De ethiek van de hacker

Koops, E.J.

Published in:
Informatie : Maandblad voor de Informatievoorziening

Publication date:
2000

Koops, B.J. (2000). De ethiek van de hacker. Verschenen in *Informatie : Maandblad voor de Informatievoorziening, 42*(april), 62-63

De ethiek van de hacker

Dr. Bert-Jaap Koops

De recente stroom aanvallen op weblocaties van Yahoo!, Amazon, CNN, eBay en vele anderen heeft veel verontwaardiging gewekt, niet alleen bij bedrijven die zich op de e-handel hebben gestort, maar ook – paradoxaal genoeg – bij hackers. Het waren immers geen intelligente inbraken door nobele hackers, maar na-aapaanvallen door 'script kiddies'. De aanvallers braken niet in om beveiligingsgaten aan te tonen, ze blokkeerden alleen de toegang tot de weblocaties door slim gebruik van protocollen die ze elders op het net hadden gevonden. Schande!, zegt een hacker-commentator. "Script kiddies download ready-made tools and use them to damage the network. Script kiddies criminally distort the essential ethos of hacking, which is to pass through the network without a trace." Wat zou dat zijn, de 'essential ethos of hacking'?

In de begindagen van de computer, de jaren vijftig, zestig en zeventig van de vorige eeuw, bestond computercriminaliteit eigenlijk nog niet. Er waren wat exotische gevallen van misbruik van mainframe-computers, die voornamelijk bij grote bedrijven, universiteiten en veiligheidsdiensten in gebruik waren. Met het verschijnen van microcomputers begin jaren tachtig, kwamen er meer mogelijkheden voor misbruik.
Maar voor de eerste generatie "computermisdadigers" golden de meeste activiteiten niet als misbruik. Integendeel, het aanvallen van computers en het vinden van beveiligingsgaten werkte juist statusverhogend. Computergebruikers noemden zich "hackers", omdat ze met velen tegelijk op computercodes "inhakten" om er alle fouten uit te halen. Het woord "hacker" was een compliment, en de hackers hadden een gezamenlijke ethiek die hun (computer)wereldbeeld uitdrukte. Steven Levy reconstrueerde deze ethiek als volgt.

1. De toegang tot computers moet onbeperkt en volledig zijn.
2. Alle informatie moet vrij beschikbaar zijn.
3. Wantrouw autoriteit en bevorder decentraliteit.
4. Hackers worden beoordeeld op hun activiteiten, niet op diploma's, leeftijd of positie.
5. Kunst en schoonheid zijn maakbaar met computers.
6. Computers kunnen je leven verbeteren.

Vooral de eerste drie, diep gewortelde, geloofsartikelen van de hacker-ethiek hebben hun stempel gezet op de geschiedenis van de computercriminaliteit.
In de jaren tachtig drong in de maatschappij geleidelijk het besef door dat aanvallen op de beschikbaarheid, vertrouwelijkheid en deugdelijkheid van computers en informatie (de BVD van informatiebeveiliging) bedreigend konden zijn voor de economie of voor de rechtsorde, nu steeds meer bedrijven en overheden afhankelijk werden van computers. Daarom voerden staten overal ter wereld Wetten computercriminaliteit in, waarin computerfraude, computersabotage, hacken, virusverspreiding en softwarepiraterij strafbaar werden gesteld.

Desondanks leefde in de hackerwereld de aloude ethiek voort, en jeugdige whizzkids bleven hacken meer als sport zien dan als misdaad.
De bekendste hackers van de jaren tachtig, Kevin Mitnick, Kevin Poulsen en Justin Petersen, begonnen als sporters en eindigden in de gevangenis. In een recent interview met Hélène Schilders blikte Poulsen terug op zijn activiteiten. "Oorspronkelijk waren hackers mensen die de computerruimtes van universiteiten en bedrijven binnenslopen om op de machines te leren werken. Gebrek aan respect voor autoriteit hoorde bij die cultuur. (…) Er circuleerde een manifest over jongeren die de macht terugnamen van 'de pakken'. Het ging ons om esthetiek en leren, niet om winst. Voordat ik radiostations ging hacken, heb ik er nooit een cent aan verdiend." Wat als sport begon, veranderde in fraude toen Poulsen op de vlucht sloeg toen hij aangeklaagd werd voor spionage: hij verdiende geld met radiospelletjes door het telefoonnetwerk te kraken. Ook Justin Petersen ging het verkeerde pad op: hij hackte banken en kredietkaartmaatschappijen en maakte geld over naar eigen rekeningen.
De virtuele klopjachten uit de begin jaren negentig op hackhelden als Mitnick en Poulsen, die tot jarenlange gevangenisstraffen werden veroordeeld, leidden tot grootscheepse protesten en morele-steunacties op het Internet. Want hoewel ze traditionele misdaden als fraude hadden gepleegd, hadden ze een onaantastbare status als Robin Hoods van de elektronische snelweg.
Je zou verwachten dat de oude hacker-ethiek geleidelijk aan uitsterft, nu de Wetten computercriminaliteit al jarenlang bestaan en ook worden gehandhaafd door diverse veroordelingen van computermisdadigers. Bij de aanvallen op vele weblocaties in februari bleek dat echter nog lang niet het geval te zijn. Tekenend is een commentaar in *The Village Voice* van Richard Thieme. "Let's get our definitions straight. Last week's attacks on dozens of Web sites were not the work of hackers. They were the work of script kiddies, and the difference is everything." Immers, hackers zijn een soort nobele wilden, die door hun inventieve en creatieve aanvallen het Internet hebben grootgemaakt. Hackers hebben de 'open source'-beweging ingezet. Hackers dwingen Microsoft om beveiligingsgaten te dichten. Kortom, aldus Thieme, "when we lump all hackers into a criminal class we are liable to forget their essential role as architects of the information age". Hackers hebben in deze visie een hoogstaand moreel besef, zij het dat deze wat afwijkt van dat van de meeste overheden. Nu kan dat morele besef van de "nobele hacker" nog zo hoogstaand zijn, er schuilt wel een levensgroot gevaar in. De sprong van goede bedoelingen naar kwade gevolgen is licht gemaakt, en wie zo'n sterke eigen ethiek heeft, loopt het risico de basisnormen van de maatschappij terzijde te schuiven ten gunste van vermeende "hogere doelstellingen" waar de maatschappij niet op zit te wachten. Bovendien zet het de deur open voor een andere soort hackers, die niet doordrenkt is van de klassieke hacker-ethiek, maar één die willens en wetens strafbare feiten pleegt.
In de praktijk worden de meeste vormen van computercriminaliteit namelijk gepleegd, niet door whizzkidachtige binnendringers, maar door ingewijden die van binnenuit aanvallen plegen op computers en gegevens. Sommige werknemers sprokkelen een kapitaaltje bijeen door salamitechnieken (het afromen van saldo's achter de komma), anderen persen hun (ex-)baas af door een logische bom in het systeem achter te laten die alleen zijzelf onschadelijk

konden maken. De jongere garde van deze soort, die is opgegroeid met de computer en met het Internet, verkent gretig de mogelijkheden om daar beter van te worden, in het volle besef dat hun activiteiten bij wet al lang verboden zijn. Virussen worden steeds venijniger en worden ingezet om geïnfecteerden af te persen. Hackers dringen door tot de diepste geheimen van bedrijven en overheden, met de bedoeling de geheimen te verkopen of om losgeld voor te vragen. Deze immorele garde heeft de "ethiek" van de no-nonsense jaren tachtig: de kans dat ze mij pakken is miniem, dus waarom zou ik er niet van profiteren?

Binnenkort dient zich een nieuwe soort computercriminelen aan, die moreel noch immoreel is, maar amoreel. Deze generatie zit niet meer achter de computer, naarstig op zoek naar een gat in de beveiliging, al dan niet uit nobele overwegingen. Deze generatie gaat zelf op pad, de elektronische snelweg op. Hij vliegt door de infrastructuur, onderzoekt wat hij tegenkomt, onderhandelt, copieert en gaat weer terug. Het zijn knowbots, slimme programmaatjes die zelfstandig taken uitvoeren op de elektronische snelweg. Ze worden op dit moment ontwikkeld, vooralsnog vooral voor nuttige zaken als het samenstellen van je persoonlijke ochtendkrant, het vinden en kopen van de goedkoopste cd naar jouw smaak, en voor het uitventen van de informatie die je graag wilt verkopen.
Maar knowbots hebben geen moreel besef, ze hebben geen gevoel voor mijn en dijn. Niets hoeft een knowbot ervan te weerhouden een illegaal gecopieerde cd te kopen, of van een collega een gehackt bedrijfsgeheim te kopen voor de ochtendkrant, of via openstaande poorten een kijkje te nemen op vaste schijven van nietsvermoedende Internetgebruikers. De nieuwe garde kent niet de klassieke hacker-ethiek van de eerste soort hackers, noch het no-nonsense-gedachtegoed van de tweede soort. Wie of wat belet hen straks om van het Internet een onderwereld te maken?

Bronnen

Steven Levy, *Hackers: Heroes of the Computer Revolution*, New York: Doubleday 1984

Perri 6, *Morals for robots and cyborgs: ehtics, society and public policy in the age of autonomous intelligent machines*, Bull 1999, verkrijgbaar via WWW <http://www.bull.co.uk>

Hélène Schilders, 'Wanted Hackers. Bericht uit de computerunderground', *Volkskrant Magazine*, 4 maart 2000

Richard Thieme, 'Hacking the Future: Why Code Crackers Will Lead the Digital Age', *The Village Voice*, 16-22 februari 2000, WWW
<http://www.villagevoice.com/issues/0007/thieme.shtml>

Dr. Bert-Jaap Koops is senior-onderzoeker bij Centrum voor Recht, Bestuur en Informatisering van de Katholieke Universiteit Brabant.