1. Intro
De dure lessen van @XS4me2all

4 juni 2014. Frank Brokken, Security Manager van de Rijksuniversiteit Groningen betreedt het prestigieuze World Forum in Den Haag. Het is de tweede dag van de Nationale Cyber Security Conferentie, met meer dan duizend experts van over de hele wereld. Er zijn veel kopstukken: hoofd Algemene Inlichtingen- en Veiligheidsdienst, hoofd Nationaal Cyber Security Centrum, de minister van Veiligheid en Justitie, hoogleraren en directeuren van grote bedrijven. Team High Tech Crime van de Nederlandse politie loopt ook rond. Zelfs de FBI is er. De beveiliging is dan ook flink opgeschroefd. Maar Brokken komt niet voor de grote namen. Hij is hier om de jongen te ontmoeten die zeven jaar geleden zijn universiteit heeft gehackt.

Ik zie Brokken wat verloren om zich heen kijken als ik hem bij de ingang tref te midden van alle mannen in pakken. Overal worden ID's gecheckt, handen geschud en druk gepraat. Met zijn grote, grijze snor en haar dat alle kanten op staat, valt hij direct op in de menigte. Ik begroet hem en probeer hem op zijn gemak te stellen. Brokken kijkt vooral om zich heen, op zoek naar zijn hacker. Die is er nog niet, maar zal straks tevoorschijn komen. We gaan namelijk hun ontmoeting filmen in een studio die we hebben ingericht bij de ingang van de conferentie. En als het item slaagt, zal de wereld te weten komen wie schuilgaat achter het Twitterpseudoniem @XS4me2all, ook wel de RUG-hacker.

Hoe kan het dat deze hacker hier, te midden van al die handhavers, zomaar wil vertellen wat hij de universiteit heeft aangedaan? De schade was immers aanzienlijk: alle servers en 250 computers besmet met malware, 100.000 euro aan herstelkosten en flink wat negatieve publiciteit. Hij zou opgepakt kunnen worden en in de bak belanden. Dat zal ook niet zijn eerste keer zijn, want hij heeft al eens eerder in de cel gezeten voor een andere hack. Toch wil hij hier schuld bekennen en zijn geweten schonen. Hij weet ook dat Brokken geen wrok voelt. Sterker nog, de security manager heeft in de media gezegd dat hij het een knappe hack vond en zijn organisatie ervan geleerd heeft. Sindsdien neemt het universiteitsbestuur security serieus. Brokken heeft me dan ook beloofd geen aangifte te doen. Daarom durft @XS4me2all hier voor de camera zijn verhaal te gaan vertellen.

Het is alweer meer dan een jaar geleden dat ik deze hacker ontmoette. Ik was toen net begonnen met het onderzoek voor dit boek. Hij is, zoals dat heet, een penetratietester: iemand die onderzoekt of hij in een digitaal systeem kan komen, in opdracht van de eigenaar van dat systeem om zo de beveiliging te testen. Dat doet hij ook in zijn vrije tijd. Soms pakt hij willekeurig een site, maar meestal krijgt hij tips uit de hacker community. Als hij ergens in kan, gaat hij niet verder - zoals destijds met de universiteit Groningen - maar meldt hij het netjes aan de beheerder van de site. Als het lek gedicht is, brengt hij het verhaal naar buiten. Zo kunnen anderen ook leren van de beveiligingsproblemen. 'Responsible disclosure' heet dit in het jargon, oftewel verantwoorde onthulling.

De hacker had wel een paar verantwoorde onthullingen voor me die al uitgebreid in de media verschenen waren. Maar er was ook nog een zaak die nog niet onthuld was: de Rijksuniversiteit Groningen. We spreken af dat ik hem interview, zijn verhaal opschrijf, dat check met hem en het vervolgens voorleg aan de universiteit. Niet onder zijn echte naam, maar onder een pseudoniem, want het zou nog wel eens uit de hand kunnen lopen. Ik maak daarom voor hem het Twitteraccount @XS4me2all aan, zodat hij van daaruit ook kan reageren op de zaak. Pas als de universiteit officieel verklaart geen aangifte te doen, zullen we bekend maken wie erachter zit.

@XS4me2all woont dan nog in een studentenkamer, een soort barakkencomplex aan de rand van Amsterdam. Hij verontschuldigt zich dat hij zich als penetratietester inmiddels wel wat beters kan veroorloven. Binnenkort verhuist hij naar een echt appartement, maar voor nu zitten we nog in hetzelfde kleine, donkere rommelhok van waaruit destijds de hack heeft plaatsgevonden. Ik zie hier en daar wat rondslingerende computerhandleidingen. Midden op tafel ligt een stapel papier van een halve meter hoog: zijn strafdossier. Hij is namelijk in 2008 veroordeeld tot achttien dagen cel vanwege computervredebreuk en deelname aan een criminele organisatie. Daarover later meer. Eerst de RUG-hack van februari 2007.

@XS4me2all is dan nog een jongen van twintig. Formeel is hij nog student, maar niet aan de Rijksuniversiteit Groningen. Eigenlijk doet hij niets meer aan zijn studie, omdat hij dagelijks tot in de late uurtjes het internet afstruint, op zoek naar nieuwe hackmethoden en steeds grotere targets. Gewoon, voor de kick. Bovendien leert hij zo veel meer dan bij zijn studie. Universiteiten zijn voor hem vooral interessant om te hacken, want die hebben een snelle internetverbinding die je dan zelf kunt gebruiken. Zo kwam hij bij Groningen uit.

Het eerste wat hij aantrof op het universiteitsnetwerk was een printserver die online stond. Het wachtwoord was versleuteld, maar hij kon wel de hash van het wachtwoord zien, oftewel de uitkomst van de versleuteling. Op internet circuleren allerlei lijstjes - rainbow tables - van dergelijke hashes waarmee je het versleutelde wachtwoord weer kunt terughalen. En ja, hij vond een match: het wachtwoord bleek 'S4k1nt0s!' te zijn. Als gebruikersnaam nam hij 'admin', want zo heten de meeste systeembeheerders en die hebben de hoogste toegangsrechten. En jawel, hij kon inloggen op de server. Even kijken of deze admin nog meer online heeft staan. Dat bleek het geval. Hij kon niet meteen overal in, want deze beheerder kon alleen in servers van zijn eigen studierichting.

De hacker herhaalde de truc met de hashes en rainbow table bij andere systemen en ontdekte dat sommige admins konden inloggen bij verschillende studierichtingen. Via die overlap kon hij makkelijker overstappen van de ene studierichting naar de andere. Hij zag ook dat ze allemaal een ConsoleOne van Novell gebruikten om het systeem te beheren en ook die stond online. Deze gebruikten de systeembeheerders om vanaf één locatie alle systemen te kunnen updaten. En zo ook @XS4me2all. Via de beheerdersingang, poort 1761 van de console, kon hij nu vanaf zijn studentkamer op het hele netwerk van de Rijksuniversiteit Groningen.

Toch ging het hem niet snel genoeg. Om niet elke server en computer afzonderlijk te hacken, had hij een ander plan bedacht. Hij nam de image en install server. Die server is normaal gesproken een hulpmiddel voor systeembeheerders om via het netwerk back-ups of updates te laden. Als een medewerker dan inlogt vanaf zijn computer, hoeft hij dat niet zelf te doen, maar gaat dat automatisch. Daar installeerde de hacker zijn eigen malware. Iedereen die nu inlogde, besmette zichzelf. Zo had hij binnen een maand toegang tot alles. Op een enkele computer zette hij ook wat malware die leek op een keylogger, gewoon om te zien of het kon, zonder hem te gebruiken want hij kon toch al overal in. Het leukste vond hij de Wake-on LAN functie, waarmee hij op afstand computers aan kon zetten. Dat deed hij dan 's nachts. "Stel je voor, is daar zo'n schoonmaker aan het werk, gaan ineens alle computers aan… Kicken!"

Daarmee was zijn missie geslaagd. Het ging hem er niet om de universiteit schade toe te brengen. Het was puur de kick om ergens in te komen. Vol enthousiasme vertelt hij erover aan andere hackers op een gesloten chatforum waar hij lid van was. Die geloven hem niet en willen bewijs zien. Dat kan: "Geef mij een film en dan laat ik die vanaf hun server draaien." Zo blijft hij nog een tijdje spelen met het netwerk, maar raakt gaandeweg verveeld. @XS4me2all heeft zijn doel immers bereikt. Totdat hij ineens ongekende activiteiten ziet op het netwerk: passwords worden gereset, firewalls opgetrokken… Shit, gesnapt. Nu uitloggen en wegwezen.

Terwijl hij de zaak eigenlijk wil vergeten, leest hij erover in de media. Op 7 maart komt RUG-woordvoerder Jos Speekman namelijk via het ANP naar buiten met het bericht dat de computers van de universiteit gehackt zijn. Op de getroffen systemen zou software geïnstalleerd zijn, waarmee cybercriminelen persoonlijke informatie kunnen stelen, zoals wachtwoorden en creditcardgegevens. Ze zouden de computers bovendien op afstand kunnen bedienen, bijvoorbeeld om illegaal content te verspreiden of spam te versturen. De universiteit vermoedt dat de computers van binnenuit door een medewerker of student zijn gekraakt. De schade wordt geschat op 100.000 euro.

Het bericht wordt overgenomen door de Volkskrant, Trouw, NU.nl, Webwereld en security.nl en komt zo ook terecht bij @XS4me2all. Hij schrikt zich rot. Hij was helemaal geen creditcardgegevens aan het stelen en die illegale content, dat waren maar een paar video's. Tot zijn verbazing ziet hij op fok.nl ook een video van Studenten TV, met daarin een interview met iemand die zich voordoet als de RUG-hacker. Dat vindt hij minder leuk: "Staat er zo'n gozer in het donker met vervormde stem… Die zei echt onzin en maakte het probleem veel groter dan het daadwerkelijk was."

In de berichtgeving leest hij ook over security manager Frank Brokken, die openlijk vertelt over het incident en zelfs zegt dat ze er veel van geleerd hebben. Deze Brokken lijkt hem wel een sympathieke man. Liefst had hij zelf met hem willen praten, om te vertellen wat hij heeft gedaan en waarom. Maar uit angst voor represailles wil hij liever niet naar buiten komen en probeert hij de zaak

te vergeten. Totdat hij in 2013 mij ontmoet. Zijn geweten knaagt; hij wil schoon schip maken. Ik zie een mooi verhaal voor mijn boek en stel voor te bemiddelen tussen beiden.

Frank Brokken werkt nog steeds bij de universiteit. In een e-mail aan hem vertel ik over mijn onderzoek en vraag ik hem om meer documentatie. Ik stel ook voor een ontmoeting te arrangeren tussen hem en de hacker, mits de universiteit afziet van strafvervolging. Hij reageert positief: “In het delen van ervaringen ben ik altijd geïnteresseerd, ik zie geen reden om op het bekendmaken van een kwetsbaarheid te reageren met juridische acties. De hacker hoeft wat dat betreft niet bevreesd te zijn en kan denk ik zelfs wel rekenen op een kopje koffie. ;-)” Zijn mail is gesigneerd met PGP, een ‘pretty good privacy’ code die aangeeft dat de mail echt van deze persoon is. Ik weet dan nog niet wat dat is en begrijp ook niets van al die codes onderin zijn mail, maar voor @XS4me2all is dit voldoende als vrijwaring. We kunnen van start.

Als ik Brokken telefonisch interview, merk ik geen wrok of frustratie van zijn kant, maar eerder bewondering voor hetgeen de hacker heeft gedaan. “Ik vind het geweldig dat die jongen het op deze manier heeft gedaan. Als jij toegang hebt tot de server die software installeert op andere machines, wordt het werk door de organisatie gedaan. Dat is prachtig.” Brokken moet zelfs hartelijk lachen als ik vertel hoe ’s nachts de computers werden aangezet en rakelt nog wat anekdotes op van grappige hacks uit zijn eigen jonge jaren: “In die jaren werkten we nog met mainframe computers, was allemaal erg nieuw. Toen toverde iemand een alziend oog op iemand anders zijn scherm en die schrok zich rot.” Hij moet er nog om lachen.

Dit lijkt me iemand die wel begrip heeft voor de hacker en ik nodig hem daarom uit voor een ontmoeting tijdens het NCSC-congres in het World Forum. Brokken wil hiervoor best uit Groningen naar Den Haag komen. @XS4me2all is echter minder blij met de setting: “Op de NCSC conferentie? Dan loop ik daar weer als die foute hacker rond. Heb je niet een iets kleinschaliger evenement? ;-)” Daar kan ik me wel iets bij voorstellen, want er zullen ook veel klanten van hem zijn. Ik stel voor dat we de ontmoeting doen zonder publiek, maar wel met camera. Zo hebben hij, Brokken en ik alsnog de keuze de onthulling al of niet publiek te maken. Dan is het goed.

Daar sta ik dus op 4 juni met de security manager. Lichten aan, geluid aan, camera draait. Wat hij niet weet, is dat @XS4me2all zich verhult als een van de cameramannen en dus meekijkt. We doen het in het Engels, want het is een internationale conferentie en we willen de buitenlanders graag laten zien hoe we hier in Nederland omgaan met responsible disclosure. Ik had hem vooraf verzekerd dat we elk moment de opname stil kunnen leggen als hij iets over zou willen doen, maar met alle gemak vertelt hij zijn verhaal: over de e-mail waarin verteld werd dat ze gehackt waren, de install server die het werk voor hem deed en waarom het belangrijk was het nieuws naar buiten te brengen.

“You are now to meet the guy who hacked your university”, roep ik zo gewichtig mogelijk. @XS4me2all komt achter de camera vandaan en geeft Brokken een hand. “So you are the bad guy?”, zegt Brokken. “Yes, I am the bad guy”, antwoordt de jongen lachend. De rest van het gesprek verloopt vanzelf. De hacker legt uit wat hij heeft gedaan en de security manager valt van de ene verbazing in de andere. @XS4me2all vertelt ook dat hij meerdere universiteiten had gehackt, maar de RUG de enige was die er openlijk over berichtte. Daarom wilde hij deze ontmoeting. Brokken besluit: “If you are open, you can turn something bad into something good.”

De camera’s gaan uit, terwijl beide heren nog druk blijven doorpraten. En als ik alweer met het volgende item bezig ben, zie ik de twee in de verte gebroederlijk naast elkaar weglopen.

Hacken betekent letterlijk het inbreken in een informatiesysteem. Je zou kunnen zeggen dat er al wordt gehackt zolang er computers zijn, maar de historische werkelijkheid is omgekeerd. We danken het hele idee van een computer aan een beroemde hacker: Alan Turing. Tijdens de Tweede Wereldoorlog wist hij de enigmacode te kraken waarmee de Duitsers hun communicatie versleutelden. Zijn ‘turingmachine’ stond model voor de eerste computers die daarna werden gebouwd. Geen van deze informatiesystemen zal ooit 100% veilig zijn, want er sluipen altijd wel fouten in waardoor ze kwetsbaar zijn voor inbraken. Om die op te sporen, zijn hackers nodig.

Goede en slechte hackers worden ook wel aangeduid als white hat en black hat hackers, ontleend aan de hoeden van de goodguys en badguys uit oude cowboyfilms. In de wereld van de cyber security zit er echter veel grijs tussen. Het voorbeeld van de RUG laat zien dat zelfs een hacker die

toch werkelijk te ver is gegaan, iets positiefs kan bereiken. Dankzij @XS4me2all heeft de universiteit gezien hoe slecht hun beveiliging was en die vervolgens op orde gebracht voor het geval er een echte kwaadwillende zou willen binnendringen in hun systeem. De meeste ethisch hackers die ik heb gesproken voor dit boek hebben geen strafblad, maar zijn wel vaak net langs de rand gegaan. De kunst bij verantwoorde onthullingen is net over die rand heen te kijken, de eigenaar op tijd vertellen wat je hebt gezien, zonder het aan te raken, ook al is de verleiding nog zo groot.

De hackers in dit verhaal hebben juist een bijzonder verantwoordelijkheidsgevoel en willen anderen helpen beveiligingsproblemen op te lossen om zo de criminele hackers voor te zijn. Ze zijn meestal rond de twintig, bijzonder intelligent en denken op net een andere manier dan anderen. Ze zien aan een site, app of andere technologie iets dat niet klopt en wat de maker en beheerder niet hebben gezien. Uit nieuwsgierigheid gaan ze door waar anderen zouden stoppen. Ze krijgen een kick uit het oplossen van de puzzel en willen laten zien dat het hen is gelukt. Daarom zetten zij zich kosteloos in om de onlinewereld veiliger te maken, maar riskeren ze om, net als @XS4me2all, opgepakt te worden voor computervredebreuk.

Hoe zou jij reageren als je een anoniem e-mailtje of telefoontje krijgt van iemand die zegt dat je site lek is, hij zou kunnen frauderen met je betaalsysteem of dat hij met zijn zelfgemaakte toegangspasje zo je gebouw binnen kan lopen? Neem je zo iemand meteen serieus? Doe je iets met het ongevraagd advies? Wil je dat eigenlijk wel, of vind je dat je eigenlijk wel wat beters te doen hebt? Gelukkig zijn er steeds meer organisaties die beleid hebben, zodat hackers hun vondsten op een verantwoorde manier kunnen onthullen. Maar de praktijk is weerbarstig. Een systeembeheerder krijgt een melding vlak voor zijn vakantie en laat die liggen voor later. Een manager die al tot over zijn oren in het werk zit, schuift de melding door naar de juridische afdeling, die er vervolgens een advocaat op afstuurt. Of wat te denken van een helpdeskmedewerkster die blijft beweren dat de site toch echt wel veilig is omdat ze dat nu eenmaal hoort te zeggen tegen verontruste klanten?

Dan gaat het mis, want de meeste ethisch hackers laten het daar niet bij. Uit plichtsbesef, zucht naar erkenning of gewoon pure frustratie, brengen ze het lek vroeg of laat toch naar buiten. Via een chatforum, Twitter, blog of journalist. Ze hadden immers gewaarschuwd. Zo zijn er in de laatste jaren vele onthullingen in de media gekomen: de OV-chipkaart blijkt na te maken, Nederlandse gemalen zijn via internet te besturen, DigiD zo lek als een mandje, patiëntgegevens liggen op straat, defensietop is af te luisteren, betaalapp niet veilig… Het lijkt wel of tegenwoordig alles te hacken is en niemand er wat aan doet.

Journalisten, politici, juristen en publiek zijn dol op deze verhalen, want achter het gevonden lek schuilt een organisatie die de boel niet goed op orde heeft. Al snel worden schuldigen aangewezen en ter verantwoording geroepen, wat soms leidt tot Kamervragen of rechtszaken. Intussen gaan andere hackers op Twitter en andere fora helemaal los op het slachtoffer. Dat is jammer, want met een beetje meer wederzijds begrip had de getroffen organisatie juist kunnen profiteren van het gratis advies en had de hacker de credits kunnen krijgen voor zijn vrijwilligerswerk.

Daarom dit boek: om ethisch hackers, systeembeheerders, managers en helpdeskmedewerkers inzicht te geven in elkaars belevingswerelden. Het is ook bedoeld voor de politici, juristen en journalisten die over hen oordelen. En omdat het vaak gaat om grote hoeveelheden persoonsgegevens, is dit verhaal eigenlijk voor iedereen, want het kan ook jou overkomen dat je gegevens op straat komen te liggen. We zijn met z'n allen inmiddels zo afhankelijk geworden van informatietechnologie, dat het goed is om te weten wat deze technologie doet met onze gegevens. Dat leer je nog het beste wanneer het mis gaat, maar het is ook goed om te weten dat er door veel mensen hard aan wordt gewerkt dat het wel goed gaat. Cyber security is misschien wel erg technisch, maar het is vooral ook mensenwerk.

In elk hoofdstuk behandel ik een zaak waarin een hacker een kwetsbaarheid vindt en naar buiten brengt, met alle gevolgen van dien. Ik heb deze zaken vooral geselecteerd op diversiteit: in technologieën, hackmethoden, type organisaties en het verloop van de onthullingen. Een ideaalbeeld van hoe het zou moeten, hebben we inmiddels wel: een hacker vindt een lek, meldt dat bij de systeembeheerder en het wordt gerepareerd. In de praktijk zijn er echter vaak meerdere lekken, gaan tips van de een naar de ander, is niet duidelijk wie eigenlijk verantwoordelijk is voor het systeem en is de uitkomst vaak een toevallige samenloop van omstandigheden. Toch zijn er in al die toeval en diversiteit patronen te herkennen, omdat mensen nu eenmaal doen wat ze gewend zijn te doen. Die patronen wil ik met dit boek laten zien en waar mogelijk doorbreken.

Maar als de perspectieven van die verschillende partijen zo belangrijk zijn voor het verloop van de verschillende zaken, wat is dan het perspectief van dit verhaal? Oftewel, wie of wat zit erachter? Eigenlijk alleen ikzelf: Chris van 't Hof, onderzoeker, presentator, techneut en socioloog. In het verleden heb ik enkele boeken geschreven over de informatiesamenleving. Dat was in opdracht van onderzoeksinstituten, met collega-onderzoekers, een redactie en een uitgever. Dit onderzoek wilde ik zelf doen, juist omdat er zulke uiteenlopende meningen zijn over het onderwerp. Ik wilde deze mensen ontmoeten en hun verhaal opschrijven, zonder een achterliggende agenda of doelgroepenbeleid van een opdrachtgever.

Dat betekent niet dat anderen er geen invloed op hebben gehad. Iedereen die ik heb geïnterviewd, heeft gelegenheid gehad om op de conceptteksten te reageren. Bijna alle cases zijn eerst in verkorte vorm verschenen in het tijdschrift Informatiebeveiliging, waar de redactie feiten en beweringen heeft gecheckt. Conceptteksten zijn ook becommentarieerd door een team van reviewers, die ik in de bijlage beschrijf en uiteraard hartelijk bedank. Ik heb deze teksten ook online gezet op helpendehackers.nl om zo reacties te sorteren. Maar uiteindelijk is het toch mijn verhaal. Daarom is het ook geschreven in de ik-vorm.

Dit verhaal begon met een anonieme hacker, die in 2007 flink over de schreef ging, maar alsnog op het rechte pad kwam. Pas in 2014 kwam hij naar buiten met zijn verhaal. Aan het einde van dit boek kom ik op hem terug. De volgende cases vinden plaats in de periode daartussen, in chronologische volgorde, om zo hun onderlinge samenhang te laten zien. We beginnen met een klassieker: de OV-chipkaart die werd gekraakt door beveiligingsonderzoekers van de Radboud Universiteit. Die zaak bekijken we in drie hoofdstukken vanuit verschillende perspectieven: die van de hackers, de overheid, de bedrijven achter het systeem, de rechterlijke macht en de journalistiek die erover schrijft. Hier verschijnt ook @brenno, oftewel journalist Brenno de Winter, die met een gekraakte OV-chipkaart gaat reizen om aan te tonen hoe makkelijk dat is.

De Winter start vervolgens Lektober, een maand met elke werkdag een melding van een website die persoonsgegevens lekt. Een van de melders is Wouter van Dongen, die met de hack een succesvol bedrijf opzet. Vervolgens gaan we kijken naar de zogenaamde SCADA-systemen, waarbij een lijst IP-adressen van een anonieme hacker leidt tot de onthulling dat de Nederlandse waterhuishouding vanaf internet te besturen is. In deze hoofdstukken zien we ook hoe media digitale kwetsbaarheden zichtbaar maken. Dat is voer voor politici die de regering ter verantwoording willen roepen. We zien hoe bestuurders worstelen met ethische hacks en hoe lastig het is om te bepalen wie uiteindelijk verantwoordelijk is voor digitale veiligheid: iedereen een beetje en daardoor uiteindelijk niemand.

In de hoofdstukken daarna gaan we kijken hoe verschillend organisaties reageren bij meldingen. Zo blijft Defensie redelijk laconiek als @UID_ gaat bellen met hun teleconferentiesysteem. ING reageert nauwelijks als @floorter beweert dat hij hun nieuwe betaalapp zo zou kunnen overnemen, maar gaat het lek wel snel repareren. Marktplaats heeft daarentegen als een van de eersten beleid voor verantwoorde onthullingen en beloont @legosteentje voor zijn melding met een witte hoed en uiteindelijk zelfs een baan. Deze zaken zijn ook in de media gekomen, maar worden nog zonder controverse afgehandeld. In de Tweede Kamer start intussen wel de discussie over hoe we moeten omgaan met ethisch hackers.

Vervolgens krijgen we weer een aantal rechtszaken. De minderjarige @jmschroder laat Habbo Hotel zien hoe hij in hun helpdesk kan inloggen, waarop het bedrijf hierachter aangifte doet van computervredebreuk. Na twee jaar wordt de jonge hacker eindelijk vrijgesproken. De 50PLUS'er Henk Krol wordt wel veroordeeld en krijgt een boete als hij laat zien hoe hij bij de medische dossiers kan van Diagnostiek voor U. Hij was daarbij volgens de rechter net iets te ver gegaan. Dat geldt ook voor de hacker van het Groene Hart Ziekenhuis. Als hij kwetsbaarheden aantoont in het netwerk van het ziekenhuis wordt hij opgepakt, wat leidt tot verontwaardiging in de media en Tweede Kamer. Later blijkt uit het onderzoek van het Openbaar Ministerie dat er veel meer aan de hand was. De laatste rechtszaak is weer voor de Radboud Universiteit. Volkswagen weet met succes hun publicatie over een gekraakt autoslot tegen te houden, dankzij een Engelse rechtbank.

Dan is het tijd voor beleid. Begin 2013 komt het NCSC met een leidraad voor verantwoorde onthullingen en krijgen steeds meer organisaties meldpunten voor helpende hackers. Niettemin blijft hacken strafbaar en zal per geval bekeken moeten worden of er een hoger doel mee gediend is. De

echte helpende hackers weten precies hoe ver ze kunnen gaan en hoe ze beveiligingsproblemen kunnen afhandelen zonder tussenkomst van media, politiek en rechter. Daarom besluiten we met enkele portretten van hen.

@stevenketelaar en @bl4sty hacken een modem en oogsten veel lof als ze dat bij KPN op het hoofdkantoor komen demonstreren. Bij de UvA is ethisch hacken gewoon een vak en worden de studenten begeleid door een ethische commissie van @1sand0s. Een andere student, @iliaselmatani ontdekt dat hij alle studieboeken van Infinitas Uitgeverijen gratis zou kunnen downloaden, maar doet het niet. We gaan samen naar de uitgever voor een goed gesprek. De laatste drie portretten zijn van helpende hackers die vooral achter de schermen opereren. De veteraan @0xDUDE heeft al bijna vierduizend meldingen op zijn naam, zonder ook maar één keer in de problemen te zijn gekomen. Nieuwkomers @rickgeex en @smiegles worden zelfs omarmd door bedrijven en overheden voor hun ethische hacks. Er is inmiddels veel veranderd in het digitale polderlandschap…

De casestudies worden zoveel mogelijk chronologisch behandeld, om zo de onderlinge verbanden te laten zien. We bekijken de gebeurtenissen telkens vanuit het perspectief van een andere betrokkene: de hacker, de eigenaar van het systeem, de journalistiek, politiek en rechtsspraak. Moet je voor dit boek weten wat een SQL-injectie is, hoe een Kamermotie werkt of wat computervredebreuk juridisch inhoudt? Nee. Als het goed is, volstaat de uitleg om te begrijpen vanuit wat voor belevingswereld betrokkenen de situatie beschrijven en hoe zij vanuit hun eigen jargon oordelen of een onthulling verantwoord is, of niet. Als het goed is, wordt dat duidelijk in de tekst. Zo niet: RTFM, zoals hackers zeggen. Oftewel, lees de bijlage met technische termen en uitleg. Daar tref je ook de bronnen die ik voor elk hoofdstuk heb gebruikt, een voorbeeldtekst voor een meldpunt responsible disclosure en een lijst met alle personages uit dit boek. Waar mogelijk duid ik hen aan met hun Twitternaam, want dat is het medium bij uitstek voor onthullingen: snel, open en - als je wilt - anoniem. Dit geeft je als lezer ook de mogelijkheid om met hen en mij hierover verder te discussiëren.

18 februari 2015