet betekende dat de PTT Hack-Tic negeerde. 'Ik was elke keer de klos om de nieuwe Hack-Tic te kopen', zei een PTT-woordvoerster in 1998 tegen de auteur van dit boek (voor een artikel in het weekblad *Elsevier,* gepubliceerd op 13 juni 1998). Op het hoogtepunt had het blad 2500 abonnees. 'Belachelijk voor een underground tijdschrift', zei Gonggrijp in hetzelfde artikel.

Nieuwe technologische ontwikkelingen zouden Hack-Tic en de PTT in elkaars armen drijven. In 1992 besluit Hack-Tic om internet te gaan aanbieden onder de naam Hack-Tic Network. Op 1 mei 1993 publiceert *de Volkskrant* een artikel over Hack-Tic. Dat zorgt voor enkele honderden aanmeldingen, veel meer dan de Hack-Ticcers hadden verwacht. Opeens is Hack-Tic afhankelijk van de PTT, blijkt als Gonggrijp weer eens extra telefoonlijnen nodig heeft om aan de vraag te kunnen voldoen. 'De beambte riep toen uit: "Maar meneer Gonggrijp, dat is toch een woonhuis? Waarom woont u er dan niet gewoon?" Elke keer als we lijnen bijbestelden moest de straat namelijk weer worden opengebroken', herinnert ex-Hack-Tic-lid Paul Jongsma zich in het Elsevier-artikel.

Overigens betekende dat niet dat de Hack-Ticcers meteen brave zakenlui werden. Hacker RGB, een afkorting voor 'Rotten Goddamned Bastard', logeerde 'een tijdje bij de gemeentepolitie in Amsterdam', meldt Hack-Tic

nummer 18/19 in 1992. RGB, in het dagelijkse leven bekend als Ronald Oostveen, wordt in 1993 opnieuw opgepakt wegens het inbreken in computers. Hij krijgt een boete van 5000 gulden opgelegd, plus een voorwaardelijke celstraf van zes maanden.

Ook de verhouding met de PTT is niet meteen geweldig. Op 22 augustus 1994 worden alle telefoonlijnen van Hack-Tic afgesloten, met als gevolg dat klanten tijdelijk geen gebruik van internet kunnen maken. Hack-Tic vermoedt een verband met een artikel in het nieuwste nummer van het Hack-Tic-tijdschrift, waarin wordt uitgelegd hoe je gratis kunt bellen. Dezelfde dag wordt Hack-Tic overigens weer aangesloten. In hetzelfde jaar worden de internetactiviteiten van Hack-Tic ondergebracht in een stichting die de naam XS4ALL meekrijgt. Het duurt niet lang of XS4ALL wordt een B.V. In 1998 wordt XS4ALL voor een onbekend bedrag, vermoedelijk vele miljoenen, verkocht aan de voormalige aartsvijand: KPN Telecom. De hackers zijn volwassen geworden.

Een nieuwe generatie

Jongere hackers hebben dan inmiddels het stokje overgenomen. In 1997 is 'The Nijntje Gang' nogal actief. Achter The Nijntje Gang gaat de scholier Peter van Dijk schuil. Hij kraakt onder meer de website van computerbladenuitgever IDG en vervangt de pagina door een afbeelding van Dick Bruna's bekende konijntje. Veel meer aandacht trekken in 1997 en 1998 de diverse inbraken in het computersysteem van internetaanbieder World Online, die lang voor de beursgang onder computerfreaks al omstreden was. Wat volgde, was een eindeloos welles-nietes-spelletje tussen journalisten als Peter Olsthoorn, die de zwakke beveiliging van het bedrijf probeerden aan te tonen, en de roemruchte woordvoerder van het bedrijf, Rob van der Linden. Uiteindelijk schrijft World Online in een wanhopige poging haar reputatie nog enigszins te redden, een hackwedstrijd uit waarmee 15.000 gulden is te verdienen. 'King', de schuilnaam van Robert Krenn, stampt het hackercollectief 'Team Delta' uit de grond. Het duurt niet lang of Team Delta weet inderdaad de WOL-computers binnen te dringen – waarna WOL ontkent gehackt te zijn. Het bedrag van 15.000 gulden wordt uiteindelijk met frisse tegenzin toch uitgekeerd; Team Delta maakt 14.000 gulden over naar Unicef. Een overzicht van de soap is nog altijd na te lezen op **www.xs4all.nl/~loser/WOL.html**.

Digitaal vandalisme

Nederland ontkomt helaas niet aan de groei van het aantal scriptkiddies. Op 10 februari 2001 zorgt de dan twintigjarige Nederlander Jan de W. uit Sneek, beter bekend als 'OnTheFly', voor wereldwijde overlast. Met behulp van een

Afbeelding 2.12 *Al voor het beursdrama moest 'World Onveilig' nogal wat flauwe grappen dulden.*

programma waarmee virussen gebouwd kunnen worden, maakt hij het Anna Kournikova-virus. Zelf weet OnTheFly maar weinig van computers. 'Ik ken geen enkele programmeertaal', schrijft hij op zijn website. Het Anna Kournikova-virus verspreidt zich via e-mail en presenteert zich als een bestand met daarin een foto van de aantrekkelijke tennisster. Slachtoffers die op de vermeende foto klikken, infecteren echter hun pc met het virus. Kournikova kijkt vervolgens in het e-mailadresboek en stuurt zichzelf dan door naar een volgende groep potentiële pechvogels. De W. krijgt in september een taakstraf van 150 uur opgelegd. Het is niet de eerste en ook niet de laatste keer dat Nederlanders op dubieuze wijze voor computernieuws zorgen.

In 2004 vallen Eric de Vogt en zijn '0x1fe Crew' diverse websites aan, waaronder enkele van de Nederlandse overheid. Door deze zogeheten Distributed Denial of Service-aanvallen (DDoS, zie verder hoofdstuk 8) komen onder meer Regering.nl, Kabinet.nl en GeenStijl.nl plat te liggen. Uiteindelijk komt de politie in actie. In maart 2005 krijgt De Vogt 240 uur werkstraf opgelegd plus 38 dagen gevangenisstraf, die hij al tijdens zijn voorarrest heeft uitgezeten. Vier van zijn medeplegers worden ook veroordeeld. Dat er niet alleen goedwillende hackers zijn maar ook digitale vandalen, is definitief tot de Nederlandse rechtspraak doorgedrongen. (Meer over De Vogt c.s. leest u eveneens in hoofdstuk 8.)

Index