

'Hacker ethics', ethical or not?

Inleiding

In de afgelopen tientallen jaren is de term 'hackers' vaak in het nieuws verschenen. Vaak gaat het om het kraken van bedrijfssystemen of het verspreiden van virussen. Wanneer men zich verdiept in de materie, blijkt dat er vaak een spraakverwarring plaats vindt. Immers, wat of wie bedoelt men met 'hackers'?

Hackers zijn oorspronkelijk een groep programmeurs welke op een zeer elegante manier software kunnen ontwikkelen. Vanuit de samenleving wordt er met gemengde gevoelens over hackers gedacht. Hieraan ligt vaak een misperceptie aan ten grondslag, wat niet geheel ten onrechte is.

Er bestaat verder een onderscheid tussen hackers uit de jaren '60 en '90. Dit is natuurlijk niet vreemd, aangezien de wereld en de technologie enorm zijn doorontwikkeld. Beide groepen hackers hadden / hebben eigen ethische code. Elke, zichzelf respecterende, hacker verplicht zichzelf om zich te houden aan deze code. Verder dient deze code vertrouwen te bieden aan de buitenwereld.

Aangezien de wereld is veranderd, is het ook niet vreemd dat deze ethische codes zijn veranderd. In dit essay zal ik een aantal codes (uit de jaren '60 en '90) beschrijven en hierover mijn waardeoordeel uitspreken. Dit alles zal leiden tot een slotconclusie of ikzelf vertrouwen heb in de ethische code van hackers.

'60 hacker ethiek

De hacker ethiek uit de jaren 60 is hoofdzakelijk een informele code. In deze code wordt afgegeven op de bureaucratische tegenwerking voor het gebruik van de technologische mogelijkheden. Hieronder volgen de (in mijn ogen) belangrijkste ethische codes en mijn waardeoordeel hierover.

1. De toegang tot computers moet onbeperkt en volledig zijn en de autoriteiten moeten gewantrouwd worden

Dit principe ligt ten grondslag aan de beperking, opgelegd vanuit de overheid en bedrijven, om de nieuwste technologie in de jaren '60 niet beschikbaar te stellen aan de burgerij.

Dit steven, om technologie breed beschikbaar te maken, was in die tijd een hele goede. Immers, door zoveel mogelijk mensen te mogelijkheid te geven om met nieuwe technologie te (leren) werken, is de kans groter om de technologische vooruitgang sneller te laten verlopen. De benodigde kennis zat namelijk niet alleen bij deze grote bedrijven, maar (in die tijd) ook bij veel hackers.

De hackers vonden dat het achterhouden van nieuwe technologieën ook de mogelijkheden van de burgers zou schaden. De burger had ook recht om zichzelf te ontwikkelen.

Een kant tekening welke geplaatst kan worden is het feit dat de technologie in die tijd ook erg duur was, waardoor veel mensen deze technologie niet konden veroorloven.

Wanneer men naar het heden kijkt, kan men concluderen dat dit steven van de hackers in de huidige tijd gelukt is. De technologieën zijn tegenwoordig voor iedereen beschikbaar, wat overigens niet alleen de verdiensten is van de hackers gemeenschap. Dit heeft ook te maken met de verandering naar een meer liberalere samenleving en de enorme vooruitgang op het technologische gebied.

Hierbij denk ik b.v. aan pc-privé projecten in Nederland, waarin de overheid burgers de kans geeft om goedkoop een computer aan te schaffen.

In de ethische code van de hacker gemeenschap in de jaren '90 komt dit principe ook weer terug, echter in iets ander vorm. De hackers uit deze tijd vinden dat ongebruikte apparatuur altijd gebruikt mag worden. Dit principe vind ik een stuk discutabeler. Het principe van de hackers uit de jaren '60 was nog een mooi, liberaal streven, het principe van 'joy riding' is in mijn ogen niet verantwoord. Het 'lenen' van apparatuur, in dit geval meestal het 'lenen' van processortijd, is niet te tolereren.

2. Alle informatie moet vrij beschikbaar zijn

Dit is voor veel hackers uit de jaren '60 het primaire principe. Volgens dit principe moet informatie zonder censuur, zonder kosten en zonder controle beschikbaar zijn. Door alle informatie vrij beschikbaar te hebben, zouden hackers (maar eigenlijk iedereen) de mogelijkheid hebben om de wereld te verbeteren en problemen op te lossen.

Het is een moralistisch mooi principe, maar ook erg naïef. Het kan immers niet zo zijn dat bepaalde informatie voor iedereen beschikbaar is. Hierbij denk ik aan informatie welke de veiligheid van burgers (onnodig) in gedrang brengt of de privacy van personen schaadt. Denk hierbij aan terrorisme informatie, informatie uit een gerechtelijk onderzoek of het hacken van b.v. emailaccounts. Als zulke informatie publiekelijk beschikbaar zou zijn, kan deze informatie ook in verkeerde handen vallen.

Zo is er in het verleden bekend geworden dat een aantal landen (kern)wapens konden ontwikkelen m.b.v. informatie van derden. Wanneer deze informatie niet beschikbaar zou zijn geweest, was het maken van deze wapens een stuk lastiger geweest.

Hackers zweren bij open-source programmatuur wat uiteraard ook geënt is op dit principe. Open-source software heeft in mijn ogen voor- en nadelen. Aan de ene kant biedt open-source de mogelijkheid om de kwaliteit van software te verbeteren aangezien meer mensen de software kunnen aanpassen, aan de andere kant is een dergelijke aanpak voor bedrijven ondoorzichtig en is de garantie niet altijd geweldig te noemen.

Bovenstaande voorbeelden geven aan dat dit een zeer naïef principe was, een principe waar ik niet geheel achter sta. Uit de oude code blijkt dat hackers het ethisch vinden om in te breken in (digitale) werkruimtes om deze informatie te achter halen. Ik ben het daar niet mee eens.

Bepaalde informatie is (en niet ten onrechte) auteursrechtelijk beschermd, waarmee in dit geval (op wettelijk en ethisch niveau) de privacy van deze persoon wordt geschaad.

Zo wordt het hacken van een emailaccount van b.v. een officier van justitie door hackers goedgekeurd, voor mij is het een inbreuk op de privacy.

Het is interessant om te zien dat in de ethische code van de jaren '90 het privacy-aspect wel wordt genoemd.

3. *Hackers moeten beoordeeld worden op hun activiteiten, niet op aanzien*

Hier ben ik het compleet mee eens. Mensen mogen niet bevooroordeeld zijn en alleen kijken naar b.v. titels en geslacht, maar moeten naar de kwaliteiten van een persoon kijken. Ik vind dit niet alleen een waarheid uit de hackers gemeenschap, maar ook in het 'normale' leven. Er zou een betere samenleving bestaan wanneer men mensen meer op waarde zouden schatten.

'90 hacker ethiek

De hackers uit de jaren 90 hebben andere ethische codes. Deels gebaseerd op de oude codes, deels gebaseerd op een meer realistische blik op de wereld. Het is echter ook zo dat een aantal van de codes elkaar tegenspreken. Dit komt hoofdzakelijk omdat de hacker gemeenschap veel diverser is dan in de jaren '60, waardoor er meerdere stromingen zijn ontstaan.

1. *Zorg ervoor dat data/apparatuur niet beschadigd raakt*

Dit eerste principe uit de nieuwe code is interessant. Vond men in de jaren '60 dat iedereen overal bij moest kunnen ('against all costs'), nu vinden hackers dat er niets beschadigd mag raken tijdens het hacken. Waar echter veel hackers zich achter verschuilen is het feit dat als er toch iets verkeerd gaat, men de *intentie* heeft gehad om niets kapot te maken. De eigenaar van deze data / apparatuur heeft hier echter niets aan, en loopt (financiële) schade op!

Daarom lijkt dit in 1^e instantie wel een goed principe, echter er wordt geen rekening gehouden met de (eventuele) gevolgen van de eigenaar. Dit principe zorgt er nu niet voor dat ik het ineens goed vind als een hacker inbreekt op mijn computer, laat staan bij een bedrijf. (Waar de risico's veel groter zijn)

2. *Bescherm de privacy*

Zoals hierboven al genoemd, wordt de privacy wel genoemd in de nieuwe ethiek. Hieruit spreekt een meer realistische blik. Ik ben het hier dan ook helemaal mee eens. De privacy van (rechts)personen is een belangrijk recht, wat ook zeer zeker geldt op dit gebied.

3. *Gebruik 'ongebruikte middelen'*

Hackers vinden het ethisch verantwoord om b.v. hardware van derden te gebruiken als deze het toch niet gebruiken. Dit is te vergelijken met het 'joy riding' principe. Niemand vindt het echter leuk als zijn/haar auto wordt "geleend" zonder toestemming, waardoor het aan gevaar wordt bloot gesteld. Nog zwaarder aangezet: iedereen zou er schande van spreken als dit hem of haar zou overkomen. Daarbij is het ook wettelijk verboden om andermans spullen te gebruiken zonder toestemming. Dit is, naar mijn inzien, niet ten onrechte. Ik ben het dan ook compleet oneens met deze ethische norm.

Wanneer ik thuis een computer heb staan, mag iemand deze alleen gebruiken mits ik daarvoor toestemming geef. Het argument "maar niemand weet ervan" is compleet belachelijk. Net alsof het stelen van eigendom, want zo zie ik het, goed gepraat kan worden wanneer de eigenaar er niets van weet.

4. *Laat geen bewijzen achter*

Een hacker mag geen bewijzen achterlaten dat hij/zij iets heeft gehackt. Dit om zo zichzelf en andere hackers te beschermen. Dit is op zijn zachts gezegd vreemd. Immers, volgens een ander principe wil men m.b.v. hacken software beter c.q. veiliger maken. Deze twee principes spreken elkaar dan ook tegen omdat volgens deze regel men een succesvolle hack niet bekend mag maken om zo ook andere hackers ervan te laten profiteren. Dit terwijl het dan juist wel bekend gemaakt moet worden om de bedrijven er ook van te laten profiteren.

Ter illustratie: een hacker ontdekt een lek in Windows. Voordat hij / zij een de bel trekt bij Microsoft, wordt er eerst van dit lek geprofiteerd. Het zou moreel meer verantwoord zijn om dit als hacker meteen te melden aan Microsoft. Dit lijkt mij ook meer in het verlengde liggen van de '60 ethische code.

5. *Door te hacken helpt men de beveiliging te verbeteren*

Dit vind ik nu een erg goed initiatief! Aangezien computersystemen tegenwoordig aangesloten zijn op het internet, is ieder systeem een potentieel doelwit van cyber inbrekers. Verder zijn bedrijven tegenwoordig zeer afhankelijk van de ICT.

Omdat een hacker zeer veel technische kennis heeft is het niet slecht om deze kennis in dienst te stellen van bedrijven om zo de beveiliging van de ICT beter te maken. Echter, waarom moet dit dan vanuit de 'underground'? Hackers proberen in te breken waarbij er een risico bestaat dat er iets misgaat bij deze bedrijven (verwijderde data, het niet kunnen gebruiken van van diensten, etc). Dit kost erg veel geld, wat op niemand te verhalen is. Zo vinden hackers dat ze een bank een dienst bewijzen als ze kunnen inbreken op een applicatie en kunnen rommelen met b.v. geldtransacties. Wie betaalt echter de kosten?

Ik ben dan ook van mening dat hackers hun kennis in dienst mogen (en misschien zelf moeten) stellen van bedrijven, maar dat dit dan van te voren aangekondigd c.q. regelt moet zijn. Er zijn gevallen bekend van hackers welke in dienst zijn getreden bij bedrijven om daar de beveiliging te verbeteren. Dit lijkt mij een veel betere en moreel meer verantwoorde oplossing.

Conclusie

Hierboven zijn een aantal ethische codes beschreven. In de jaren '60 waren deze, naar mijn inzien, vooral naïef. In de jaren '90 werd er meer rekening gehouden met de moderne samenleving (minder naïef) maar werden principes als 'joy riding' goedgekeurd.

Beide codes hebben daardoor goede, maar ook slechte kanten. Zo vind ik vooral bij de '90 code het verbeteren van de beveiliging van software een erg goed steven, maar keur ik het 'joy riding' compleet af. Daarnaast vind ik dat hackers steeds minder vanuit de 'underground' moeten gaan opereren. Het reguleren van de zeer nuttige en specialistische kennis, waardoor de ICT alleen maar beter kan worden, moet beter gecontroleerd en begeleid worden. Het argument van de hackers dat ze dan niet goed meer kunnen functioneren vind ik niet sterk genoeg tegenover alle voordelen en de risico's welke de samenleving nu loopt ten opzichte van de hacking activiteiten.

Zoals ik in de introductie al aangaf wordt er met gemengde gevoelens over hackers gedacht. Na een aantal ethische principes te hebben genoemd, vind ik dat deze bewering ook terecht is. Het is nu eenmaal niet gewenst (in mijn ogen) om andermans eigendommen te 'lenen', (ongewenst) in te breken op systemen en gevoelige informatie openbaar te maken.