Inhoud

DEEL I: Digitale criminaliteit

DEEL II: Privacy

DEEL IV: Je privacy beschermen

1

"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, ook bekend als 'rms', softwareactivist**

Je leest in dit hoofdstuk:

- Wat cybercrime, oftewel digitale criminaliteit, is.
- Waarom hackers én crackers louter minachting hebben voor scriptkiddies.
- Welke ethische normen hackers hebben.

Het verschil tussen hackers en cybercriminelen

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 groepen is flink met elkaar vermengd. Dat komt niet in de laatste plaats doordat ingenieuze hackeracties die niet bedoeld waren voor financieel gewin, soms toch illegaal waren of dat door wetswijzigingen zijn geworden. Daartegenover staat dat sommige hackerpraktijken zo succesvol zijn gebleken, dat ze zelfs door opsporingsinstanties zijn overgenomen.

Definitie van cybercrime of digitale criminaliteit

Voordat we het over digitale criminaliteit (oftewel cybercrime) kunnen hebben, moeten we vaststellen wat we precies bedoelen met deze term. Want dat is nog best lastig. Op internet circuleren verschillende definities. Voor sommige mensen is iets cybercrime als het doelwit een computer is. Dat klinkt redelijk, maar als iemand een winkel inloopt en vervolgens hard wegholt met een van de toonbank gegriste laptop, is dat dan cybercrime? Of 'doodordinaire' diefstal?

Andere definities zeggen dat iets cybercrime is als je een computer hebt gebruikt bij het voorbereiden of uitvoeren van een misdaad. Ook dat klinkt best redelijk in eerste instantie. Totdat je bedenkt dat een telefoon ook een computer is (die bovendien ook nog eens met internet verbonden is). Is elke zakkenroller die z'n iPhone heeft gebruikt om de eerstvolgende tram naar het Waterlooplein te vinden, nu opeens een cybercrimineel?

Wat als we beide definities combineren? 'Cybercrime is een misdaad waarbij een computer, of een computernetwerk, als middel en als doel is gebruikt.' Ah, fijn, nu zijn we er, zo lijkt het. Gebruik je je laptop om een ander te dwingen tot webcamsex? Cybercrime. Je breekt in bij het Pentagon met een op een *darknet* verkregen splinternieuwe hackmethode, een zogeheten zero day exploit? Cybercrime.

Maar wat dan te denken van *social engineering*? Dat is het slim manipuleren van mensen om toegang te krijgen tot andermans computersystemen of netwerken. Daarvan is bijvoorbeeld sprake als je met brutale bluf iemand een wachtwoord aftroggelt. Het 'middel' waarmee de misdaad wordt uitgevoerd, een mens, is echter geen computersysteem. Toch rekenen we dit in de praktijk wel tot digitale criminaliteit. Een heel groot deel van hacks van computersystemen komt namelijk tot stand door het exploiteren van menselijke zwakheden.

Hoe verenigen we deze definities met elkaar? Een bruikbare, doch niet perfecte, definitie is: cybercrime is elke misdaad waarbij een computer of computernetwerk op enig punt in het proces essentieel is voor de aard van het misdrijf. De zakkenroller had ook gewoon bij de tram kunnen gaan staan wachten. De laptopdief had ook een portemonnee kunnen grissen, of een dure ketting. Maar de zedendelinquent kiest expliciet voor internet, met zijn alomtegenwoordige webcams, als habitat voor z'n roofdiergedrag. En de social engineer gebruikt haar gladde praatjes exclusief om een computersysteem of netwerk binnen te dringen.

Onbetwistbaar is deze definitie niet. Maar alleen al door haar imperfectie maakt ze duidelijk dat de online wereld er eentje is van veel nuanceverschillen. Wat ook wel zal blijken, nu we het gaan hebben over het verschil tussen hackers, crackers en scriptkiddies.

Hackers, crackers en scriptkiddies

Niet alle criminelen zijn hackers, en niet alle hackers zijn crimineel. Toch worden de termen vaak door elkaar gebruikt. Onterecht, maar begrijpelijk. Want voor zover nerds sexappeal kunnen hebben, heeft de hacker het in overvloed. In Hollywood is de hacker een moderne Robin Hood óf een zwart-wit getekende superschurk met charme. Verderop in dit hoofdstuk gaan we daar nader op in.

De realiteit is uiteraard anders, maar dankzij de vele sensationele berichtgeving is dat inzicht zeldzaam. Om het nog verwarrender te maken, hanteren kenners verschillende termen voor verschillende soorten hackers. Zo zijn er white-hat- en black-hathackers, maar ook scriptkiddies, crackers en computercriminelen zonder speciale titels. En lang niet allemaal hebben ze kwade bedoelingen.

Het begin van de hacker
Oorspronkelijk is de titel hacker een erenaam, maar door chronisch misbruik van de term weet bijna niemand dat meer. Net zomin als maar weinigen beseffen dat de term hacker uit het midden van de 20ste eeuw dateert.

Voor veel computerpuristen is er maar één mogelijke uitleg van de term hacker: *iemand die bijzondere technische creativiteit aan de dag legt.* Of dat nu bij het programmeren is of bij het vouwen van origami (papier is immers ook een technologie). Die creativiteit kan zich op allerlei manieren uiten. Een apparaat iets anders laten doen dan waarvoor het is bedoeld, is een hack. Het bouwen van slimme software die burgers de mogelijkheid geeft op basis van openbare informatie meer invloed uit te oefenen op de democratie, is een vorm van hacken (specifiek: *civic hacking*). Net als vindingrijke grappen uithalen met technologie, zoals de middenstip tijdens de rust van een sportwedstrijd laten veranderen in een reusachtige ballon, iets wat studenten van het Massachusetts Institute of Technology deden in 1982.

De term 'life hack', die populair werd aan het begin van dit millennium, is na het voorgaande eenvoudig te duiden. Daar gaat het om creatieve manieren om je leven beter te maken.

Hacks

Een overzicht van hacks-als-practical-jokes is te vinden op **hacks.mit.edu**. Het betreft dan hacks op het Massachusetts Institute of Technology (MIT). Overigens hoeft een goede grap op MIT al lang niet meer technologisch van aard te zijn om een hack te mogen heten. MIT heeft een boek over dergelijke hacks gepubliceerd, *Nightwork – A History of Hacks and Pranks at MIT* door T.F. Peterson (ISBN 978-0262661379).

De definitie van een hack als creatief-technologische daad vindt zijn oorsprong in de jaren zestig. Toen kwam op het prestigieuze Massachusetts Institute of Technology (MIT) de Tech Model Railroad Club bijeen. Inderdaad: de nu zo gevreesde hacker heeft zijn oorsprong bij een clubje jonge heren die met speelgoedtreintjes speelden. De MIT-studenten beperkten zich echter al snel niet meer tot treintjes. Toen op MIT een computer werd geïnstalleerd, werd dat het doelwit voor hun knutsel-

drift. De computer in kwestie was een PDP-1 van de inmiddels ter ziele computerfabrikant Digital Equipment Corporation. Sinds 1998 bestaat Digital niet meer, maar het bedrijf vond de eens roemruchte zoekmachine AltaVista (later gekocht door Yahoo) uit.

Je partner vindt je nieuwe laptop niet mooi? Toon dan deze foto van de PDP-1. (Foto: Matthew Hutchinson, CC-BY 2.0.)

De PDP-1 had op de studenten ongeveer net zo veel aantrekkingskracht als AltaVista dat had op de eerste internetgebruikers. Het was geen fraai apparaat om te zien, maar voor de MIT-studenten was de machine onweerstaanbaar. Dat komt omdat een computer zich op een fundamentele manier onderscheidt van alle andere apparaten die ooit zijn gebouwd. Een computer is kneedbaar, flexibel, of, in het jargon: programmeerbaar. Een hamer zal altijd een hamer zijn en nooit als schroevendraaier kunnen fungeren (omgekeerd zou je dat nog kunnen proberen, maar erg effectief ben je waarschijnlijk niet). Maar een computer kan een andere functie te krijgen door hem andere instructies, oftewel een ander computerprogramma, te geven.

En dat was precies wat de MIT-studenten deden. Ze gebruikten de dure PDP-1 voor doelen waar de serieuze systeembeheerders van de universiteit absoluut niet om konden lachen. Zo kreeg Pete Samson het voor elkaar om de PDP-1 vierstemmige muziek te laten produceren met het programma *Harmony Compiler*. PDP-muziek is nog steeds te horen op **www.dpbsmith.com/pdp1music/**.

De PDP-1 werd ook gebruikt voor spelletjes. De ietwat illustere reputatie van hackers begon ook op MIT. Het werd namelijk al snel duidelijk dat de PDP-1 heel bruikbaar was om gratis mee te bellen. In die tijd werd het telefoonnetwerk nog aangestuurd met bepaalde geluiden, en die kon je nabootsen met de PDP-1. (Meer hierover in hoofdstuk 2.)

Waarom nu juist de term hacking werd gebruikt voor deze bezigheden, is niet helemaal duidelijk. Sommigen houden het erop dat het de tijdgeest van de jaren zestig was. Het knutselen aan motoren was in die tijd eveneens populair en heette *chopping*. Dat woord kan, net als 'hacking', zoiets betekenen als 'aan mootjes hakken'. De theorie klopt echter vermoedelijk niet. Al in de jaren vijftig gebruikten radioamateurs de term hacking voor het gebruiken van je technische creativiteit om de verbinding te verbeteren.

Feit is dat 'hacker' een erenaam blijft voor veel technologieliefhebbers die nog nooit de wet hebben overtreden (of althans niet in ernstige mate). Zo noemen de ontwikkelaars van het besturingssysteem FreeBSD zich nog altijd 'hackers', en hun mailinglijst (**lists.freebsd.org/pipermail/freebsd-hackers/**) heeft dan ook die naam. Dichter bij huis: Nederland kent vele zogeheten hackerspaces (**hackerspaces.nl**) waar je creatief met technologie kunt knutselen.

Verder lezen over hackergeschiedenis

Wie specifiek geïnteresseerd is in hoe het de MIT-studenten verder verging, leze het uitstekende boek *Hackers: Heroes of the Computer Revolution* van Stephen Levy (ISBN 978-0141000510).

De hacker en Hollywood

Het huidige imago van de hacker is wel wat anders dan dat van een onschuldige, knutselende student. Noem het woord hacker en velen den-

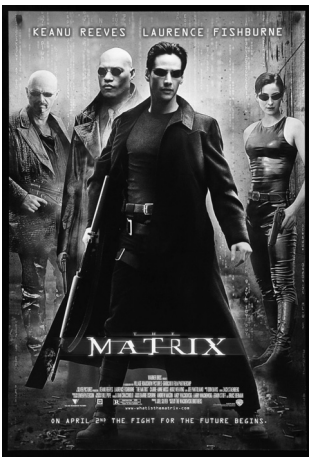
ken aan een computercrimineel of aan de digitale incarnatie van een superheld. Voor een deel is dat te wijten aan Hollywood.

De film *WarGames* uit 1983 bracht het begrip hacker naar veel huiskamers. Hoofdpersoon David Lightman ontketent daarin bijna een nucleaire oorlog doordat hij inbreekt in een computer van het Amerikaanse leger. De formele schuldige in deze nogal moralistische film is de oorlogszuchtige mens, maar de onderliggende boodschap over het jonge, met computers spelende grut is net zo duidelijk: pas op voor de hacker! In 2007 werd dezelfde boodschap nog eens herhaald in de film *Live Free or Die Hard.* Daarin maakt Bruce Willis op gewelddadige en technologisch niet al te verfijnde wijze een einde aan de praktijken – en het leven – van hackerschurk Thomas Gabriel.

Als hackers niet als dreiging worden gezien, worden ze wel verregaand verheerlijkt. Voor de film *Hackers* uit 1995 is ieder positief woord er een te veel. *Hackers* laat een stel semi-hippe jeugdigen zien die – tof! – al hackend de wereld beschermen tegen een boosaardig oliebedrijf. Dat Angelina Jolie meespeelt, zou voldoende moeten zeggen. In *Swordfish* (2001) chanteert een crimineel een hacker om mee te werken aan een poging om de Amerikaanse overheid te beroven. De crimineel blijkt later een voormalig agent te zijn die het geld wil gebruiken om ondergronds tegen terrorisme te vechten. Jazeker, *hackers making the world safe for democracy.*

Het verst doorgeschoten in de hacker-mythologisering is de Amerikaanse producer en schrijver J. Michael Straczynski, maker van de tv-serie *Babylon 5*. Straczynski laat in deze serie zogeheten *technomages* opdraven, priesterachtige figuren die met behulp van techniek bijna magische daden kunnen verrichten. Of nee, toch niet. Het verst doorgeschoten zijn de Wachowski-zussen. In *The Matrix* (1999) verandert hoofdpersoon en hacker Neo tegen het einde in een soort arhat, de boeddhistische naam voor iemand die de totale verlichting heeft bereikt, en de realiteit ziet voor wat deze werkelijk is. Daar moet wel bij worden gezegd dat de Wachowskis de mentaliteit van hackers goed weergeven.

De TV-serie *Mr. Robot* (2015-2019), te zien via Amazon Prime, is een realistische uitzondering. De hoofdpersoon, Elliot Alderson, is een cybersecurityexpert, die daarnaast bijklust als activistische hacker. Alderson strijdt tegen het bedrijf E Corp, door hem consequent 'Evil Corp'



Filmposter van de eerste The Matrix-film (Warner Bros).

genoemd. Bijzonder aan de serie is dat vrijwel alle getoonde hacks technisch kloppen. Bedenker Sam Esmail was namelijk zelf ooit een hacker.

Subsoorten van de hacker

Aan filmregisseurs heb je dus niet zo veel bij het maken van een werkbare indeling van de hackerwereld. Gelukkig hebben hackers zelf logischer ideeën over de groepen waarin hun subcultuur te verdelen valt. Grofweg zijn er vier soorten hackers. De laatst genoemde categorie in de volgende opsomming wordt niet tot de hackers gerekend.

White hats

Gandalf, de tovenaar uit J.R.R. Tolkien's *The Lord of the Rings*, is altijd een populaire bijnaam geweest onder computerliefhebbers. Want wat wil een nerd nu nog meer als rolmodel dan een wijze tovenaar die met behulp van zijn grote magische kennis het goede van het kwade helpt winnen? Het is vermoedelijk geen toeval dat white-hathackers ook wel wizard worden genoemd.

Gurus en wizards

White hats worden ook wel gurus of wizards genoemd. Een guru is vaak door de wol geverfd, een wizard onderscheidt zich meestal door zijn bijna magische beheersing van één specialisme.

Toch komt de term white hat niet uit een fantasierijk boek, maar uit wildwestfilms. Traditioneel hebben in Amerikaanse westerns de schurken zwarte en de helden witte hoeden. Daarmee is gelijk duidelijk hoe een white-hathacker zichzelf ziet: als iemand die zijn technische vaardigheden voor 'goede' doelen aanwendt, of zich in elk geval niet te buiten gaat aan 'kwade'.

Wat dan precies goed of kwaad is, lijkt nogal afhankelijk te zijn van de definities die de hacker er zelf op nahoudt. In het algemeen zullen white-hathackers zich aan de wet houden en technologie slechts gebruiken voor constructieve doelen. Ze zullen zich bijvoorbeeld niet willen bezighouden met het vernielen van websites (het zogeheten *defacen*) of ander destructief gedrag, zoals het zonder toestemming of op grove wijze inbreken in computersystemen.

In plaats daarvan houden white hats zich bezig met wat wellicht nog het best kan worden beschreven als creatief aanrommelen met techniek. Net als in de jaren zestig is het zeer des white hats om een apparaat iets te laten doen wat het eigenlijk niet behoort te doen. Ook het met toestemming van de eigenaar testen van de beveiliging van een computersysteem is typisch white-hatgedrag, een activiteit die ook wel *pentesting* wordt genoemd, een afkorting van *penetration testing*. Technologische grappenmakers zoals de eerder genoemde studenten die practical jokes uithaalden op MIT, zijn over het algemeen ook white-hathackers.

Het summum van white-hathackerdom is echter op creatieve wijze iets geheel nieuws uit de grond te stampen. Linus Torvalds, de maker van het besturingssysteem Linux, wordt door velen in de white-hatgemeenschap als hacker gezien.

Alle white hats hebben één ding gemeen. Ze moeten niets hebben van black hats of crackers (zie verderop) en worden erg boos als in de pers daden van deze kwaadwillende hackergroepen worden toegeschreven aan hackers. Wat white hats betreft, zijn zij de enigen die de naam 'hacker' mogen dragen.

Dat werpt echter wel een definitieprobleem op. Een hacker die vanuit een dictatuur zoals China zijn computervaardigheden aanwendt om democratische oppositiegroepen te helpen, overtreedt duidelijk de Chinese wet. Toch zullen weinig Europeanen of Amerikanen zo'n hacker tot

Linus Torvalds, bedenker van het ingenieuze besturingssysteem Linux. Wordt door veel white hats om die reden beschouwd als hacker. (Foto: krd / cc-by-sa-3.0.)

slecht willen bestempelen. Ook zijn er white hats die inbreken in computersystemen, maar daar niets kapot maken. Hoewel dat in veel landen (waaronder Nederland) illegaal is, voeren deze hackers zelf aan dat ze louter hun nieuwsgierigheid willen bevredigen, en de eigenaar van het gehackte computersysteem zelfs een dienst bewijzen, door duidelijk te maken dat zijn beveiliging niet deugt. Die eigenaar, zo luidt de theorie, kan dan maatregelen nemen zodat zijn computersysteem hierdoor veiliger wordt.

Grey-hat- of ethische hackers

Welwillende maar illegaal opererende hackers worden ook wel ethische of grey-hathackers genoemd.

Helaas voor deze groep hackers is het volgens de Nederlandse wet illegaal om je zonder toestemming toegang verschaffen tot een computersysteem van een ander. Maximaal staat op deze zogeheten computer-

vredebreuk zelfs vier jaar gevangenisstraf. Het verbod op computervredebreuk kijkt niet naar de intenties van de inbreker. De hacker 'Kaas', oftewel de Nederlander Ewout Z., kreeg in maart 2005 120 uur dienstverlening en drie maanden voorwaardelijke gevangenisstraf opgelegd. Dat was zijn straf vanwege het inbreken in een Amerikaans computersysteem. Daar bemachtigde Kaas de bouwtekeningen van het Pentagon. Hij informeerde onmiddellijk de eigenaren van het systeem en vertelde ze hoe ze hun computers beter konden beveiligen. Dat noopte de rechter echter niet tot vrijspraak, hoewel deze in het vonnis wel rekening hield met de goede bedoelingen van Kaas.

Om dergelijke naamgevingsproblemen te voorkomen, worden deze welwillende maar illegaal opererende hackers ook wel *grey-hat-* of ethische hackers genoemd.

Hacker te huur

White-hathackers zijn geliefd bij het bedrijfsleven. En omdat een white-hathacker ook moet eten, verhuren vele white hats hun capaciteiten in het testen van computerbeveiligingen. Voor dergelijke *penetratietests* of *pentests* worden soms zogeheten *tiger teams* ingezet. Een *tiger team* is een verzameling van hackers die in samenwerking al haar inbraakvernuft richt op één doel.

The Jargon File

Meer weten over hoe sommige white-hathackers zichzelf zien? Lees dan *The Jargon File*, een handleiding tot (een deel van de) hackergemeenschap op **tinyurl.com/jargonfile**.

Black hats of crackers

De black hat laat zich niet beperken door triviale zaken als de wet of goed fatsoen. Hij of zij gebruikt zijn kennis en vaardigheden zonder aarzelingen voor illegale doelen. Soms voor geldelijk gewin, maar commerciële motieven zijn niet zijn enige drijfveer. Er zijn plenty black hats die geen cent verdienen met hun daden en genoeg white hats die in een bijzonder aardige auto kunnen rijden van hun verdiensten als beveiligingsexpert.

Een typisch voorbeeld van niet-lucratief black-hatwerk is het illegaal verspreiden van software. Er is een heuse subcultuur binnen de black-hatgemeenschap ontstaan die zich louter bezighoudt met het houden van onderlinge wedstrijdjes om zo snel mogelijk nieuwe software van een eventuele kopieerbeveiliging te ontdoen, het zogenoemde kraken of cracking, en het gekraakte product vervolgens bij een zo groot mogelijk publiek aan te bieden. Dat dit volgens de wet niet mag, spreekt voor zich, maar over het algemeen worden deze black-hathackers er niet veel rijker van. Zulke black hats heten, mede om deze reden, ook wel crackers.

In de allereerste gesproken westernfilm ooit, The Great Train Robbery uit 1903, droegen bandieten zwarte hoeden.

Cracking

De term cracking slaat in zijn algemeenheid op het doorbreken van een beveiliging zonder toestemming, of dat nu gebeurt bij een computersysteem of bij een programma waarvoor eigenlijk betaald had moeten worden.

Om begrijpelijke redenen zijn de echt goede black hats een stuk geheimzinniger over hun identiteit dan white-hathackers, die soms zelfs conferenties organiseren. De black hat dient niet verward te worden met de *scriptkiddie* (zie verderop).

Grey hats of ethical hackers

Deze term wordt gebruikt voor hackers wier activiteiten niet eenvoudig zijn te bestempelen als white hat of black hat. Eerder is al de Nederlandse hacker Kaas genoemd, die zich zonder toestemming toegang ver-

schafte tot een computer waarop bouwplannen van het Pentagon stonden, doch enkel om de staat van de beveiliging te testen.

Maar er zijn meer en beroemdere voorbeelden van ethical hackers. Een bekende grey hat is de Noorse hacker Jon Lech Johansen (**nanocr.eu**). Hij wordt mede verantwoordelijk gehouden voor het produceren van het computerprogramma DeCSS, waarmee dvd's zonder problemen kunnen worden gekopieerd. Een van de redenen die wel is aangevoerd voor het maken van DeCSS is dat het voordien niet mogelijk was om legaal gekochte dvd's op een Linux-computer te kunnen afspelen. Maar daar kon de overwegend Amerikaanse filmindustrie noch de Noorse overheid veel begrip voor opbrengen. Johansen heeft dan ook meerdere rechtszalen van binnen gezien.

De ethische grens

Lange tijd was het voor ethical hackers acceptabel om te proberen in te breken in computersystemen, enkel om te testen of de beveiliging wel deugt. Daar werden dan wel twee voorwaarden aan gesteld. De hacker mocht geen schade aanrichten, en hij of zij diende de eigenaar achteraf te informeren. Uiteraard zonder voor dergelijk advies geld te vragen. Hoewel deze inbraakpraktijken bij niet-hackers nog wel eens wat opgetrokken wenkbrauwen opriepen, was het vanuit historisch perspectief niet zo vreemd dat er ethical hackers waren die hier weinig problemen mee hadden. Zo lang geleden is het nog niet dat inbreken in computers in veel landen legaal was, bij gebrek aan goede wetgeving. Tegenwoordig worden dergelijke spontane hackacties wel steeds zeldzamer, ook al omdat er met 'ethisch hacken' goed geld te verdienen valt. Waarom zou je dan nog het risico lopen om met je skills de wet te overtreden? (Zie kader *Bug bounties*.)

Hacktivisten

Deze groep hackers is politiek of sociaal bewogen en gebruikt een scala van technische gereedschappen om de eigen doelen te verwezenlijken. Dan kan op een nette manier, maar ook op illegale wijze. Aanhangers van hacktivistenorganisatie Anonymous (**twitter.com/YourAnonNews**), die onder meer van zich liet horen na de moord op Afro-Amerikaan George Floyd, breken bijvoorbeeld regelmatig de wet. Maar Anonymous is een decentrale organisatie. Het is niet duidelijk wie er 'lid' van is of wie de organisatie bestuurt, als er überhaupt al sprake is van een traditioneel bestuur.

Bug bounties

Om de energie van creatieve computeraars nuttig te gebruiken, bieden veel grote IT-bedrijven, maar ook het Amerikaanse ministerie van Defensie, tegenwoordig beloningen aan voor techneuten die beveiligingskwetsbaarheden in hun software of online diensten vinden. Dit worden *bug-bountyprogramma's* genoemd, en de beloningen kunnen fors oplopen. Zo biedt Intel tot 250.000 dollar. Maar ook bij Marktplaats en IKEA valt geld te halen. Op **hackerone.com/leaderboard/** is een lijst te vinden van hackers die momenteel succesvol zijn in het vinden van dit soort kwetsbaarheden. De Nederlandse internetaanbieder XS4ALL, die per 1 maart 2020 ophield te bestaan als zelfstandige onderneming, bood volgens mede-oprichter Paul Jongsma al in 1993 een 'bug bounty' aan. Wie 'root' kon worden – oftewel de baas over het computersysteem – en dat netjes meldde, kreeg een gratis abonnement voor het leven.

Waar Anonymous ongrijpbaar is, houdt de Duitse Chaos Computer Club (**ccc.de**) elk jaar een conferentie. Niks 'duistere hoekjes van internet', je pakt gewoon de trein naar Leipzig en koopt een toegangskaartje. De CCC is ook keurig ingeschreven als non-profitorganisatie in Duitsland ('eingetragener Verein', voor wie het precies wil weten). Wat natuurlijk niet betekent dat elk lid van de CCC, laat staan elke bezoeker van deze conferenties, zich altijd aan de wet houdt.

Het is dus niet eenvoudig om hacktivisten in te delen in white hats of black hats. En dat is ook logisch. Wie zich verzet tegen de bestaande wetgeving of machthebbers, heeft soms weinig keuze als het gaat om de wet te overtreden. Het is lastig om legaal activist te zijn, als je in een land woont waar de overheid bijvoorbeeld de vrijheid van meningsuiting heeft gekortwiekt.

Woon je als hacktivist in een land waar je wel mag demonstreren en vrij van internet gebruik kunt maken, dan kun je ook vinden dat je de wet moet overtreden om een bepaalde misstand aan de kaak te stellen – of je kunt vinden dat dit te ver zou gaan. Hacktivisten zijn kortom net mensen, met alle nuances en individuele verschillen die daarbij horen.

Scriptkiddies
White-hat- én black-hathackers haten scriptkiddies, ook wel skiddies of skids genoemd. Met reden. Een scriptkiddie is iemand die vooral veel technische vernielzucht toont, bijvoorbeeld door computers te kraken, informatie te wissen of websites te verminken (*defacen*).

Zijn deze vandalistische neigingen al voldoende reden voor white hats om scriptkiddies te diskwalificeren als waardig medemens, ook black hats hebben het niet op scriptkiddies. En wel omdat scriptkiddies vrijwel nooit zelf enige technische creativiteit aan de dag leggen, maar gebruikmaken van de slimme vindingen van echte hackers.

Via internet is veel software beschikbaar waarmee ook mensen zonder specialistische kennis virussen kunnen maken of bij computers kunnen inbreken. Scriptkiddies gebruiken die software om zich technisch vaardiger voor te doen dan ze zijn. Black hats, die hard hebben moeten werken voor hun kennis, walgen daarom van deze poseurs.