

Inhoud

1	Hackers, crackers en scriptkiddies	3
	Spraakverwarring over de criminele fauna	5
	Het begin van de hacker	5
	De hacker en Hollywood	7
	Subsoorten van de hacker	9
	White hats	9
	Black hats of crackers	12
	Grey hats of ethical hackers	13
	Hacktivists	13
	Scriptkiddies	15
	Computercriminelen zonder eretitels	15
2	Geschiedenis van hacking en digitale criminaliteit	17
	Definitie van computercriminaliteit	19
	De eerste computermisdaad	19
	Computercriminaliteit en hacking in de twintigste en eenentwintigste eeuw	20
	Vroege computercriminaliteit	20
	White-hat- en grey-hathackers in opkomst	22
	Het Hackermanifest en de Grote Hackeroorlog	24
	Hackers als spionnen	25
	Kevin en Kevin, twee beroemde black hats	27
	Overall scriptkiddies	29
	Computercriminaliteit in Nederland	29
	Hacken in de lage landen	29
	Een nieuwe generatie	32
	Digitaal vandalisme	32

Inhoud

3	Habitats en hangplekken van hackers	35
	De verborgen kanten van internet	37
	World Wide Web	38
	E-mail	39
	Usenet	39
	IRC	40
	IM	41
	Peer-to-peer-sharing (P2P)	42
	FTP	43
	Telnet en SSH	43
	Groupware	44
	Het hackergedachtegoed: openbaarheid voor alles	44
	Security by obscurity	47
	De gulden middenweg: responsible disclosure	48
	Hackertijdschriften	48
	Hackerconferenties	52
	Buitenlandse conferenties	52
	Nederlandse conferenties	53
4	Vandalisme: virussen, wormen en Trojaanse paarden	59
	Digitaal ongedierte	61
	Virussen maken	62
	Speciale virussen	63
	Worm	63
	Trojaans paard	64
	Een beknopte virusgeschiedenis	66
	Virussen bestrijden	67
	Gedragsregels	67
	Tekenen van infectie	70
	Virusscanners	71
5	Spionage: spyware, key loggers en beheer op afstand	75
	Wat is spyware?	77
	Waarom is spyware een probleem?	78
	Voortplantingsdrang	78
	Verborgenheid	80
	Vernielzucht	80
	Soorten spyware	81
	Trackingcookies	81
	Gedragsspionnen	82
	Pop-upvensters	83

Browserhijackers	84
Key loggers	84
Dialers	85
Remote administration	86
Oplichters	87
Methodes om besmet te worden	87
Zeven tekenen van spyware-infectie	88
Tegenaanval in drie stappen	89
1. Gooi Internet Explorer eruit	89
2. Houd regelmatig grote schoonmaak	90
3. Bewaar een pistool onder uw kussen	92
James Bond bestaat niet, 'Q' wel	93
Overheden in actie tegen spyware	94
6 Inbraak: hacking, wardriving, social engineering	97
Hacken en computerkraken: wat is het?	99
Basis van het hacken	100
Verkenning: poortscanners, vulnerability scanners en packet sniffing	100
Het verwerven van toegang: root worden en exploits	102
Buffer overflows	103
Het vinden van exploits	103
Social engineering: de mens als exploit	105
Waarschuwingssignalen	107
Binnen! Over het doel van de hack	108
Na de hack	109
Oorlog om draadloze netwerken	110
Wardriving	111
Warwalking	112
Warstorming	112
Warchalking	113
Draadloos hacken	113
Het hacken van mobiele telefoons en PDA's	114
Bluetooth wardriving	115
Bluetooth sniping	115
Blue jacking	115
Blue snarfing	116
Bedrijven in de verdediging	117
Firewall	117
Intrusion Detection System	117
Demilitarized Zone (DMZ)	117
Penetratietests en tiger teams	118
Honeypots en honeynets	118
Uw huis is uw kasteel	119

Inhoud

Draadloze tegenmaatregelen	122
Wijzig het ingebakken wachtwoord	122
Zet nummerherkenning uit	122
Zet MAC-herkenning aan	122
Gebruik geheimtaal	124
Zet bliksemafleiders in	124
7 Oplichting: spam, phishing en digitale kameleons	127
De kosten van spam	129
Hoe spam gemaakt wordt	130
Adressen vergaren	130
Spam verzenden	132
Maatregelen tegen spam	136
Technische maatregelen	136
Wetgeving en rechtszaken	137
Zelf in actie komen	139
Phishing	140
Pharming	142
Host file spoofing	142
DNS-cache poisoning	143
Een digitale kameleon: cross site scripting (XSS)	144
8 Sabotage: DoS-aanvallen, mailbommen en zero-dayaanvallen	147
Einde van de dotcom-utopie	149
DoS-aanvallen	150
DoS-methode 1: overbelasten	150
DoS-methode 2: destabiliseren	151
DoS-methode 3: vernielen	152
DDoS-aanvallen	152
Onwillige helpers	154
Mailbom	155
Gevaar voor internet	155
Dreigt een internet-apocalyps?	156
Zero day	158
9 Anarchisme: anonimiteit, smokkel en geheimtaal	161
Uw identiteit ligt op straat	163
Internetsporen vermijden	164
Sporen op de pc wissen	170
Bestanden	171
Internetoverblijfselen	171

Windows-sporen	171
Software-resten	172
Actie!	172
Smokkelen met P2P	173
Niet-anonieme P2P-netwerken	174
Anonieme P2P-netwerken	175
Encryptie	175
E-mail: PGP	177
Chatten: SimpLite	178
Verborgen inkt: steganografie	179
De digitale kantoortuin: groupware	180
10 Professionele speurders	185
De politie is je beste onlinekameraadje	187
Computerforensisch onderzoek	189
Open systemen	192
Gesloten systemen	193
Beeldonderzoek en biometrie	195
Sprak- en audio-onderzoek	195
Wapenfeiten	196
Particuliere instanties in Nederland	198
Meldpunt Kinderporno	198
Meldpunt Discriminatie Internet	199
11 Wetgeving	201
De wet op het net	203
De computer als doelwit	204
Inbreken	204
Afluisteren	205
Vernieling en sabotage van computersystemen	207
Wissen en manipuleren van gegevens	211
De computer als middel	212
Vermoedelijke veranderingen door de Wet Computercriminaliteit II	213
Het Cybercrime-verdrag	214
12 Opsporing via internet	217
Beter goed gejat	219
WHOIS, of: de personen achter een website	219
E-mailadressen vinden	222
Adresgegevens en telefoonnummers van personen en bedrijven achterhalen	224
Nationale Telefoongids	225

Inhoud

Infobel	226
Kamer van Koophandel	226
Reverse lookups	227
Bartportal	228
Zoek op nummer	228
Persoonlijke informatie vinden via chatdiensten	229
MSN Scanner in gebruik	229
Zoeken naar MSN-profielen	230
Andere chatdiensten	231
Persoonlijke informatie vinden via sociale netwerken	232
Slimmer zoeken met Google	234
Het nut van een metazoekmachine	234
Speuren met lokmails en social engineering	235
13 Opsporing via hard- en software	239
De (on)mogelijkheid om experts na te doen	241
Vaste schijven repareren	243
Gewiste bestanden terughalen	245
De geheimen van een mobiele telefoon	247
Het uitlezen van internetresten	249
Wachtwoorden van bestanden achterhalen	251
Het nut van metadata	254
Steganografie opsporen	257
A Terminologie	259
Terminologie	260
B Wetten en verdragen	275
Relevante artikelen uit het Wetboek van Strafrecht	276
Cybercrime-verdrag	282
Preamble	282
Chapter I – Use of terms	284
Chapter II – Measures to be taken at the national level	284
Section 1 – Substantive criminal law	284
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	284
Title 2 – Computer-related offences	286
Title 3 – Content-related offences	286
Title 4 – Offences related to infringements of copyright and related rights	287
Title 5 – Ancillary liability and sanctions	287
Section 2 – Procedural law	288

Title 1 – Common provisions	288
Title 2 – Expedited preservation of stored computer data	290
Title 3 – Production order	290
Title 4 – Search and seizure of stored computer data	291
Title 5 – Real-time collection of computer data	292
Section 3 – Jurisdiction	293
Chapter III – International co-operation	294
Section 1 – General principles	294
Title 1 – General principles relating to international co-operation	294
Title 2 – Principles relating to extradition	294
Title 3 – General principles relating to mutual assistance	295
Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	296
Section 2 – Specific provisions	298
Title 1 – Mutual assistance regarding provisional measures	298
Title 2 – Mutual assistance regarding investigative powers	300
Title 3 – 24/7 Network	301
Chapter IV – Final provisions	301

Index

307