

# Geschiedenis van hacking en digitale criminaliteit

**E**en 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 eenentwintigste 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

## Hoofdstuk 2 – Geschiedenis van hacking en digitale criminaliteit

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 leidinggevendenden 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 mee-gespeeld 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](http://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](http://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.

---

## Hoofdstuk 2 – Geschiedenis van hacking en digitale criminaliteit

In 1978 gaat het eerste BBS de lucht in, een bedenkensel 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](http://www.fok.nl) en [www.geenstijl.nl](http://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://bbstlist.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 systeem-beheerder 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 bezoeken 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 wesperval (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](http://www.hagbard-celine.de) en [www.schaechl.de/kk](http://www.schaechl.de/kk)).



### Boek

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

## Hoofdstuk 2 – Geschiedenis van hacking en digitale criminaliteit



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



Afbeelding 2.5 Nabestaanden gaven Duitse media...



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](http://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](http://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](http://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.

## Hoofdstuk 2 – Geschiedenis van hacking en digitale criminaliteit



**Afbeelding 2.8** De website van het Mitnick-bevrijdingsfront. Onder aan de pagina staat een verwijzing naar [LabMistress.com](http://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 aanvraag bij zijn reclasseringsambtenaar. Inmiddels heeft Mitnick zijn eigen beveiligingsbedrijf ([www.mitnicksecurity.com](http://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 vlote 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](http://www.freekevin.com) en [www.freedomdowntime.com](http://www.freedomdowntime.com). Meer geïnteresseerd in een ouderwets boevenverhaal? Ga dan naar [www.takedown.com](http://www.takedown.com), de site van computereexpert 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](http://www.securityfocus.com).

### Overall 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 goedgegelovig slachtoffer is met Back Orifice (tegenwoordig BO2K geheten en te downloaden op [www.bo2k.com](http://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 inlichtingnummer 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.

**Hoofdstuk 2 – Geschiedenis van hacking en digitale criminaliteit**



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

**KOTSBANK**

nummer	afrekeningsbedrag	aan	nummer	bedrag
nummer	aanrekenen	aanrekenen van	nummer	aanrekenen
01.0	48,-00		01.0	48,-00
01.0			01.0	11,-00

**TRANSFERPROVISIE**

De beste manier om de Hack-Tic redactie te bereiken is via elektronisch mail (zie telefoon). Erven is een goede tweede. Als je schrift of belt moet je er rekening mee houden dat het soms erg lang kan duren, als er al iemand terug belt. Het is jammer, maar we hebben per persoon maar twee armen, dus het is niet anders.

**PTTers opgelet**

**Interessante informatie wil vrij zijn**

Halt je technische kennis die maar beter niet in handen van het publiek kan vallen? Werk je diep in de buik van het systeem en is het oplossen van informatie naar Hack-Tic je enig overgebleven uitgang van succes? Hack-Tic publiceert voor een techniek-enthousiast publiek dat de schouwtaal van het telefoonnet nog niet te waarden. Dus net op floppy en in een e-mail!

We zijn vooral op zoek naar interessante informatie die ons een stuk leven kan helpen binnen PTT-Telecom. Software voor computers, manuals voor LDPAN, WERKMET, SENS, BRIT, en de 06 en 09 centrales, we noemen maar wat. Helaas, gewone zaken als een intern telefoonboek worden hier hoog gewaardeerd.

Natuurlijk, als je bias er achter komt wordt je ontlagen, maar zeg nou zelf: maakt dat het leven niet een beetje spannender?

**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-woordvoester 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 Jongasma 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

## Hoofdstuk 2 – Geschiedenis van hacking en digitale criminaliteit

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 computerbladuitgever 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 wellen-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, stampet 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](http://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

- @Stake 114
- 0x1fe Crew 33, 153
- 2600: The Hacker Quarterly 22, 48
- 419-scam 136
- Abene, Mark 24
- Adams, Douglas 207
- Ad-Aware Personal 91
- Administrator 102
- Advanced Research Projects Agency 37
- Adware 77
- AID 191
- AIM 41, 231
- Analytical Engine 20
- Anna Kournikova-virus 33
- Anonimiteit controleren 170
- Anonimiteitsservice 165
- Anonymous P2P 43
- Anonymous remailers 39
- Anti-Phishing Working Group 140
- AntiVir Personal Edition Classic 72
- Antivirussoftware 62, 71
- AOL Instant Messenger 231
- ARPA 37
- Asymmetrische versleuteling 177
- Avalanche 174
- Avast! 4 Home Edition 72
- AVG Anti-Virus 72
- Azureus 42, 175
- Babbage, Charles 20
- Back Orifice 65
- Bartportal 228
- Bayesiaans filter 137
- BBS 23
- BDE 188
- BDR 187
- Beeldonderzoek 195
- Berg, Nienke van den 188
- Berners-Lee, Tim 37
- Besluit universele dienstverlening en eindgebruikersbelangen 94
- Bestandssysteem 246
- Beveiliging 117
  - Demilitarized Zone 117
  - firewall 117
  - honeynet 118
  - honeypot 118
  - Intrusion Detection System 117
  - penetratietest 118
  - tiger team 118
- Beveiligingscertificaat 141
- BGP 133
- Binary Revolution 48
- Biometrie 195
- Bittorrent 174
- Black-hathacker 12, 108
- Blacklist 137
- Blacklisted 411 49
- Blankenship, Loyd 24
- Blanckesteijn, Herbert 153
- Blaster 63
- Blue box 22
- Blue jacking 115
- Blue snarfing 116
- Bluetooth 114
  - kraken 114
- Bluetooth Device Security Database 125
- Bluetooth sniping 115
- Bluetooth wardriving 115
- Bluetooth-beveiliging 125
- Border Gateway Protocol 133
- Botnet 134
- Bouyeri, Mohammed 254

## Index

- Browserhijacker 84
- Brzezinski, Dirk-Otto 25
- Buffer overflow 103, 156
- Bulletin Board System 23
- Bureau Digitaal Rechercheren 187
- Bureau Digitale Expertise 188
- Buyukkokten, Orkut 232
- Campina 165
- CAN-SPAM-wet 138
- Cap'n Crunch 22
- Carl, Peter 25
- Chaos Communication Congress 52
- Chatten 178
- Christensen, Ward 24
- CIA-delicten 214
- Claria 91
- Clarke, Ian 175
- Code Red 156
- Code Red II 156
- Complement set filtering 137
- Computer Fraud and Abuse Act 203
- Computer Misuse Act 203
- Computercriminaliteit 21
  - aanval op AMX-IX 210
  - afluisteren 205
  - auteursrecht 213
  - computer als middel 212
  - Cybercrime-verdrag 214
  - defacen 211
  - definitie 19, 203
  - discriminatie 213
  - gegevens wissen en manipuleren 211
  - geschiedenis 19
  - illegale kopieën 212
  - in Nederland 29
  - inbreken 204
  - kinderporno 212
  - Kournikova-virus 211
  - sabotage 207
  - spam 209
  - Trojaans paard 211
  - vernieling 207
- Computercrimineel 5, 15
- Computerforensisch onderzoek 189
- Computerized Bulletin Board System 24
- Computerkraken 99
- Computervirus
  - Zie Virus
- Cookie 166
- Cracking 12
- Creditcardfraude 142
- Cross site scripting 144
- Cryptografie 39
- Cryptografieanalyse 192
- CSF 137
- Culpoos delict 209
- Cult of the Dead Cow 14, 49
- CWSredder 91
- Cybercrime-verdrag 191, 214
- Dark hacktivism 14
- DARPA 37
- Data-analyse 193
- Datacommunicatieanalyse 192
- Datenschleuder 49
- DDoS 33, 119, 152
  - botnet 154
  - Trojaanse paard 154
  - Zombie 154
- DDoS-kabouters 153
- DeCSS 46
- DECT-verkeer 206
- DEF CON 52
- Defacen 9, 15, 38, 108
- Demilitarized Zone 117
- Denial of Service 150
- Dialer 85
- DialerDetect 92
- Digitale rechercheur 187
- Digitale Technologie (NFI) 190
- Digitale Tipp-ex 255
- Dijk, Peter van 32
- Dinnissen, Paul 29
- Distributed Denial of Service 33, 119
- Distributed Denial of Service Attack 152
- DMZ 117
- DNS 142, 156
- DNS-cache poisoning 143
- DNS-rootservers 156
- DOB 25
- Dogpile 234
- Domain Name System 142, 156
- DomainKeys 137
- Donner, Piet Hein 188
- DoS 150
  - destabiliseren 151
  - mailbom 155

- overbelasting 150
- vernielen 152
- Draadloos hacken 113
  - WEPCrack 113
- Draadloze netwerken 110
- Draper, John 22
- Echo/Chargen 151
- EDonkey 174
- Electromagnetic Pulse 152
- Elektronische vingerafdruk 242
- Elk Cloner 66
- E-mail 38
- E-mailadres opsporen 222
- E-mailheaderspoofing 136
- EMP 152
- EMule 42
- Encase Forensic 242
- Encryptie 124, 175
  - Enigmail 177
  - GnuPG 177
  - GPGshell 177
  - Groove Virtual Office 180
  - Hushmail 178
  - OpenPGP 177
  - PGP 177
  - ROT13 176
  - SimpLite 178
  - SSL 176
  - StegoMagic 179
- Engressia, Joe 22
- ENIAC 20
- Enigmail 177
- Entropy 175
- Ethereal 102
- EXchangeable Image File format 256
- Exploit 44, 102, 151
  - Buffer overflow 103
  - social engineering 105
  - vinden 103
- ExploitTree 103
- FakeAP 124
- Fanning, Shawn 173
- FastTrack 174
- Federal Trade Commission 87
- File system 246
- File Transfer Protocol 43
- FIOD-ECD 190
- Firewall 117, 120
  - Kerio Personal Firewall 121
  - Sygate Personal Firewall 122
  - thuisgebruik 120
  - ZoneAlarm 121
- Forensische software 242
- Forrester Data 129
- Fox-IT 198
- F-Prot Antivirus for DOS 72
- Freenet 43, 175
- Frequency hopping 115
- FrSIRT 104
- Fserve 40
- FTC 94
- FTP 43
- Full disclosure
  - mailinglijst 46
- Galactic Hacker Party 55
- Gates, Bill 129
- Gator eWallet 83
- GeenStijl 82, 153
- Gegevensfiltering 193
- Geheimtaal 124, 175
- Gewiste bestanden terughalen 245
- GNUUnet 43, 175
- GnuPG 177
- Gnutella 174
- Gonggrijp, Rop 29
- Google-zoektips 234
- GOVCERT 199
- GPGshell 177
- GrayBird.E 64
- Grey-hathacker 13
- Greylist 137
- Groep Digitaal Rechercheren 189
- Groove Networks 44
- Groove Virtual Office 180
- Grote Hackeroorlog 24
- Groupware 44, 180
- Grubestic, Tony 158
- Guru 9
- H.O.P.E 53
- Hacken
  - basis 100
  - doel 108
  - draadloos 113
  - exploit 102

## Index

- mobiele telefoon 114
- Packet sniffer 101
- PDA 114
- poortscanner 100
- protocol analyzer 101
- root kit plaatsen 110
- root worden 102
- sporen wissen 109
- toegang krijgen 102
- vulnerability scanner 101
- WiFi-netwerk 110
- Hacker
  - black hat 12
  - ethische 10
  - grey hat 13
  - hactivist 13
  - in films 7
  - Jon Lech Johansen 13
  - 'Kaas' 11
  - oorsprong 5
  - soorten 9
  - white hat 9
- Hacker Manifesto 24
- Hackerfilosofie 44
- Hackers at Large 54
- Hacking 7
- Hacking at the End of the Universe 54
- Hacking in Progress 54
- Hackingonderzoek 192
- Hack-Tic 29, 50
- Hactivist 13, 108
- Hagbard Celine 25
- Hakin9 50
- Harmony Compiler 6
- Hash 243
- Heine, Heinrich 203
- HERF 152
- Hess, Markus 25
- High Energy Radio Frequency 152
- HijackThis 92
- Hitman Pro 2 91
- Hoax 70
- Hofstadgroep 15, 163, 229
- HoHoCon 55
- Homebrew Computer Club 23
- Honeynet 118
- Honeypot 25, 118
- Host file spoofing 142
- Hotmail 229
- HTTP-protocol 166
- Huebner, Hans 25
- Hunter 25
- Hushmail 178
- HyperText Transfer Protocol 166
- ICQ 41, 231
- IM 41
- INFO2 246
- Infobel 226
- Instant Messaging 41, 178
- IntermixMedia 94
- International Mobile Equipment Identity 248
- International Mobile Subscriber Identity 248
- Internet 37
- Internet Protocol 164
- Internet Relay Chat 40
- Internetsporen 249
  - cache 249
  - CCleaner 249
  - cookies 249
  - geschiedenis 249
  - index.dat 249
  - Red Cliff Web Historian 249
  - Super Winspy 250
- Internettelefoonboek 224
- Interregionaal Team Digitale Experts 188
- Intrusion Detection System 117
- IP-adres 164
- IP-nummer 142, 156, 164
- IP-spoofing 105, 151
- IRC 40, 131
  - channel 40
  - Fserve 40
- ITDE Haaglanden 188
- Jacquard, Joseph Marie 19
- Jaschan, Sven 66
- Java 166
- Johansen
  - Jon Lech 46
- Jongsma, Paul 31, 229
- Joybubbles 22
- Kamer van Koophandel 226
- Kaspersky Anti-Virus Personal 71
- KaZaA 174
- Keijzer, Max 29

- Kerio Personal Firewall 121
- Key logger 84
  - Magic Lantern 85
- KeyGhost 93
- KEYKatcher 93
- KeyLogger 93
- KGB-hackers 27
- Klez.H 66
- KLPD 187
- Koch, Karl 25
- Koops, dr. Bert-Jaap 215
- Korps Landelijke Politiediensten 187
- KPN Telecom 32
- Kraken 12
- Krenn, Robert 32
- LOpht Heavy Industries 114
- Land 151
- Lawrence Berkeley Laboratory 25
- Leet speak 108-109
- Legion of Doom (LOD) 24
- LimeWire 174
- Linden, Rob van der 32
- LinkedIn 233
- Luddiet 20
- MAC 122
- MAC-adres opzoeken 123
- Mailbom 155
- MailWasher 139
- Malware 77
- Massachusetts Institute of Technology 5
- Masters of Deception (MOD) 24
- McNealy, Scott 163
- MD5 242
- MDI 199
- Media Access Control 122
- Media-analyse 192
- Meldpunt Discriminatie Internet 199
- Meldpunt Kinderporno 198
- Message Digest algorithm 5 242
- MessageLabs 129
- Metadata 254
  - Microsoft Word 254
  - Bitform Discover 254
  - digitale afbeelding 256
  - EXIF 256
- Metamorfische virussen 62
- Metasploit Framework 103
- Metatdata
  - ExifPro Image Viewer 256
- Mitnick, Kevin 27, 105
- MITS Altair 21
- Mobiele telefoon 114, 247
- Morris, Robert Tappan jr. 64
- Mostly Harmless 50
- MSN Groepen 15
- MSN Groups 229
- MSN Messenger 15, 41, 229
- MSN Scanner 229
- MSN-profielen uitlezen 229
- Murray, Alan 158
- MyDoom 156
- Napster 173
- National High Tech Crime Center 188
- Nationale Telefoongids 222, 225
- NEABBS 29
- Nederlands Eerste Algemene Bulletin Board System 29
- Nederlands Forensisch Instituut 190, 241
- NFI 190, 196
  - beeldonderzoek 195
  - biometrie 195
  - gesloten systemen 193
  - open systemen 192
  - Spraak- en audio-onderzoek 195
- NHTCC 188
- Nuke attack 151
- Ohio State University 158
- Oikarinen, Jarkko 40
- O'Kelly, Morton 158
- Olsthoorn, Peter 32
- OnTheFly 32
- Oostveen, Ronald 32
- Open relay 133
- Open source 45
- OpenPGP 177
- Opsporing
  - adresgegevens 224
  - AIM 231
  - Bartportal 228
  - Dogpile 234
  - e-mailadres 222
  - e-mailheader 224
  - Ezoek 223
  - Google 234

## Index

- ICQ 231
- Infobel 226
- Inventio Metanamesearch 222
- Kamer van Koophandel 226
- LinkedIn 233
- lokmail 235
- MESA 223
- MSN Scanner 229
- MSN-profielen uitlezen 229
- MSN-profielen zoeken 230
- Nationale Telefoongids 225
- Orkut 232
- persoonlijke informatie via chat 229
- reverse lookup 227
- social engineering 235
- Steganografie 257
- telefoonnummers 224
- TULP2G 248
- via sociale netwerken 232
- Yahoo! Messenger 231
- zoek op nummer 228
- OPTA 39, 138
  - onderzoek naar dialerschade 85
- Orkut 232
- Outlook 139
- P2P 42, 173
  - anoniem 175
  - gebruikers traceren 173
  - niet-anoniem 174
  - pottenkijkers 174
  - principe 173
  - spyware 174
- Packet sniffer 206
- Packet sniffing 100
  - Ethereal 102
- Packet Storm 104
- PC Anywhere 86
- PC Inspector File Recovery 246
- PC Inspector Smart Recovery 247
- PDA 114
- PDP-1 5
- PeerGuardian 2 174, 196
- Peer-to-peer 42, 173
- Penetratietest 118
- Pengo 25
- Persoonlijke informatie 229
- Pew Internet & American Life 129
- Pew Internet & American Life Rapport 159
- PGP 177
- Pharming 142
- Phishing 39, 140
  - preventie 141
- Phrack 51
- Phreaker 22-23
- Ping of Death 151
- Polymorfische virussen 61
- Poort 100
  - e-mail 100
- Poortscan 103
- Poortscanner 100
  - Nmap Security Scanner 101
- Pop-upvenster 83
- Poulsen, Kevin 27
- Pretty Good Privacy 177
- Privacy 163
  - Airmiles 163
  - Google 163
- Privé-sleutel 177
- Protocol analyzer 101
- Proxy 133
- PTT 31
- Publieke sleutel 177
- Redfang 114
- Redundancy 150
- Regt, Tom de 29
- Remote administration 86
- Responsible disclosure 48
- Reverse engineering 192
- Reverse lookup 227
- Rifiuti 246
- Robinson, Willis 21
- Root 102
- Root access 102
- ROT13 176
- Router 150
- Safe Internet Foundation 78
- Salami-aanval 21
- Sasser 66
- Schools, Sallie 77
- Scriptkiddie 15, 32, 108
- Secure Sockets Layer 176
- Security by obscurity 47
- Seks 107
- Sender ID 137
- Service Set Identifier 122
- Seuss, Randy 24

- Shaked, Yaniv 114
- Shareaza 42, 87, 174, 196
- SIDN 219
- SIM-kaart 247
  - IMEI 248
  - IMSI 248
  - telefoonboek 248
  - uitlezen 248
- SIOD 191
- Sklyarov, Dmitry 252
- Slammer 66, 155
- Smurf Attack 150-151
- Snocap 174
- Sobig.F 63, 66
- Sociaal hacken 105
- Sociaal netwerk 232
- Social engineering 105
  - herkennen 107
  - methoden 105
- Social network 232
- Spaink, Karin 199
- Spam 39, 77, 119
  - 419-scam 136
  - adressen kopen 131
  - adressen vergaren 130
  - Advanced Email Verifier 132
  - Atomic Email Hunter 131
  - draadloos 134
  - e-mailverifiers 132
  - historie 129
  - Internet Relay Chat 131
  - kosten 129
  - maatregelen 136, 139
  - schade 129
  - spidering 131
  - Usenet 131
  - verzenden 132
  - werking 130
  - wetgeving 137
  - Whois Extractor 131
- SPam via Instant Messaging 135
- SPam via Internet Telephony 135
- Spam voorkomen 136
  - afzenderverificatie 137
  - Bayesiaanse filtering 137
  - blacklist 136
  - complement set filtering 137
  - greylist 137
  - whitelist 137
- Spamfighter 140
- Spamfilter 139
- Spamrun 132
- SpamWeasel 140
- SPIM 135
- Spinrite 243
- SPIT 135
- Spitzer, Eliot 94
- Sporen op de pc
  - bestanden 171
  - internetoverblijfselen 171
  - softwareresten 172
  - Windows 171
- Sporen wissen
  - Crap Cleaner 172
  - Eraser 172
  - Window Washer 172
- Spraak- en audio-onderzoek 195
- Spybot Search & Destroy 91
- Spyware 39, 77
  - besmet raken 87
  - bestrijden 89
  - BO2K 86
  - browserhijacker 84
  - cd-lade openen 88
  - Claria 83
  - Comet Cursor 87
  - CoolWebSearch 84, 91
  - definitie 77
  - dialer 85
  - Euniverse 84
  - Exeem 87
  - Gator 83
  - gedragsspion 82
  - Ghost Keylogger 85
  - Gouden Gids 82
  - infectie herkennen 88
  - KaZaA 87
  - key logger 84
  - MarketScore 82
  - onderzoek 78
  - opbrengst 79
  - oplichter 87
  - pop-under 83
  - pop-up 83
  - pop-upvenster 87
  - remote administration 81, 86
  - soorten 81
  - SpectorSoft 85



## Index

- Sub7 86
- trackingcookie 81
- verborgenheid 80
- verniezucht 80
- Virtuele Katja 82
- voortplantingsdrang 78
- Xupiter 84
- Spyware Assassin 87
- Spywarebestrijding
  - Ad-Aware Personal 91
  - CWS shredder 91
  - DialerDetect 92
  - door de overheid 94
  - HijackThis 92
  - Hitman Pro 2 91
  - Spybot Search & Destroy 91
  - Windows AntiSpyware 91
- SQL Server 156
- SSH 44
- SSID 122
- SSL 176
- Steganografie 165, 179, 257
  - StegDetect 257
- Steganografieanalyse 192
- StegoMagic 179
- Stichting Internet Domeinregistratie Nederland 219
- Stoll, Clifford 25
- Stratix 129
- Surfola 165
- Switch Proxy 169
- Sygate Personal Firewall 122
- SYN-flooding 150
- 't Klaphek 51
- Team Delta 32
- Teardrop 151
- Telnet 43
- The Conscience of a Hacker 24
- The Future of the Internet 159
- The Mentor 24
- The Nijntje Gang 32
- The Wily Hacker 25
- Tiger team 118
- Tijdgat, Onno 29
- TLD 219
- Toetjerrorist 165
- Tomlinson, Ray 38
- Tonino, Joost 170
- Top Level Domain 219
- Torvalds, Linus 10
- Trace! 2 255
- Trackingcookie 79, 81
- Trainingsmogelijkheden 8
- Trojaans paard 64
- TULP2G 45, 248
- UDP Packet Storm 150
- Ultimate Toolkit 242
- Usenet 39
- Vaste schijf repareren 243
- Verkeersgegevens 196
- Versleuteling 39, 124, 175
- Virus
  - Blaster 63
  - definitie 61
  - eigenschappen 61
  - geschiedenis 66
  - GrayBird.E 64
  - I Love You 66
  - Klez.H 66
  - maken 62
  - metamorfisch 62
  - Netsky 66
  - polymorfisch 61
  - Sasser 66
  - Slammer 66
  - Sobig.F 63
  - Trojaans paard 64
  - verspreiding 66
  - Welchia 63
  - worm 63
- Virusbestrijding 67
  - gedragsregels 67
  - infectie herkennen 70
  - scanner 71
- Virusbouwprogramma 62
- Virusgenerator 44
- Virusscanner 71
  - AVG Anti-Virus 72
  - AntiVir Personal Edition Classic 72
  - Avast! 4 Home Edition 72
  - F-Prot Antivirus for DOS 72
  - Kaspersky Anti-Virus Personal 71
  - online 72
- Vogt, Eric de 33, 153
- Vulnerability scanner 100
  - Nessus 101

- Waarschuwingsdienst 199
- Wachtwoord achterhalen 251
  - Elcomsoft 252
  - Free Word/Excel Password Wizard 252
  - ShoWin 253
  - slechte beveiliging 251
  - woordenlijst 251
- Wallace, Sanford 77, 87
- Warchalking 113
- Wardriving 111
- Warstorming 112
- Warwalking 112
- Web proxy 133, 165
  - Privoxy 168
  - The Cloak 166
  - TOR 167
- Webroot 79
- Webserver 150
- Welchia 63
- WEP 113, 124
- WEPCrack 113
- Wet Computercriminaliteit 203
- Wet Computercriminaliteit II 205
  - wijzigingen 213
- Wetboek van Strafrecht 203
  - artikel 137c-g 213
  - artikel 138a 204
  - artikel 139c 205
  - artikel 139d 206
  - artikel 161septies 208
  - artikel 161sexies 207
  - artikel 240b 213
  - artikel 326 212
  - artikel 350a 211
  - artikel 350b 212
  - artikel 351 210
- White-hathacker 9, 99, 108
- Whitehouse, Ollie 114
- Whitelist 137
- WHOIS 131, 219
  - Allwhois 220
  - Centralops 220
  - persoonsgegevens 220
- WiFi 110
  - beveiliging 122
- Wi-Fi Protected Access 124
- WiFi-beveiliging
  - encryptie 124
  - FakeAP 124
  - MAC-herkenning 122
  - nummerherkenning uit 122
  - wachtwoord 122
  - WEP 124
  - WPA 124
- WiFi-netwerk
  - hacken 110
- WiFi-router 120
- Wikipedia 45
- Windows AntiSpyware 91
- Wired Equivalent Privacy 124
- Wireless Local Area Network 110
- Wizard 9
- WLAN 110
- Wool, Avishai 114
- World Online 32, 149
  - hackwedstrijd 32
- World Wide Web 37-38
- Worm 63
- Wozniak, Steve 22
- WPA 124
- WWW 37
- XS4ALL 32
- XSS 144
- Yahoo! Messenger 41, 231
- Zalewski, Michal 255
- Zero-day exploit 104
- Zero-dayaanval 158
- Zeta Reticulli 181
- Zimmermann, Phil 177
- Zoek op nummer 228
- Zombie 134
- ZoneAlarm 121