HELPENDE HACKERS

Verantwoorde onthullingen in het digitale polderlandschap

Chris van 't Hof

TEK TOK

HELPENDE HACKERS

Verantwoorde onthullingen in het digitale polderlandschap

Chris van 't Hof

TEK TOK

Helpende hackers

Chris van ‘t Hof

Helpende hackers. Verantwoorde onthullingen in het digitale polderlandschap.

2e herziene druk, juli 2015

Auteur: Chris van ‘t Hof
Redactie: Pascal Messer
Eindredactie: Anna Teresa Bellinzis en enkele lezers van de 1e druk (maart 2015)

Non-fictie
ISBN 978-90-823462-0-6

www.helpendehackers.nl | @helpendehackers

Inhoudsopgave

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 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 ontslagen van rechtsvervolging. 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.

2. Radboud opent de poorten

Onderzoekers kraken de crypto van de Mifare Classic

Deze zaak is in meerdere opzichten een klassieker. De Mifare Classic chip werd in 2008 gebruikt in miljarden toegangs- en betaalsystemen, waaronder ook de OV-chipkaart en toegangspassen tot overheidsgebouwen. De onderzoekers die de chip wisten te kraken, ontketenden een grote maatschappelijke controverse. De rechtszaak die erop volgde, biedt interessante jurisprudentie voor komende zaken. We zien ook hoe beveiliging bepaald wordt door bedrijfseconomische afwegingen: zolang de schade meevalt, loont het niet over te stappen op een duurder systeem. Maar bovenal is dit een zaak die bepalend is geweest voor hoe we nu in Nederland denken over verantwoorde onthullingen.

Hier ontmoeten we ook iemand die we in dit boek nog vaker zullen tegenkomen: professor Bart Jacobs van de Digital Security Group. De eerste keer dat ik Jacobs sprak was in 2004. Ik was toen onderzoeker bij RAND en deed met een collega interviews voor een overzicht van de Nederlandse R&D in informatiebeveiliging. We waren natuurlijk eerst naar de technische universiteiten geweest. En oh ja, iemand had gezegd dat we ook nog even langs een professor van de Radboud Universiteit moesten, want die ‘deed iets’ met smartcards. Toen we twee uur later buiten stonden realiseerden we ons dat hier in Nijmegen iets bijzonders ging gebeuren. De kersverse hoogleraar Security & Software Correctness had zojuist elf promotieplaatsen gecreëerd voor onderzoek naar de beveiliging van smartcards. Daarnaast was hij met de andere universiteiten een hele opleiding aan het optuigen voor computer security-onderzoekers: het Kerckhoffs Instituut, vernoemd naar de 19^{e}eeuwse cryptograaf.

Op 11 september 2013 bezoek ik professor Jacobs weer. Het nieuwe studiejaar gaat net van start en overal zie ik posters en vlaggen met K3rckhoffs 1nst1tute. Er is nu naast de masteropleiding Digital Security ook een bachelor opleiding, waar zich zeventig studenten hebben aangemeld. Volgens de informatie op de site leren ze naast basisvakken zoals cryptografie, websecurity en netwerksecurity ook “als een aanvaller te denken door zelf kwetsbaarheden op te zoeken en ook te hacken”. Bijvoorbeeld door ‘social engineering’, oftewel eerst het vertrouwen winnen van mensen om ze vervolgens geheimen te ontfutselen, zoals wachtwoorden. Krijgt hij nooit kritiek, omdat hij mensen opleidt tot hackers? Nee, daar wordt volgens Jacobs nooit moeilijk over gedaan. Bovendien krijgen de studenten ook juridische en ethische vakken.

Er is in de tussentijd veel gebeurd. Jacobs is uitgegroeid tot een bekende figuur in de media. Als er iets gehackt is of een systeem faalt, weten journalisten hem te vinden voor een goede quote. Jacobs is tegelijkertijd voorzitter van de raad van advies van Bits of Freedom en lid van de Cyber Security Raad van het Ministerie van Veiligheid en Justitie – actiegroep versus de overheid. Het is volgens hem ook typisch Nederlands om dissidenten te incorporeren: hackers worden aangenomen en actiegroepen mogen mee overleggen. Dat vindt hij een goede zaak. Maar bovenal hecht hij veel aan zijn onafhankelijke positie als hoogleraar. De universiteit laat hem ook vrij in zijn uitspraken en heeft hem twee keer beloond met een mediaprijs. Hij is ook benoemd tot Officier in de Orde van Oranje-Nassau. En in 2012 ontving hij een prestigieuze Advanced Grant ter waarde van 2,5 miljoen euro van de Europese Onderzoeksraad.

In 2004 had ik geen flauw idee wat de professor van plan was met de smartcards, maar inmiddels weet ik beter. Na RAND ging ik werken bij het Rathenau Instituut, onder andere aan het dossier RFID: Radio Frequency Identitification, oftewel chips die communiceren via radiogolven. Als socioloog en elektricien zag ik meteen dat deze kleine chipjes een belangrijke sleutel gaan worden tussen menselijke en digitale netwerken. Pasjes, poortjes, scanners en tags; alles krijgt een nummer en we gaan leven in een internet van dingen. In ons onderzoek was de OV-chipkaart

een bijzonder vruchtbaar onderwerp. Vele interviews, kamerstukken, bijeenkomsten en krantenartikelen verder begreep ik hoe ingewikkeld het is om een elektronisch kaartje in te voeren in het Nederlandse polderlandschap. Met dus wat meer kennis van zaken zit ik nu weer tegenover professor Jacobs.

Zijn onderzoeksgroep, de Digital Security Group, kent inmiddels veertig leden. Een van hen is Roel Verdult. Eind 2006 was hij op zoek naar een afstudeerproject. Begeleider Flavio Garcia zette hem aan het werk met de zogenaamde ‘Ghost’. Dit is een apparaat dat een RFID-smartcard kan nadoen. Het ding was al sinds het begin van de groep in gebruik, maar werkte niet goed door diverse bugs. De student ging aan de slag en een half jaar later had hij de Ghost aan de praat. Om dit ook te demonstreren gaf Garcia hem een opdracht: “Probeer hier op het terrein gratis te parkeren.”

Het toenmalige parkeerterrein van de Radboud Universiteit werkte namelijk met een smartcard-systeem gebaseerd op RFID. Dat werkt als volgt. Bezoekers krijgen een pasje met daarin een chipje dat een antenne heeft in de vorm van een spoeltje. Naast de slagboom staat een leesapparaat dat telkens een signaal uitzendt van 13.56 MHz. Houd je het pasje erbij, dan wekt die straling in het spoeltje voldoende stroom op om het chipje aan de praat te krijgen en informatie heen en weer te sturen. Die informatie blijkt bij dit systeem relatief simpel: een nummer zonder enige cryptografische bewerking. Verdult weet de Ghost een geloofwaardig nummer te laten produceren en de poort gaat open.

In mei 2007 is student Gerhard de Koning Gans ook op zoek is naar een afstudeeronderwerp. Hij wordt hij ook op het project gezet en komt met een alternatief voor de Ghost: de Proxmark III. Die kan niet alleen de kaart nadoen, maar ook het apparaat dat de chip uitleest. Nadeel is echter dat het niet dezelfde taal spreekt als de chips die ze onderzoeken. Ze moeten dus het hele ding herprogrammeren en gaan samen aan de slag. Jacobs hoort van de vorderingen en weet nog wel een betere target: de OV-chipkaart. Die werkt namelijk met dezelfde soort chips: de Mifare van NXP. Hij had de uitgever van de kaart, Translink Systems, al eens benaderd voor een test. Maar die reageerde volgens de

professor in de trant van: “Sodemieter op, alles is veilig”. Nu kan hij de twee studenten erop zetten om te kijken of dat ook werkelijk zo is.

In de OV-chipkaart worden twee type chips gebruikt. In de wegwerpkaart zit een Mifare Ultralight. Net als de parkeerkaart geeft die gewoon een nummer af dat door de lezer bij het OV-poortje wordt herkend. Die lezer geeft dan een signaal terug aan de chip waarmee hij zichzelf uitzet en niet nog een keer gebruikt kan worden. Verdult zet de Ghost aan het werk als wegwerpkaart. Die doet het. Hij kan het apparaat bovendien zo programmeren dat hij zichzelf niet uitzet na gebruik. Hiermee kan hij dus oneindig vaak gratis reizen. Iets dergelijks was al eens eerder gedemonstreerd, dus niet zo spannend.

De gewone OV-chipkaart is een stuk spannender. Die heeft namelijk een zwaardere chip: de Mifare Classic. Die geeft niet zomaar een nummer af, maar doet cryptografische bewerkingen met het zogenaamde Crypto-1 algoritme. De lezer geeft de chip een nummer, waar hij zijn geheime algoritme op loslaat en pas als die het juiste nummer teruggeeft kan de communicatie starten. Hier schiet de Ghost te kort. Maar De Koning Gans heeft zijn Proxmark inmiddels zover dat deze ook de taal van de chip verstaat. Nu kunnen ze zowel de chip als de lezer nabootsen, die eindeloos met elkaar laten communiceren en zo kijken naar patronen. Elke dag komen ze dichter bij het vinden van het geheime algoritme.

Hier staat meer op het spel dan alleen het kunnen kraken van een chip, het gaat ook om het bevestigen van Kerckhoffs principe. Auguste Kerckhoff, de man naar wie het instituut is vernoemd, stelde namelijk in 1883 dat een systeem van versleuteling even veilig moet zijn, als alles behalve de sleutel publiek bekend is. Te vaak gaan mensen er namelijk van uit dat als anderen niet weten hoe het systeem werkt, ze het ook niet kunnen kraken. De meeste cryptografen zijn het niet mee eens met deze ‘Security by obscurity’. De werking moet openbaar zijn, zodat die getest kan worden. Het geheim moet in de sleutel zitten: die moet zoveel mogelijkheden hebben, dat die niet binnen redelijke tijd te raden is. Pas dan is een systeem veilig.

Hun project krijgt steeds meer interesse van de rest van de groep. Er hangt iets in de lucht. Jacobs: “Dat heeft zijn eigen dynamiek en daar ga ik niet in sturen. Maar ik werd me er wel snel bewust van hoe gevoelig het was. Die chip zat niet alleen in de OV-chipkaart, maar ook in de pas die toegang geeft tot ministeries.” NXP heeft in die tijd wereldwijd al meer dan een miljard chips verkocht voor allerhande toegangssystemen. Hij besluit daarom alle betrokken onderzoekers samen in één kamer te zetten, naast Verdult, De Koning Gans en hun begeleider Garcia ook: Jaap-Henk Hoepman, Ravindra Kali, Vinesh Kali, Ruben Muijrers, Peter van Rossum en Wouter Teepe. Iedereen zou namelijk de universiteit kunnen binnenlopen en er mag niets gelekt worden. Online communicatie wordt versleuteld. “We konden pas naar buiten komen als we echt resultaten hebben, dus: kopiëren, saldo veranderen, dat soort dingen”, aldus Jacobs.

Terwijl de onderzoekers druk aan het puzzelen zijn in hun geheime kamer, gaat Nederland langzaam maar zeker over op de OV-chipkaart. Steeds meer stations en voertuigen worden voorzien van leesapparatuur waarmee reizigers kunnen in- en uitchecken. Rotterdam loopt voorop, met als eerste volledige dekking in metro en trams. In Amsterdam starten de eerste proeven. De ambitie is dat binnen een paar jaar iedereen met één kaart door het hele openbare vervoer kan. De regie wordt ondergebracht in een consortium van de vervoersbedrijven onder de naam Trans Link Systems, want de kaart moet het niet alleen de reizigers makkelijker maken, maar vooral ook de vervoerders. Zo hebben ze een meer realistisch overzicht van waar er gereisd wordt, zodat ze het aanbod kunnen aanpassen en de verschillen in kosten en inkomsten beter verdelen. En als je dan zo makkelijk een kaartje kunt kopen, waarom niet ook een broodje? Dit wordt het nieuwe betalen.

De eerste gebruikersonderzoeken in Rotterdam zijn positief. Reizigers vinden de kaart makkelijker dan de strippenkaart en zien de voordelen van de poortjes: zo houden we die vervelende junks en zwervers uit het OV. Maar er is ook kritiek. In Amsterdam wordt het Gemeentelijk Vervoersbedrijf op de vingers getikt door het College Bescherming Persoonsgegevens. De vervoerder wil

namelijk reclame gaan koppelen aan reisgedrag, zonder toestemming van de reiziger. Bovendien zijn die gegevens niet echt veilig opgeslagen volgens het CBP. Bekijken we de nieuwsberichten uit die periode, dan zien we vooral journalisten die bij de poortjes wachten tot iemand problemen heeft met in- en uitchecken: microfoon erbij en je hebt een leuk item. Partij Groen Links is ook kritisch en zet een site op: ov-chipklacht.nl. De partij die zich van oudsher inzet voor goed openbaar vervoer, krijgt al snel vijfduizend klachten binnen en roert zich steeds vaker in Kamerdebatten over de kaart.

Dan is er nieuws uit Duitsland. Karsten Nohl van de universiteit van Virginia en Henryk Plotz van de Hamboldt universiteit in Berlijn beweren dat ze de Mifare Classic hebben gekraakt. Ze hebben het heel anders gedaan dan de jongens uit Nijmegen, namelijk met chip-slicing. Door de kaart laagje voor laagje af te schrapen worden delen van de schakeling zichtbaar. Hier zouden ze het verborgen algoritme uit hebben afgeleid. In december 2007 presenteren ze hun bevindingen tijdens de jaarlijkse bijeenkomst van de Chaos Computer Club. Niet alles, want ze zijn bang voor een rechtszaak. Het is ze nog niet gelukt zelf een kaart te maken, maar de zaak wordt breed uitgemeten in de media. Nu wordt het wel erg moeilijk voor de onderzoekers van de Digital Security Group om stil te blijven.

Jacobs wordt gevraagd om een reactie op de Duitse kraak. Verdult wil zijn bevindingen eigenlijk pas publiceren bij zijn afstuderen, maar nu moet hij wel iets onthullen. Zij kunnen immers wel een functionerende kaart produceren, de Duitsers niet. Jacobs besluit Koen de Regt van RTL een primeur te geven: de Ghost die werkt als wegwerpkaart. Verdult mag het zelf demonstreren in de metro van Rotterdam. Jacobs raadt hem wel aan zich niet te laten verleiden tot politieke of andere verreikende uitspraken. “Blijf bij je expertise”, zegt hij tegen de jonge onderzoeker.

Het RTL-nieuws van maandag 14 januari 2008 opent met ‘Gratis metro met gehackte OV-chipkaart’. De Regt heeft er een mooi item van gemaakt van maar liefst acht minuten. We zien Verdult bij de poortjes in- en uitchecken. Met zijn laptop past hij steeds

weer het saldo van zijn Ghost aan. Dan zien we een interview met Jannemiek Zandee van Trans Link Systems die beweert dat de kaart toch echt veilig is. Op de achtergrond blijft Verdult rondjes lopen door de poortjes die nog steeds geen foutmelding geven. Een sterk staaltje journalistieke beeldretoriek.

Het item leidt tot Kamervragen. De woensdag erop wordt een hoorzitting belegd met diverse beveiligingsexperts, waaronder ook Verdult en Teepe. Een debat over de kaart stond al gepland op donderdag en nu richt alle aandacht zich op staatsecretaris Tineke Huizinga. Ze gaat dan weliswaar niet over Trans Link Systems - een onafhankelijk consortium van de vervoersbedrijven - maar er is zoveel subsidie ingegaan, dat de staat wel wat mag eisen. Bovendien is een goed openbaar vervoer van landsbelang en als er zoveel partijen bij betrokken zijn, zal toch iemand de regie op zich moeten nemen. De oppositie vindt dat zij dat moet doen.

Huizinga is dan nog niet zo lang staatsecretaris van Verkeer. Ze was na een moeizame kabinetsformatie in 2007 door de Christen Unie dankzij voorkeursstemmen naar voren geschoven. Eigenlijk weet ze vrij weinig van technologie en vervoer en nu krijgt ze dit hoofdpijndossier. Huizinga vraagt daarom voorafgaand aan het Kamerdebat de Radboudonderzoekers om raad. Hun advies: “Laat een onafhankelijke contra-expertise uitvoeren. Je hoeft ons niet te geloven, hoor…”.

In het Kamerdebat van 17 januari belooft de staatssecretaris een “aanvalsplan” om “het beschadigde beeld van de OV-chipkaart te herstellen”. In het plan komen afspraken met de betrokken partijen over beveiliging, privacy, tarieven, distributie, reisgemak en “de wijze waarop de regie op de voortgang van het invoeren van de OV-chipkaart blijvend wordt georganiseerd”. De vervoerders en consumentenorganisaties onderschrijven de inhoud van dit plan en presenteren het gezamenlijk op 29 februari. Daarnaast wordt onderzoek gestart naar de veiligheid van de kaart, oftewel de contra-expertise. Dit wordt uitgevoerd door TNO.

TNO komt binnen een paar weken tot de conclusie dat de wegwerpkaart weliswaar is na te maken, maar fraude uiteindelijk zal worden ontdekt door de achterliggende administratie die dan de kaart blokkeert. Bovendien zijn daar geavanceerde middelen

voor nodig. Voor elk ritje een nieuwe kaart maken, is daarom niet echt een criminele business case. Er is volgens de onderzoekers dus niets te vrezen. Dan maar nog een onderzoek, dit keer van de Engelse Information Security Group, Royal Halloway, van University of London. Die komt tot dezelfde conclusie. Bovendien hebben de onderzoekers daar al langer ervaring met de Oystercard. Die werkt met hetzelfde systeem en daar is ook niet mee gefraudeerd. Mocht er dan toch gefraudeerd worden, dan moeten de vervoersbedrijven een plan hebben om over te stappen naar een nieuwe chip, aldus de contra-expertise.

De kamer blijft echter kritisch naar Huizinga. In de tweede week van maart staat een hoorzitting gepland, waarin Huizinga de resultaten van het onderzoek mag toelichten. Die zitting komt er echter niet, want ze mag zich dan weer tegenover de Kamer verantwoorden. Het is de Digital Security Group namelijk vrijdagmiddag 7 maart gelukt de Mifare Classic en dus ook de gewone OV-chipkaart te kraken en ze willen ermee naar buiten komen. De bewindsvrouw heeft slechts een dag om zich voor te bereiden.

Wat was er gebeurd in de geheime kamer aan de Radboud Universiteit? Verdult en zijn collega's hebben met hun zelfgemaakte kaartlezer en kaart eindeloos in- en uitgecheckt. De enen en nullen gaan heen en weer en worden steeds weer bewerkt volgens het geheime Crypto 1 algoritme. Ze hebben al ontdekt dat ze zelf een sleutel in een blanco kaart kunnen zetten en daarmee allerlei variaties kunnen uitproberen: eerst een sleutel van alleen nullen, daarna een met alleen maar enen en vervolgens allerlei variaties daar tussenin. Dit is reverse engineering: door het gedrag van een apparaat na te bootsen erachter komen hoe het werkt.

Verdult houdt steeds de in- en output bij in een tabel. Als ze alle mogelijkheden willen proberen moeten ze 2^{48} keer de sleutel veranderen. Dat zou volgens hun eigen berekening 44.627 jaar kosten. De Koning Gans ontdekt echter dat de random generator geen willekeurig getallen genereert, maar telkens op dezelfde manier opstart en dan in twee uur een rondje langs dezelfde getallen maakt. Zo kunnen ze het aantal mogelijke sleutels

drastisch terugbrengen tot 2^{16}, oftewel 65.536 keer. Dan kan het in een paar uur. En zo komen ze er op 3 maart achter welke berekening de chip op de sleutel loslaat. Ze hebben het achterliggende algoritme gevonden dat dan al vijftien jaar geheim is gehouden. Om dit te kunnen demonstreren, maken ze zelf een eigen OV-chipkaart. Op 7 maart 2008 is deze af.

De vondst kan een mooi artikel worden voor ESORICS, het European Symposium on Research in Computer Security in oktober dat jaar. Met een peer review procedure van zeker een half jaar is de deadline akelig dichtbij. Echt veel tijd voor een verantwoorde onthulling hebben ze dus niet. Dan ontdekken ze nog iets anders, wat nog veel alarmerender is: de toegangspassen voor de overheidsgebouwen zijn nog veel makkelijker na te maken. Waar elke OV-chipkaart nog een eigen sleutel heeft, wordt die bij deze passen nauwelijks gevarieerd. Sommige gebouwen hebben zelfs maar één sleutel voor alle passen. Met deze kennis kan iemand dus zomaar ongemerkt een militaire basis, bank of de Tweede Kamer binnenwandelen.

Jacobs belt daarom die vrijdag meteen met Roelof de Wijkerslooth, de voorzitter van het College van Bestuur van de universiteit en zegt: “Ik druk op de rode knop.” Een vooraf afgestemd plan treedt in werking. De collegevoorzitter verschijnt binnen tien minuten op het lab, ziet hoe de onderzoekers met hun eigen pas een deur openen en neemt direct contact op met het Ministerie van Binnenlandse Zaken. De volgende dag, zaterdag, krijgt de Digital Security Group bezoek van het Nationale Bureau voor Verbindingsbeveiligingen. Dat zijn de rijkscryptografen van de Algemene Inlichtingen- en Veiligheidsdienst. Ze zijn geschokt dat dit zomaar kan, maar ook gerustgesteld dat de bevindingen niet direct worden gepubliceerd. Zondag worden TLS en NXP ingelicht om tijdig maatregelen te nemen. Na de hetze rondom de wegwerpkaart hadden de onderzoekers de kaartuitgever en chipbouwer al betrokken in hun vorderingen. Nu moet er snel gehandeld worden. Hans de Jong van NXP komt die maandag kijken in Nijmegen en ziet met eigen ogen hoe de onderzoekers hun chip klonen. Die middag gaat hij langs bij TLS en informeert ook hen.

De onderzoekers schrijven een persverklaring die ze eerst voorleggen aan de betrokkenen. De AIVD is content. NXP is minder blij. De chipfabrikant vindt dat er teveel details worden vrijgegeven, maar is niet bij machte de perspublicatie tegen te gaan. Die woensdag krijgt de wereld te horen hoe slecht het is gesteld met de beveiliging van de Mifare Classic. Guusje ter Horst, die als minister van Binnenlandse zaken de coördinatie op zich heeft genomen, informeert die dag ook de Tweede Kamer. Pas dan krijgt ook staatssecretaris Huizinga het te horen. Haar debat over de contraexpertise staat al de volgende dag gepland. Om zich daarop voor te bereiden worden Verdult en zijn collega's weer opgeroepen haar te adviseren.

De vrijdag daarop komt NXP weer naar de Radboud Universiteit om te praten over vervolgstappen. Directeur Rausch overhandigt Jacobs een fles wijn en feliciteert de onderzoekers met de resultaten. Hij stelt dat NXP graag met hen wil samenwerken om de chips veiliger te maken, maar dat moet dan wel onder een geheimhoudingsverklaring. Jacobs ziet niets in zo'n verklaring, want zo kunnen hij en zijn collega's er niet meer over publiceren. En dat is precies wat ze willen doen. De deadline voor ESORICS is 7 juli. NXP mag in de tussentijd ook het artikel lezen, maar dan moet Rausch zelf een geheimhoudingsverklaring tekenen. Zo heeft iedereen tot oktober de tijd om maatregelen te nemen. Zes maanden moet genoeg zijn bij een verantwoorde onthulling.

De AIVD kan zich wel vinden in de termijn van een half jaar en heeft geen bezwaar tegen de publicatie. Sterker nog: de onthulling zal de beveiliging van de Nederlandse gebouwen alleen maar ten goede komen. Govcert, het Computer Emergency Response Team van de overheid, stuurt een waarschuwing uit met instructie hoe te handelen: 'Factsheet FS-2008-03. Kwetsbaarheden Mifare Classic chips in toegangspassen'. Hierin staat dat het Crypto1 algoritme is gekraakt, de passen nagemaakt kunnen worden en welke maatregelen genomen kunnen worden. Het advies is dat ook snel te doen, want de details van de kwetsbaarheden worden binnen enkele maanden vrijgegeven.

Staatsecretaris Huizinga is inmiddels alweer wat OV-chipdebatten verder. In het debat van 15 april 2008 neemt ze de contra-expertise van de universiteit van Londen als leidraad voor haar beleid. Daarin staat onder andere dat de vervoersbedrijven een migratieplan moeten hebben om over te stappen op een nieuwe chip als blijkt dat op grote schaal misbruik wordt gemaakt van de kaart. Ze waarschuwt vooral geen overhaaste beslissingen te nemen en “hibbel de dribbel op een nieuwe chip over te stappen”.

Dan is de oppositie het zat. Op 16 april 2008 dienen ze een motie van wantrouwen in tegen Huizinga. Het initiatief komt van Groen Links Kamerlid Wijnand Duijvendak. Als ik hem een maand later spreek, vertelt hij me dat ze hier toen al maanden mee bezig waren. Hij verwijt haar geen leiding te nemen, terwijl zij de enige is die er wat aan kan doen. En die kraak, daar kun je op wachten. “Dit leidt tot chronische zakkenrollerij”, aldus Duijvendak. De motie wordt gesteund door Groen Links, SP, VVD en PVV, maar haalt net geen meerderheid. De kraak was dan wel niet de oorzaak van de hetze, maar wel de katalysator van al het ongenoegen rondom de kaart en de staatssecretaris.

De jonge onderzoekers van de Radboud Universiteit zijn op dat moment in London. Een van de argumenten in de contra-expertise is namelijk dat het wel mee zou vallen met de fraude want de London Oystercard is al langer in gebruik en daar wordt ook niet mee geknoeid. Proberen dus. Op een rustig stationnetje zetten ze de Ghost en Proxmark aan het werk. Ze checken in en uit en veranderen het saldo. Alles werkt en tevreden gaan ze terug naar de luchthaven. Daar zien ze een goededoelenbus: “Doe hier uw Oystercard in en steun een goed doel!”. Ze zouden de kaart kunnen opwaarderen tot 100.000 Britse pond en hem in de bus te doen… Ze twijfelen en moeten nog hun vliegtuig halen… Toch maar niet doen.

Eenmaal thuis schrijven ze hun eerste concept van het artikel: ‘Dismantling Mifare Classic’. Roel Verdult kan dan ook eindelijk afstuderen. Het voorwoord van zijn scriptie ‘Security analysis of RFID tags’ begint met “The process during my master thesis was an experience I will never forget”. Gaat het hier over de commotie rondom de OV-chipkaart? Nee, het gaat om de moeizame relatie tussen hem en de Ghost. Over hoe zwaar het was dit apparaat

aan de praat te krijgen en hoe blij hij was toen hij het werkelijk kon testen. In de rest van het stuk kunnen we lezen hoe hij en de Ghost diverse beveiligingsproblemen vinden in RFID-chips. Voor de problemen met de beveiliging van de Mifare Classic verwijst hij netjes naar het artikel dat hierover zal verschijnen bij ESORICS. Op 25 juni 2008 levert hij de definitieve versie van zijn scriptie in. De echte rel moet dan nog beginnen. Jacobs ontvangt namelijk diezelfde dag een brief van NXP: ze starten een rechtszaak tegen de professor en zijn universiteit.

3. Crypto is geen cultuuruiting, onthullen wel

De zaak NXP versus Bart Jacobs en de Radboud Universiteit

Op 25 juni 2008 krijgt professor Bart Jacobs een boze brief van Rausch. De NXP-directeur heeft uiteindelijk toch de geheimhoudingsverklaring getekend en het ESORICS-artikel gelezen. Jacobs had weliswaar niet aan het artikel meegeschreven, maar was toch maar als auteur toegevoegd voor het geval hij het voor zijn jongens moest opnemen. Dat blijkt nu inderdaad nodig, want Rausch richt zijn brief aan Jacobs persoonlijk en vermaant hem in dreigende bewoordingen af te zien van de publicatie. Het bevat namelijk geheime informatie die toebehoort aan NXP. De universiteit moet niet denken dat ze zomaar alles kunnen onthullen, ongeacht hoe schadelijk dat is voor derden en de samenleving als geheel. Je publiceert toch ook niet hoe je chemische of nucleaire wapens maakt? Bewustwording creëren over eventuele veiligheidslekken in de chip kan ook anders. NXP wil best wel een verklaring ondertekenen waarin staat dat het de onderzoekers is gelukt de chip te kraken. Gaan ze toch door met deze onverantwoorde publicatie, dan wordt alle schade die NXP en anderen hierdoor oplopen verhaald op de universiteit en Jacobs zelf.

De universiteit schrijft terug dat NXP al langer op de hoogte was van de tekortkomingen in de beveiliging en er bovendien alternatieve beveiliging voorhanden is. “De door de onderzoekers geconstateerde intrinsieke zwakten van de chip maken het op zijn minst aannemelijk dat door NXP niet wordt voldaan aan het beveiligingsniveau dat afnemers en eindgebruikers van de chip mogen verwachten. Wie voortgaat een dergelijk gebrekkig product op de markt te brengen, moet niet klagen dat vanuit de wetenschap de gebreken van het product op een wetenschappelijk onderbouwde wijze onder de aandacht worden gebracht”, aldus de Radboud Universiteit.

De door NXP aangeboden verklaring wijzen ze af. Die zal niet dezelfde impact hebben als de publicatie van een wetenschappelijk artikel, want de bevindingen moeten verifieerbaar aangetoond worden. Mocht NXP de publicatie alsnog onrechtmatig vinden, dan kunnen ze de kwestie ook aan de rechter voorleggen. Dat is ook wat de chipfabrikant doet. Op 10 juli vindt het kort geding plaats. De uitspraak is 18 juli. De deadline van het artikel is dan al verlopen, maar de onderzoekers krijgen nog wat extra dagen om zo de uitkomst af te wachten.

Rechtbankverslagen zijn interessante bronnen als het gaat om onderzoek naar controversen. Voor- en tegenpartijen moeten alles uit de kast halen om hun standpunten te onderbouwen. We zien welke wetgeving van toepassing is bij vergelijkbare zaken. Gebeurtenissen, personages en zelfs briefwisselingen zoals hierboven geciteerd, worden keurig in de tijd geplaatst, gedocumenteerd en gepubliceerd. En dat alles onder ede. Het vonnis van de rechtbank van Arnhem van 18 juli is dan ook met recht een belangrijk historisch stuk in dit verhaal.

We lezen hier hoe de advocaat van NXP eist dat de onderzoekers hun publicatie terugtrekken. Dwangsom: één miljoen euro. Ook moet de universiteit ervoor zorgen dat niemand anders, zoals de reviewers van het artikel, iets lekt over de hack. Het algoritme en de manier waarop het gevonden is, moeten geheim blijven. De eis wordt ondersteund met een beroep op auteursrecht, geheimhouding, onrechtmatige daad, computervredebreuk en inperking vrijheid van meningsuiting vanwege een groot maatschappelijk belang. Volgens de verdediging zijn auteursrecht en geheimhouding niet van toepassing op een algoritme en staan de regels rondom de vrijheid van meningsuiting aan hun kant. Het maatschappelijk belang is juist gediend bij de onthulling van de tekortkomingen in de beveiliging die te wijten zijn aan de maker: NXP.

Laten we de eisen van de advocaat van NXP, in dit geval de ‘klager’, hier stuk voor stuk doorlopen, want ze zijn allemaal relevant voor ook andere verantwoorde onthullingen. Ten eerste, auteursrecht. Het Crypto1-algoritme komt volgens de klager in aanmerking voor artikel 10 lid 1 als het een “eigen oorspronkelijk

karakter” heeft en “het persoonlijk stempel van de maker” draagt. NXP komt daarom met een verklaring van iemand die de maker zou zijn. Onbekend blijft wie dat is, maar hier dus iemand die ergens begin jaren negentig bij Phillips een rekensommetje heeft bedacht en nu moet beweren dat het een vorm van kunst is. Gaat de rechter daarin mee, dan maakt Radboud zich schuldig aan het verveelvoudigen (artikel 13) en publiceren (artikel 12) van deze cultuuruiting. Bovendien hebben zij hiervoor bewust doeltreffende voorzieningen omzeild (artikel 29a) door de beveiliging te breken.

Volgens het verweer kan hier geen sprake zijn van auteursrechtelijk beschermd werk. “Een algoritme is niets meer dan een wiskundige of logische formule waar een cijferreeks doorheen wordt gehaald. Van enige creativiteit is geen sprake. De keuze van een algoritme is banaal of triviaal, geheel arbitrair en hooguit gebaseerd op praktische afwegingen als rekensnelheid, technische eisen van de apparatuur, het vereiste beveiligingsniveau, overwegingen van gebruiksgemak en andere louter technische/functionele randvoorwaarden.” Bovendien zal het algoritme zelf niet eens in de publicatie staan, alleen de manier waarop zij het hebben verkregen.

Rechter Boonekamp gaat hierin mee. De verklaring van de maker wijst weliswaar uit dat zijn keuzes “subjectief” waren, maar het is een wiskundige formule en geen cultuuruiting. Het algoritme was ook niet bedoeld om gepubliceerd te worden en kan dan ook niet als publicatie beoordeeld worden. En als NXP het wel zo wil zien, waarom beroept zij zich dan op geheimhouding? Argument twee, oftewel “bekendmaking van geheime bedrijfsgegevens” (Wetboek van Strafrecht, artikel 273 lid 1 sub 2) gaat dus ook van tafel.

Na deze enigszins flauwe beschuldigingen volgt het echte werk. NXP klaagt Radboud aan vanwege een “onrechtmatige daad”. Oftewel, de onderzoekers doen bewust iets wat anderen schade toebrengt (Burgerlijk Wetboek 6, artikel 162). Met hun artikel faciliteren ze immers derden “met relevante basiskennis en minimale middelen om beveiligingssystemen te misbruiken”. Ze zijn daarmee medeplichtig aan computervredebreuk, oftewel “opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk” (Wetboek van Strafrecht artikel 138a).

NXP zal door de publicatie ook behoorlijke schade lijden. Normaal kost het hen tweeënhalf jaar om chips te vervangen en dat moet nu dus sneller. Daarnaast zullen vele tienduizenden partijen die nu de chip gebruiken schade lijden en die mogelijk willen verhalen op NXP. Tot slot verwacht de chipmaker, naast omzetverlies door daling van verkoop, ook een aanzienlijke reputatieschade. Vandaar die miljoen euro dwangsom.

Nu komt het punt waar het allemaal om draait: de vrijheid van meningsuiting. Volgens artikel 10 lid 2 van het Europese Verdrag voor de Rechten van Mens komt dat recht met een zekere verantwoordelijkheid. Die vrijheid kan ingeperkt worden wanneer het gaat om het voorkomen van strafbare feiten of ter bescherming van de rechten van anderen. Volgens NXP is dat hier het geval. Publicatie is onverantwoord omdat niet alleen NXP zelf de nodige bedrijfsschade zal oplopen, maar ook alle organisaties die de chip gebruiken. Daarmee is het een maatschappelijk belang. Bovendien is het publiek al geïnformeerd over de onveiligheid van de chip, dus waarom dan nog de details publiceren?

De verdediging brengt hier tegenin dat er geen sprake is van het faciliteren van kwaadwillenden. Hiervoor ontbreekt ook de opzet van hun kant. Doel is aan te tonen dat ‘Security through obscurity’ niet werkt, oftewel het Kerkhoffsprincipe. Het artikel bevat geen stappenplan voor het kunnen kraken en klonen van de chip en er staat niet hoe en met welk apparaat je signalen kunt uitlezen en nabootsen. Om het artikel te begrijpen moet je ook wel over de nodige wetenschappelijke deskundigheid beschikken. Maar bovenal: het risico van misbruik en de daaruit voortvloeiende schade wordt veroorzaakt door de zwakheden in het ontwerp van de chip. Daarvoor is NXP verantwoordelijk en niet degene die dit aantoont. Het algemeen belang is er juist bij gediend als “de ontdekte misstand op verifieerbare wijze aan de orde wordt gesteld” en “dezelfde ontwerpfouten in de toekomst niet meer worden gemaakt”, aldus de verdediging van de universiteit.

Rechter Boonekamp verwoordt in zijn eindoordeel goed wat er speelt bij verantwoorde onthullingen. “Bij het ontdekken van beveiligingsproblemen ontstaat het dilemma hoe met deze kennis

om te gaan. Bij directe publicatie kunnen belangen geschaad worden. Langdurige geheimhouding leidt doorgaans tot trage reacties waardoor misbruik lang mogelijk blijft. Het is gangbaar in de computer security community om beveiligingslekken na een korte vertraging bekend te maken, als redelijk evenwicht. Ook deze aanpak is hier gevolgd.” Wat volgt is een hele uiteenzetting van hoe Jacobs en De Wijkerslooth destijds alle betrokkenen tijdig hebben geïnformeerd.

Hij ziet in de publicatie dan ook geen onrechtmatige daad: het is een theoretische verhandeling en geen instructie om te hacken. De onderzoekers dragen hiermee bij aan een betere beveiliging van elektronische systemen, zoals overigens ook reeds door de AIVD is beaamd. De rechter is ook niet gediend van de doemscenario’s die de advocaat van NXP schetst. Het gaat hier toch vooral om bedrijfsbelangen. Mocht er dan toch schade ontstaan, dan is die te wijten aan de onveilige chip en niet aan de onderzoekers. Die hebben naar eer en geweten gehandeld en hoeven geen boete te verwachten als ze publiceren. NXP moet tot slot aan hen de proceskosten vergoeden: 7.570 euro.

De onderzoekers, maar vooral ook collegevoorzitter De Wijkerslooth zullen bijzonder opgelucht en blij zijn geweest. Niet alleen kunnen ze nu hun artikel indienen, maar bovenal is hier een principiële strijd beslecht, in het voordeel van academische vrijheid. Een ieder die nu op een verantwoorde manier beveiligingsproblemen wil melden, kan steunen op deze zaak. Het kraken van crypto is geen schending van intellectueel eigendom of geheimhouding, maar een rechtmatige daad. En hacken mag dus, als het een hoger maatschappelijk doel dient en je het op een verantwoorde manier onthult. Zo werkt jurisprudentie: ethisch hackers kunnen naar deze zaak verwijzen als zij zelf ooit aangeklaagd worden.

Roel Verdult is intussen nog steeds niet afgestudeerd. Maar dankzij zijn werk aan de OV-chipkaart wordt hij wel uitgeroepen tot student van het jaar. De huldiging is 13 november. De initiator van de prijs, Science Guide, doet verslag. We krijgen eerst iets meer te lezen over Verdults achtergrond. Dat hij gaat afstuderen, lag helemaal niet in de lijn der verwachtingen. Hij was eerst naar

de mavo gestuurd en deed daarna havo. Pas later bleek dat hij dyslectisch is. Via de bachelor Informatica kwam hij bij de school van Jacobs terecht. En nu krijgt hij in een afgeladen Passenger Terminal Amsterdam een lofrede van Neerlands beroemdste professor: Robert Dijkgraaf. Die prijst Verdult vanwege zijn creatieve, innovatieve en verantwoordelijke aanpak bij het uitzoeken van de kwetsbaarheid van de OV-chipkaart en schets alle maatschappelijke commotie die het teweegbracht. Dan is het woord aan Gerard Kleisterlee, topman bij Philips, waar NXP voorheen onderdeel van was.

Kleisterlee zou een cheque overhandigen aan een veelbelovende bèta start-up, maar grijpt de gelegenheid aan om zijn visie te geven op het OV-chipdebacle. Al die ophef in de politiek over het veilig kunnen functioneren van de OV-chipkaart vindt hij zwaar overdreven. “Foutjes die er wel of niet in zitten, die zijn al die aandacht niet waard. Daar moeten we ons niet op richten, ook niet als iemand even aantoont dat het niet meteen helemaal perfect werkt… Stel, er zitten wat onvolkomenheden in? So what! Wie zou het bij zijn gezond verstand de moeite waard vinden om zo’n dagelijks gebruiksvoorwerp te kraken?” De Science Guide-verslaggever citeert ook een buitenlandse bezoeker die met de ouders van Verdult praat. “You should be proud of your son. He really must have scared the shit out of the top people at Philips.”

De reactie van Kleisterlee is kenmerkend voor veel van de partijen die betrokken waren bij de invoering van de kaart. Zo sprak ik 28 mei 2009 met Pedro Peters, de directeur van de RET. Hij was er van het begin af aan bij toen het consortium TLS werd opgericht door zijn organisatie, samen met de NS, GVB, HTM en Connexxion. Ze wilden van de papieren kaartjes af en een systeem hebben waarmee alle kosten en inkomsten makkelijk te verrekenen zijn. Voor de RET was een belangrijk voordeel dat ze de perrons konden afsluiten voor zwartrijders en ongure types. Peters was enthousiast en had haast, want zijn stad, Rotterdam, ging als eerste over op de kaart.

De RET-directeur vertelt zijn verhaal terwijl achter hem een paar dozen staan met vervalste strippenkaarten. Die heeft iemand gewoon nagemaakt met een kleurenprinter, een low tech hack.

Peters: “Al die discussie rondom privacy en het kraken van de kaart vind ik inmiddels toch wat … hoe kan ik het uitdrukken … wat oubollig. Mensen zijn bang voor vernieuwingen, grijpen elk incident aan om tegen te zijn en kijken niet naar het grotere plaatje. Het kraken vind ik nog het meest belachelijk. Op zich goed dat die jongens dat hebben gedaan. We hebben er zelfs nog aan meegewerkt. Maar het is gewoon voor criminelen niet interessant.”

Peters heeft hier wel een punt. De chip is weliswaar te kraken, maar het is zowel voor hen als de fraudeurs een kosten-batenanalyse of dat ook werkelijk gebeurt, zoals TNO al in hun contra-expertise voorspelde. De fraudeur zal niet al die moeite doen voor een gratis kaartje en het aantal fraudegevallen is zo klein dat dit nog onder het bedrijfsrisico valt. Peters vertelt me hoe in de administratie van TLS elke transactie achteraf wordt gecheckt. Klopt er iets niet, dan wordt de kaart binnen 48 uur geblokkeerd. Dat is op dat moment inderdaad al een keer gebeurd. Een journalist van RTV Rijnmond reisde namelijk in januari 2009 twee dagen rond met een chipkaart die door de Radboud Universiteit was opgewaardeerd met één eurocent. De OV-chipkaartadministratie had de afwijking geconstateerd maar dacht dat het ging om een afrondingsfout.

Als hij dat afzet tegen wat de kraak hen heeft gekost, zijn volgens hem de verhoudingen zoek. “Het heeft ons een jaar vertraging opgeleverd omdat we van de staatssecretaris geen toestemming kregen voor het uitzetten van het oude systeem. Het naast elkaar houden van die twee systemen heeft ons acht miljoen extra gekost. Daarnaast zijn we veel inkomsten misgelopen omdat we het zwartrijden niet konden terugdringen. Deze kosten wegen niet op tegen een mogelijk risico. Vergelijk dat eens met hoeveel er gefraudeerd wordt met pinpassen en creditcards, maar dat doen ze niet.”

Bij Mcomm hoor ik vergelijkbare frustraties. Dit bedrijf verzorgt de leesapparatuur en de communicatie met de TLS-database. Ik spreek daar directeur Peter van Dijk, die de invoering van de OV-chipkaart vooral ook zag als een mooie gelegenheid om een nieuwe manier van elektronisch betalen van de grond te krijgen. De chipknip, chipper en aanverwanten hadden gefaald omdat er

niet echt een grootschalige toepassing was. Als straks elke reiziger zo'n kaart krijgt, kunnen er meer dienstverleners aansluiten, zoals de broodjeszaken op de perrons. Nu is het systeem gekraakt en zal de Nederlandse bank hen geen vergunning verlenen als elektronische geldinstelling. Tot zover de nieuwe chipknip. Jammer.

Staatssecretaris Huizinga had al in 28 november 2008 met een 'Actualisering Aanvalsplan' een migratieplan aangekondigd voor een beter beveiligde chip. Maar omdat in de periode daarna kabinetten steeds weer vallen en opnieuw geformeerd worden, verloopt de Nederlandse politieke besluitvorming behoorlijk traag. Totdat de journalistiek de zaak oppakt. In een nieuwsitem van 24 januari 2011 zien we Brenno de Winter en Jeroen Wollaars in- en uitchecken met een gemanipuleerde kaart. De kersverse minister Schultz wordt ter verantwoording geroepen en belooft een nieuwe chip.

Hoe verging het de overige betrokken? Jacobs groeide zoals gezegd uit tot een bekende beveiligingsexpert die vaak in de media verschijnt als er weer iets gekraakt is. Ook de jonge onderzoekers hebben hun carrière voortgezet. Gerard de Koning Gans is inmiddels gepromoveerd en werkt nu bij het Team High Tech Crime van de Nederlandse politie. Roel Verdult promoveert uiteindelijk in 2015 en zien we in hoofdstuk zestien terug als hij een autoslot weet te kraken in 'De hash van Dismantling Megamos'. Die zaak loopt voor hem echter minder goed af.

4. Zo lek als een mandje

Journalisten testen TLS-backoffice met anonieme kaarten

In de turbulente periode rondom de kraak van de OV-chipkaart zit journalist Brenno de Winter vaak bij de Kamervergaderingen en schrijft hij erover op de IT-nieuwssite Webwereld. De demissionaire kabinetten in de periode rondom het OV-chipkaartdebacle kunnen weliswaar weinig ingrijpende beslissingen nemen, maar er wordt in de Kamer nog wel druk over doorgepraat. Vooral in de commissievergaderingen. Daar komen Kamerleden bij elkaar die een bepaald onderwerp in hun portefeuille hebben. Ze bediscussiëren hier niet alleen de plannen die nog naar de Kamer moeten, maar doen ook hoorzittingen waarbij ze externe experts raadplegen.

Bij een van de vele hoorzittingen over de OV-chipkaart wordt Bart Jacobs gevraagd om zijn mening. De professor noemt de kaart “een open portemonnee”, maar wordt volgens De Winter niet serieus genomen. Een woordvoerder van TLS vertelt dat er ondanks de aangetoonde kwetsbaarheden in de chip niet gefraudeerd wordt. Hun backoffice houdt alles goed in de gaten en blokkeert vervalste kaarten meteen. De Winter gelooft hier niets van. In 2010 was er al een strafzaak geweest tegen een fraudeur, die uiteindelijk werd veroordeeld tot zestig uur taakstraf. Hij dient daarom een WOB-verzoek in om stukken te openbaren.

Als dat weinig oplevert, wil hij zelf wel eens testen of die backoffice goed reageert. Hij koopt een RFID-leesapparaat, downloadt de software OV-saldo, waardeert een wegwerpkaart op en gaat er drie weken mee reizen. Hij betrekt ook anderen in zijn actie. Eerst schrijft hij voor de novembereditie van PC-Active een handleiding: ‘OV-chip kraken voor beginners’. Vervolgens vraagt hij anderen ook te gaan reizen met een van zijn kaarten: de SP Tweede Kamerfractie en journalisten van Webwereld, RTV Rijnmond, Trouw en de NOS. Na een paar weken vrij reizen wordt

slechts één van de tien kaarten geblokkeerd en dan alleen bij de NS. Dit is nieuws. Hij maakt er een item van met @wol, de NOS-journalist Jeroen Wollaars.

Op het NOS Journaal van 25 januari 2011 zien we de twee journalisten op stations met een laptop hun kaarten opwaarderen en in-en uitchecken. De sfeer komt over als een grappige kwajongensstreek. Controle in de trein is best even spannend, maar er gebeurt inderdaad niets. Daarna komt Anita Hilhorst van TLS aan het woord. Ze stelt dat TLS wel degelijk fraude heeft geconstateerd, maar de kaarten nog niet heeft geblokkeerd, omdat het Openbaar Ministerie er onderzoek naar doet. De interviewer is niet overtuigd, want als iemand met een niet-persoonlijke kaart reist, hoe kan het OM die persoon dan te pakken krijgen? “Tsja, dat weet alleen het OM”, aldus Hilhorst.

De dag na de uitzending volgt een spoeddebat in de Tweede Kamer. Haast is geboden, want op 3 februari zal in Den Haag de strippenkaart worden afgeschaft. Dan kan alleen nog maar met de OV-chipkaart gereisd worden. Maar, is het systeem daar wel veilig genoeg voor? De verantwoordelijke minister op dit dossier is inmiddels Melanie Schultz. Ze krijgt die avond nog wel de gelegenheid de problematiek uiteen te zetten en de Kamerleden te informeren met een brief, maar door tijdgebrek komt er niet echt een debat. De dag erna, 27 januari, staat een Algemeen Overleg gepland. Dan hebben alle fracties de tijd hun standpunten te verkondigen en vragen te stellen aan de minister. Het debat gaat vooral over de kosten van het systeem. Laat ik me hier beperken tot wat er gezegd wordt over het hacken van de kaart.

Eerste aan de microfoon is Bashir van de SP, de fractie die zelf ook met de gemanipuleerde kaart reisde: “De minister noemde gisteren de OV-chipkaart zo lek als een mandje en lijkt daarmee, gelukkig, ook afstand te nemen van de vreselijke erfenis waar de vorige kabinetten haar mee hebben opgezadeld. Ik kan mij namelijk voorstellen dat de minister iedere ochtend huilend wakker wordt van alle dramatische ontwikkelingen rond deze OV-chipkaart. Wellicht wil zij daar zelf meer over vertellen.” Hij komt ook met de oplossing: “Gaat zij afdwingen dat de nieuwe kaart met open-source technologie gaat werken? Op die manier is het

namelijk mogelijk dat computerexperts de beveiliging verbeteren in plaats van dat zij deze, zoals nu, als een spannend kruiswoordraadsel zien dat zij proberen op te lossen.” Open source betekent dat de code van een programma openbaar is en dus ook door iedereen getest kan worden. Hackers geven daarom voorkeur aan open source, terwijl veel bedrijven zich liever niet zo kwetsbaar opstellen en hun broncode geheim houden.

Terwijl het Kamerlid het in zijn betoog opneemt voor helpende hackers, wordt hij telkens onderbroken door Aptroot van de VVD. Als Bashir het heeft over computerexperts roept de VVD-er: “En SP-medewerkers!” En, als hij eindelijk de beurt krijgt van de voorzitter: “Tegen die bekendmaking heb ik geen bezwaar. Ik heb er wel bezwaar tegen dat een medewerker van een Kamerfractie actief deelneemt aan het manipuleren van de OV-chipkaart.” Bashir: “Wij hebben de gegevens van de onderzoeksjournalisten gekregen en wij hebben zelf getest of hun beweringen kloppen.” De voorzitter kapt deze discussie af door te stellen dat er al aangifte is gedaan en het Openbaar Ministerie wel zal bepalen of er gefraudeerd is.

Monash van de PvdA blijft erbij dat hacken van de kaart een misdrijf is en vraagt de minister hoe het zit met de opsporing van fraude. Van Gent van Groen Links heeft het daarentegen over “provo’s, zoals ik ze wil noemen, van deze tijd: de hackers die het overheidsfalen genadeloos blootleggen. (…) Een hacker of een journalist die met open vizier werkt en het aantonen dat de kaart lek is als duidelijk doel heeft, treft echter geen blaam, maar hulde. (…) Ik zou zeggen: don’t shoot the messenger.”

Haverkamp van CDA noemt de invoering van de kaart een “leertraject” en zegt: “Ik maak dan ook een compliment aan al die mensen die er zo veel vrije tijd in hebben gestoken om te laten zien dat, als je heel goed zoekt, er nog ruimte is voor verbetering van de OV-chipkaart.” Voor grootschalige fraude is hij niet bang, want: “Ik ben in het rijke bezit van een OV-chipkaartreader. Ik had het ding al voor de grote hausse besteld. Ik durf hier wel een openbaring te doen: mijn ICT-kennis schiet tekort om de OV-chipkaart te hacken.”

De Jong van de PVV is het daar niet mee eens: “Ik heb op het internet gekeken: dat programmaatje staat in de top 100 van de

populairste downloadsites. Ook kreeg ik zojuist het bericht dat alle hackapparaatjes uitverkocht zijn. Er is dus een run op die apparaatjes.” Daarna gaat het debat vooral over hoe groot de fraude zal gaan worden en of ertegen opgetreden moet worden.

De minister stelt de Kamer gerust dat er een nieuwe chip komt: “Ik durf hem bijna niet te noemen, want op het moment dat je hem noemt, is hij alweer gekraakt, maar hij heet de SmartMX.” Die is inderdaad in tegenstelling tot de Mifare wel open source. Over de kraak zegt ze: “Je maakt gratis gebruik van het openbaar vervoer en je misleidt dan ook nog personen door net te doen alsof je wel betaald hebt. Dat is gewoon strafbaar. Dat je probeert om systemen te ‘challengen’, daar kan ik me iets bij voorstellen, maar op het moment dat je anderen gaat uitlokken om er ook gebruik van te maken en er ook gebruik van maakt, is dat gewoon iets wat je niet zou moeten doen.” Van Gent vraagt haar nog wel of de minister niet zelf hackers in dienst wil nemen om de beveiliging te testen? Nee, die heeft TLS zelf wel in dienst. Dat bedrijf is van de vervoerders en niet van de staat, dus zij gaat daar niet over.

De nieuwe chip wordt niet in korte tijd ingevoerd, maar volgens natuurlijk verloop. In de tussentijd hebben we dus te stellen met het risico van fraude, maar dat geldt ook voor bankpassen en al helemaal voor de strippenkaart. De invoering gaat dus gewoon door en het enige wat men kan doen is optreden tegen misbruik. Slob van de CU vraagt tot slot of dit wel prioriteit heeft bij het OM en welke straffen op de overtreding staan. De minister zegt dat ze dat niet weet, maar haalt na aandringen het voorbeeld aan van de man die in 2010 werd opgepakt en vervolgd voor chipkaartfraude. Als Slob blijft doorzeuren roept ze luid: “Ik zeg het in de camera: zestig uur taakstraf!”

Het OM gaat inderdaad onderzoek doen. TLS heeft namelijk drie dagen voor de uitzending aangifte gedaan van fraude met anonieme OV-chipkaarten en Brenno de Winter wordt uitgenodigd voor verhoor. Dat vindt plaats op 22 juni. Later vertelt hij me dat de ondervraging maar liefst vier uur heeft geduurd en dat hij dat allemaal best heftig vond. Hij stuurt me ook het uiteindelijke oordeel van de rechter, oftewel de ‘Afdoeningsbeslissing in de

zaak Device09’ van 5 september 2011. Daarin is te lezen wat er volgens het OM allemaal in de tussentijd is gebeurd.

Volgens TLS had hun afdeling Clearing & Settlement op 12 januari verdachte transacties geconstateerd. Uit de in- en uitchecksaldi van de dag ervoor blijkt dat verschillende kaarten gemanipuleerd zijn en ermee is gereisd. De betreffende vervoersbedrijven zijn verzocht camerabeelden veilig te stellen. HTM en GVB leveren beelden waarop te zien is dat De Winter op de verdachte momenten in- en uitcheckt. Hiermee is aangetoond dat hij zwartrijdt, al had hij dat natuurlijk ook in het nieuwsitem laten zien. Hem wordt daarom ten laste gelegd: computervredebreuk (artikel 138ab Sr), vervalsen van een waardenkaart (artikel 232 Sr) en het voorhanden hebben van stoffen, voorwerpen of gegevens waarvan hij weet dat ze bestemd zijn tot het plegen de genoemde strafbare feiten. Maximale gevangenisstraf: respectievelijk vier en zes jaar.

Net als bij de zaak tussen Radboud en NXP, kan de aanklacht gepareerd worden met de Universele Verklaring van de Rechten van de Mens. Hier komt nog een belangrijk verschilpunt bij: De Winter is journalist en geniet volgens diezelfde rechten net wat extra bescherming. Het gaat hier niet alleen om de vrijheid van meningsuiting, maar ook om de vrijheid van nieuwsgaring, zelfs als dat gebeurt op basis van bronnen met een illegale herkomst. De rechter haalt hiervoor interessante jurisprudentie aan. Kort daarvoor heeft namelijk een andere onderzoeksjournalist, Alberto Stegeman, met een vervalste personeelspas toegang gekregen tot beveiligd gebied in Schiphol. Hij heeft aangetoond dat de beveiliging niet op orde was, zich weliswaar schuldig gemaakt aan strafbare feiten, maar diende hiermee een hoger maatschappelijk doel. De journalist was daarbij zorgvuldig en integer te werk gegaan en is daarom vrijgesproken.

Wil De Winter niet vervolgd worden, dan moet hij aan dezelfde voorwaarden voldoen. Ten eerste: is hij een journalist? Dat blijkt volgens de rechter het geval. Hij doet namelijk al langer onderzoek naar de kaart en heeft hierover in diverse media gepubliceerd. Vervolgens: heeft hij zorgvuldig en integer gehandeld? Ja, hij heeft de kaart slechts kort gebruikt en soms zelfs samen met een geldige kaart. TLS heeft hierdoor nauwelijks

vermogensschade opgelopen. Hij heeft de onthulling bij TLS aangekondigd en hen om een reactie gevraagd. Het enige wat de rechter hem nog wel kwalijk neemt, is dat hij er in zijn publicaties bij had moeten zeggen dat wat hij doet eigenlijk strafbaar is, om zo uitlokking te voorkomen.

Dan de belangrijkste vraag: is hier een maatschappelijk belang mee gediend? Volgens TLS zelf niet. Dat de kaart vervalst kan worden, is immers al aangetoond en geen nieuws. Volgens De Winter wel. Waar de Radboudonderzoekers nog een jaar over deden, is nu, dankzij de beschikbare middelen, kinderspel. Bovendien wil hij aantonen dat de backoffice niet zoals TLS beweert adequaat reageert op mogelijke fraude. De rechter laat dit verder in het midden en baseert zijn oordeel vooral op het effect dat de actie had. Het nieuwsitem leidde namelijk tot een spoeddebat in de Tweede Kamer. Daarin heeft de minister van Infrastructuur en Milieu aangekondigd dat de productie van een beter beveiligde chipkaart eind 2011 zou kunnen beginnen. Hiermee is dus een maatschappelijk belang gediend en De Winter wordt niet vervolgd.

TLS kreeg in 2010 van de overheid 6,7 miljoen euro voor de invoering van een nieuwe chip met een hoger beveiligingsniveau. De keuze valt uiteindelijk niet op de SmartMX, maar de Infinionchip. Deze voldoet wél aan het Kerckhoffprincipe: het algoritme is openbaar zodat iedereen kan testen hoe veilig het is. Als het goed is, heeft elke kaart een sleutel die zodanig ingewikkeld is dat het wel even duurt voordat die geraden worden. Maar ze kunnen niet zomaar in één keer overstappen op een nieuwe chip, want er zijn op dat moment miljoenen kaarten in omloop. Dus kiest TLS voor natuurlijk verloop: pas als je een nieuwe aanvraagt, krijg je de Infinion.

Hoe lang kun je dan nog frauderen? De eerste chips werden ingevoerd in 2011 en een kaart is vijf jaar geldig. Dus pas in 2016 zijn alle kaarten vervangen en kunnen ook de readers zo worden ingesteld dat ze de Mifare niet meer accepteren. Tot die tijd kun je dus nog frauderen. Het enige wat TLS kan doen, is achteraf saldi vergelijken van in- en uitgecheckte kaarten en bij fraude de kaart blokkeren en aangifte doen. Een fraudeur kan dan dus nog steeds

minimaal twee dagen gratis reizen. Als ik informeer bij TLS of er nog gefraudeerd wordt, krijg ik van voorlichtster Anita Hilhorst te horen dat het best meevalt: slechts enkele kaarten per maand. Uiteraard alleen met de Mifare-chip en niet de Infinion. Die kaarten worden dan geblokkeerd zodat er niet meer mee gereisd kan worden.

De Winter is in de tussentijd bezig een dossier op te vragen bij het OM, om te kijken of er ook opsporingsmiddelen zijn ingezet. Hij ziet dit namelijk als een manier om journalisten tegen te werken. Dat dossier krijgt hij niet. Uiteindelijk wel de schriftelijke versie van de uitspraak. Als deze maandag 5 september eindelijk wordt gepubliceerd, heeft De Winter net een zwaar weekend achter de rug. De Diginotar-affaire is dan net losgebarsten, de aanleiding voor hem om een nog grotere actie op touw te zetten: Lektober, een maand met elke werkdag een melding van een lekke website.

5. @brenno en de superknallers

Webwereld schudt Nederland wakker met een maand lang lekken

In de nacht van vrijdag 2 op zaterdag 3 september 2011 loopt Brenno de Winter door het Media Park in Hilversum. Dat is een mooi toeval, want het NOS Journaal heeft brekend nieuws en zoekt snel een IT-deskundige voor commentaar. De Winter wil wel en wordt die vrijdagnacht ter plekke ingelast. Minister Donner van Binnenlandse Zaken geeft die nacht om 01.00 uur vanuit het ministerie van Binnenlandse Zaken een persconferentie. Hij begint lachend met “Goedemorgen” en leest vervolgens zichtbaar onzeker een tekst voor:

“Uit onderzoek van beveiligingsbedrijf Fox-IT blijkt dat de certificaten van Diginotar zijn gecompromitteerd. Dat betekent dat een gebruiker van overheidssites niet langer de garantie heeft dat hij ook daadwerkelijk op een site van de overheid zit. Gebruikers kunnen bij het benaderen van de websites ook de melding krijgen dat de site niet langer betrouwbaar is.”

De overheid moet snel nieuwe certificaten invoeren en neemt voor nu het beheer van het bedrijf over. Donner wordt vervolgens ondervraagd door Jeroen Wollaars over de ernst van de hack, maar kan daar niet echt op antwoorden. Het onderzoek loopt nog. Terug in de studio geeft Brenno de Winter commentaar. Volgens hem is dit het zoveelste voorbeeld van overheidsfalen bij ICT-projecten. Hij vindt het vooral kwalijk dat er geen plan B is voor als een stuk technologie niet meer te gebruiken is, zoals nu het geval is.

Diginotar is dan een Nederlands bedrijf dat certificaten uitreikt aan websites over de hele wereld. Als je zo’n site bezoekt, checkt je browser dat certificaat bij Diginotar. Klopt alles, dan verschijnt het bekende slotje links boven in de browser. Nu blijkt Diginotar zelf gehackt te zijn en kunnen anderen dus zelf certificaten aanmaken en nepsites echt doen lijken. Nu moeten bijvoorbeeld

advocaten rechtbankstukken fysiek inleveren bij de rechtbank. Terwijl er ook andere leveranciers zijn waar je een reservecertificaat had kunnen kopen. Maar dat heeft de overheid dus niet gedaan.

De hack bleek mogelijk omdat de beveiliging schrikbarend slecht was: servers waar verschillende type certificaten op draaiden waren niet gescheiden en alles was toegankelijk onder één wachtwoord. Dat ontdekte beveiligingsbedrijf Fox-IT. Een paar dagen voor de onthulling zagen ze ook dat de hackers certificaten hadden aangemaakt voor Gmail in Iran. Uit het IP-verkeer bleek dat het mailverkeer van 300.000 Iraanse gebruikers onderschept kon worden. Door wie was onduidelijk. Nu blijkt ook het certificaat van DigiD niet meer te vertrouwen en daarmee ook de online dienstverlening van bijvoorbeeld de Belastingdienst en het UWV. Donner schat het op enkele honderden sites.

De overheid had dus vertrouwd op een certificatenleverancier die zelf niet te vertrouwen was. Dit is het begin van een lange reeks discussies in de media en de Tweede Kamer over de taak van de overheid bij het beveiligen van websites.

Dan mengen ook de hackers zich in de discussie. Op 17 september 2011 ontvangen Nederlandse journalisten en de vaste Kamercommissie Binnenlandse Zaken een ‘Brandbrief van de nationale hackergemeenschap inzake ICT-beveiliging overheid’. De brief is ondertekend door Koen Martens, van de Nederlandse vereniging hackerspaces. Hij spreekt namens een hele lijst stichtingen met bijzondere namen: Hack42 te Arnhem, ACKspace te Heerlen, TkkrLab te Enschede, Bitlair te Amersfoort, Randomdata te Utrecht, Frack te Leeuwarden, Sk1llz te Almere, eth0, 2600nl.net en HXX. Zelf zit hij bij Revelation Space te Den Haag. Deze spaces, waar hackers samenkomen en elkaar de nieuwste technieken leren, treden gewoonlijk nauwelijks op de voorgrond. Nu spreken ze de politiek en via de media het brede publiek aan, want “wij hackers zijn het simpelweg zat om keer op keer te moeten vernemen dat bij de implementatie van grote ICT-overheidssystemen kinderlijke vergissingen worden gemaakt die de privacy van burgers aantasten en soms zelfs tot gevaar voor mensenlevens leiden”, aldus Martens.

In de brief noemen de hackers Diginotar en de OV-chipkaart als voorbeelden van systemen waar de beveiliging niet op orde is. “Dit zijn geen ingewikkelde hacks, maar fouten die mensen zonder opleiding kunnen misbruiken. Daarvoor is standaard programmatuur op internet voorhanden. Het gaat om elementaire beveiligingsprincipes die structureel niet worden toegepast en een blind vertrouwen in techniek, gestoeld op onvoldoende begrip van de risico’s… De hackergemeenschap voelt zich geroepen deze zaken aan de kaak te stellen. Echter, er heerst op dit moment een klimaat waarin de boodschapper wordt gestraft en de betreffende departementen en bedrijven niet tot verantwoording worden geroepen. Wij zijn daarom terughoudend in het delen van informatie over deze beveiligingslekken.” Hij besluit dat zij beschikken over de juiste kennis en kunde en dit graag ter beschikking stellen aan de volksvertegenwoordigers.

Brenno de Winter heeft als journalist de brief ook ontvangen en doet twee dagen later een rondje langs de betrokken Kamerleden. Daar blijken verschillende woordvoerders wel oren te hebben naar helpende hackers. PvdA’er Heijnen stelt zelfs een regeling voor, want “deze klokkenluiders moeten beschermd worden en niet achtervolgd. Ze leggen immers het falen van ICT-systemen bloot.” De Winter legt het voorstel van Heijnen voor aan de woordvoerders van andere partijen. Ze reageren positief. Als hij het aantal zetels van de partijen optelt, komt hij op 120 en concludeert dat het voorstel goede kans maakt als het in de Kamer zou worden besproken. Maar zover komt het echter niet.

Vervolgens wordt De Winter gehoord in de Tweede Kamer. Hij stelt dat de overheid structureel faalt bij informatiebeveiliging omdat het onvoldoende leeft onder de managers bij de overheid. Daarom onthult hij een plan dat hij al langer had: de komende maand publiceert hij elke werkdag over een nieuw beveiligingslek. Dan zal iedereen zien hoe slecht het is gesteld in Nederland. De journalist wordt namelijk nogal eens benaderd door hackers die lekken hebben gevonden, maar die niet zelf naar buiten willen brengen. Tot nu toe twijfelde hij nog over de onthullingen, want ze zouden misschien verkeerd kunnen vallen bij politie, justitie en het publiek. Maar nu is de tijd rijp.

Oktober 2011 zal de geschiedenis ingaan als Lektober. Deze omvangrijke actie kan De Winter niet in zijn eentje doen, dus gaat hij samenwerken met Webwereld. Hij schrijft op dat moment ook al voor NU.nl, maar de ICT-nieuwssite leent zich naar zijn inschatting meer voor dit plan. Het is toch iets dat het midden houdt tussen journalistiek en actievoeren. Hij heeft dan al veel lekken, maar als de site een week voor oktober de actie aankondigt, gaat de teller al snel richting de vijfhonderd meldingen. Die worden teruggebracht tot 28 onthullingen, elke werkdag één.

Lek 1 krijgt hij van Wouter van Dongen, die in het volgende hoofdstuk aan het woord zal komen. Deze onderzoeker was net begonnen met zijn eigen bedrijf. Bij wijze van marktonderzoek had hij de websites geanalyseerd van bijna alle Nederlandse gemeenten en vond hij veel sites die kwetsbaar zijn voor SQL injections en Cross Site Scripting. SQL, Structured Query Language, is een taal waarin een website communiceert met de achterliggende database. Ga je op een site, in een tekst box waar je bijvoorbeeld je naam zou moeten invullen, SQL-code zetten, dan kun je via de site de achterliggende database aansturen. Je kunt bijvoorbeeld zoeken op een naam van een persoon en daar gegevens over opvragen. Je kunt die gegevens ook aanpassen of de database opdracht geven een beheerdersaccount voor je aan te maken. Zo kun je dus eigenlijk de site helemaal overnemen.

Cross Site Scripting, ook wel XSS, is een vergelijkbare techniek. Ook hier ga je een code invoeren waar het niet hoort, bijvoorbeeld in de adresbalk of de cookies die vanuit je browser naar de site worden gestuurd. Je kunt dan een sessie die een andere gebruiker heeft met de site overnemen en je naar die site voordoen als die gebruiker, of andersom. Deze kwetsbaarheden zijn al langer bekend en de website moet zo worden ingesteld dat de kwalijke codes worden afgevangen, maar dat wordt dus niet altijd goed gedaan. Dat is op zich niet zo heel vreemd, want dat waren toen en nog steeds de twee meest voorkomende kwetsbaarheden bij websites.

In het verslag van De Winter lezen we hoe Van Dongen met deze technieken iemands DigiD zou kunnen overnemen. Dit is weliswaar een kwetsbaarheid in de site van de gemeente, maar

De Winter ziet hierin vooral het falen van Logius, de uitvoeringsorganisatie van Binnenlandse Zaken die het DigiD-stelsel beheert. Die zou moeten controleren of de urls niet worden gemanipuleerd, dat er met cookies kan worden geknoeid of dat er op andere manieren een sessie wordt onderschept. Er is wel een checklist voor de gemeenten, maar daar staat niets in over beveiligingseisen. Hij concludeert: “Het is niet de eerste keer dat Logius in opspraak raakt over geblunder met beveiliging. Precies een maand geleden bracht de organisatie een advies uit over de DigiNotar-crisis. Daarin stelde het bestuursorgaan dat er geen reden was om te twijfelen aan de integriteit van de PKI Overheid-certificaten. Dat was niet waar, aangezien de systemen voor PKI-overheid wel degelijk ook waren gekraakt door de inbreker.”

Het artikel besluit met een aankondiging: “Dit DigiD-lek is alvast een opwarmer voor Lektober, waarin Webwereld iedere werkdag van de maand oktober een privacylek blootlegt. Hiermee willen we de aandacht vestigen op de slechte bescherming van privacygevoelige gegevens in de semipublieke sector en bij bedrijven.” Een greep uit de titels:

‘SQL-injectie bij Erasmus MC’
‘Overheid lekt wachtwoorden Raad van State’
‘Accounts ov-chipkaart.nl volledig te kapen’
‘Database BOVAG wagenwijd open’
‘Eindhoven Lektober Lekkenkampioen’
‘Vliegschool lekt BKR-gegevens en strafblad’
‘UU lekt privédata tienduizenden studenten’

Het ritme van de herhaling en de diversiteit aan organisaties die de boel niet goed op orde hebben, schetsen een beeld dat zo’n beetje alles in Nederland te hacken is. Achter dit geschakeerde beeld zit een terugkerende verhaallijn. Het gaat meestal om een verouderde site waar een SQL-injectie mogelijk is. Soms kunnen ook cookies afgevangen worden en sessies worden overgenomen door Cross Site Scripting. Verder wordt de techniek niet beschreven, want het gaat voornamelijk om wat voor data je ermee zou kunnen inzien. Sites lekken bijvoorbeeld tabellen met namen, adressen en woonplaats of combinaties van gebruikersnamen en wachtwoorden van mensen die zich op de

site hebben aangemeld. Soms ook financiële en medische gegevens die ze ooit hebben ingevuld. Het gaat in ieder geval telkens om persoonlijke gegevens, die ook van jou of mij kunnen zijn.

De organisaties waar het lek is gevonden worden gevraagd om een reactie, die ze meestal geven, de ene keer defensief en ontkennend, de andere keer toegeeflijk of zelfs dankbaar voor de melding. In de regel is de site nog voor de publicatiedatum gefikst. Slechts drie melders worden bij naam genoemd. De rest is ‘een bron’, of ‘een hacker’, of de huismelder met het pseudoniem ‘Pompidompidom’.

Hoe ging de redactie te werk? Wat was hun ethische code om verantwoord te onthullen? Volgens De Winter werd een lek altijd eerst gemeld bij de eigenaar van de site. Dat was nog een hele klus, want hij had toen al 480 meldingen en daar kwamen er gaandeweg nog eens 317 bij. Ze hadden dan ook vooraf samenwerking gezocht met Govcert. De Vereniging Nederlandse Gemeenten deed ook mee en had zelf contact gezocht met Webwereld, want ze hadden door Van Dongens onderzoek de onthullingen al zien aankomen. Zo konden veel meldingen al achter de schermen afgehandeld worden. Voor de Lektobernieuwsitems moest het gaan om sites die persoonsgegevens verwerken. Daarmee is het veiligheidslek ook een privacyprobleem, wat het tot een publieke zaak maakt. Ze kregen daarom ook veel meldingen over medische sites, omdat het daar om nog gevoeligere persoonsgegevens gaat. Maar het moest vooral ook een interessante mix zijn: grote en kleine organisaties, bedrijfsleven en overheid. De lezer moest het gevoel krijgen dat het ook hem kan overkomen.

De Winter zou oorspronkelijk alle stukken schrijven, maar dat werd al snel teveel. Jasper Bakker nam er zes over. Sander van der Meijs, Bas Bareman en Andreas Udo de Haes schreven er elk ook één. Onderling hadden ze afgesproken organisaties en hun websites bij naam te noemen worden, tenzij ze daarmee de gebruikers in gevaar zouden brengen. Eén melding ging bijvoorbeeld over een datingsite en die was bij publicatie nog niet gefikst. Je zou nog steeds de e-mailadressen van gebruikers

kunnen opvragen en ze ook identificeren, omdat ze zich hadden ingeschreven met hun werkmailadres. Ook een GGZ werd niet bij naam genoemd, vanwege de gevoelige data. Systeembeheerders zouden ze ook niet bij naam noemen. Woordvoerders weer wel, want die hebben een publieke functie. Degenen die de lekken gemeld hadden, zoals Wouter van Dongen, werden alleen bekend gemaakt als ze dat zelf wilden.

Geenstijl had ook een reeks lekken gevonden bij de gemeente Eindhoven en brengt ze op 8 oktober samen met Webwereld naar buiten. Deze weblog noemt zichzelf “Tendentieus, Ongefundeerd & Nodeloos kwetsend” en gaat zoals te verwachten wat grover te werk. Het artikel opent: “Deze gemeentewebsites zijn allemaal LEK! En dan bedoelen we niet een beetje lek. Maar echt gigantisch omfg niet te geloven wat een enorm gat daar passen moeiteloos vijf Boeing 747’s naast elkaar in. Zo lek dus.” Wat volgt, is een lijst van vijftig urls van gemeentelijke sites, met screenshots en uitleg hoe je erin kunt. Dat kan vrij eenvoudig, want vele draaien op oude Windowsmachines die je met gewone DOS-commando’s kan aansturen: “Je tikt gewoon dir + schuine streep en alle geheime databases verschijnen gewoon op het scherm. Stelletje amateurs!”, aldus Geenstijl. Webwereld gaat iets subtieler te werk. Hier geen screenshots van de gehackte sites, maar de bekende redactieformule. Boven een afbeelding van gatenkaas prijkt de titel ‘Lektober superknaller: Megalek treft 50 gemeenten’.

De superknallers leiden tot Kamervragen. SP’er Sharon Gesthuizen stuurt diezelfde avond vanaf haar iPhone een dringende mail naar minister Donner van Binnenlandse Zaken. Kamerleden El Fassed (Groen Links) en Heijnen (PvdA), staan in de cc. Ze vraagt de minister om alvast te reageren op de vijftig lekke sites. Graag voor 13 oktober, want dan staat er een groot ICT-debat op het programma.

Donner reageert op 11 oktober met een brief: ‘Betreft lekken in een aantal gemeentelijke sites’. Hij schrijft dat Lektober inderdaad heeft aangetoond “dat ICT-beveiliging bij overheidsorganisaties tekortschiet”. Dit is volgens de minister in eerste instantie de verantwoordelijkheid van die organisaties zelf, maar gezamenlijk

vormen zij een keten waar de veiligheid afhangt van de zwakste schakel. Hij heeft daarom Logius opdracht gegeven de getroffen organisaties af te sluiten van DigiD. Ze worden pas weer aangesloten als hun beveiliging op orde is. Dat kost hen misschien geld en is lastig voor de burger, maar vertrouwen in het systeem als geheel is belangrijker. Voor alle andere gemeentelijke sites komt er een audit, die begin 2012 afgerond moet worden en jaarlijks herhaald wordt.

Dit kordate optreden van de minister staat in schil contrast met het imago dat hij heeft als het gaat om ICT-dossiers. Een maand voor dit debat was hij in Nieuwspoort, om het iOverheid rapport van de Wetenschappelijke Raad voor Regeringsbeleid in ontvangst te nemen. De WRR had een overtuigend verhaal over onbeheersbare informatiestromen bij de overheid en riep de regering op de regie te nemen. Wat deed de minister? Hij hield een iPad omhoog en zei: “Kijk, eindelijk een apparaat waar ik wat aan heb. Hier kan ik mijn papiertje op leggen en met mijn vulpen aantekeningen maken.” Het was niet zozeer de flauwe grap die ergernis in de zaal sorteerde, maar vooral de manier waarop hij alle problemen met een glimlach wegwuifde. Iemand naast me verzuchtte: “En dit is dus de belangrijkste man in de ICT van Nederland...”

In het debat ‘Diginotar en ICT problemen bij de overheid’ van 13 oktober maken diverse Kamerleden gebruik van het archaïsche imago van de minister om hem op zijn plek te zetten. Sharon Gesthuizen van de SP begint als eerste vragensteller: “Minister Donner gaat zeggen dat de wereld misschien wel in zeven dagen is geschapen, maar dat hijzelf niet bij machte is om wonderen te verrichtten.” Donner corrigeert haar: “Zes dagen!” en laat verder haar aanvallende inleiding over zich heen komen. Vragenstellers na haar spreken de minister aan als de man met de vulpen. Webwereld bericht over het debat: ‘Politiek witheet door Lektober, wil actie Donner’.

Aanleiding voor het debat was Diginotar dat in eerste instantie een incident leek, maar nu zoveel kwetsbaarheden naar buiten kwamen, konden de Kamerleden spreken van een structureel probleem en de regering ter verantwoording roepen. Gesthuizen: “Hadden we het maar over een incident, maar helaas is dat niet

zo. Het is eerder regel dan uitzondering dat ICT-projecten bij de overheid tot veiligheidsproblemen leiden.” Ze noemt de OV-chipkaart, DigiD en “alles waarmee wij nog geconfronteerd zullen worden gedurende deze ‘lektober’”. Ze roept op tot een parlementair onderzoek en het inschakelen van een digitale brandweer met doorzettingsmacht.

Haar collega’s Heijnen (PvdA), Hachchi (D66), El Fassed (GroenLinks), Elissen (PVV), Koopmans (CDA) en Hennis-Plasschaert (VVD) doen de argumentatie nog eens dunnetjes over, elk met eigen oplossingen. Relevant voor dit verhaal is hoe er door de Kamerleden wordt gesproken over de Lektoberhackers. Hachchi: “In de afgelopen weken hebben hackers de beveiliging van computersystemen van de overheid blootgelegd. Is de minister bereid te onderzoeken hoe de overheid de beveiliging van haar computersystemen kan verbeteren met de expertise van hackers, zonder dat de hackers hier strafrechtelijke consequenties van ondervinden?”

Heijnen over Lektober: “Als burgers gaten aanwijzen in de beveiliging van overheidssites, zouden wij hun eigenlijk een bos bloemen moeten geven. Tegelijkertijd kunnen we ons afvragen of door de activiteiten van burgers geen schade ontstaat. Is het eigenlijk niet veel beter als de dames en heren hackers – en dan doel ik op het vriendelijke deel ervan, want het onvriendelijke deel zal ik niet willen aanspreken – een bv’tje maken, van negen tot vijf werken op een adres dat we allemaal kennen en daarna gewoon de rekening sturen?”

Donner weet zich hier niet echt raad mee. Eerst stelt hij dat ze de Diginotarhackers ook niet met open armen hebben ontvangen, dus waarom deze hackers wel? Maar de overheid maakt wel gebruik van “informatie van hackers dat bij bepaalde instanties de voordeur openstaat”. Dan: “Waar ze zich aanbieden, zullen wij ze inhuren.” En vervolgens: “Mijn beeld is dat zodra hackers er hun brood mee verdienen, het een beveiligingsinstituut wordt en dat de volgende hacker zal inbreken bij dat beveiligingsinstituut. Je kunt ze er dus maar beter niet hun dagelijks brood mee laten verdienen.” Het bv’tje van Heijnen ziet hij in ieder geval niet zitten. Maar, hoe het dan wel moet, blijft vaag.

Dan komt Ivo Opstelten aan het woord. Als minister van Veiligheid en Justitie is hij de ‘coördinerende minister op het terrein van cyber security’, dus degene die wel zou moeten weten hoe om te gaan met verantwoorde onthullingen. Opstelten: “Wij staan positief tegenover het inzetten van externe deskundigen, maar hackers zijn inbrekers als zij kwade bedoelingen hebben, dus ik moet wel een scheiding maken tussen al of niet te goeder trouw. De woordvoerders en ik zullen het erover eens zijn: mits binnen de juridische kaders valt.” Maar dat is nu juist het punt. De Lektoberhackers plegen stelselmatig computervredebreuk, maar wel voor een goed doel.

D66-lid Hachchi vindt dat ze gevrijwaard moeten worden van vervolging en dient daarom een motie in. Dit is in het Kamerjargon “een uitspraak van één of meer Tweede Kamerleden om aan te geven dat een onderwerp belangrijk is, met een oproep aan de regering om actie te ondernemen”. Om een beetje gevoel te krijgen voor hoe zoiets gaat, volgt hier de integrale tekst:

“De Kamer, gehoord de beraadslaging, overwegende dat hackers gebreken in de beveiliging van computersystemen van de overheid kunnen ontdekken, zoals het geval was bij de stemcomputers en de ov-chipkaart; overwegende dat het in het algemeen belang is dat hackers hier melding van maken bij de overheid; overwegende dat hackers illegaal systemen binnendringen wat strafrechtelijke consequenties kan hebben; overwegende dat de ICT-kennis van hackers ver vooruitloopt op die van de overheid; verzoekt de regering, te onderzoeken hoe de overheid de beveiliging van haar computersystemen kan verbeteren door gebruik te maken van de kennis van hackers zonder dat hackers hier strafrechtelijke consequenties van ondervinden, en gaat over tot de orde van de dag.”

De indiening van deze motie wordt volgens de voorzitter voldoende ondersteund, maar de ministers zijn er niet blij mee. Donner verschuilt zich achter Opstelten, want als het gaat over immuniteit is dat iets voor Justitie. Opstelten: “Ik moet nadrukkelijk zeggen dat het aannemen van deze motie door ons wordt ontraden omdat het niet kan. Wij maken graag gebruik van hackers, maar binnen de grenzen van onze rechtsstaat en binnen de grenzen die de wet toestaat.” PvdA, SP, GroenLinks, D66 en

PvdD stemmen voor de motie. VVD, PVV, CDA, CU en SGP zijn tegen - een meerderheid, waarmee de motie wordt verworpen.

Dit is dus hoe onthullingen kunnen doorwerken in Kamerdebatten. Vaak wordt er niets mee gedaan, omdat de Kamerleden die over ICT gaan het op dat moment niet opportuun achten. Komt een lek uitgebreid in de media en gaat het ook nog eens om de persoonsgegevens van hun electoraat, dan wordt het alweer een stuk interessanter om zich ermee als vertegenwoordiger te profileren. Zijn er meerdere lekken, dan hebben we een structureel probleem en genoeg voer voor een pittig debat dat, zoals in dit geval, doorloopt tot diep in de nacht. De winst van die avond is dat er uitvoerig werd gesproken over wie nu verantwoordelijk is voor de veiligheid van Nederlandse overheidssites. Maar voor helpende hackers leverde het niet veel op. Wat ze doen blijft in feite strafbaar.

In dit juridisch vacuüm kreeg Webwereld dan ook aardig wat dreigementen over zich heen van mensen die het niet eens waren met hun wijze van actievoeren. Zo ontving De Winter een dreigende brief van een burgemeester. Als Webwereld iets over zijn gemeente zou onthullen, wordt alle schade op hen verhaald. Iemand van een bedrijf dat websites bouwt, dreigde aan de telefoon zelfs hem aan de hoogste boom op te knopen. Als hij hier later over vertelt, kan hij hier nog wel om lachen: “Ik zei: ‘kunt u wat rustiger praten. Ik kan het niet bijhouden met het opschrijven van uw citaat’.” Over een ander incident is hij minder vrolijk. Als hij op een gegeven moment uit de trein stapt, komt er op het perron een vrouw achter hem aan en trekt hem aan zijn schouder. Ze zegt: “Heb het nu wel gehad met Lektober” en geeft hem een klap vol in het gezicht. De Winter is totaal verbouwereerd, maar doet uiteindelijk geen aangifte van het incident.

De redactie van Webwereld ging het erom het brede publiek bewust te maken van digitale kwetsbaarheden door ethische hacks op een verantwoorde manier te onthullen. Dat was gelukt. Brenno de Winter werd dankzij deze actie en die van de OV-chipkaart door Villa Media uitgeroepen tot journalist van het jaar. Nu over naar Wouter van Dongen, de melder van Lek 1. Ook voor

hem was het een zware periode en hield hij er uiteindelijk toch nog iets leuks aan over.

6. DongIT en het DigiD debacle

Ethisch hacken als business case

Wie de site van Dong-IT opzoekt, ziet nog de sporen van de onthullingen uit 2011. Op de voorpagina staan het rapport met de scan van kwetsbaarheden bij gemeentesites, het journaalitem waarin hij erover vertelt en de overheidsrichtlijnen voor veilig gebruik van DigiD. Een rode knop met slotje vraagt: “Hoe veilig is uw website?” Blijkbaar zijn er steeds meer mensen die deze vraag stellen aan Wouter van Dongen, want hij heeft nu zes mensen in dienst en er staan nog drie vacatures open. Is ethisch hacken een business case? Hoe heeft Lektober hem daarbij geholpen?

Ik spreek Van Dongen op zijn kantoor aan de Schipholweg in Leiden. Hij vertelt dat hij al vanaf zijn puberteit gekke dingen uithaalde met websites. Waarom? “Het is de drive om zaken te manipuleren, terwijl ik niet altijd wist wat ik aan het doen was.” Hij deed twee studies, Informatica en System & Network Engineering, en studeerde cum laude af. Tijdens zijn studie ontwikkelde hij al websites in opdracht en was hij veel bezig met security. “Als je net wat anders denkt dan anderen, dan is het internet een grote speeltuin. Webontwikkeling met als focus websecurity is daarin het hogere segment. Daar wilde ik mij volledig op richten.” Zijn afstudeeropdrachten deed hij bij KPMG en het Nederlands Forensisch Instituut. Daarna werkte hij een tijdje bij Fox-IT en in 2011 zette hij zijn eenmanszaak om in een bv. Op dat moment ontdekte Van Dongen een gat in de markt: lekke websystemen bij gemeenten.

De aanleiding is een kennis die bij een gemeente werkt die net een nieuwe site heeft. De kennis is er erg enthousiast over en zegt tegen Van Dongen dat hij er maar eens naar moet kijken. Dat doet hij en uiteraard kan hij het niet laten hier en daar wat vreemde tekens in te voeren. En jawel, de codes worden niet afgevangen en hij kan de achterliggende database aansturen door misbruik te maken van een lek in TYPO3, het achterliggende

content management systeem. Vervolgens kan hij inloggen aan de beheerderkant van de site en komt daar allerlei mailsystemen en databases tegen. Daarnaast ziet Van Dongen nog een probleem: ze gebruiken veel onveilige standaardinstellingen van TYPO3. Het systeem blijkt bijvoorbeeld wachtwoorden van bezoekers gewoon op te slaan als platte tekst, dus zonder enige versleuteling. Ook de cookies worden onbeveiligd opgeslagen. Hij zou hier kunnen Cross Site Scripten en een sessie van een nietsvermoedende gebruiker van de site overnemen. Alles bij elkaar best gevaarlijk dus, maar op zich makkelijk te verhelpen.

De gemeente zit op dat moment in een gebruikersvereniging van nog veertig gemeenten die hetzelfde CMS gebruiken: de TYPO3-gemeenschap. Als ze daar horen wat Van Dongen heeft gevonden, vragen ze hem of hij op 29 september 2011 een presentatie wil houden over webbeveiliging. Dat wil hij wel, want het is een mooie gelegenheid om zijn kunnen te tonen en nieuwe klanten te vinden. Het moet geen theoretisch verhaal worden over beveiliging, maar concreet en confronterend. De vereniging geeft hem toestemming om te zoeken naar praktische voorbeelden bij de aangesloten gemeenten en daar screenshots van te maken voor de presentatie.

Alle gemeenten handmatig testen is nogal veel werk. Van Dongen schrijft daarom een script voor een automatische scan en die levert hem een overzicht van alle websystemen, ook de verborgen systemen en testsystemen. Hij ziet welke databases, services en versies erop draaiden en krijgt toegang tot tientallen content management systemen, mailsystemen en honderden databases van raadsinformatiesystemen en gemeentewinkels. Daarin staan duizenden persoonsgegevens van burgers, inclusief hun wachtwoorden. Diverse sites bieden DigiD aan, zonder beveiligde cookies. Daar zou hij dus ook sessies kunnen overnemen en iemands persoonlijke gegevens veranderen of toeslagen aanvragen. Na een week weet hij genoeg: het is echt heel erg slecht gesteld met de beveiliging van gemeentelijke websystemen.

Intussen krijgen verschillende gemeentemedewerkers lucht van zijn onderzoek en gaan hem bellen. Meestal willen ze gewoon

weten of hij al wat gevonden heeft. Maar er zijn er ook bij die beginnen te dreigen met maatregelen tegen hem. Hij krijgt zelfs een advocaat aan de lijn, die belt namens een bedrijf dat veel websites maakt voor gemeenten. Van Dongen realiseert zich dat hij hier op een groot probleem is gestuit en gaat op zoek naar steun om dit op een verantwoorde manier naar buiten te brengen. Zo komt hij terecht bij Brenno de Winter. Die schrijft er een stukje over voor Webwereld van 16 september: ‘Hoster lekt honderden gemeentedatabases’.

Het gaat om leverancier GemeenteOplossingen en 342 databases die in theorie ook leeg te halen zijn. Een deel daarvan bestaat uit testdatabases die geen operationele gegevens bevatten, maar het gaat in totaal wel om tientallen gemeenten, aldus De Winter. Verder wordt verteld dat onder andere het Raadsinformatiesysteem van de Gemeente Bloemendaal toegankelijk is. Best gevoelige informatie dus. De leverancier had volgens De Winter ontspannen gereageerd, want het probleem was inmiddels opgelost en de wachtwoorden zijn aangepast. Het stuk besluit cynisch: “Gemeenteoplossingen stuurt alle burgemeesters hierover een fax.”

De Winter en Van Dongen besluiten dat er nog een artikel komt over DigiD, maar dat kan nog even wachten. Van Dongen krijgt intussen ook bezoek van een journalist van Nieuwsuur, die hem interviewt over de gevonden kwetsbaarheden. Maar eerst geeft hij nog zijn presentatie bij de gebruikersvereniging, want die is op 29 september, twee dagen voor de start van Lektober. Vanwege de commotie met de advocaat en boze gemeentemedewerkers gaat hij uiterst voorzichtig te werk. Hij heeft veertig screenshots van kwetsbaarheden en zorgt ervoor dat de namen van gemeenten, systemen en gebruikers niet te lezen zijn. Wachtwoorden streept hij door. Het verhaal valt gelukkig goed. Van Dongen: “De sfeer kwam meteen los. Het publiek was geboeid en stelde goede vragen.” Hij laat ook zien welke standaardinstellingen in hun CMS ervoor zorgen dat de wachtwoorden makkelijk te kraken zijn. Hoe hij de DigiD-sessies kan onderscheppen, begrijpen ze volgens hem niet helemaal. Hij krijgt daarom veel vragen van de gemeentelijke

systeembeheerders of hij hun site ook even wil doorlichten. Daarna begint Lektober.

Nieuwsuur 1 oktober 2011. Het tv-item begint met onheilspellende muziek. We zien Van Dongen achter de computer, terwijl de voice-over zegt: “Wouter van Dongen is veiligheidsexpert en dringt binnen op een gemeentewebsite. Hij gebruikt Cross Site Scripting.” In het interview wilde hij niet zeggen welke gemeente, maar de journalist weet te vertellen dat het gaat om Amsterdam. Hij stelt dat het geen incident is, maar past in een lange reeks ICT-blunders bij de overheid. Ook Diginotar wordt erbij gehaald. Vervolgens komt Brenno de Winter in beeld: “Het blijkt dat er zoveel privacygevoelige informatie wordt gelekt, dat we elke dag wel kunnen vullen met een voorbeeld. En dat gaan we komende maand ook eens doen.” De maandag daarop, 3 oktober verschijnt zijn artikel: ‘Lek 1: Blunder Logius maakt DigiD-fraude kinderspel’.

De hele keten van onveilige schakels verschijnt dus in de media: GemeenteOplossingen, de TYPO3-gemeenschap, Bloemendaal, Amsterdam, Logius… Achteraf begrijpt Wouter wel dat journalisten deze partijen noemen, om zo het probleem concreet te maken, maar op dat moment is hij er niet blij echt mee. Hij wilde het gewoon oplossen, maar in plaats daarvan kreeg hij voornamelijk dreigende telefoontjes van gemeenten, bedrijven en hun advocaten.

De dag na de onthullingen wordt hij gebeld door iemand van Logius. Van Dongen denkt in eerste instantie: “Daar gaan we weer. Die waren natuurlijk niet zo blij met het artikel van Webwereld.” Maar tot zijn verbazing wordt hij juist vriendelijk te woord gestaan. De uitvoeringsorganisatie van Binnenlandse Zaken nodigt Van Dongen uit om zijn bevindingen te komen presenteren en is zelfs bereid hem ervoor te betalen.

Op 5 oktober verschijnt Van Dongen op het Logiuskantoor voor zijn presentatie. Tijdens zijn verhaal ziet hij de toehoorders geïnteresseerd kijken en druk aantekeningen maken. “Dat verbaasde me, want wat ik gevonden had, was toch echt laaghangend fruit. Als je techneut bent, is XSS niet zo moeilijk, maar ik las daar in de implementatierichtlijnen van DigiD niks

over. Dus ik had onder andere tips over http-only cookies, de webserver instellingen en vulnerability scans.”

Tijd voor wederhoor. Wat vinden de mensen van Logius hier nu zelf van? Als ik woordvoerder Michiel Groeneveld mijn concepttekst stuur, struikelt hij meteen over de oorspronkelijke titel van dit hoofdstuk: ‘Dong-IT en het DigiD-lek’. Daar is hij het niet mee eens en we besluiten ‘lek’ om te zetten in ‘debacle’, want: “De fout lag bij de webdiensten van de gemeenten en niet bij DigiD. Dit is in een gesprek op 5 oktober bij Logius bevestigd door Dong-IT. Nadat een burger met zijn DigiD is ingelogd, kon door de lekken aan de kant van de gemeenten de opgebouwde sessie van de webdienst met de burger worden overgenomen”, aldus Groeneveld. OK, afnemers moeten hun systemen goed op orde hebben, maar wie checkt dat? Volgens hem de gemeente: “De dienstaanbieder blijft altijd zelf verantwoordelijk voor de veilige en correcte werking van de systemen die op DigiD aansluiten.”

Wat Logius wel kan doen, is gemeenten die slordig blijken om te gaan met de veiligheid, af te sluiten van de inlogprocedure van DigiD. Dat is ook wat gebeurde na het Kamerdebat van 11 oktober 2012, dat in het vorige hoofdstuk is beschreven. Volgens Logius waren dat destijds dertig gemeenten, waarvan de meeste vrij snel weer zijn aangesloten. Uiteindelijk was er maar één gemeente die een jaar geen gebruik heeft kunnen maken van DigiD, maar daar lagen volgens Groeneveld andere redenen aan ten grondslag.

In de maanden daarna wordt bij de overheid hard gewerkt aan beleid om de gemeenten op orde te krijgen. Er komt zelfs een verplichting vanuit het ministerie van Binnenlandse Zaken aan de gemeenten om periodiek een ICT-Beveiligingsassessment DigiD te doen. Logius publiceert hiervoor op 21 februari 2012 een beveiligingsrichtlijn met daarin zowel procedurele als technische normen voor veilig gebruik van DigiD. Het Kwaliteits Instituut Nederlandse Gemeenten (KING) richt samen met de Vereniging Nederlandse Gemeenten (VNG) een Informatiebeveiligingsdienst (IBD) voor gemeenten op, die 1 januari 2013 officieel van start gaat.

Lektober is dan alweer een jaar geleden en het lijkt Van Dongen een goed moment om te kijken hoe het ervoor staat bij de gemeenten. Hij laat weer zijn scan over al hun sites gaan en concludeert in zijn rapportage: “24% van alle gedetecteerde gemeentelijke systemen kan mogelijk beïnvloed worden door de kwetsbaarheden met een hoge of kritische impact rating. De verouderde software op deze systemen zou relatief eenvoudig misbruikt kunnen worden door kwaadwillenden. Het onderzoek toont aan dat de huidige inspanningen om gemeentelijke systemen te beveiligen nog niet afdoende effect hebben gehad.”

De Informatiebeveiligingsdienst gaat dan net van start en ik ben benieuwd of ze iets hebben gedaan met het onderzoek van Dong-IT. Ik stuur een mail naar de woordvoering van de IBD met het concepthoofdstuk in de bijlage. Ook hier direct een reactie. Sonja Kok schrijft: “Ik kan u op voorhand al aangeven dat wij de melding van de heer Van Dongen destijds uiteraard serieus hebben genomen. Net als alle meldingen die wij binnen krijgen. Zeker gezien onze verantwoordelijkheid in deze. Vanuit het responsible disclosure principe, waar wij grote waarde aan hechten, hebben wij de heer Van Dongen eveneens van alle genomen stappen en de resultaten op de hoogte gebracht.”

Dat is mooi, maar als ze het concepthoofdstuk heeft gelezen, is ze minder positief over Van Dongens bevindingen: “Het onderzoek van Dong-IT in januari is onvoldoende om deze conclusie te rechtvaardigen.” Oftewel, de inspanningen om gemeentelijke systemen te beveiligen zouden wel afdoende effect hebben gehad. “Gemeenten voeren al jarenlang audits uit. Sinds 2013 is hier het verplichte ICT-Beveiligingsassessment DigiD aan toegevoegd.” Over het DigiD-debacle wil ze nog wel even kwijt: “Op dat moment bestond er nog geen IBD. Wat doet de IBD nu: gemeenten vanuit hun eigen verantwoordelijkheid concrete handvatten geven om structureel het onderwerp informatiebeveiliging op te pakken.”

Het is interessant hoe verschillend de partijen aankijken tegen informatiebeveiliging. Van Dongen heeft vooral gekeken wat technisch mogelijk is: kan hij het hacken en zo ja, hoe is het te fixen? De journalisten zijn vooral geïnteresseerd wat de eventuele impact kan zijn van lekken op gebruikers en wie daarvoor

verantwoordelijk is. De minister heeft politieke daadkracht getoond door de gemeenten af te laten sluiten en instellingen opdracht gegeven de procedures aan te scherpen. Logius en IBD kijken vervolgens vooral of die procedures ook goed worden opgevolgd en staan nieuwsgierige burgers graag te woord om uit te leggen dat dat ook gebeurt.

Heeft Van Dongen tot slot nog klanten overgehouden aan het hele DigiD-debacle? Direct na Lektober kwamen er inderdaad een aantal gemeenten naar hem toe om hun TYPO3 door te lichten. Zijn tweede onderzoek, een jaar later, leverde niets op. Gemeenten werden toen weliswaar verplicht security audits te doen, maar lieten die vooral doen door de bekende consultancy bedrijven. Enigszins verbolgen stelt hij dat gedacht wordt dat inschakeling van die grote bedrijven met bekende namen en bijbehorende tarieven altijd garant staat voor een goede oplossing.

Van Dongen en zijn team gingen zich daarom in 2013 vooral richten op bedrijven, want daar viel toch de meeste winst te behalen. Totdat hij werd benaderd door een webbouwer die ook gebruik maakt van TYPO3, het CMS waar het allemaal mee begon. Hij was net na Lektober al eens bij hen langs geweest voor een presentatie en nu komt het bedrijf met een interessant voorstel. Ze moeten als onderdeel van de aangescherpte DigiD-richtlijnen hun code door een onafhankelijke derde partij laten auditen. Dong-IT lijkt hen de juiste partij daarvoor.

Als ik hem in november 2014 vraag hoe het ervoor staat, vertelt Van Dongen dat ze een groot aantal gemeenten in hun portfolio hebben en pentesten uitvoeren voor bekende grote bedrijven. Als de TYPO3-sitebouwer een systeem voor een gemeente oplevert, zetten ze Dong-IT in de offerte als securitymodule, zonder daarvoor iets extra’s voor henzelf in rekening te brengen. Zo voldoen zij en de gemeenten aan de richtlijn, kan Van Dongen als helpende hacker doen waar hij goed in is en worden de gemeentesites, drie jaar na Lektober, langzaam maar zeker steeds veiliger. Ethisch hacken is dus een business case. Maar je moet als melder wel veel geduld hebben als het gaat om overheidsorganisaties. Dat geldt ook voor hackers

die onthullen uit ideologische motieven. Die zien we terug in het volgende hoofdstuk.

7. @okoeroo en de pompen van Veere

SCADA-systemen blijken bloot op internet te staan

14 feb 2012. EenVandaag opent met onheilspellend nieuws: “Het blijkt kinderlijk eenvoudig om vanachter je eigen computer een hele polder onder water te zetten. Sluizen, gemalen en pompen, maar ook slagbomen in tunnels en elektriciteitscentrales, kun je op afstand bedienen via internet.” De redactie heeft dat zelf vastgesteld en vindt het zo alarmerend dat ze voorafgaande aan de uitzending de Nationale Coördinator Terrorismebestrijding en Veiligheid heeft gewaarschuwd.

Dan komt ‘internetbeveiliger’ Oscar Koeroo in beeld: “Wat ik gezien heb, is dat machines bloot aan het internet staan.” Hij zou zelfs aan zijn moeder kunnen uitleggen wat ze moet doen om die machines over te nemen. Bijvoorbeeld de pompen van Veere, die met een dijk de zee van binnenwater afscheiden. Die kun je stilzetten of de andere kant op laten draaien, totdat de dijk het niet meer houdt en Veere onderloopt. Rob van der Zwaag, burgemeester Veere wordt ter verantwoording geroepen: “Gisteren hebben we de stekker eruit getrokken en nu wordt het opgelost.”

Dit incident staat niet op zich. In heel Nederland staan dergelijke systemen gewoon online. De redactie laat zien hoe ze bij het Leger des Heils de verwarming hebben uitgezet. Dat is nog een onschuldig voorbeeld. In Amerika heeft iemand op deze manier gevangenisdeuren op afstand geopend. In Nederland zijn vooral de watersystemen kwetsbaar. Terroristen, kwaadwillende mogendheden, ja zelfs onverantwoordelijke 13-jarigen, kunnen bij de online systemen en zo Nederland laten onderlopen. Na wat experts die dit beamen komen Kamerleden Hennis-Plasschaert en Hachchi in beeld. Ze zijn geschokt en beloven opheldering te vragen bij de minister. Want waterbeheer is in Nederland een kwestie van nationale veiligheid.

Was Nederland werkelijk in gevaar? En hoe kon het dat deze dreiging toen pas aan het licht kwam? Ik vraag het op 19 februari 2014 aan Oscar Koeroo, ook wel @okoeroo. Hij werkt op dat moment in de Chief Information Security Office bij KPN – REDteam. Dat betekent dat zijn team af en toe het BLUEteam van KPN probeert te hacken om zo de beveiliging te testen. Op zijn site oscar.koeroo.net is te midden van allerlei computercodes te lezen dat hij een ‘Grid Computing Security Nerd’ is en een ‘computer (ab)user extraordinaire’. Hij vertelt me dat hij weliswaar de kwetsbaarheden bij Veere had aangetoond en nog wat andere dingen had gevonden. Maar, de onthulling dat al die systemen zo bloot op het internet staan, was kort daarvoor gedaan op Twitter, door ene @ntisec. Die had al de lekke systemen gepubliceerd, zonder waarschuwing vooraf aan de eigenaren, laat staan met tijd om de lekken te dichten. Dit is geen responsible, maar full disclosure.

Op het moment van de onthulling werkte Koeroo nog bij Nikhef, het nationale instituut voor subatomaire fysica. Daar ontwikkelde en beheerde hij een systeem om de computers van onderzoeksinstituten met elkaar samen te laten werken in de European Grid Infrastructure. Hij is nog steeds trots dat hij het toegangssysteem tot de grid zelf heeft ontworpen en het nu nog door vierhonderd organisaties wordt gebruikt. De beveiliging is uiteraard topprioriteit en wordt continue getest. Als iemand een kwetsbaarheid vindt, kunnen ze dat melden via Report-vulnerability@egi.eu. De melder krijgt dan meteen een bericht van ontvangst en de vraag of hij ook zijn naam vermeld wil zien. Credits voor een melding is namelijk belangrijk in academische kringen. Een team beoordeelt de kwetsbaarheid direct en als het kritiek is, laten ze al het andere werk vallen om er meteen mee aan de slag te gaan. Hier dus een goed voorbeeld van geïnstitutionaliseerd ethisch hacken. Maar hoe anders ging het nu met de Nederlandse systemen. Koeroo wilde er iets aan doen.

Het systeem waar het hier om gaat is SCADA: Supervisory Control and Data Acquisition. Dit wordt wereldwijd veel gebruikt. Niet alleen bij pompen, maar bijvoorbeeld ook bij verkeersseinen, vliegtuigen, straatverlichting, generatoren, van alles... Het verstuurt en bewerkt meet- en regelsignalen van deze machines

online. Als je inlogt, zie je een schema van een systeem met getallen die continue veranderen. Meestal kun je alleen kijken, maar bij sommige systemen kun je ook de waarden aanpassen. Heb je het wachtwoord, dan kun je inloggen. Bij sommige systemen zijn de wachtwoorden niet ingesteld en volstaat ‘admin’, ‘welkom’ of kun je er zo in. Je hoeft dan dus alleen maar het internetadres te vinden. Dat kan via shodanhq.com, een zoekmachine voor alle apparaten die online staan. Zoek je op SCADA, dan krijg je een hele lijst IP-adressen, die je ook nog eens kunt ordenen naar locatie, bijvoorbeeld Nederland. Dat is dus wat @ntisec had gedaan en begin januari 2012 zet hij alles online.

Koeroo ziet de lijsten met IP-adressen langskomen op Twitter en mailt met andere informatiebeveiligers om te helpen zoeken naar kwetsbare systemen en er wat aan te doen. Zelf start hij bij het gemaal van Veere, want dat wordt expliciet genoemd. Hij typt in zijn browser een IP-adres dat @ntisec had getwitterd en ziet direct een beheeroverzicht van de installatie. Inloggen was niet eens nodig. Het overzicht geeft aan wie de controle over de apparatuur nu in handen heeft, maar het blijkt dat je ook kan aangeven wie dat is. Jezelf bijvoorbeeld en dan kan de originele beheerder er niet meer in. Koeroo ziet ook hoe je de apparatuur kunt uitlezen en aansturen. Dan weet hij genoeg en stopt. Hij wil geen schade veroorzaken aan de machinerie en belt de beheerder.

“Hallo met Oscar Koeroo van Nikhef, Incident response-team. Iemand heeft problemen met jullie machines en netwerk gevonden en jouw naam en IP-adres getwitterd.” Koeroo vertelt wat hij ziet op zijn scherm. De man reageert defensief: “Nee hoor, daar kun je niet bij, want dat is een apart netwerk” en verbreekt de verbinding. Als Koeroo later in de trein zit, wordt hij teruggebeld. De man probeert hem te overtuigen dat hij toch niets kan met de apparaten, want de werking is zeer specifiek. Daar neemt Koeroo geen genoegen mee: “Ik werk in een lab waar we dagelijks SCADA-systemen instellen. Wat nou als ik het uitzet? Of omgekeerd laat draaien?” Nee, dat moet hij vooral niet doen. Het blijft een moeizaam gesprek. @okoeroo gooit er daarom maar een tweet uit: “Heb contact gehad met de beheerder, maar helaas

niet met het resultaat waarop ik hoopte.” Binnen een uur krijgt hij een DM van @jblokzijl: “Wil je er wat meer over vertellen?”

Joost Blokzijl is redacteur bij het tv-programma EenVandaag. Hij is daar degene die over de ICT-onderwerpen gaat. De pers dient volgens hem een publiek belang bij verantwoorde onthullingen. “In het algemeen, als iemand iets meldt, wordt het niet gefikst. Maar als wij er iets mee doen, weet je dat er wat verandert. Wij zijn de waakhond. Ze weten dat als de tv erbij komt dat heel veel mensen het zien.” Tegelijkertijd is het wel moeilijk om een goed item te maken van dergelijke abstracte materie. “Elke maand is er wel een hack. Maar wij zijn wel tv voor algemeen publiek. Ik denk altijd maar: mijn ouders moeten het ook kunnen snappen”, aldus de redacteur.

Als volger van @ntisec had hij zelf ook de IP-adressen op Twitter voorbij zien komen. Het lukte hem zelfs de persoon achter dit pseudoniem te spreken, maar die wilde alleen anoniem op tv. Daarom benaderde hij @okoeroo en die wil het wel voor de camera uitleggen. Koeroo vraagt wel eerst toestemming aan zijn afdelingshoofd, die op zijn beurt naar de directeur stapt. Het gaat immers om gevoelige informatie die dan aan de naam van Nikhef zou worden gekoppeld. Directeur Frank Linde reageert echter meteen enthousiast: “Goed om te laten zien dat wij hier slimme jongens hebben en ook in den lande aan security doen.” Koeroo wordt daarmee het gezicht bij de onthullingen. Met EenVandaag spreekt hij een termijn af van twee weken om het probleem volledig in kaart te brengen.

In het verslag van Koeroo is te lezen wat hij tegenkomt op de verschillende IP-adressen. Je kunt ook op een kaart precies zien waar servers staan in Zeeland: Zoutelande, Serooskerke, Domburg en die vallen allemaal onder de gemeente Veere. Op nummer 62.132.58.89 verschijnt een inlogscherm van een Zyxelmodem. Je hoeft hier geen naam in te vullen, alleen een wachtwoord. Hij probeert ‘admin’. Nee, die was het niet. Dan ‘veere’ en jawel, hij ziet een configuratiescherm van een router. Hij kan vervolgens inloggen op de router op het kantoor in Domburg en komt zo in het netwerk van hun SCADA-controlecentrum. Daar ziet Koeroo ook machines in dorpen die hij nog niet op de lijst had

staan. Ze werken allemaal met ‘Aquaview’, dat blijkt de beheersoftware te zijn.

Overal waar hij komt, kijkt hij, laat de instellingen voor wat ze zijn en maakt een screenshot. De afbeeldingen tonen mooi het dilemma van de ethisch hacker: je wilt laten zien dat je ergens in kunt en schade aan zou kunnen richten, zonder dat werkelijk te doen. Net op het moment dat je het beheer zou kunnen overnemen, moet je snel een foto maken en dan wegwezen. Kwaadwillenden zouden daar verder gaan: systemen verstoren en ze zelfs zo instellen dat de oorspronkelijke beheerders er niet meer in kunnen of een namaakoverzicht krijgen dat zegt dat er niets aan de hand is. De Zeeuwse polder is inderdaad in gevaar en niemand weet het behalve Oscar Koeroo. En @ntisec natuurlijk.

Andere media gaan intussen ook aan de haal met de lijst van @ntisec. Webwereld had op 18 januari al onthuld dat de douches van Spijkernissen aan- en uitgezet konden worden. Tweakers zette op 20 januari zelfs een hele lijst met kwetsbare systemen online, gevolgd door een diepgaand artikel: ‘Scadabeveiliging: een structureel probleem’. Journalist Joost Schellevis opent met een treffend voorbeeld: een gefrustreerde werknemer in Australië heeft met de SCADA van de rioolzuivering geknoeid en 800.000 liter afvalwater geloosd. Rivieren en parken vervuild, dieren dood. Nu wordt het serieus. Het stuk leidt zelfs tot Kamervragen.

EenVandaag moet dus snel met iets goeds komen, maar heeft meer tijd nodig. Blokzijl: “Een krantenstukje is zo getikt, wij moeten iets visueel maken. Bij ICT is dat vreselijk moeilijk.” Dankzij Oscar Koeroo heeft hij nu een concreet verhaal voor de kijker: een echte nerd die door een grote serverruimte loopt, beelden van sluizen, gemalen en pompen en een geschokte burgemeester die ter verantwoording wordt geroepen. Veiligheidsexpert Peter de Rooij vertelt voor een kaart van Nederland wat er zou gebeuren als er geknoeid wordt met de pompen van Veere. De dijk is al zwak en als er teveel water achter zit, kan die bezwijken en loopt een heel gebied onder.

De redactie neemt zelf ook contact op met de gemeente Veere. Blokzijl stuurt de systeembeheerder wat screenshots van

de beheersite, maar die blijft ontkennen dat er wat aan de hand is. Totdat Blokzijl zegt dat de apparaten werken met software van Aquaview. Dat blijkt het sleutelwoord te zijn om de man te overtuigen. Koeroo: “Dit geeft aan dat je als verantwoordelijk onthuller altijd nog het slachtoffer moet overtuigen van het probleem. In de fysieke wereld is het helder wanneer iemand gewond is en dat de pleister midden op de wond moet worden geplaatst. In de digitale wereld ligt dit wat vluchtiger en is het maar de gok of de ander begrijpt wat je hebt verteld.”

Nu nog een ander geval, om te laten zien dat het hier niet gaat om een incident. Blokzijl had via @ntisec voldoende targets, alleen: hoe ver kun je gaan? “Strikt juridisch mag je niet hacken of zelfs aanzetten tot. Maar als het belang van het nieuws groot is, dan mag je een klein beetje de wet overtreden.” Ze kwamen uit bij een IP-adres dat bij het Leger des Heils blijkt te horen. Het is een verwarmingssysteem. De journalist kan er zo in en zet de verwarming een uur lang uit. Een onschuldig incident, maar wel hard bewijs. De handeling wordt gefilmd en de beheerster van de locatie is bereid haar verbazing te uiten voor de camera.

Het is dus een structureel, landelijk probleem. Aan het woord is Eric Luijff, veiligheidsdeskundige bij TNO. Hij blijkt al sinds 2001 te waarschuwen voor de kwetsbare SCADA-systemen. De overheid wist dit dus al. De Nationale Coördinator Terrorismebestrijding en Veiligheid zou dit gevaar het jaar daarvoor al hebben opgenomen in hun Cyber Security Beeld Nederland. Maar waarom wordt er dan niets aan gedaan? De redactie stuurt het onderzoek van Koeroo ook naar de NCTV. Blokzijl wordt direct teruggebeld. Een woordvoerder verklaart dat de beveiliging van die sluizen de verantwoordelijkheid is van de gemeente zelf. Maar, het zojuist nieuw opgerichte Nationale Cyber security Centrum kan de gemeenten wel technische ondersteuning geven en stuurt het rapport door naar de gemeente Veere.

Bij een landelijk probleem horen Kamervragen. Janine Hennis-Plasschaert, dan nog Kamerlid, zegt onomwonden tegenover de EenVandaag-camera: “Laat maar eens een hele polder vollopen en de bewoners daar niet op voorhand over waarschuwen. De risico’s zijn echt niet te overzien. Dit is een kwestie van nationale

veiligheid. NCTV is op de hoogte van de risico's, maar test dit blijkbaar niet." Hachchi van D66 zegt ook geschokt te zijn en heeft inmiddels ook al Kamervragen gesteld aan minister Opstelten. De sluizen van Veere zijn dan nog niet onthuld, want het item moet nog worden uitgezonden. Ze heeft wel het artikel van Tweakers gelezen waarin gewaarschuwd wordt voor kwetsbare SCADA-systemen, compleet met het Australische afvalwaterdrama.

De dag na de EenVandaag-uitzending, 15 februari, wordt er in de Tweede Kamer uitgebreid gesproken over de SCADA-problematiek. Het is een overleg waar minister Opstelten van Veiligheid en Justitie in gaat op allerhande veiligheidsvraagstukken: gedoe met brandweerauto's, het falende communicatiesysteem C2000 van de politie, bevoegdheden veiligheidsregio's en natuurlijk de pompen van Veere. En zoals wel vaker in de Kamer, gaat de discussie al snel van losse incidenten en woordspelingen voor ingewijden, naar een fundamentele discussie over taken en verantwoordelijkheden van de verschillende bestuurslagen in de Nederlandse overheid. Oftewel, moet de staat gaan controleren of al onze SCADA-systemen goed beveiligd zijn of niet?

De Kamerleden hebben het item gezien en citeren er lustig uit. Berendsen van D66 als eerste: "Het schijnt kinderlijk eenvoudig te zijn om ons land onder water te zetten. Dat blijkt uit een gisteren uitgezonden reportage van EenVandaag. Vanachter je thuiscomputer zet je zo de waterpompen uit. Een hacker zou het mij en zelfs deze minister kunnen leren; de minister zegt zelf immers altijd dat hij een digibeet is." Opstelten interrumpeert haar: "Dat zeg ik niet." Ze vervolgt: "De zogeheten SCADA-systemen, die worden gebruikt voor onze infrastructuur, zijn slecht beveiligd. Ik wil hierover opheldering van deze minister en van zijn collega van BZK. Opnieuw blijkt dat de ICT-kennis bij de overheid tekortschiet. Zelfs de meest basale beveiligingsmaatregelen zijn niet genomen. De wachtwoorden liggen voor de hand en de software is niet up-to-date."

Dan komt Janine Hennis-Plasschaert van VVD aan het woord, die zelf ook in het item te zien was. Volgens journalist Blokzijl heeft zij tijdens dit overleg sms-contact met hem, om zo feiten te

checken. Ze herhaalt de punten van Berendsen en doet er nog een schepje bovenop. “In de uitzending werd terecht gesteld dat we niet op een figuur als Osama bin Laden hoeven te wachten. Het zou kunnen gaan om 13-jarigen die uit zijn op een lolletje, maar ook om buitenlandse mogendheden met minder gezellige bedoelingen of activisten die nadrukkelijk een punt willen maken. Naar verluidt wilde de NCTV niet voor de camera reageren, omdat de verantwoordelijkheid voor de beveiliging van dit soort systemen bij gemeenten en waterschappen zou liggen.” Terwijl “de NCTV stelde dat aanvallen op SCADA-systemen een ernstige bedreiging voor de nationale veiligheid zouden kunnen zijn – was er tot mijn verbazing blijkbaar niemand die het ook even controleerde”.

Nadat enkele andere Kamerleden de argumentatie nog even dunnetjes overdoen, is het woord aan minister Opstelten. Hij heeft het item niet gezien, maar heeft er wel over gelezen op NU.nl. De veiligheid van de SCADA-systemen in Nederland is volgens de minister van groot belang, maar de verantwoordelijkheid daarvoor ligt bij de eigenaar. “Laten wij die verantwoordelijkheden alsjeblieft niet te snel verschuiven. Daar ligt de kern. Het toezicht op de veiligheid ligt bij de sectorale toezichthouders, die vallen onder de relevante vakdepartementen. Naast de algemene wet- en regelgeving bestaat op het sectorale niveau relevante wet- en regelgeving, met daarbij voor de diverse sectoren van toepassing zijnde verplichtingen, zoals de zorgplicht en het nemen van passende beveiligingsmaatregelen.”

Na deze enigszins bureaucratische afschuiving, wil de minister nog wel benadrukken: “Als de nationale veiligheid in het geding is of als dat dreigt te gebeuren, is er één verantwoordelijke; dat ben ik.” Daarom heeft hij het Nationale Cyber Security Center opgericht. Die heeft een coördinerende rol en reageert adequaat bij dreigingen en incidenten. Er wordt ook geoefend, zelfs met penetratietesten. Die acties maken deel uit van de Nationale Cyber Security Strategie, waarin het gevaar van SCADA-systemen wordt onderkend.

Hennis-Plasschaert: “Dat waren mooie en geruststellende woorden, maar het blijft voor mij onduidelijk hoe het kan dat Nederland zich al langer bewust is van de kwetsbaarheid van de

systemen, maar dat niemand even controleert of de systemen inmiddels veilig zijn. (…) Hoe kan het zo zijn dat, als de NCTV, TNO en anderen – ook vanuit het buitenland – waarschuwen voor de kwetsbaarheid van de SCADA-systemen, uiteindelijk een reportage van EenVandaag nodig is om dit af te dwingen?”

Minister Opstelten had, toen hij over Veere las, naar eigen zeggen meteen rondgebeld voor uitleg. Volgens hem moeten we de ernst van dit incident “zakelijk, glashelder en zeer nuchter beschouwen. De hacker had de pomp kunnen uitschakelen, waardoor het rioolwater niet had kunnen worden afgevoerd. Dit had voor overlast en milieuverontreiniging kunnen zorgen, maar er was geen bedreiging van de nationale veiligheid”. Bovendien heeft EenVandaag het nog voor de uitzending bij de NCTV gemeld en is er direct actie ondernomen. “Het nationaal centrum heeft vervolgens contact opgenomen met de gemeente, heeft advies gegeven en heeft ondersteuning aangeboden. Zo gaat dat in de praktijk.”

Dat het NCSC eigenlijk al ruim voor die tijd bezig was met een SCADA-factsheet en checklist zegt hij er gemakshalve niet bij. Hij lijkt ook zeker niet de indruk te willen wekken dat ze overal bovenop zitten, want dat is “een typische vorm van overacting van een niet goed functionerende overheid die allerlei dingen naar zich toe trekt die zij niet waarmaakt en die zij niet waar kan maken, waardoor de sectoren die het echt moeten doen, achterover gaan leunen”. Opstelten omkleedt de argumentatie met een paar inside jokes en stelt voor de discussie 20 maart voort te zetten. Dan is ook hun SCADA-checklist klaar.

Hennis-Plasschaert: “Ik dank de minister voor de uitvoerige beantwoording en de grappenmakerij tussendoor; dat maakt het ook nog fijn om hier te zijn. Gisteren was in het item van EenVandaag te zien dat ook verwarmingssystemen op afstand kunnen worden uitgezet. Ik ben inmiddels bevroren; ik weet niet hoe het de anderen vergaat, maar ik heb het ijskoud. Misschien worden wij nu dus getest, maar ik zou graag met de minister willen afspreken dat wij nog één keer testen tussen nu en het AO van 20 maart, zodat wij niet voor verrassingen komen te staan en voor het AO van 20 maart aanstaande zeker weten dat de SCADA-systemen veilig zijn. Is dat een deal?”

Nee, de minister wil niet ingaan op haar verzoek voor een pentest en zal ook zeker geen veiligheidsgaranties geven. Liever blijft hij in gesprek en dankt haar voor haar schot voor de boeg. Hennis-Plasschaert: “Dat is heel goed. Ik snap dat de minister geen 100% garantie kan geven, maar ik vermoed dat er mensen zijn die de overheid en de lagere overheden in de aanloop naar 20 maart gaan uittesten. Wees daar dus alert op en maak uw reputatie waar!” Elissen van de PVV roept: “Dit was een Hennis-alert!” en de voorzitter bedankt iedereen voor hun inbreng en belangstelling.

De volgende dag, 16 februari, zijn er ook Kamervragen voor minister Schultz van Infrastructuur en Milieu, dit keer gesteld door SP-leden Bashir en Gesthuizen. Verder is de discussie hetzelfde. Is de minister op de hoogte dat sluizen, gemalen en bruggen kinderlijk eenvoudig vanaf een thuiscomputer op afstand kunnen worden bediend? Op welke andere plaatsen in Nederland wordt gebruik gemaakt van hetzelfde onveilige SCADA-systeem? En waarom is er nog niets aan gedaan terwijl er al jaren wordt gewaarschuwd? Deze vragen worden niet direct beantwoord, maar pas 12 maart.

Schultz zegt dan dat zij niet over alle watersystemen gaat. Alleen die van Rijkswaterstaat vallen onder haar gezag en die zijn veilig. Ze heeft zelfs een “Voorschrift Informatiebeveiliging Rijksdienst (VIR) als continu proces ingericht. Structureel wordt bewaakt of de beveiliging aanpassing behoeft. Als daar aanleiding toe is, worden corrigerende maatregelen getroffen”, aldus de minister. Webwereld kopt diezelfde dag: ‘Minister: SCADA-systemen van het Rijk zijn veilig’.

Op 7 maart stuurt het NCSC een waarschuwende factsheet uit: ‘Beveiligingsrisico’s van online SCADA-systemen’. Hierin is te lezen dat het centrum signaleert dat de belangstelling van hackers en onderzoekers voor de beveiliging van SCADA-systemen toeneemt. “Hoewel het gebruikelijk is dat onderzoekers hun ontdekkingen eerst aan de eigenaren van de systemen melden, zijn er ook onderzoekers die hun bevindingen direct publiek maken (bijvoorbeeld via sociale media zoals Twitter of op openbare websites zoals Pastebin). Daarnaast worden vaak ook

journalisten geïnformeerd.” Eigenaren moeten rekening houden met mogelijk ‘digitaal vandalisme’, maar vooral ook vrezen voor negatieve publiciteit en imagoschade. Dit spreekt misschien voor zich, maar het is wel een manier om de aandacht te trekken van niet-technische bestuurders. Wat volgt, is een uiteenzetting over zoekmachines, hacking tools, het advies systemen liefst offline te laten en een uitgebreide checklist.

Opstelten prijst de checklist aan in een Kamerbrief van 19 maart. Eerst herhaalt hij zijn standpunt: “Het beveiligen van dergelijke systemen is primair de verantwoordelijkheid van de eigenaren van de SCADA-systemen. De overheid houdt echter, gezien het grote belang dat door de overheid aan bepaalde sectoren wordt toegekend, toezicht op bepaalde sectoren.” Maar, er is nu wel een “checklist die organisaties kan helpen om zelf vast te stellen of hun SCADA-omgeving afdoende beveiligd is op basis van maatregelen die als ‘good practice’ beschouwd worden”.

Blijkbaar heeft het NCSC achter de schermen contact gehad met @ntisec, de oorspronkelijke melder. Ik ga daarom op zoek naar hem, om erachter te komen waar het SCADA-drama is begonnen.

8. Dan gaan we nat

De IP-lijsten van de anonieme @ntisec

Hoe communiceer je met iemand die niet gevonden wil worden? Het enige wat ik heb van @ntisec is een Twitteraccount en daar staat niet voor niets bij ‘Anonymous’. De eerste tweet die ik van hem vind over de SCADA-kwestie is er een van 10 december 2011. “Dutch computer controlled floodgates might be at risk of hacking attacks. Floodworks like the Maeslantbarrier are managed by #SCADA systems.” Hierna volgen wat nieuwslinks en de vraag waarom niemand dit oppikt. De beruchte onthullingen vind ik echter niet. Blijkbaar zijn ze gewist. Gelukkig heeft iemand er nog een screenshot van gepost. Hier zien we de IP-adressen van Shell in Quatar en de Gasunie, helaas zonder datum. Wel staat er een reactie van @ncsc_nl bij: “Ik kom later bij je terug. Bedankt voor je positieve houding tot nu toe en de info die je hebt gegeven.” Later: “Tot die tijd kunnen we prima zo communiceren, ik zal ook nadenken over een makkelijk anoniem kanaal”, waaruit blijkt dat er elders conversatie heeft plaatsgevonden tussen beiden.

Ik probeer het via de Twitter-DM en vraag @ntisec of ik hem kan interviewen over de SCADA-onthullingen, uiteraard zonder opname en onder pseudoniem. Dat kan, maar dan wel via Pigdin of Xabber, want die hebben een otr-functie, oftewel: off the record. Ik probeer beide applicaties uit, maar na de zoveelste foutmelding over certificaten en dingen die ik niet begrijp ga ik weer terug naar Twitter. Gelukkig wil hij nog wel antwoord geven op wat korte vragen. Waarom deed hij de onthullingen en waarom juist op dat moment? @ntisec: “Het verband is eigenlijk stuxnet en het gevoel dat er dan ook infrastructuur in NL kwetsbaar moet zijn. Eind 2011 en 2012 ben ik gaan zoeken naar lekken als een soort burgerlijke controle. Veel dingen hebben nooit het nieuws gehaald.”

Stuxnet was toen volop in het nieuws geweest. Het is een worm, een zichzelf vermenigvuldigend computerprogramma en

was gebruikt om Iraanse kerncentrales onbruikbaar te maken. Het was via een usb-stick naar binnen gesmokkeld en had zich daar door de programmatuur van de SCADA-systemen gevreten, waardoor de centrifuges op hol sloegen. Andere landen zouden ook slachtoffer zijn. De VS en Israël zouden erachter zitten, een duidelijk voorbeeld van cyberwarfare die danig uit de hand dreigde te lopen. @ntisec wilde dus aantonen dat Nederland ook vatbaar zou zijn voor zo'n aanval door kwetsbare plekken te publiceren.

Later vervolgt hij: "En ben ook doorgelicht door de FBI omdat ik wat SCADA #0Days publiek had gemaakt. En 120.000 kwetsbare SCADA-systemen die daardoor direct toegankelijk waren zonder überhaupt eerst een login of password nodig te hebben. Zoek maar 'FBI US Cert' in combinatie met @ntisec. Daarnaast heeft de FBI via Sabu geprobeerd mij uit te lokken om kwetsbare Israëlische systemen voor hem te vinden. Dat heb ik ook gedaan. Ik hoop dat je inziet hoe gevaarlijk het was om zo dicht met Sabu samen te werken. De meesten die dat deden zitten nu vast of zijn opgepakt."

Over Sabu had ik al eens gelezen in het boek 'We are Anonymous' van Parmy Olson. Deze Latijns-Amerikaanse New Yorker was een van de leidende figuren achter Anonymous en de splintergroep Lulzec. Eind 2010 hadden ze de websites van VISA, Mastercard en Paypal platgelegd, omdat die de rekeningen van klokkenluider Julian Assange hadden geblokkeerd. Ook Sony, het Vaticaan en Scientology Church waren niet veilig voor deze hackers. Sabu werd opgepakt door de FBI en ging vervolgens voor hen werken, in ruil voor strafvermindering. Door zijn toedoen zijn veel leden van Anonymous opgepakt. Als @anonymouSabu verstuurt hij op 11 januari 2011 deze tweet aan @ntisec: "You got Israeli #SCADA server pl0x for us?"

In het boek van Olson wordt ook Pastebin vaak genoemd. Het is een ongecensureerde site waar iedereen van alles op kan zetten en daarom ook populair bij hackers die anoniem onthullingen willen doen. @ntisec stelt voor dat ik hier mijn concepttekst op zet, zodat hij erop kan reageren. Dus ik schrijf terug: "Is wel een nieuw medium voor me dus hopelijk verkloot ik

het niet...”. Als ik me aanmeld op Pastebin als Ctof ga ik alvast wat rondkijken of ik iets vind over SCADA. En warempel, hier staat de conversatie tussen hem en het NCSC. De eerste post is van 6 januari 2012. @ntisec begint met wat ASCII-art. De karakters en spaties vormen samen #C4D4. Een geheime code? Of een manier om SCADA te schrijven zonder dat het in de zoekmachines gevonden wordt? Hoe dan ook, ik ga er vanuit dat het hier dezelfde persoon betreft en lees zijn redeneringen achter de onthullingen.

“OK, hier gaan we weer.

Welkom ncsc_nl ook anonymous dus heel goed van jullie, ook al ken ik nu al enkele mensen die onderdeel zijn van.

Alles wat ik openbaar heb laten zien, is makkelijk door elke scriptkid te vinden en zelfs door mensen die geen enkel idee hebben waar ze mee bezig zijn. Ik heb alleen laten zien wat er vrij zonder wat voor skills en hacks te gebruiken direct toegankelijk is voor elke leek.

Nu is dat op zich voor het overgrote deel van de NL bevolking geen probleem. Op de meeste ip’s zijn alleen loginvelden te zien en admin/12345 is dan wel het meest slimme wat je kunt proberen. Maar goed jij ofwel jullie weten net zo goed als ik dat het vaak vrij makkelijk is om toch even wat verder te gaan dan dat. Dat heb ik tot nu toe natuurlijk niet gedaan!!!!!!!

Maar ik weet wel hoe dat moet.

Wat ik aan de kaak wil stellen als zijnde klokkenluider is dat er via simpele wegen, (alle links die ik heb getweet zijn binnen 3 uren gevonden) infrastructuren zijn te vinden die niet vindbaar horen te zijn.

Het is simpelweg niet nodig om bijv. een rioleringsstation van Doetinchem openbaar op het WWW te laten zien als zijnde wat het werkelijk is. Neem dan een ander protocol, of zorg ervoor dat het niet direct duidelijk is waar je mee te maken hebt.

Echter ook andere protocollen hebben voor mensen die weten waar ze over praten geen veiligheid wat betreft vindbaarheid.

Het is misschien omdat het toevallig kan heel makkelijk om de stront uit Doetinchem te kunnen pompen vanuit je bed in Rotterdam, maar slim is het in elk geval niet.

Waarom niet een ouderwets oneway alarm dat afgaat en een mannetje met piketdienst dat fysiek kan reageren op momenten dat dit nodig is.

En dan hebben we het alleen nog maar over stront.

Hoe zit het met Gemalen, Stroomvoorziening, Gas, watervoorziening, (wie controleert hoeveel chloor er wel of niet wordt toegevoegd), waterzuivering, en voor NL het meest gevaarlijke waterbeheer. Stormvloedkeringen, Sensoren, Weerstations, Afsluiters, spuigaten en sluizen?

Het is allemaal te vinden en niemand inclusief @ntisec heeft het overzicht.

Ik denk dat het tijd wordt dat al deze vectoren eens worden bekeken zodat ik weer rustig kan slapen.

WAAROM!!!!!

Dit is slechts het begin. Staten zullen hoe verder deze fin- crisis zich ontwikkelt steeds meer gaan misbruiken wat er te misbruiken valt. Waarom geen misoogst in je buurland zodat jij een goede marktwerking hebt? Kom op de chinezen kunnen nu al zorgen dat we morgen helemaal plat gaan en jullie weten danwel vermoeden dat ook.

Laten we het digitale eens wat meer terug in handen nemen als het gaat om de veiligheid en volksgezondheid van ons land.

Primaire infrastructuur moet fysiek gecoördineerd worden. En dat kost misschien wat meer geld maar schept werkgelegenheid.
\

Mochten jullie nog een creatief denker en ZZP-er in dienst willen nemen die het overzicht heeft binnen de 0day en hacker scene
**
Dan lijkt me dat leuk.

Denken buiten je boekje wordt op dit gebied heel belangrijk.

Groeten en doe er AUB wat aan anders”

Hierna volgt weer een stukje ASCII-art. De tekens vormen samen de tekst “DAN GAAN WE NAT”. De reactie van NCSC volgt de dag erna. Net als op Twitter, ook hier weer de bijzonder vriendelijke toon. Er staat een PGP-signature onder, dus waarschijnlijk is het ook echt het centrum dat hier reageert.

“-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

@ntisec,

Hierbij onze reactie op je uitgebreide post op pastebin.com/Fv4eazzF

De problematiek die je aansnijdt, is maatschappelijk zeer relevant en bevindt zich op het snijvlak waar cyber security en fysieke veiligheid elkaar raken.

Gisteren hebben we al kunnen vaststellen dat onze doelen deels overlappen. Dat zit voor jou in je eigen veiligheid en welbehagen, voor ons in de veiligheid van Nederland, en in het directe verlengde daarvan natuurlijk de veiligheid van de burgers: dat zijn we allemaal.

Je wilt aan de kaak stellen dat mogelijk kritieke en kwetsbare systemen vindbaar zijn op internet. Het naar buiten willen brengen van een misstand is heel begrijpelijk en wij zijn daar in principe voor. Sterker nog, wij zijn van mening dat dit de beveiliging van de betreffende systemen ten goede kan komen, mits die misstanden op een verantwoorde wijze worden onthuld.

Wat ons betreft, is het verantwoord om de misstand in concept aan te tonen en de verantwoordelijke organisatie te informeren voordat je details publiceert. Daarbij hoort volgens ons ook dat je de desbetreffende organisatie een realistische termijn geeft om maatregelen te (laten) nemen, voordat je tot publicatie overgaat. Vroegtijdige publicatie zou immers zelfs tot een verhoogd risico kunnen leiden. Anderen (kwaadwillenden) die er eerder nog geen kennis van hadden, zouden misbruik van kwetsbaarheden kunnen maken. Dan help je indirect de verkeerde partij.

Nogmaals: ons doel overlapt.

Wij willen graag samenwerken om dat doel te bereiken. Als je de informatie met ons deelt die je al gevonden hebt en die je eventueel nog gaat vinden, dan kunnen wij onze contacten gebruiken om ervoor te zorgen dat die informatie terecht komt op de juiste plek. Zo kunnen wij de juiste organisaties en personen informeren die daar over gaan. Wij zullen daarbij naar jou toe transparant zijn over de status van elke melding. De credits voor het melden van mogelijke kwetsbaarheden behoren de melder (jou) toe. Wij willen geen credits van kwetsbaarheden die we niet zelf hebben gevonden hebben.

Hoe kritisch een systeem is, of het wel of niet via internet toegankelijk zou moeten zijn en wat dat betekent voor de beveiliging ervan, kan per systeem verschillen. Wij vinden het belangrijk om zorgvuldig te werk te gaan en organisaties te helpen om passende maatregelen te nemen.

Je hebt gelijk als je zegt dat er veel te vinden is en niemand het overzicht heeft. Dat overzicht is als een puzzel met een nog onbekend aantal stukjes. Dit is een probleem dat veel partijen, zowel binnen overheid als bedrijfsleven, zich realiseren. Alleen door goede samenwerking is die plaat compleet te krijgen en wij kunnen jouw hulp daarbij gebruiken.

Ga je de samenwerking met ons aan? Over de exacte invulling van de samenwerking kunnen we natuurlijk nog verder praten. We

zijn altijd op zoek naar mensen met kennis, inzicht en goede intentie.

Groet,
Nationaal Cyber Security Centrum."

NCSC gaat er dus iets aan doen en @ntisec krijgt de credits, maar hij moet de systeemeigenaren wel de tijd geven de boel voldoende dicht te timmeren. Op zich best bijzonder dat een ambtenaar dit toezegt namens een zojuist opgericht instituut van het ministerie voor Veiligheid en Justitie. Zelf zou ik verwachten dat er dan eerst intern overleg moet plaatsvinden en er na een maand of zo een diplomatiek antwoord komt. Of was dit juist een mooie gelegenheid om het kersverse instituut op de kaart te zetten? Voor @ntisec zelf ging het allemaal niet snel genoeg, want 20 januari, dus twee weken later, zien we deze post op Pastebin.

"Ik heb aan het @NCSC_NL gemeld wat ik wel heel erg gevaarlijk vond. Het gaat dus niet alleen om de zoekopdracht alleen. Dat is niet het probleem. Het probleem is dat veel #SCADA infrastructuur die wordt gebruikt in processen niet zijn gemaakt om aan het web te hangen, en veel #exploits, #backdoors en #0days bevatten. De invloed van deze systemen variëren van het sturen van processen in een koekjesfabriek, tot het groen sein geven en wissels omzetten van de NS, danwel al het gas van Slochteren naar het binnenhof pompen.

Deze systemen blijken zo lek als een mandje. En ik beweer dat ik daar in kan als het moet!

Maar dat maakt mij in Nederland een Terrorist ook al ben ik alleen een klokkenluider.

Deze systemen horen niet #webfaced danwel aan het openbare internet gekoppeld te zijn!
TERUG MET DIE OUDE VERTROUWDE #AIRGAP = dus losgekoppeld van het internet.

Ik heb dingen gemeld aan het @NCSC_NL over ondermeer:

#GASUNIE -> Krijg te horen dat dit geen gevaarlijk systeem was (BEWIJS=GEEN)
#SCHIPHOL -> Niets op terug gehoord
#Ministerie van Verkeer & Waterstaat -> Niets op terug gehoord
#Riolerings Webscada systeem van de riolering in
#DOETINCHEM -> Niets op terug gehoord
#Balast nedam -> Niets op terug gehoord.
#Gaspompstation/Gaswinning CANADA ->Niets op terug gehoord

Ik ben nu dus begonnen met het openbaar maken van legale #SCADA problemen in Nederland alleen maar om aan te geven wat voor een werkelijk gevaar wij lopen.

De systemen die ik heb laten zien daar loop je legaal binnen en kun je slagbomen openen en dichtdoen. Verlichting aan en uit, Kachel op stand 10 zetten en alarmsystemen in of uitschakelen.

Niets ernstig nog.

Moet het dan eerst misgaan voordat dit wordt opgepikt danwel openbaar eens goed wordt onderzocht?

Met vriendelijke groet,

contact via twitter @ntisec”

Daarna stopt de conversatie. Ik zie nog wel op 15 februari een tweet: “Found a new #DUTCH #SCADA threat so big I cant fulldisclose right now. I gave the @ncsc_nl 2-1/2 weeks to fix it Then #FULLDISCLOSURE.”

Wat was hier gebeurd? Ik vraag het Barend Sluijter, beleidsmedewerker bij het NCSC, met wie ik al eerder over mijn onderzoek heb gesproken. Hij is een generalist die goed overzicht heeft van de zaken die er lopen, dus stuur ik hem eerst een mail. Volgens Sluijter werkt de persoon achter de Pastebin-correspondentie inmiddels niet meer bij het centrum, maar hij heeft de zaak wel goed gedocumenteerd achtergelaten. Ik kan

langskomen en dan zal hij, samen met zijn collega Tarik el Yassem uitleg geven.

Op de zevende etage van het zwaar beveiligde V&J-gebouw ga ik voor de tweede keer door veiligheidsdeuren en ID-checks en tref ik beide heren aan een vergadertafel. El Yassem zit klaar met een stapeltje prints. Hieruit blijkt dat de tweets en Pastebinposts inderdaad van een medewerker zijn. Sluijter vertelt dat ze al bezig waren met de SCADA-systemen. Bij NCSC had het Team Expertise & Advies er al eens over gepubliceerd. Binnenkort zou weer een nieuwe factsheet uitkomen. Hun Team Monitoring & Response volgt wat er leeft in de community via diverse kanalen, dus ook @ntisec. Toen hij namen en wachtwoorden begon te tweeten vonden ze dat ze contact moesten opnemen. De medewerker had het snel afgestemd met het management, ging zo de communicatie aan en stuurde @ntisec een concept van de factsheet.

Het NCSC had ook al diverse systeemeigenaren geïnformeerd. Dat had formeel niet gehoeven, want gemeenten vallen niet onder de bevoegdheid van hun ministerie en de grote watersystemen zijn van Rijkswaterstaat, maar het leek hen toch belangrijk dat wel te doen. Vervolgens was het lastig om te zien of de eigenaren van de SCADA-systemen er dan ook werkelijk wat mee doen. Sluijter: “Er zitten zoveel partijen tussen, dat je er veel energie in moet steken om te achterhalen of en hoe het opgelost is. Er zijn ook partijen die niet reageren.” Ze hebben dus gedaan wat ze konden.

Als ik beide heren vraag of ze de zaak hadden aangegrepen om het kersverse centrum te profileren, is het antwoord: “Nee, we hadden onze tijd misschien beter kunnen gebruiken met de echte problemen. Profileren was ook niet het doel.” Ze zijn ook niet zo gediend van full disclosure, oftewel het publiceren van veiligheidslekken zonder waarschuwing vooraf. Dan is er even veel aandacht in de media, maar dat ebt ook weer snel weg. En communiceren met iemand die anoniem wil blijven, is toch ook wel lastig: “Je moet eigenlijk niet vanuit anonimiteit werken, want je bouwt een relatie op. Als je belooft niet te vervolgen, moet je wel weten aan wie je dat doet”, aldus Sluijter.

Ik maak een verslag van dit gesprek, verwerk het samen met het stuk over @okoeroo tot een concepttekst en check dit met alle andere betrokkenen. Als ze akkoord hebben gegeven, zet ik het op Pastebin, zodat @ntisec erop kan reageren. De teller begint meteen te lopen: 87 hits in een paar minuten. Blijkbaar leeft het onderwerp in deze anonieme chatomgeving. @ntisec leest ook mee en schrijft meteen een reactie op Twitter: “Is Barend Sluijter hier op #twitter te vinden? En is Tarik el Yassem hier op Twitter te vinden?” Tsja, daar krijgt hij natuurlijk geen reactie op. De medewerkers zijn ook niet zo blij met deze persoonlijke benadering door iemand die zelf anoniem wenst te blijven. Maar goed, ook zij zien de Pastebinteller oplopen, wellicht ook enigszins ongerust over wie al die nieuwsgierigen zijn.

@ntisec reageert die dag ook via Pastebin op mijn concepttekst. Eerst denk ik dat er iets mis is met de instellingen van mijn computer, want er staan allemaal rare tekens in. Ach, natuurlijk: dit zijn tekens die ervoor zorgen dat wij mensen de woorden wel kunnen herkennen en zoekmachines niet. Op zich slim, ware het niet dat al die trefwoorden al in mijn tekst staan. Maar goed, het ziet er wel cool uit, dus ik laat ze zo. Over het EenVandaag-item schrijft hij dat eigenlijk hij en niet Oscar Koeroo in het item zou komen:

“ɔʙℓσκzɯℓ єи ικ нα∂∂єи єєи αfsρяααк. ικ zσυ ωєℓ σρ τν κσмєи αиσиιєм!!!. zσυ нιєя єєи σикσsтєи νєяgσє∂иg νσσя кяɯgєи ναи 250 єυяσ υιτєи∂єℓɯк нєв ικ мɯ єχтяα ιиgєzєт нєм тє нєℓρєи ααи χтяα ιиfσямαтιє єи нєт ℓєк вɯ нєт ℓєgєя ∂єs нɯℓs. мααя ωєя∂ ικ ииєт υιτgєισ∂ιg∂ мɯи νєянααℓ тє ∂σєи. нɯ κσσs тσєи νσσя σs¢αя. ∂αт ωαs ∂єик ικ νєιℓιgєя єи мακκєℓɯкєя νσσя нєм. νσєℓ∂є мɯ fℓиик gєиααι∂ ∂σσя вℓσкzɯℓ.”

Hij legt ook uit waarom hij 15 februari tweette: “Found a new #DUTCH #SCADA threat so big I cant fulldisclose right now. I gave the @ncsc_nl 2-1/2 weeks to fix it Then #FULLDISCLOSURE” Het ging volgens hem om een bedrijf gespecialiseerd in extern hosten van SCADA-systemen. Ook daar kon hij zo in, meldde dit, maar kreeg geen reactie. Hij kon wel zien dat het bedrijf na enkele dagen plat ging en alles probeerde dicht te timmeren. Er zaten bij hem dus nog behoorlijk wat frustraties over de gang van zaken.

Toch moet hij niet onderschatten wat het item van Blokzijl teweeg heeft gebracht, want op diezelfde 15 februari was er dus in de Tweede Kamer uitgebreid gesproken over de SCADA-problematiek. Het was een overleg waar minister Opstelten van Veiligheid en Justitie inging op de vragen over taken en verantwoordelijkheden van de verschillende bestuurslagen in de Nederlandse overheid. Oftewel, moet de staat gaan controleren of al onze SCADA-systemen goed beveiligd zijn of niet? Dat het NCSC toen al bezig was met een SCADA-factsheet en checklist moet Opstelten naar mijn inschatting geweten hebben, maar hij noemt ze niet in het debat. Wellicht wilde hij de totstandkoming van de tekst niet te verstoren of was hij het gewoon vergeten. Hoe dan ook, op 20 maart wordt de discussie voortgezet, met de SCADA-checklist erbij en is er in ieder geval toch wel iets gebeurd.

Voor @ntisec zelf was dat alles minder relevant. Hij ging meteen full disclosure en heeft al teveel zijn nek uitgestoken, want inmiddels heeft de VS hem ook in het vizier. De FBI stuurt namelijk 23 juli 2012 een waarschuwing rond met zijn naam erin. In het bericht is te lezen dat hackers in februari en maart toegang hadden gekregen op een SCADA-systeem van het airconditioningbedrijf US Business 1 in New Jersey. Ze hadden de IP-truuk toegepast en konden zo ventilatiesystemen, verwarmingen en airconditioners aansturen. Aanleiding voor de hack was volgens de FBI een post van @ntisec op 21 januari met de titel: '#US #SCADA #IDIOTS', gevolgd op 23 januari door '#US #SCADA #IDIOTS part-II'. Het Department of Homeland Security heeft daarom een waarschuwing gestuurd naar bedrijven met vergelijkbare systemen. Wat ze er uiteraard niet bij vermelden is dat ze @ntisec via Sabu's Twitteraccount uitdagen met nog meer SCADA-onthullingen te komen. Waarom is niet duidelijk, maar waarschijnlijk om hem te pakken te krijgen.

De identiteit van deze hacker blijft dus verborgen. Ook in dit verhaal. En terwijl de overheid in Nederland en de VS druk bezig zijn met zijn onthullingen, doet hij er nog een: hij heeft via Anonymous toegang gekregen tot een teleconferentiesysteem van Defensie. Maar ook deze vondst wordt publiekelijk gemaakt

door een andere hacker: @UID_ ook wel bekend als beroepshacker Rickey Gevers.

9. @UID_ belt de kazerne

Teleconferentiesysteem van Defensie blijkt toegankelijk met fabriekswachtwoord

Beroepshacker Rickey Gevers, ook wel @UID_, kreeg van @ntisec een tip over een videoconferentie-systeem van het Nederlandse Ministerie van Defensie. Het systeem zou gewoon online staan en je zou erin kunnen met het standaard fabriekswachtwoord dat is te vinden in een handleiding die op internet staat. Gevers logde in en zag dat hij in de account kon van een topman bij Defensie. Hij toonde dit aan een journalist van de Volkskrant, die eerst zijn advocaat en daarna Defensie belde. Een woordvoerder zei dat het Defensienetwerk veilig was. Maar, als de krant bij de drukker ligt, ziet Gevers dat het systeem uit de lucht is gehaald. Er was dus weldegelijk een lek en het werd tijdig gedicht, zonder dat hij als melder in de problemen kwam. Hier een hacker die precies weet hoe ver hij kan gaan bij computervredebreuk, wellicht juist omdat hij er al eens eerder voor is veroordeeld.

@UID_ is, zoals zijn Twitterprofiel meldt, een ‘criminal brought to justice’. Als ik Gevers thuis opzoek, vertelt hij me hoe hij in 2008 werd opgepakt. Team High Tech Crime van de Nederlandse politie had een tip gekregen van de FBI. Michigan University was gehackt en het IP-adres leidde naar Amsterdam. Ze hadden ook zijn Hotmailadres, maar dat was alles. Als de agenten op 27 augustus 2008 de locatie van het IP-adres bezoeken, treffen ze een studentencomplex aan en gaan ze op zoek naar iemand die daar de internetverbindingen verzorgt. De campus blijkt een open Wi-Fi te hebben waar wel 500 studenten gebruik van maken, dus dat wordt nog lastig zoeken. Ze laten de systeembeheerder het e-mailadres zien en vragen of hij de persoon erachter kent. “Ja, die ken ik wel want hij mailt me elke dag. Die woont daar…”

Het is nog vroeg in de ochtend als het arrestatieteam de studentenkamer binnenvalt. Met tien man tegelijk stormen ze naar binnen: “Wakker worden, wakker worden!” Gevers denkt eerst dat het een studentengrap is en hoort nog half versuft vanuit zijn hoogslaper iemand zeggen: “Oh, hij is er niet.” Hij roept: “Ja hoor, ik ben hier” en gooit zijn dekens opzij. Voor hij het weet, wordt hij ruw uit zijn hoogslaper gerukt en tegen de grond gewerkt. “Nou, neem straks maar wat schone kleren mee”, zegt een van de agenten tegen hem, “want dit gaat nog wel even duren.”

Tijdens zijn verhoor vraagt een van de agenten: “Wat wil je later doen?” Gevers: “Ja eigenlijk wat jullie nu aan het doen zijn. Maar dat heb ik behoorlijk verkloot nu.” Uit het onderzoek dat hierop volgt, blijkt dat er nog vier andere hackers waren. Samen hebben ze ingebroken bij diverse universiteiten in Nederland, Europa en de VS. De vijf jonge mannen ontmoeten elkaar in de rechtszaal voor het eerst in het echt en krijgen daar te horen wat hen ten laste wordt gelegd: wachtwoorden stelen, malware installeren en video’s uitwisselen via servers van universiteiten. Ze worden daarom veroordeeld voor computervredebreuk, schending van copyright en deelname aan een criminele organisatie. Gevers wordt uiteindelijk veroordeeld tot achttien dagen cel.

Gevers komt weer vrij en besluit zijn hackersvaardigheden voortaan in te zetten om anderen te helpen hun beveiliging op orde te brengen. Hij gaat aan de slag bij Digital Investigation als forensisch onderzoeker, oftewel digitale sporen veiligstellen en analyseren om zo de politie te helpen bij het oplossen van cybercrimezaken. Pim Takkenberg, de teamleider die destijds ook de arrestatie verrichtte spreekt nog steeds met veel waardering over deze carrièreswitch: “Rickey is het toonbeeld van hoe je kunt leren van fouten en dat op een positieve manier kunt gebruiken.” Niettemin blijft Gevers nog wel contact houden met het schemergebied van de hackerswereld, zoals Anonymous. En zo komt de tip over Defensie bij hem terecht.

Op maandag 20 februari 2012 krijgt @UID_ via Twitter een DM van @ntisec. Hij had een tip gekregen van Anonymous, maar vindt het lek van dermate hoog kaliber dat hij zijn vingers hier liever niet aan wil branden. Daarom had hij de journalisten Blokzijl

en De Winter benaderd om het te onthullen, maar dat deden ze niet. Hij vraagt @UID_ of hij ernaar wil kijken. Dat wil Gevers wel en via een beveiligde verbinding krijgt hij de handleiding van een CISCO-videoconferentiesysteem, een IP-adres en de opdracht in te loggen met het default wachtwoord.

Gevers logt in en ziet tot zijn verbazing de pagina van directeur Marinebedrijf A.J. de Waard. Hij checkt de IP-adressen, telefoonnummers en namen of dit wel echt het systeem van Defensie is. Het klopt. Vervolgens probeert hij nog wat andere pagina's in het systeem. Het blijkt dat hij eindeloos veel wachtwoorden kan intypen en dus andere accounts gewoon met brute force zou kunnen openen. Gevers is geschokt en weet niet goed hoe hij dit naar buiten moet brengen. Hij wil natuurlijk niet weer de gevangenis in. Hij benadert daarom, net als @ntisec, een journalist om de onthulling voor hem te doen. Hij komt uit bij Victor de Kok van de Volkskrant. Gevers weet uit ervaring dat deze krant advocaten heeft die kunnen omgaan met responsible disclosure en nodigt de journalist uit om te laten zien wat hij heeft gevonden.

Die woensdag ontvangt Gevers journalist De Kok op zijn studentenkamer om samen in te bellen. Gevers zit achter de laptop en de journalist is continue aan de telefoon met zijn advocaat. Ze loggen in als de directeur Marinebedrijf en bellen de directie van de Jan de Noordazaal, een kazerne in Den Helder. Helaas, er wordt niet opgenomen. Ze zouden ook kunnen bellen naar warroom@denhaag of testsite@US, maar dat lijkt hen te riskant. De journalist belt daarom zelf met de gewone telefoon naar de kazerne om het lek te melden. Daar wordt hij direct doorverbonden naar een woordvoerder die in eerste instantie niet begrijpt wat er aan de hand is en later terugmeldt dat het betreffende systeem niet in gebruik is. Gevers ziet echter aan de logfiles dat het systeem een uur geleden nog is gebruikt en zeker niet door de minsten. Daar heeft de woordvoerder geen weerwoord op. Gevers ziet vervolgens dat het systeem offline wordt gehaald.

De Kok kan nu overgaan tot de onthulling en kopt vrijdag 24 februari 'Communicatie Defensie eenvoudig te kraken'. Hierin is te lezen dat de Volkskrant er getuige van was dat cybercrime-expert Rickey Gevers die woensdag inlogde op het systeem. Ze hebben

geen vergaderingen afgeluisterd maar konden wel zien dat een topman met de rang van commandeur die maandag en dinsdag nog zeker vijf keer heeft vergaderd via het systeem. Een woordvoerder van Defensie meldt dat de “cyber-veiligheidsafdeling waarschuwt voor dergelijke systemen, omdat die makkelijk gehackt kunnen worden”.

Wat is er volgens Defensie gebeurd? De woordvoerder blijkt Maarten Hilbrandie te zijn en ik neem contact met hem op. Hij vertelt me dat hij direct na het telefoontje van de journalist naar hun communicatiesystemen heeft gekeken, maar niets vreemds zag. Die systemen staan ook niet online, volgens hem. Pas toen kwam hij erachter dat er nog een ander systeem was, dat wel via internet ging. Dat was inderdaad tegen de regels in en het werd daarom donderdagavond 21.25 uur offline gehaald.

Het bericht in de Volkskrant de dag erna wordt direct overgenomen door andere journalisten, waaronder ook GeenStijl. Hun parodie is te leuk om niet geheel hier te citeren, al zal ik de tachtig reacties die erop volgden maar achterwege laten.

“KGGGTTT! (...) GGGGGGRRRRT! *PIEPKRAAK!* Hier spreekt de CHARLIE BRAVO DELTA 4!! Met de generaal! Hoort u mij!!??? Aan alle eenheden (..) KGGGGT! (..) Het spel is op de wagen!!! Wij herhalen: Het SPEL is op de wagen! (..) *PIIIIIEEEEEEP!!!* Wij staan bij de rode vlag! KGGGT! Hoort u ons? (..) De koe staat in de wei! *KRRRRAAAK!* Wachtwoord: default! (..) code 4. Basiskamp aan Zandhaas. PIEPKRAAK! Het wachtwoord = default. KKRRGGGTT! Aan commando DienstenCentra: Radarbeelden naar @ntisec. Lock and load. (..) PIEPKGGGGT!! Alle units naar anonymous. Wachten op toestemming van DM)-commandeur. PIEP!!! (..) KGGTT!!! Kilo Utrecht Dirk Tango (..) Directeur van Marinebedrijf CDRT dr. ir. A.J. de Waard weet er van. (..) KRRRRAAAK! Alle schermen op zwart, wij herhalen alle scherman op zwart! Mayday mayday. Alarmcode 64.7. (..) KGGGGG. Gaarne even googlen. (..PIEP!..) Control+ ALT + delete? En shift dan? Wij krijgen nu binnen op de telex: Feb 21 09:15:24 Received SourceFormatEvent from video link 17 (1280×720@60, digital, ok) PIIIIEEEEPKRAAK! Kunt u dat

bevestigen? Goedver, de lijn is zo dood als pier. Hallo? HALLO? *TUUUTUUUUT!!!* BOEM!” (sic)

Ook de Tweede Kamer mengt zich in de discussie. De dinsdag daarop, 28 februari loopt het Kamerlid Wassila Hachchi van D66 tijdens het wekelijkse Vragenuurtje naar de interruptiemicrofoon. We kennen haar nog van haar motie over helpende hackers tijdens het debat een half jaar daarvoor. Ze is zelf ook militair geweest: van 2003 tot 2007 was ze officier bij de Logistieke Dienst van de Koninklijke Marine. Daarna bekleedde ze nog diverse andere functies bij Defensie. Ze weet dus hoe het er daar aan toe gaat en richt zich via de voorzitter tot minister Hans Hillen van Defensie:

“Een topman van de materieelorganisatie van Defensie, een militair met sterren op zijn schouders, is afgeluisterd terwijl er gevoelige informatie werd gewisseld, om maar niet te spreken van namen, telefoonnummers en IP-adressen van mensen. Moderne communicatie is noodzakelijk voor Defensie, maar moet zo veilig mogelijk gebeuren. Ik heb hierover vijf vragen aan minister Hillen. Welke vergaderingen zijn afgeluisterd? Welke gegevens zijn op straat komen te liggen? Hoeveel mensen zijn er afgeluisterd? Ik heb begrepen dat het om een stuk of zeven systemen gaat. Zijn er meer systemen die risico lopen? Wat gaat minister Hillen doen?”

Hillen probeert het eerst af te schuiven op de media: “Voorzitter. Vroeger was het misschien zo dat alles wat in de krant stond waar was. Dat is echter al heel lang geleden. Als er in de krant staat dat de top van Defensie gehackt is, dan is dat aantrekkelijker om te schrijven dan dat het gaat over het inbreken op een computer die niet van de top was.” Volgens de minister ging het niet om de top, maar een onderhoudsbedrijf. “Er werden via dit systeem gegevens uitgewisseld over de problemen met het onderhoud van schepen op de werf, om zo reiskosten te besparen.” Hij stelt dat ze op geen enkele manier zijn gehackt, maar heeft voor de zekerheid wel een waarschuwing laten uitgaan naar de hele Defensieorganisatie.

Hachchi neemt hier geen genoegen mee. “Met de mantel der liefde bedekt hij zaken: er is eigenlijk niet zoveel aan de hand. Ik

vraag mij af of dit in het belang van Defensie is. Hoe serieus kijkt de minister naar incidenten?” Het gaat haar om bewustwording. En of het nu gaat om een uitvoeringorganisatie of het departement aan het Plein, uiteindelijk is het informatie van Defensie. Aldus, wat gaat de minister doen? Want ze heeft geen zin om nu te horen dat alles in orde is en hier over een paar weken weer te staan omdat er echt iets aan de hand is.

Na wat heen en weer gepraat mengt Arjan el Fassed, Kamerlid Groen links, zich in de discussie. “Voorzitter. Week in, week uit horen wij berichten van basale veiligheidszaken die niet op orde zijn, of het nu is bij grote bedrijven als KPN, bij lagere overheden of bij de Rijksoverheid. Fabriekswachtwoorden worden bijvoorbeeld niet veranderd; dat is ook hierbij het geval. Nu is het zo dat Defensie het liefst met een tank door de straat wil rijden terwijl de voordeuren van karton zijn.” Hillen zegt toe dat de tank is afgeschaft en dat Defensie overal zal nagaan of er wachtwoorden zijn en checken of de systemen veilig zijn. Dat zal wel even duren, want de organisatie is groot. Maar zodra hij daarover bevindingen kan melden, zal hij dat in zijn verslaggeving aan de Kamer laten weten.

Van minister Hillen hebben we daarna niets meer gehoord over de hackbaarheid bij Defensie, maar voor de Kamerleden is dit weer de zoveelste onthulling die roept om ingrijpen van de overheid. Opstelten is met het NCSC dan druk bezig beleid op te zetten. Daarover later meer. Eerst eens kijken hoe het nu is afgelopen met Arjen de Waard, de directeur die tegen de regels in het onveilige systeem gebruikte. Als ik met het Ministerie van Defensie bel, krijg ik hem aan de lijn. “Met kolonel De Waard” hoor ik, met een typische zware militaire intonatie. Ik vertel hem over mijn onderzoek en de onthullingen van Gevers. “Ah, het VTC”, reageert hij direct. “Pardon?” “Het Video Teleconferentie Systeem. Ik reisde toen veel heen en weer tussen Den Helder en Den Haag en kreeg dit van de jongens van Onderhoud. Was wel handig.” Volgens hem was er geen verbinding mogelijk met andere Defensie onderdelen. Wat betreft het lek reageert hij luchtig: “Ja, ze hadden weleens dat fabriekswachtwoord moeten veranderen. Was niet zo netjes”.

Of de kolonel nu zelf verantwoordelijk was voor het aanpassen van wachtwoorden, dat de jongens van Onderhoud hem daarop hadden moeten wijzen, of dat Defensie haar systemen zo moet instellen dat dergelijke toestanden niet meer kunnen voorkomen, laat ik even in het midden. Van belang voor dit verhaal is dat we hier weer een keten aan onveiligheden aantreffen die pas na een melding wordt ontrafeld en hopelijk beter wordt beveiligd. Gevers en De Kok hebben Defensie weinig tijd gegeven het lek te dichten, maar het heeft wel gewerkt, zonder dat ze werden vervolgd. Ook de kolonel zelf blijkt volgens hemzelf en volgens de afdeling Voorlichting geen negatieve consequenties te hebben ondervonden door de onthulling.

Rickey Gevers komt een jaar later weer uitgebreid in het nieuws als hij bij Digital Investigation een database van 750 GB in handen krijgt. Uit hun onderzoek blijkt de data afkomstig uit het zogenaamde Pobelka-botnet en er staan heel veel wachtwoorden in van Nederlandse organisaties. Hij meldt het bij de politie en het NCSC, maar die doen er niet veel mee. Daarom onthult hij februari 2013 zijn vondst via Jeroen Wollaars, die er een NOS-item van maakt. Iedereen die denkt getroffen te zijn kan bij Digital Investigation checken of ze ook in de database staan. Ze krijgen verzoeken van securitybedrijven, luchtverkeer, banken, ziekenhuizen, waterbedrijven, chemie…. Bij vrijwel alle pogingen is het antwoord “ja”. Dan komt de overheid wel in actie. De daders worden uiteindelijk niet gepakt, maar hopelijk heeft door alle aandacht wel iedereen zijn wachtwoord weer eens aangepast.

Gevers komt ook nog een paar keer in de media terug met zijn verhaal over zijn bekering tot de goede kant van cyber security. Dit, ter lering voor jonge hackers en om hen zo ook op het rechte pad te houden. Tot slot speelt hij nog een hoofdrol in het boek ‘Komt een vrouw bij de hacker’ van Maria Genova. Ze wil weten hoe het is om gehackt te worden en na een lange zoektocht vindt ze alleen Gevers bereid dit te doen.

Dit is nog maar een greep uit Gevers’ heldendaden, waarvan er nog meer zullen volgen. Hij is een hacker met lef, die wil laten zien wat hij kan en best een beetje risico wil nemen om Nederland een stuk veiliger te maken. Het contrast kan bijna niet groter zijn met de hacker uit het volgende hoofdstuk: Floor Terra, een zeer

behoedzame onderzoeker, maar een die minstens zoveel heeft betekend voor responsible disclosure.

10. @floorter: a man in the middle

ING ontkent lek in Mobiel Bankieren App, maar komt wel met meldpunt

Joost Blokzijl van EenVandaag, die eerder de pompen van Veere onthulde, heeft begin 2012 nog een andere leuke scoop. Floor Terra, ook wel @floorter, heeft ontdekt dat de nieuwe bankierenapp van de ING kwetsbaar is voor een man-in-the-middle-attack. Dat, terwijl al 800.000 mensen de app hebben gedownload en ongeveer 300.000 hem dagelijks gebruiken. Hij meldt het lek, maar er gebeurde niets. Pas als hij er een blog over schrijft en EenVandaag erbij komt, luistert de bank en wordt de bug gefikst. Zonder enige erkenning voor Terra's vondst, terwijl juist deze onderzoeker van bijzondere waarde zal blijken voor responsible disclosure in Nederland.

Floor Terra is iemand met een goed gevoel voor zowel complexe technologie als het maatschappelijk welzijn. Na zijn studie Sterrenkunde was hij een tijdje docent Natuurkunde, ontwierp hij software en verzorgde hij beveiligde verbindingen bij Stichting Respect my Privacy. Bij het Nikhef deed hij data-analyse en onderhield hij de controle- en meetsoftware. Nu werkt hij als 'technoloog' bij het College Bescherming Persoonsgegevens. Op zijn blog floort.net/blog snijdt hij actuele veiligheidskwesties aan. Responsible disclosure heeft hij er altijd bij gedaan, in zijn vrije tijd. Als hij een beveiligingsprobleem vindt, meldt hij het eerst bij de eigenaar van het systeem en niet zoals anderen wel eens doen bij de pers.

Eind 2011 lanceert ING een nieuwe bankierenapp. Alles in de campagne is gericht op betaalgemak, "altijd en overal". Terra ziet het maatschappelijk belang van de veiligheid van zo'n app, want er zullen veel mensen binnenkort betalingen mee gaan doen. Als iemand de communicatie tussen de mobiel en de bank kan onderscheppen, zou die de transactie kunnen aanpassen en geld

overmaken naar een andere rekening. Dat heet een man-in-the-middle-attack en kan voorkomen worden met een zogenaamde Secure Socket Layer: een encryptieprotocol dat werkt met certificaten om wederzijds te bewijzen dat je bent wie je zegt dat je bent. Terra kijkt daarom naar het ontwerp van de app, of er inderdaad SSL wordt toegepast en certificaten worden uitgewisseld. Dat is het geval, alleen: de app controleert die certificaten niet. Je kunt dus een nepcertificaat nemen en alsnog de man-in-the-middle spelen.

Tenminste, dat is zijn vermoeden. Hij zou het kunnen uittesten, maar dan zou hij de app werkelijk hacken. Hij wil niet de wet overtreden, dus belt hij eerst met de ING-helpdesk. De medewerker aan de lijn verzekert hem dat de app wel echt veilig is, maar neemt de melding in ontvangst en belooft erop terug te komen. Na enkele weken wachten, is er nog geen antwoord, dus zet Terra zijn vermoedens op 15 januari 2012 op zijn blog. Hij eindigt zijn betoog met de vraag: “Mag ik concreet aantonen dat de applicatie slecht beveiligd is om mijn stelling te onderbouwen?”

Journalist Joost Blokzijl leest de blog ook en ziet meteen een interessant item voor EenVandaag. Het was weliswaar net als de SCADA-systemen een abstract onderwerp, maar mobiel betalen is in opkomst en er worden vraagtekens bij gezet. Het gaat ook om veel gebruikers en dat maakt het meer nieuwswaardig. Hij benadert de bank, maar die wil geen commentaar geven. De Nederlandse Vereniging voor Banken ook niet. Floor Terra wel, maar als ethisch hacker wil hij wel ING voldoende tijd geven om het lek te dichten. Ze spreken een termijn af van twee maanden. Dat moet genoeg zijn.

EenVandaag opent 21 maart 2012: “Mobiel Bankieren ING maandenlang onveilig, dat zeggen beveiligingsexperts tegen EenVandaag. Ze spreken over een blamage en een beginnersfout van ING.” De redactie weet goed een schimmige sfeer te creëren. De ING-reclame is te zien op een slecht scherm en wordt ruw verstoord door computergepiep. We zien Terra half in het donker zitten. Terwijl willekeurige code over het scherm rolt, zegt hij: “Hier klopt iets niet. Die app is niet veilig. Beginnersfout.” Bart Jacobs, van de Digital Security Group uit Nijmegen vliegt door het beeld:

“Dit is een blamage. Hierom wordt ING in securitykringen hard uitgelachen.” De toon is dus meteen gezet. Dan volgt de uitleg.

Voice-over: “Al 800.000 mensen hebben hem gedownload, 300.000 van hen gebruikt hem dagelijks, maar is de app wel veilig genoeg?”

Terra: “De klanten lopen weldegelijk een risico.”

Voice-over: “Dit is Floor Terra, student Natuur- en Sterrenkunde en laten we zeggen ‘goed met computers’. Want hacker wil hij zichzelf niet noemen, dat mogen anderen over hem zeggen. Feit is dat hij een lek ontdekte (…) Er ontbrak volgens de hacker iets in de basisbeveiliging.”

Terra: “In eerste instantie dacht ik, ze zullen toch niet *dit* vergeten zijn? Dat heb ik gecontroleerd en binnen een uurtje had ik het zo uitgewerkt dat ik kon afluisteren wat voor verkeer er over ging. Ik kon mijn eigen server ertussen zetten en doen alsof ik de ING was.”

Wat hij ontdekt zou hebben, wordt verbeeld met een animatie van een bank, mobiel en slot dat met veel computerherrie doorgekruist wordt. Vervolgens komt Jacobs in beeld. Na lof voor Terra’s werk, omdat hij het lek eerst bij ING had gemeld, legt de hoogleraar Computerbeveiliging uit dat dit zeker misbruikt zou kunnen worden. Jacobs: “Dit hadden ze zelf moeten ontdekken. ING heeft haar kwaliteitscontrole niet op orde. Daar zou ik me zorgen over maken als ik in de directie van ING zou zitten.”

EenVandaag meldt dat gebruikers een nieuwe app moesten downloaden. Die zou nu wel veilig zijn. Terra verduidelijkt: “Dat kun je zien aan dat slotje.” Het lek is dus gefikst, maar ING wil dat niet erkennen. De bank zelf wil ook niet voor de camera en reageert alleen schriftelijk. In de verklaring meldt een woordvoerder omwonden dat de app wel veilig is, zonder enige melding van Terra’s hulp:

“Onze klanten kunnen veilig gebruik maken van de Mobiel Bankieren App. Honderdduizenden klanten maken dagelijks gebruik van de app. Zowel op veiligheid als op gebruiksgemak doen wij daarom absoluut geen concessies. De veiligheid staat op een zeer hoog niveau. De app is op vele manieren getest en beveiligd, niet altijd volledig zichtbaar voor experts van buiten. Sinds de lancering in november 2011 zijn er geen fraudegevallen

geconstateerd. Natuurlijk willen we dat dit zo blijft. Een team van specialisten werkt iedere dag aan de verdere ontwikkeling van onze dienstverlening via de Mobiel Bankieren App om de veiligheid en het gebruiksgemak te kunnen blijven garanderen. In de ontwikkeling van de app luisteren wij goed naar de gebruikers. Wij hebben van klanten tips gekregen om de app te verbeteren. Zo hebben wij naar aanleiding van deze tips onlangs nog het adresboek toegevoegd. Ook op het gebied van veiligheid krijgen wij aanbevelingen die wij onderzoeken en waar relevant overnemen. Wij zijn onze klanten zeer dankbaar voor alle waardevolle feedback en nemen deze zeer serieus."

De avond van de uitzending van EenVandaag krijgt @floorter een tweet van @mount_knowledge: "ING app SSL issue is oud nieuws. Ik schreef hier in november al over." En inderdaad, in de blog van Richard van den Berg wordt het probleem al netjes uitgelegd. @floorter: "In dat geval heeft de ING dus keihard tegen mij gelogen toen ze zeiden dat er nooit eerder zoiets gemeld was." En "Als dit soort security meldingen niet centraal gecoördineerd worden, is dat op zichzelf ook een probleem". Terra was dus zeker niet de eerste die het lek ontdekte.

Eind 2013 schrijf ik een column over deze zaak voor het tijdschrift Informatiebeveiliging. Vlak voor ik de tekst naar de redactie stuur, krijg ik nog een DM van @floorter: "Positief bericht: http://www.ing.nl/de-ing/veilig-bankieren/veiligheidsbeleid-van-deing/meldpunt-kwetsbaarheden/index.aspx." Als ik klik op de link verschijnt een ING Meldpunt Kwetsbaarheden. Hier is te lezen: "Responsible disclosure. Bent u deskundig en ontdekt u een kwetsbaarheid in onze systemen? Help ons dan door deze kwetsbaarheid te melden. Zo kunnen we samen de veiligheid en betrouwbaarheid van onze systemen verbeteren."

In de tekst eronder worden duidelijk de spelregels uitgelegd voor verantwoord onthullen: plaats geen backdoor, wijzig geen gegevens, verander niets aan het systeem, probeer niet vaker binnen te komen dan nodig, doe geen brute force (oftewel eindeloos wachtwoorden uitproberen) en deel de kwetsbaarheden niet met anderen. Als je deze regels volgt, zal de bank geen aangifte doen en kun je zelfs rekenen op een beloning. Anoniem

melden mag ook. Er staat ook een e-mailadres bij waar je meldingen kwijt kunt: responsible-disclosure@ing.nl. Ik stuur de tekst die hierboven staat naar dit adres en vraag of de onthulling van Terra de aanleiding was voor dit meldpunt. Dit adres is daar natuurlijk niet voor bedoeld, maar niettemin krijg ik al na vier uur antwoord van ene Inge Witteman:

“ING heeft responsible disclosure ingevoerd, omdat wij het belangrijk vinden dat klanten veilig kunnen bankieren. Wij stellen ons daarom open voor deskundigen om ons hierbij te ondersteunen door een gevonden mogelijke kwetsbaarheid aan ons te melden. De invoering van responsible disclosure is een actie vanuit de verschillende Nederlandse banken in samenwerking met de NVB. Responsible disclosure wordt ook in andere branches toegepast om een kwetsbaarheid in een systeem te kunnen melden. De specifieke zaak van Floor Terra is hiervoor niet de aanleiding geweest.”

Er is inderdaad veel gebeurd in het tussenliggende anderhalf jaar. Het NCSC heeft hun ‘Leidraad om te komen tot een praktijk van responsible disclosure’ gepubliceerd en die is overgenomen door verschillende organisaties, met de telecombedrijven en banken voorop. De ambtenaren hebben voor de leidraad veel overleg gehad met het veld, onder andere met Floor Terra. Als de leidraad eenmaal uitkomt, stelt Terra in samenwerking met andere betrokkenen een voorbeeld tekst op die organisaties op hun site kunnen zetten. Die is nog steeds te raadplegen op www.responsibledisclosure.nl en staat ook in de bijlage van dit boek. Maar als je terugkijkt waar de spelregels voor verantwoord onthullen vandaan komen, wijst alles in de richting van een specifieke bron. Minister Opstelten heeft de leidraad gewoon van Marktplaats. Daarom gaan we eerst kijken hoe het er daar aan toegaat.

11. @legosteentje verdient een witte hoed

Marktplaats.nl als voorloper in responsible disclosure

Marktplaats is een interessant doelwit voor hackers. De site trekt gemiddeld 1,3 miljoen bezoekers per dag en er gaat veel geld in om. Alleen al de vele inlognaam- en wachtwoordcombinaties kunnen waardevol zijn voor criminelen. Veel mensen gebruiken immers nog steeds één wachtwoord voor verschillende sites. De beveiliging van Nederlands grootste veilingsite wordt daarom regelmatig getest. Tijdens de zogenaamde Beer, Pizza & Hacking-avonden, proberen ontwikkelaars de zwakke plekken in elkaars code te vinden en zo te leren waar ze voortaan op moet letten. Het is voor dit bedrijf dan ook vanzelfsprekend om goed om te gaan met meldingen van hackers van buiten. Voor hen is er een speciaal responsible disclosure beleid. Vind je een veiligheidslek dan kun je dat dus melden en zelfs een beloning krijgen. Als je maar wel handelt volgens protocol: meld ons het lek zonder het eerst met anderen te delen, geef ons de tijd om het te dichten en veroorzaak geen schade. Een van de hackers die dat begin 2012 deed, was de toen 19-jarige Pieter Vlasblom, ook wel @legosteentje.

Vlasblom zit dan op het Rijn IJssel MBO, maar vindt school eigenlijk maar niks: geen uitdaging. Stage vindt hij leuker. Daar gaat hij aan de slag met een applicatie die automatisch advertenties plaatst op Marktplaats. Al snel komt hij er achter dat hij beter zelf iets in elkaar kan knutselen en dat doet hij in de open-sourcetaal Ruby. Vervolgens doet hij wat hackers van nature doen: er van alles in stoppen om te kijken wat er gebeurt. Zo zet hij in plaats van gewone tekst HTML-code met JavaScript in de advertenties, oftewel Cross Site Scripting (XSS). Het werkt: de advertentie gedraagt zich nu als site en @legosteentje zou zo

bezoekers van Marktplaats met pop-ups naar een andere site kunnen leiden.

Hij vindt het toch wel spannend wat hij heeft gevonden en durft niet meteen naar de eigenaar van de site te gaan. Daarom probeert hij het op 2 maart 2012 eerst met een voorzichtige tweet: “Heb een securityprobleempje bij Marktplaats gevonden.” Prompt reageert @basanneveld: “We komen graag met je in contact indien je een bug gevonden hebt. We hebben een responsible disclosure program tinyurl.com/7orv6ap.” Vlasblom denkt eerst dat hij in de problemen kan komen, maar Anneveld benadrukt dat hij vooral uitleg wil en ze beginnen te mailen. De site wordt binnen een dag weer gefikst. Vlasblom krijgt vervolgens tot zijn verbazing 350 euro voor zijn vondst en een pakje: een Classified White Hat in a Black Box, oftewel een witte hoed in een zwarte doos. @legosteentje is nu een erkende white hat hacker.

Na een paar maanden zit zijn stage-opdracht er weer op, maar hij wil eigenlijk niet terug naar school. Hij gaat daarom maar eens op de koffie bij Anneveld en vraagt of hij stage kan lopen bij Marktplaats. Jazeker, dat kan en vanaf juni 2012 gaat hij aan de slag. Vlasblom schrijft, weer in Ruby, een applicatie die Marktplaats test op zwakheden: SQL-injections, poortscans, XSS, etc. Een soort geautomatiseerd @legosteentje. Als de applicatie wat vindt, dan geeft Vlasblom de kwetsbaarheid meteen door naar de betreffende afdeling.

Over dit verhaal kunnen we kort zijn: het is prachtig als het zo loopt. Van belang voor dit boek is dat Marktplaats op het moment van de onthulling, voor zover ik weet, de eerste Nederlandse organisatie was met zo’n expliciet responsible disclosure beleid. Het is volgens mij ook een voorbeeld geweest voor de richtlijn die door het NCSC het jaar erna is gepubliceerd.

De initiatiefnemers van dit beleid zijn Robin Schuil (medeoprichter en Innovation Program Manager) en Bas Anneveld (Manager Site Operations). Schuil wordt ook later bij veel bijeenkomsten een warm pleitbezorger voor responsible disclosure, met het verhaal van @legosteentje als showcase. De richtlijn van destijds is in de tijd aangepast, maar als we kijken naar een screenshot uit die periode zien we dat hun ‘Responsible

Disclosure Program' verdacht veel lijkt op de leidraad zoals die later door het NCSC wordt gepubliceerd. Het Marktplaatsprogramma is echter wel meer gericht op de melder en noemt ook expliciet beloningen. Hun tekst is ook in het Engels, want je weet maar nooit waar de melding vandaan komt:

"We recognize the important role that security researchers and our community play in keeping Marktplaats and our customers secure. If you believe you've found a vulnerability, we would like to work with you to investigate it as quickly as possible. Please send us as much information as possible to help us better understand the nature and scope of the possible issue."

Hierna volgen de spelregels. Vind je een lek in de site, meldt het dan direct via security-bug@marktplaats.nl en zet het niet op een of ander forum. Klinkt op zich logisch, maar in die tijd gaan nog veel meldingen full disclosure. Beschrijf in je melding precies wat voor lek je gevonden hebt en waar het zit. Geef hen tot slot voldoende tijd het lek te dichten. Hoeveel dat is hangt af van de ernst van het lek, maar ze houden het op dertig dagen. Daarna mag je het publiekelijk bekend maken. Wat je vooral niet moet doen is schade toebrengen aan het systeem of data van andere gebruikers inzien.

Volg je deze regels en ben je de eerste die het lek vindt, dan kom je in aanmerking voor een beloning. Die varieert weer naar de ernst van de bug, maar is gemiddeld 350 euro in Paypalvouchers. Je krijgt bijvoorbeeld niets als je wachtwoorden hebt gekraakt met brute force of social engineering, ziet dat ze kwetsbaar zijn voor een DDoS aanval of als je een bug vindt die eigenlijk bij een andere partij zit dan Marktplaats. Dit zijn namelijk kwetsbaarheden die organisaties altijd wel zullen hebben. Tot slot belooft Marktplaats dat ze binnen drie dagen reageren op je melding, die vertrouwelijk afhandelen en je tijdens het proces op de hoogte houden. Ze zullen ook geen aangifte doen, tenzij je je niet houdt aan het bovenstaande spelregels.

In de periode dat @legosteentje zijn witte hoed krijgt, is er dus nog geen richtlijn vanuit de overheid. Dat gebeurt pas een jaar daarna, maar minister Opstelten zegt in het Algemeen Overleg van 10 april 2012 wel alvast dat de richtlijn eraan komt. Op de

agenda staat: ‘Cyber Security en veiligheid overheidswebsites’. Aan bod komen de onderwerpen die we al eerder tegen kwamen: Diginotar, ICT-beveiligingsassessments DigiD bij gemeenten en de sluizen van Veere. De discussie gaat al snel over de rol die het NCSC hierbij moet spelen en hoe we in Nederland moeten omgaan met ethische hackers.

In dit debat is Hennis-Plasschaert (VVD) weer als eerste aan het woord: “De SCADA-brief van het kabinet van enkele weken geleden stelt enigszins gerust. Tegelijkertijd kan ik niet genoeg benadrukken dat als departementen, gemeenten en waterschappen allemaal hun eigen dingetje blijven doen, de overheid en dus ook grote delen van onze vitale infrastructuur zo lek als een mandje blijven. Regie is cruciaal.”

Elissen (PVV) is content met de brief van Opstelten. “Het Nationaal Cyber Security Centrum heeft een beetje orde in de chaos weten te scheppen, door een eenvoudige checklist te publiceren en handzame informatie te verstrekken waarmee eigenaren van SCADA-systemen op weg worden geholpen.”

Recourt (PvdA) neemt het op voor wat hij noemt “de jongens en meisjes die op een zolderkamertje zitten te sleutelen. Je kunt hun activiteiten met een strafrechtelijke bril bekijken, maar ik denk dat je jezelf daarmee tekortdoet. Ik zie namelijk een hoop creativiteit. Je moet die mensen niet meteen verder in het criminele milieu wegzetten. Dat krijg je natuurlijk, want als de overheid niet geïnteresseerd is, zijn criminele organisaties dat zeker wel. Ook die zijn namelijk op zoek naar dezelfde kennis.”

Hennis-Plasschaert doet deze handreiking naar ethisch hackers af als een banenplan en gooit het over een andere boeg: een meldplicht datalekken. Als blijkt dat organisaties onzorgvuldig zijn geweest met de beveiliging van persoonlijke data, dan zouden ze verplicht moeten zijn dat te melden bij degene over wie die data gaan. Hier had ze een jaar geleden al een voorstel voor ingediend, maar dat is dan nog steeds in behandeling.

Hachchi (D66) brengt de discussie weer terug bij de ethisch hackers en richt zich tot minister Spies met een eigen onthulling: “Om te beginnen merk ik op dat ik blij ben dat de minister van Binnenlandse Zaken mijn voorstel bekijkt om studenten of whizzkids, zoals zij ze noemt, bij hacktesten te betrekken. Ik blijf

graag op de hoogte van de ontwikkelingen – dat geldt misschien ook voor mijn collega's – hoewel de minister heeft aangegeven dat zij die niet aan de grote klok wil hangen. Ik heb ook met de minister gesproken over een richtlijn voor de wijze waarop met hackers moet worden omgegaan. De overheid weet zelf niet goed op welke manier zij met hackers moet omgaan. Computerexperts die misstanden melden, krijgen wisselende reacties. De ene gemeente is dankbaar en dicht het lek, de andere gemeente doet aangifte of stelt de hacker meteen aansprakelijk. Ook heb ik begrepen dat de jurisprudentie over de vraag wanneer een hack al dan niet strafbaar is, nog onvoldoende is uitgekristalliseerd. Daarom heb ik voorgesteld om tot een richtlijn te komen voor de manier waarop met hackers moet worden omgegaan." Ze onderstreept de noodzaak van een richtlijn wederom met een uitvoerige uiteenzetting van de zaak Veere.

Verder verloopt het debat net als de voorgaande debatten. De Kamerleden eisen meer informatie over de staat van cyber security in Nederland en willen een daadkrachtiger optreden van de overheid. Enkelen stellen zelfs voor dat NCSC een soort Opta wordt, die kan controleren en boetes kan uitdelen. Minister Opstelten stelt iedereen gerust dat eraan gewerkt wordt, maar: "Het NCSC is geen toezichthouder die de beveiligingsarrangementen van alle bedrijven opvraagt. Dat moeten we ook niet hebben, want dan gaat iedereen achteroverleunen." De liberale minister wil zich dus niet te veel bemoeien met de lokale gang van zaken, maar hij voelt wel wat voor verantwoorde onthullingen:

"Dan kom ik bij het punt van mevrouw Hachchi over de ethische hackers, waar mijn collega Spies ook nog op in zal gaan. Het is van belang dat hackers eenduidig worden behandeld. Op dit moment wordt gewerkt aan de procedure van responsible disclosure. Hierbij wacht de hacker met openbaarmaking van een lek totdat het lek is gedicht. Het Nationaal Cyber Security Centrum speelt hierin een rol als intermediair om kennis van hackers bij bedrijven te adresseren. Verder wordt onderzocht hoe ethische hackers op een verantwoorde wijze een rol kunnen spelen bij het inzichtelijk maken van kwetsbaarheden. Volledigheidshalve

betekent dit niet dat hackers een vrijbrief krijgen om lekker aan de slag te gaan.”

Blijkbaar is er achter de schermen veel gesproken over de ethisch hackers. Er komt dus een richtlijn en er is een instituut dat dit alles gaat begeleiden: het NCSC. Volgens beleidsmedewerker Barend Sluijter is dit debat van 10 april 2012 hun startsein geweest om naar buiten te treden met beleid voor responsible disclosure. Ze waren toen al aan het praten met veel van de personages die in dit boek de revue passeerden: Floor Terra, Oscar Koeroo, Brenno de Winter, Lodewijk van Zwieten, Bart Jacobs en Robin Schuil. Ze hadden zelfs @ntisec uitgenodigd, maar die kwam niet.

Het zal nog tot de jaarwisseling duren totdat Opstelten de richtlijn kan delen met de Kamer. Pas in mei 2013 wordt de tekst daar ook behandeld. In de tussentijd gebeurt er van alles waardoor de druk op een goede handreiking van NCSC flink wordt opgevoerd. Eerst wordt een van de Kamerleden zelf hoofdpersoon in een onthulling. Henk Krol, voorzitter van 50PLUS komt namelijk in de online dossiers van Diagnostiek voor U, gaat er direct mee naar de media en wordt veroordeeld voor computervredebreuk. In die periode vindt een hacker beveiligingslekken bij het Groene Hart Ziekenhuis. Ook hij wordt vervolgd en veroordeeld. Achter de schermen wordt ook nog een minderjarige vervolgd voor het hacken van de Habbo helpdesk. In al deze zaken is Brenno de Winter weer een katalysator voor flink wat discussie in de media en de Tweede Kamer.

@legosteentje gaat in die tijd gewoon rustig door met waar hij goed in is. Zo heeft hij Spotify gecrossscript en ook dat leverde hem een mooi pakket met goodies op. Zelf kom ik met hem in contact als een hacker op 5 maart 2013 een lek van mijn website op Twitter zet. Full disclosure dus. @legosteentje is de eerste die me ervoor waarschuwt en dankzij hem kan ik het lek snel dichten. In juli 2013 wordt zijn stage omgezet in een baan. Marktplaats is dan overgenomen door eBay en wordt gezien als een voorloper in ethisch hacken. Vlasbloms meldingen gaan dan de hele wereld over naar andere takken van eBay.

Tijdens de afronding van dit boek in december 2014 kijk ik nog één keer hoe het gaat met @legosteentje. In een bericht van 17

juli lezen we dat hij security wel een beetje beu is. Na deze tweet stopt de berichtgeving van @legosteentje. Nu is hij @ChunkrGames, een Youtube-gamecommentator. In zijn video's zie je hoe hij door de virtuele wereld Minecraft loopt en hoor je bij alle acties zijn enthousiaste commentaar. De video's lijken er vooral op gericht anderen te leren hoe het spel te spelen. Ook daarin is hij redelijk succesvol: 51.277 abonnees en 2.622.932 views. Ondanks zijn witte hoed is hij toch meer een gamer dan hacker. Dat geldt ook voor ons volgende personage: @jmschoder die de virtuele wereld Habbo Hotel bijna toevallig hackt. Met hem loopt het echter minder goed af.

12. @jmschroder belt de Habbohelpdesk

Minderjarige hacker na twee jaar voor de rechter

Habbo is een MMOCC: massive multiplayer online chatting community. Het begon in 2000 als een chatsite voor een Finse rockband en is inmiddels uitgegroeid tot een wereldwijd platform voor miljoenen tieners. Als Habbie heb je een eigen profielpagina en avatar waarmee je rondloopt in een virtuele omgeving. Je kunt er chatten en spelletjes spelen met anderen. Lid worden is gratis, maar voor enige entourage en privileges moet betaald worden in echte euro's. De lokale muntsoort Credit schommelt rond de tien eurocent. Hiermee kun je ook handeldrijven met medespelers.

Sulake, het bedrijf achter Habbo, heeft allerlei allianties met grote merken, want het is de perfecte plek om jongeren te bereiken. Ze hebben volgens hun site 273 miljoen geregistreerde gebruikers in 150 landen, waarvan 90% tussen de 13 en 18 jaar oud is. Van deze gebruikers brengen er 5 miljoen elke maand een bezoek aan de site van gemiddeld 41 minuten per keer. "The time is spent together with friends in an environment created by both brands and users", aldus Sulake. Omzet 2012 was 22 miljoen euro, met negatief winstresultaat. Het bedrijf is ook vaak overgenomen door anderen. Onze eigen Telegraaf Media Groep was tot maart 2013 eigenaar van de Nederlandse afdeling van Sulake.

Habbo Hotel is ook in zichzelf een levendige economie, met eigen regels en beloningen. Er mag officieel niet gegokt of gespeculeerd worden, maar spelers proberen van alles uit om dat toch te doen. Onderlinge communicatie wordt actief gestimuleerd, maar wel gefilterd: elk scheldwoord wordt vervangen door 'bobba'. Na enkele incidenten met pedofielen wordt ook actief gejaagd op seksueel expliciet gedrag. En er zijn natuurlijk ook hackers die met inloggegevens van anderen virtuele goederen kunnen overnemen.

Om ervoor te zorgen dat iedereen zich gedraagt in de virtuele wereld, lopen er continu moderatoren rond. Ze houden de interactie gaande en treden op bij misstanden. Spelers die zich misdragen, krijgen een waarschuwing en kunnen zelfs uit het spel worden verbannen. De moderatoren zijn ook te benaderen via help.habbo.nl. Het platform voor deze helpdesk wordt geleverd door de customer support multinational Zendesk. Als je een account hebt in Habbo, kun je van daaruit automatisch inloggen op hun Player Support. Je hoeft dus niet apart in te loggen, maar krijgt automatisch een account.

De 15-jarige Hans Schröder doet dat begin mei 2011 toevallig andersom. Hij heeft een vraag aan de helpdesk en logt niet in met zijn Habbo-account, maar maakt een nieuwe aan in de Zendesk Player Support. Hij stelt zijn vraag, krijgt antwoord en gaat weer naar Habbo Hotel. Daar maakt hij met hetzelfde e-mailadres een nieuwe account aan en ziet hoe die weer automatisch wordt gekoppeld aan die van Zendesk. Dat is op zich niet zo vreemd, maar het valt hem wel op dat hij die nieuwe account niet eerst via de mail moet bevestigen.

Donderdagavond 12 mei vertelt hij dit tegen een vriend met wie hij aan het skypen is. Ze komen op het idee om een nieuwe Habbo-account aan te maken, maar dit keer met het e-mailadres van de Zendeskmedewerker die hem geholpen heeft, gewoon om te kijken of het werkt. En inderdaad, ook deze account hoeven ze niet via de mail te verifiëren. En dat terwijl deze medewerker natuurlijk een ander scherm heeft. Zo komen ze in de backend van de helpdesk en zien ze 15.000 openstaande vragen van spelers. Schröder: “Je kon gebruikers opzoeken, alle tickets zien die werden afgehandeld, IP-adressen… Ik had meteen wel door dat ik daar niet thuis hoorde. Op een gegeven moment komt iemand er wel achter dat dit lek bestaat.”

Hij besluit daarom de volgende dag met Habbo te bellen. Het is dan al vrijdagavond en in het weekend zijn ze niet bereikbaar. Hij probeert het maandag 16 mei nog eens en krijgt ene Marion aan de lijn. Schröder: “Ik werd niet serieus genomen, ze zag de problematiek niet. Ze zei wel: Als je daarin zit, moet je daar onmiddelijk uit en niet meer ingaan.” De medewerkster stelt voor

dat hij zijn vraag stelt via de helpdesk van Zendesk en verbreekt de verbinding. Even later belt Schröder nog een keer. Nu krijgt hij Beau aan de lijn. Zij neemt hem wel serieus. Schröder: “Het was een goed gesprek. Ze zei: ‘Fijn dat je het meldt. Mail wat je precies hebt.’ Beau wilde namelijk de gebruikers informeren en vroeg om de klantgegevens die ik kon zien. Ze vroeg ook mijn eigen IP-adres om dat van de anderen te onderscheiden.”

Schröder zet netjes alle 15.000 klantgegevens in een Excelsheet en mailt die naar Beau. Hij verwacht dan nog wel een bedankje te krijgen, of een bosje bloemen, maar hij krijgt niet eens een bevestiging. Woensdag 18 mei doet hij er dan nog maar een mailtje achteraan: “Hallo, ik had nog geen bevestiging ontvangen of de mails waren aangekomen, en u vroeg ergens in het telefoongesprek volgens mij mijn IP-adres maar ik was deze vergeten te geven dus bij deze.” Nu krijgt hij wel antwoord. Beau schrijft: “Hey Hans! Ik wil je bij deze nog ontzettend bedanken voor al je hulp. Alles is goed binnen gekomen, we gaan ermee aan de slag!”

Op 20 mei krijgt Schröder een mail van Habbo. Tot zijn verbazing leest hij: “Op donderdag 12 mei hebben wij opgemerkt dat onbevoegden tijdelijk op illegale wijze toegang hebben verkregen tot ons klantenservice systeem https://help.habbo.nl/home. Wij hebben deze personen onmiddellijk de toegang geblokkeerd, het probleem verholpen en onze beveiliging verhoogd. We hebben echter redenen om aan te nemen dat de mensen die hebben ingebroken, ook de informatie zouden hebben kunnen inzien van jou omdat je ons onlangs een e-mail hebt gestuurd via de Habbo Help Tool.” Wat volgt, is een reeks spijtbetuigingen, algemene veiligheidstips en, als extra veiligheidsmaatregel, het verzoek om opnieuw je e-mail te bevestigen. De getroffen spelers krijgen als troost een virtuele roos van Habbo.

Schröders e-mailadres was natuurlijk een van de 15.000 contacten die via de account van de helpdeskmedewerker gelekt waren en nu worden hij en al die anderen gezien als slachtoffer van een hack. Is hijzelf dan de dader? Hij denkt van niet, want zelfs de eerst zo onwelwillende helpdeskmedewerker Marion heeft hem toegevoegd als een van haar weinige vrienden in het

spel. Onder de spelers staat hij daarom ook bekend als de melder van het lek en daar is hij best trots op. Totdat hij erachter komt dat op diverse hackersfora lijsten worden gepubliceerd met gebruikersnamen en wachtwoorden van Habbies. Zijn naam en mailadres staan erbij als afzender. Nu werkt zijn bekendheid tegen hem, want ze denken dat Schröder er ook echt achter zit en gaan hem lastig vallen - niet alleen binnen het spel, maar ook via Skype en zelfs thuis. De lol is dan wel af voor Schröder en hij stopt met Habbo Hotel.

Na bijna een jaar van afwezigheid logt hij weer eens in. Hij krijgt namelijk nog steeds vriendenverzoeken via de mail en wil dit uitzetten. Tot zijn verbazing ziet hij dat zijn account geblokkeerd is en krijgt hij deze melding: “Overtreding Algemene Voorwaarden – Ban: Permanent (id: 1739595). Je ban verloopt 1-6-12 15:05.” Dit is een vreemd bericht, want is hij nu permanent verbannen of niet? Eigenlijk vindt hij het nog best grappig en op 5 mei 2012 twittert @jmschroder de tekst van de melding aan @Habbo_Staff, met eronder de vraag: “permanent??” De Habbo Staff reageert: “Deze vragen kun je stellen via de Habbo Help Tool via ‘contact’ op onze homepage. De dames daar helpen je graag verder :).” Nu is Schröder helemaal verbaasd. Is dit bedoeld als grap, of is het gewoon een medewerker die niet weet wie hij is? Hij probeert het in ieder geval, maar op de helppagina moet hij weer een account aanmaken en dat lukt niet.

11 september 2012. Hans Schröder is bijna zeventien jaar en druk bezig met zijn eindexamen als hij een brief ontvangt van de politie. Hij wordt uitgenodigd voor verhoor en moet 24 september verschijnen op bureau IJ-tunnel Amsterdam. Hij schrikt zich rot, staat helemaal te trillen en loopt meteen naar zijn computer om te googlen op computervredebreuk. Dan herinnert hij zich Brenno de Winter. Hij volgt de journalist op Twitter omdat hij zijn artikelen interessant vindt. @jmschroder stuurt diezelfde dag @brenno een DM en de twee beginnen druk te chatten. Schröder: “Brenno wist meteen waar ik het over had. Hij was heel behulpzaam en wist me goed gerust te stellen.” De Winter helpt Schröder ook aan een advocaat: Steven Kroesbergen.

Deze advocaat wil hem kosteloos bijstaan in deze zaak en gaat op 27 november ook mee naar het verhoor. Moeder Schröder is er ook bij. Op het bureau blijkt de politie wel begrip te hebben voor de situatie van de jongeman. “Ik werd op mijn gemak gesteld door de politie. Ze hadden goede vragen. Ik had het gevoel dat ze aan mijn kant stonden, maar misschien gaat dat altijd bij een verhoor.” Kroesbergen neemt ook contact op met Habbo en krijgt een reactie via de mail: “Hans kennen we en wij willen niet dat hij vervolgd wordt (…) richt je op andere verdachte.”

Het blijkt ook dat de advocaat-generaal van het Openbaar Ministerie Schröder eigenlijk ook niet had willen vervolgen en de zaak al eerder had geseponeerd. De persoon achter de aangifte, Vincent Beerends, countrymanager bij Sulake, had echter een beklag ingediend volgens artikel 12 van het Wetboek van Strafvordering. Dat is een verzoek aan het OM haar beslissing te herzien en alsnog tot vervolging over te gaan. Daarom moest Schröder toch op verhoor komen en komt er alsnog een rechtszaak.

6 maart 2013 verschijnt Schröder met zijn advocaat Kroesbergen aan het gerechtshof in Amsterdam. De jongen is best onder de indruk van al de mensen in gewaad, maar zijn ontzag verdwijnt al snel als hij doorkrijgt dat de rechter vrij weinig weet van internet. Hij moet zelfs uitleggen wat Skype is. Er zou nog een verdachte zijn, maar die is er niet. Ook Beerends van Sulake is er niet, of zoals dat heet in rechtbanktermen: “Klager is, hoewel behoorlijk opgeroepen, niet in raadkamer verschenen.” Kroesbergen vraagt bovendien aan de rechter of Beerends als marketingmanager van de virtuele wereld eigenlijk wel gemachtigd is namens Habbo een zaak aan te spannen. De rechter vraagt daarom de griffier om Beerends maar even bellen.

Diezelfde dag verschijnt een artikel in Adformatie: “Het Nederlandse kantoor van de sociale netwerk- en spelsite Habbo zal worden opgeheven. Dat bevestigt Vincent Beerends, country manager bij Habbo Netherlands: ‘De Nederlandse website en community zal gewoon voor Nederlandse spelers beschikbaar blijven, maar alle werkzaamheden van het Nederlandse team zullen door het Finse hoofdkantoor worden overgenomen.’ De voormalige joint venture tussen Telegraaf Media Groep en het

Finse moederbedrijf Sulake komt hiermee dan ook tot een einde.” Als de griffier die dag Beerends aan de telefoon krijgt, vertelt hij dat hij als countrymanager van Sulake weliswaar bevoegd was Habbo te vertegenwoordigen, maar nu niet meer want het Nederlandse kantoor is opgeheven en hij is dus zijn baan kwijt. De rechtbank besluit dat de klager ophoudt te bestaan en Schröder daarmee wordt ontslagen van verdere rechtsvervolging.

Pas als alles voorbij is, gaat De Winter over tot de onthulling in de media. Hij wilde namelijk de zaak niet beïnvloeden met zijn berichtgeving. Op 14 juni 2013 kopt hij op NU.nl ‘Online game sleepte minderjarige voor rechter om tonen lek’. Hierin beschrijft hij hoe Schröder de helpdesk hackte en de gang naar de rechter. Advocaat Kroesbergen noemt de zaak bizar en vindt het gedrag van Habbo “kwalijk en laakbaar”. De Winter heeft Sulake zelf ook om een reactie gevraagd. Een woordvoerster die verder niet bij naam wordt genoemd zegt: “We hadden reden er belang aan te hechten dat de zaak grondig werd onderzocht”, want “de veiligheid van de gebruikers is enorm belangrijk voor ons en we zijn gedreven een leuke en veilig community te bieden. Mocht die ooit in gevaar komen dan zullen we altijd in het belang van de gebruikers handelen.”

Als ik dit stukje later teruglees op NU.nl, lijkt het me een interessante zaak voor mijn onderzoek. Want hoe kan het toch dat iemand met ogenschijnlijk goede bedoelingen zo hard wordt aangepakt? En dan ook nog zo jong. Bovendien staat de hacker er met voor- en achternaam in, dus is hij te traceren. We spreken af op Skype. Het eerste wat ik zie is dat Schröder omringd is door computerschermen. “Ha, een echte hacker!”, roep ik enthousiast. “Nee, ik ben geen echte hacker hoor”, corrigeert hij me, “die schermen zijn om te gamen. Geen Habbo, maar vooral Battlefield 4. Met drie kun je beter om je heen kijken.” OK, hij is dan inmiddels ook al achttien jaar.

Schröder doet dan Business & IT-Management aan het HBO en vertelt met enige distantie over zijn Habbohack, zoals ik die hierboven beschrijf. Over de uitkomst vertelt hij dat hij enorm opgelucht was toen hij de uitspraak hoorde. Hij kon toen eindelijk zijn examen afmaken, zonder de continue stress van een

mogelijke boete of taakstraf die boven zijn hoofd hing. Hij vindt het nog steeds jammer dat hij nooit excuses heeft gekregen van Sulake: “Ik had het idee dat ik als voorbeeld werd gebruikt, zodat anderen dat niet doen. Wat ik vond was vrij ernstig, maar de manier waarop is iets wat een negenjarige kan.”

Voor dit onderzoek is het echter wel jammer dat het niet tot een treffen in gekomen in de rechtszaal. De advocaat van Habbo had dan moeten bewijzen dat Schröders hack geen hoger doel diende en waarom zijn onthulling onverantwoord zou zijn geweest. Dat zou interessante jurisprudentie zijn geweest voor toekomstige zaken. Schröder zou naar mijn inschatting ook niet meer vervolgd worden omdat Habbo zelf had gevraagd de data te downloaden. Of dat ook werkelijk zou zijn gebeurd, blijft nu gissen.

Schröder heeft nog wel zijn e-mailcorrespondentie met de Habbomedewerkers en stuurt me die toe, samen met een kopie van de beschikking van de rechter. Daar kan ik mee aan de slag. Habbo Nederland is dan wel opgeheven, maar met de namen van de betrokkenen en LinkedIn kom ik toch bij de juiste personen terecht. De ex-Habbohelpdeskmedewerkster Beau bevestigt Schröders verhaal over de Excelsheet en IP-adres en vertelt dat de beslissing tot aangifte kwam van hogere hand: “Uiteindelijk is alles via HQ gegaan (Sulake, Helsinki), zo ook vrijwel alle beslissingen die zijn genomen. Omdat wij voor Team NL werkten en het moesten oppakken, staan onze namen vermeld onder de meeste files. Het contact tussen Hans en ons is niet zwart/wit te omschrijven, het was natuurlijk een heftige situatie dus er zit een enorm grijs vlak tussen. Vooral op ethisch gebied voor, denk ik, alle betrokken partijen. We moesten uitpluizen wat er gaande was, hoe het heeft kunnen gebeuren en wat er precies zichtbaar was.”

Degene die het leidde was dus de country manager Vincent Beerends. Als ik hem vindt en vervolgens vraag naar een reactie is hij eerst afwijzend: “Ik heb geen interesse om hieraan mee te werken. Succes met je boek in ieder geval!” Maar, als ik hem de reactie van de helpdeskmedewerkster voorleg, schrijft hij: “Ik wil je wel meegeven dat dat besluit zowel van mij als van hogerhand is gekomen. We hebben nogal wat te stellen gehad met dhr.

Schröder destijds. Nu weet ik dat hij een andere versie heeft van het verhaal en doet voorkomen alsof hij een lek in ons systeem ontdekte. Dat er een lek was, onderschrijf ik, maar daar heeft dhr. Schröder meerdere keren daarvoor misbruik van gemaakt. Bewijzen van door hem verspreide persoonlijke informatie van spelers op diverse hacking websites liggen daar aan ten grondslag."

Zou de jonge ethisch hacker dan toch te ver zijn gegaan? Als ik Schröder deze reactie toestuur, schrijft hij terug: "Ik heb het eerste mogelijke contactmoment direct benut dus dat ik meerdere keren daarvoor er misbruik van zou hebben gemaakt, is onzin. Daarnaast heb ik nooit gegevens publiekelijk gemaakt, hooguit zoals dhr. Beerends aangeeft 'verspreid' maar dan onder het mom van het falen van Habbo aantonen en het niet dichten van het lek waardoor het een maand later door een ander op serieuze manier is misbruikt." Hij stuurt me wat linkjes van hackersfora waar inderdaad 15.000 gebruikersnamen en wachtwoorden staan. Die zijn er na zijn vondst opgezet door een onbekende, die ze waarschijnlijk ook weer van iemand anders had. In ieder geval niet van hem.

Wie heeft dan het Habbolek misbruikt? In de beschikking van de rechter zie ik de naam van de tweede verdachte. Schröder wil liever niet teveel over hem vertellen, maar ook met die naam kom ik uit bij een persoon, die qua profiel de juiste lijkt te zijn. Als ik verder zoek kan ik de naam verbinden aan een rekeningnummer en de naam van een onlinehandeltje in computertablets. Dit staat echter op een klachtensite, waar mensen kunnen melden dat ze opgelicht zijn door dit bedrijf. Is dit dezelfde verdachte? Zou kunnen, maar het zou ook weer een persoonsverwisseling kunnen zijn. Ik besluit het maar hierbij te laten. Je kunt natuurlijk niet zelf voor rechter gaan spelen.

In die tijd speelt er nog een zaak, die wel wordt uitgevochten aan de rechtbank, met een helder rechterlijk oordeel over wat wel en niet is toegestaan bij ethisch hacken. Henk Krol komt, net als Hans Schröder, bijna per toeval in een systeem waar hij niet in zou mogen. Dat hij dit via de media onthult en zelfs bijzonder gevoelige persoonsgegevens heeft ingezien, is volgens de rechter nog te begrijpen omdat hij een misstand wilde aantonen. Maar dat

Krol meerdere keren inlogde en dat ook nog in bijzijn van journalisten, ging te ver en hij krijgt daarvoor een boete.

13. Hacker Krol haalt net iets teveel uit de kast

Dossiers bij Diagnostiek voor U blijken beveiligd met slechts vijf cijfers

16 april 2012. Een lid van de politieke partij 50PLUS is bij GGZ Eindhoven op bezoek bij zijn psychiater. Daar verneemt hij hoe de arts inlogt bij het Cyberlab van Diagnostiek voor U. Hoe, daar verschillen de meningen over. De een zegt dat hij het wachtwoord van de arts hoorde toen die aan de telefoon zat, een ander zegt dat de arts zijn code zelf aan de patiënt gaf en een derde beweert dat de code met een post-it naast de monitor was geplakt. Hoe dan ook, de psychiater was slordig met zijn vijfcijferige code die hij gebruikte als inlognaam en wachtwoord. En dat voor zo'n site. Hiermee kun je namelijk de resultaten van bloed- en urineonderzoeken raadplegen.

Twee dagen later zit het 50PLUS-lid achter zijn eigen computer en probeert de code uit. Inderdaad, hij kan erin en ziet tot zijn schrik allerlei medische dossiers. Hij belt daarom direct met partijlid en journalist Henk Krol. De volgende dag zitten ze samen achter de computer in Best, waar de redactie van de Gaykrant zit. Krol krijgt ook toegang tot de site en zoekt op zijn eigen naam. Hij staat er zelf niet in, maar ziet wel dossiers van anderen, waaronder ook bekenden. Hij probeert nog wat namen en ziet onder andere uitslagen van drugs-en soa-testen. Als bewijs print hij een aantal dossiers uit en streept de namen door.

Krol belt Diagnostiek voor U en vraagt naar de leidinggevende. De telefoniste zegt dat hij zijn melding schriftelijk moet indienen. Hij voelt zich niet erg serieus genomen en belt daarom een bevriende journalist bij Omroep Brabant voor advies. Die stuurt meteen een cameraploeg. De twee 50PLUS'ers loggen in aanwezigheid van de cameraploeg in bij Cyberlab. Krol bladert weer door de dossiers. De oorspronkelijke vinder van het lek wil niet in beeld, maar print wel negen pagina's aan dossiers uit. Terwijl de journalisten opnames maken van het scherm, gaat

ineens de site uit de lucht. Blijkbaar zijn ze gesnapt. Of is de melding dan toch doorgekomen?

Omroep Brabant zendt het item uit op 19 april. We zien Krol aan een bureau zitten achter een computer. De voice-over zegt: “De medische gegevens van duizenden patiënten hebben wij zojuist ingekeken, terwijl wij allebei geen medicus zijn. Jij kwam met een inlogcode en een wachtwoord, hoe ben je eraan gekomen?” Intussen zien we een computerscherm, waarop allerlei variaties van Jansen voorbij komen. Als Krol vertelt hoe “kinderlijk eenvoudig” het is om in te loggen, zien we het inlogscherm van het Cyberlab, waar iemand 12345 intikt. Krol: “Iedereen die op deze site rondspeelt en vijf cijfertjes intikt…” Zo makkelijk dus.

Krol vertelt dat hun leden - spreekt hij hier als provinciaal Statenlid en het gaat over Brabantse patiënten, of bedoelt hij de leden van de Gaykrant? - zich zorgen maken dat iedereen zo bij hun gegevens kan. Bijvoorbeeld verzekeringsmaatschappijen. Dan doorloopt hij de prints met uitslagen: “Je ziet dat mensen veel te veel drinken, drugs gebruiken, dat mensen bepaalde medicijnen gebruiken, dat mensen al dan niet seropositief zijn (…) Gewoon alles wat uit het bloed is af te leiden, is voor heel veel mensen oproepbaar.” De verslaggever roept enthousiast: “Gegevens die te misbruiken zijn?!” “Absoluut”, antwoordt Krol. “Je zou mensen kunnen chanteren. Als werkgever kun je kijken: wat voor risico’s haal ik in huis?” Hij heeft daarom meteen met de provincie gebeld, maar die stelde dat ze daar niet over gaan. Het Ministerie van Volksgezondheid zou er daarom iets aan moeten doen. Krol besluit plechtig met verheven stem: “Dit mag nooit meer zo voorkomen. Het kán niet zo zijn, dat buitenstaanders met slechts het intikken van vijf cijfertjes zo gemakkelijk bij zulke privégegevens kunnen komen. Dat hád niet mogen gebeuren, dat mág niet meer gebeuren en er moet alles aan gedaan worden dat het niet meer kán gebeuren.”

Omroep Brabant bericht die dag ook op hun site over de zaak. De redactie krijgt uiteindelijk wel de leiding van Diagnostiek voor U te spreken. Directrice Astrid van der Put vertelt geschokt te zijn en dat ze de site direct uit de lucht hebben gehaald. De dag erna doet ze aangifte bij de politie, want: “Zoals het er nu naar uitziet, is

er sprake van computercriminaliteit. Twee mensen van partij 50PLUS hebben zich toegang verschaft tot het systeem door de bestaande inlognaam en wachtwoord van een arts, die toegang had tot de gegevens van zijn patiënten, te misbruiken.” De omroep kopt die dag: ‘Diagnostiek voor U wijst vooral naar anderen na lekke website’.

In de berichtgeving komt ook Brenno de Winter aan het woord. Volgens hem overtreedt Diagnostiek voor U de Wet Bescherming Persoonsgegevens. Het gaat immers om “bijzondere gegevens” en dan mag je volgens die wet een hoger beveiligingsniveau verwachten “conform de stand der techniek”. Oftewel vandaag de dag voldoen alleen inlognaam en wachtwoord niet meer, maar zou je voor zoiets moeten inloggen met bijvoorbeeld nog een pasje of sms-code erbij. Dit inloggen met meerdere middelen is de zogenaamde meerfactor authenticatie.

Het College Bescherming Persoonsgegevens laat in deze berichtgeving ook van zich horen en noemt het “een ernstige zaak”. Het college kan er echter op dit moment niet zoveel aan doen en is dan ook groot voorstander van een meldplicht, waarvoor op dat moment een wetsvoorstel in de maak is. Dan zal de verantwoordelijke het datalek meteen zelf moeten melden en de slachtoffers inlichten. Zo niet, dan mag het CBP een boete uitdelen, tot wel 200.000 euro. Omroep Brabant refereert hier aan het voorstel voor een meldplicht datalekken, dat we al eerder tegenkwamen in de vorige Kamerdebatten als mogelijk nieuw handhavingsinstrument bij helpende hackers.

Zo ook op 20 april, de dag na de uitzending en tien dagen nadat Opstelten in de Kamer een richtlijn heeft toegezegd. Dit keer wordt de meldplicht onder de aandacht gebracht door PvdA-Kamerlid Attje Kuiken. Ze komt zelf ook uit Brabant en kaart de zaak Diagnostiek voor U aan als treffend voorbeeld van datalekken die gemeld moeten worden. “Het wordt tijd dat het College Bescherming Persoonsgegevens behalve alleen blaffen ook eens kan bijten”, stelt ze. Het voorstel krijgt ook steun van GroenLinks en CDA, waarmee een Kamermeerderheid is voor een meldplicht datalekken.

Tot een wetsvoorstel komt het echter niet. De dag erna kondigt Rutte namelijk aan dat, na zeven weken onderhandelen in het

Catshuis over de begroting voor 2013, het niet was gelukt tot overeenstemming te komen met gedoogpartner Wilders. Het Kabinet valt. Wetsvoorstellen kunnen dan alleen bij hoge uitzondering uitgevoerd worden en de Kamerdebatten gaan dan vooral over een datum voor de verkiezingen. Die zijn 12 september en de partij 50PLUS doet ook mee als landelijke partij, met een nieuwe lijstrekker: Henk Krol. De flamboyante ex-hoofdredacteur van de Gaykrant doet het goed in de media met zijn ferme uitspraken over het lot van de ouderen en komt uiteindelijk als tweemansfractie in de Kamer. De hack verdwijnt dan voor Krol naar de achtergrond, maar niet voor Diagnostiek voor U en justitie.

Het Cyberlab is 2 mei 2012 weer online. De politie is dan ook gestart met onderzoek naar aanleiding van de aangifte van DVU. Het Openbaar Ministerie verhoort de betrokkenen, onder wie ook de psychiater van wie de vijf cijfers afkomstig waren. Dit is pikant, want informatie over patiënten, ook al zijn ze verdachten, valt eigenlijk onder het medisch beroepsgeheim. De Winter weet over dit onderzoek enkele interessante details te melden. De arts zou de gegevens zo hebben gegeven, ook al was er geen vordering. Nog pikanter is dat tijdens het onderzoek blijkt dat medewerkers van justitie al toegang zouden hebben tot Cyberlab. De server waar deze applicatie op draaide, hield geen logboeken bij, dus moest in de applicatie zelf gekeken worden wie wanneer had ingelogd. Daar zouden deze justitiemedewerkers dus kunnen zien wie als behandelaar van wie welke dossiers beheert. Ook dat is medische informatie, verkregen zonder vordering.

Het OM besluit dat Krol voor de rechter moet verschijnen vanwege computervredebreuk. Als hij dit op 4 december verneemt in een brief aan hem, meldt hij dit direct aan Omroep Brabant, die het die dag naar buiten brengt. In de media neemt De Winter het voor hem op: “Ik vind dat mensen die deze zaken aan de kaak stellen zich veilig moeten voelen.” Maar bovenal: “Het lijkt wel alsof justitie zaken aanspant om te voorkomen dat misstanden worden aangetoond. Ik snap het niet goed. Het lijkt alsof slecht nieuws niet gehoord mag worden.” De psychiater, het medisch centrum, de applicatiebeheerders en justitiemedewerkers

gingen allemaal onzorgvuldig om met de medische informatie, terwijl Krol wordt vervolgd. “Ik vind de misstand belangrijker dan de daad”, aldus de journalist.

De Winter laat het er niet bij en doet namens NU.nl een rondje langs de net geïnstalleerde Kamerleden. Hij legt hen de vraag voor of de Inspectie voor de Gezondheidszorg de beveiliging van patiëntengegevens beter in de gaten moet houden. De woordvoerders van D66, CDA, PvdA, SP en natuurlijk 50PLUS zijn het met hem eens. Volgens CDA-Kamerlid Hanke Bruins Slot kan de Inspectie voor de Gezondheidszorg “niet zomaar achterover leunen. Op zijn minst verwacht ik dat de IGZ nagaat of de gegevens nu wel voldoende beveiligd zijn”. Astrid Oosenbrug van PvdA is ook nieuw en als ex-systeembeheerder een van de weinige Kamerleden met ICT-ervaring. Ze vindt dat het lek aantoont dat “het algemeen besef rond het belang van goede beveiliging er nog niet is”. De regering zou hebben toegezegd nog dit jaar met kaders rond beveiliging van medische gegevens te komen. Ze wijst naar het Nationaal Cyber Security Centrum, dat de zaak goed in de gaten zou moeten houden. De Winter kopt op 16 december: ‘Kamer wil controle IGZ op beveiliging medische dossiers’.

De dagvaarding volgt 8 januari 2013 en de zitting is op 1 februari. EenVandaag maakt er alvast een item van en opent op 31 januari: “Henk Krol weet niks van computers, maar wordt nu vervolgd voor computervredebreuk”. Krol vertelt beteuterd dat hij bij veroordeling zijn Kamerlidmaatschap en Koninklijke onderscheiding zal kwijtraken. In de beelden die volgen, wordt eerst het item van Omroep Brabant nog eens dunnetjes overgedaan. We zien weer de beelden van de site, afgewisseld met een verongelijkte Krol vanachter de geprinte laboratoriumuitslagen, met commentaar van De Winter.

De EenVandaag voice-over meldt vrolijk dat, nu Krol zich voor de strafrechter moet verantwoorden, hij een graag geziene gast is op hackersbijeenkomsten. Vervolgens zien we de 50PLUS’er vanaf een podium een zaal toespreken: “Ik heb zelf geen enkel nut bij wat je noemt een computerinbraak. Ik heb ook niet dagen achter het scherm gezeten om op een sneaky manier ergens

binnen te komen. Nee, ik heb willen aantonen dat de gegevens van heel veel mensen in gevaar waren. Dankjewel.” Als hij na een bescheiden applausje een doos hackersbier krijgt, wil hij nog wel even kwijt: “Vroeger zeiden ze in de buurt, daar heb je die van die ouwelullenpartij. Maar nu kan ik trots door de straat als hacker!”

Even checken via de mail wat enkele bekenden in de zaal ervan vonden. Arda Gerkens, dagvoorzitter en namens HCC medeorganisator van het congres kan er nog steeds wel om lachen: “Henk was redelijk hilarisch omdat hij natuurlijk een echte digibeet is.” Oscar Koeroo (die van ‘Veere’) is kritischer en schrijft: “Mijn mening is dat hij zijn verdiende straf heeft gehad, omdat hij te ver is gegaan. Hij heeft meer dan nodig het lek aangetoond, gedemonstreerd aan diverse mensen en medische informatie ingezien die hij eigenhandig heeft weggestreept. Dit is geen lek verantwoord aantonen, maar de sensatie zoeken.” Hij vond het daarom ook jammer dat Krol tijdens de conferentie zijn verhaal deed en meteen weer wegging. Er was geen ruimte voor vragen of discussie.

Het betreft hier Alt-S, een IT-securitycongres van 22 januari. Op de site, door @legosteentje gemaakt, staat te lezen dat het als doel heeft “de kloof tussen bedrijfsleven en hackers te overbruggen”. Maar eigenlijk is het meer een soort schaduwconferentie. Het NCSC heeft namelijk die dag hun eigen securityconferentie, met prominent op de agenda hun nieuwe leidraad voor responsible disclosure. Het aantal aanmeldingen is echter zo groot, dat het centrum er veel heeft moeten weigeren. Daar is vervolgens druk over getwitterd door hackers die de afwijzing opvatten als uitsluiting en vervolgens zelf een congres zijn gaan organiseren. Het NCSC heeft nog geprobeerd ze te lokken met een grotere locatie, maar dan is ALT-S al een feit.

Een van de eersten die zich aanmeldt bij Alt-S is @meneer, oftewel zelfstandig beveiligingsexpert Andre Koot. Hij spreekt direct na Krol en is daar omdat hij pleit voor ‘trusted dislosure’. Er zou een onafhankelijk meldpunt moeten komen waar je ook anoniem meldingen kunt doen van beveiligingsproblemen. Experts nemen het dan over, zonder tussenkomst van rechtsgang en journalistiek. Hier is het uiteindelijk niet meer van gekomen, maar het was wel een mooi initiatief. Over de zaak Krol versus

Diagnostiek voor U vertelt hij mij later: “Dit kan ik met de beste wil van de wereld geen hacken noemen. Door een open deur naar binnenlopen, is ook geen inbreken. Ik denk dat Krol terecht verontwaardigd was en geen idee had hoe hij dit naar buiten kon brengen dan door het zelf maar te laten zien. Het te lage niveau van beveiliging had hij misschien alleen bij het CBP kunnen melden, maar of hij dat kon doen is maar zeer de vraag. Het CBP heeft niet echt een toegankelijk loket.”

Koot maakt zich echter niet zo druk over Krol, maar vooral dat Diagnostiek voor U ermee wegkwam zulke hoogst vertrouwelijke gegevens onvoldoende te beveiligen. Hij begint daarom zelf een actie en vraagt diverse mensen om mee te doen. Op 30 januari 2013 krijg ik van hem deze mail:

“Beste Chris,
Ik heb een handhavingsverzoek ingediend bij het CBP naar aanleiding van de Henk Krol-casus. Ik vind de manier waarop het OM en de Raad van Bestuur om de materie heen draaien niet past, er is alleen aandacht voor de melder van het lek. Dat ging niet goed, maar het probleem is groter. Ik kreeg van Brenno een sjabloon van een verzoek, dat gaat morgen de deur uit.”

Koot vraagt mij om mee te doen. Hij verwacht niet dat we ontvankelijk verklaard worden omdat we geen belanghebbende zijn, maar wellicht helpt het wel om een onderzoek te laten starten. In de bijlage tref ik een brief die is gericht aan Jacob Kohnstam, de voorzitter van het CBP. Na een uiteenzetting van alle gebeurtenissen rondom Diagnostiek voor U wijst Koot de voorzitter op een van hun eigen bepalingen:

“Er wordt naar mijn mening niet voldaan aan artikel 13 Wbp, waarin wordt gesteld dat de beveiliging is voorzien van “passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking”. Daarbij moet rekening worden gehouden met de stand der techniek. Daarvan is geen sprake als: bij bijzondere persoonsgegevens eenvoudig te achterhalen authenticatie wordt gebruikt; bij bijzondere persoonsgegevens gebruik wordt gemaakt van zogenaamde éénfactor authenticatie; er onvoldoende waarborgen zijn dat

onbevoegden in het dossier van niet eigen patiënten wordt gekeken."

Volgens Koot moet het college daarom handhavend optreden. Zelf voel ik er eerlijk gezegd niet zoveel voor om ook zo'n brief te sturen. Want waarom zou ik me hiermee moeten bemoeien? Maar omdat ik dan net met dit onderzoek ben begonnen, lijkt het me wel interessant om te kijken of ik een reactie kan krijgen. In die zin ben ik dus wel een soort belanghebbende, ook al is het puur eigenbelang. Ik schrijf:

"Geachte heer Kohnstam,
Als het goed is, heeft u al meerdere verzoeken tot handhaving gekregen in de zaak Henk Krol vs Diagnostiek voor U. Daar wil ik deze aan toevoegen. Ik ben niet direct betrokkene in die zin dat het gaat om mijn persoonsgegevens. Wel ben ik betrokken bij deze zaak als onderzoeker. Ik ben namelijk bezig met een boek over responsible disclosure, waarin ik ook aandacht besteed aan deze zaak. Volgens diverse media bent u een onderzoek gestart, maar ontloopt de zorginstelling haar boete als ze binnen een bepaalde termijn orde op zaken heeft gesteld. Dat is vreemd, want er zijn immers al persoonsgegevens gelekt. Deze zaak wordt wel op een presenteerblaadje aangereikt. Het zou mooi zijn als het CBP dit aangrijpt om zorginstellingen op hun verantwoordelijkheden te wijzen."

Om het allemaal wat officiëler te doen lijken print ik de brief uit, onderteken ik hem en doe ik hem op de brievenbus. Uiteindelijk heb ik er niets meer van gehoord. Dat had ik eerlijk gezegd ook niet verwacht, want ik heb eigenlijk niets met de zaak te maken, maar het was wel het proberen waard. Nog zes anderen sturen dan naar aanleiding van Koots vraag een brief, met meer nobele intenties dan ik, dus wellicht hebben zij wel een reactie gekregen. Koot zelf in ieder geval wel, ook al was het pas na enige maanden. Het CBP heeft zijn verzoek inderdaad niet in behandeling kunnen nemen omdat hij geen klant of andere relatie is van Diagnostiek voor U. Het college zegt er wel onderzoek naar te gaan doen. De actie van Koot verschijnt ook in de media. Op 3 februari kopt De Winter op NU.nl: 'Beveiligingsexperts eisen CBP-onderzoek gehackte kliniek', met eronder citaten uit onze brieven.

Aldus: vele experts met meningen in de media, diverse Kamervragen, twee cyber security bijeenkomsten met de zaak op de agenda, een Inspectie voor de Gezondheidszorg die tot de orde wordt geroepen en een handhavingsverzoek naar het CBP... Dit is slechts een greep uit de context waarin de rechtszaak plaatsvindt. Daar komt voor Krol zelf bij dat er niet alleen een strafrechtelijke procedure tegen hem loopt, maar Diagnostiek voor U ook een civielrechtelijke procedure start om de schade op hem te verhalen.

De advocaat van DvU, Henk van Dijk vertelt tegen journalist René Schoemaker van Webwereld dat het gaat om 85.329 euro aan materiële schade. In dit bedrag zit een audit van 23.500 euro die is uitgevoerd door een extern bedrijf en een schade van 10.500 Euro bij de GGZ Eindhoven, waar de vijfcijferige psychiater werkt. De rest bestaat uit de uren die de medewerkers van Diagnostiek voor U hebben gemaakt aan “externe communicatie en het oplossen van het beveiligingsprobleem”. Daarnaast zullen veertien personen van wie Krol hun dossier zou hebben ingekeken, elk afzonderlijk ook een schadeclaim indienen. De Winter gaat achter hen aan en krijgt te horen dat het voor deze patiënten niet duidelijk was waar ze hun handtekening onder hadden gezet. Een van de eisers dacht zelfs dat het ging om de verlenging van een behandeling. Een andere had zijn claim voor de zitting ingetrokken, omdat hij onder druk zou zijn gezet door GGZ Eindhoven.

De zitting is 1 februari en op 15 februari 2013 komt de rechtbank Brabant Oost met het vonnis. De hele procesgang, met details over hetgeen de betrokken hebben gedaan, is weer netjes gedocumenteerd in een rechtbankverslag. Daarin is uitgebreid te lezen hoe de officier van justitie haar aanklacht onderbouwt en welke argumenten de verdediging er tegenover stelt. Wat de twee 50PLUS’ers destijds hebben gedaan weten we nu wel. Voor het doel van dit boek is het vooral interessant om te lezen hoe een standaardformulering uit het Wetboek van Strafrecht wordt vertaald naar een omslachtige beschrijving van hacken:

“Aan verdachte is ten laste gelegd dat hij op een of meer tijdstippen op of omstreeks 19 april 2012 te Best en/of Eindhoven, althans in Nederland, (telkens) tezamen en in vereniging met een

ander of anderen en/of alleen, (telkens) opzettelijk en wederrechtelijk in een of meer geautomatiseerde werken, te weten de webserver van [site], of in een deel daarvan, is binnengedrongen, waarbij de toegang is verworven met behulp van een valse sleutel en/of door het aannemen van een valse hoedanigheid, immers heeft/hebben hij, verdachte, en/of zijn mededader(s) meermalen, althans eenmaal, ingelogd op die webserver, met gebruikmaking van inloggegevens en wachtwoord, tot welk gebruik hij en/of zijn mededader(s) niet gerechtigd is/zijn en/of (vervolgens) (medische) dossiers/gegevens bekeken, waarna verdachte vervolgens meermalen, althans eenmaal, gegevens, die waren opgeslagen, werden verwerkt of werden overgedragen door middel van dat/die geautomatiseerd(e) werk(en) waarin verdachte zich wederrechtelijk bevond, voor zichzelf of een ander heeft overgenomen, afgetapt of opgenomen, immers heeft hij, verdachte, meermalen, althans eenmaal, deze (medische) dossiers/gegevens gekopieerd/(uit)geprint."

Het gaat hier dus om computervredebreuk, oftewel artikel 138ab lid 1 en 2 van het Wetboek van Strafrecht. De vraag is of deze onrechtmatige daad geoorloofd is omdat het een hoger maatschappelijk belang dient, in dit geval de privacy van de Brabantse patiënten en de schending daarvan tegen te gaan door het naar buiten brengen van het lek. Dan valt het onder de vrijheid van meningsuiting. Het is wellicht ook daarom dat de officier van justitie juist begint die redenering om te keren en is volgens hem Krol de privacyschender:

"Het recht op privacy van derden was in het geding. Het ging om gevoelige, medische gegevens van derden, die zonder hun goedvinden, zelfs buiten hun medeweten, zijn geraadpleegd. De maatschappelijke relevantie van het aan de kaak stellen van de misstand was veel beperkter dan de verdachte doet voorkomen. Het zogenaamde 'gat' in de beveiliging zat niet zozeer in de technische opbouw van de website, maar in het feit dat door een gebruiker op onzorgvuldige wijze is omgegaan met inloggegevens. Het door de verdachte opgevoerde doel van zijn handelen had ook op een minder vergaande manier bereikt kunnen worden. Verdachte en medeverdachte hadden zich

kunnen beperken tot het inloggen in het systeem, zonder verder specifieke dossiers met daarin voornoemde gevoelige gegevens te bevragen. Ze hadden zich in ieder geval kunnen en moeten beperken tot het openen van het dossier van medeverdachte. Zowel voor het geval dat verdachte van mening is dat hij heeft gehandeld als ethisch hacker, als voor het geval hij heeft gehandeld als journalist, heeft hij een zorgvuldige en noodzakelijke stap overgeslagen. Hij heeft gegevensbeheerder niet op een afdoende wijze op de hoogte gesteld voordat hij het hele verhaal naar buiten heeft gebracht. Een telefoontje met een telefoniste was in dat licht niet voldoende."

Volgens de officier van justitie wegen in dit geval "het recht op de bescherming van de integriteit van het geautomatiseerde systeem" en "het recht op privacy van de betrokken derden" zwaarder dan "het recht op de vrijheid van meningsuiting en nieuwsgaring van de verdachten". Artikel 10 van het EVRM staat een strafvervolging, noch een strafoplegging van verdachte in de weg.

De advocaat van Krol keert de redenering weer om: het zijn niet de verdachten, maar de andere betrokkenen die de privacy van de patiënten in gevaar brengen. Ten eerste Diagnostiek voor U, omdat er geen regels werden gesteld aan wachtwoorden. Daardoor was het te makkelijk voor de verdachten om in te loggen vanaf hun eigen computer. Bovendien: "Het systeem hield niet bij vanaf welk IP-adres werd ingelogd. Het hield alleen bij welke dossiers werden geraadpleegd." Krol bracht zijn bevindingen vervolgens zelf naar buiten omdat hij "op dat moment lid van de schrijvende pers en Statenlid was". Hij had bewijs nodig en deed dat door enkele dossiers te printen en te anonimiseren. Ook justitie zelf treft blaam volgens de advocaat, wegen het schenden van het medisch beroepsgeheim: "De identificeerbare gegevens van een patiënt waren voor iedereen met de inloggegevens toegankelijk. Zelfs ook voor justitie, zegt de aangever."

Nu de rechter. Dat er computervredebreuk is gepleegd, daar is iedereen het dus wel over eens. Dat de mede 50PLUS'er zich ervan wilde distantiëren toen Omroep Brabant erbij kwam, doet daar volgens hem niets aan af. Beiden zijn schuldig. Maar, is hier sprake van zeer bijzondere omstandigheden en hogere belangen

die een dergelijke inbreuk rechtvaardigen? Volgens hem zijn hierbij drie factoren van belang. Eerst moet worden beoordeeld of verdachten hebben gehandeld in het kader van een wezenlijk maatschappelijk belang. Zo ja, hebben zij gehandeld volgens de regels van proportionaliteit en subsidiariteit, oftewel gingen ze niet verder dan noodzakelijk om hun doel te bereiken en was er geen andere, minder vergaande, manier om dat te kunnen bereiken?

In het eerste punt kan de rechter volledig meegaan: het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens is zeker een wezenlijk maatschappelijk belang. Dat Krol zelf wilde vaststellen of de bevindingen van de medeverdachte juist waren, vervolgens ging inloggen op de website en enkele dossiers ging raadplegen, begrijpt hij ook. Zo ook de prints als bewijs, want Krol heeft daarbij zorgvuldig gehandeld door ze te anonimiseren. Hiervoor krijgen hij en de medeverdachte dus geen straf.

Maar, en nu komt het, Krol heeft meerdere keren de gegevens geraadpleegd en uitgeprint en dat ook nog in aanwezigheid van de journalisten van Omroep Brabant. Dat is volgens de rechter buitenproportioneel. Bovendien was het “allerminst noodzakelijk om voor de oplossing van het door verdachte gesignaleerde probleem meteen naar de media te stappen”. Hij had namelijk geen concrete aanwijzingen dat andere personen over deze inloggegevens beschikten. Het probleem was namelijk niet veroorzaakt door een technisch gebrek aan het computersysteem, maar door een gebruiker die onzorgvuldig met zijn inloggegevens was omgegaan. De onthulling had daarom ook anders en zonder de media gekund, oftewel op subsidiaire wijze. Krol is immers Statenlid en verslaggever, dus mag verwacht worden dat hij in staat is zonder al te veel moeite de juiste persoon binnen de organisatie te benaderen. Krol bedoelde het goed, maar heeft gewoon teveel uit de kast gehaald. Hij krijgt hiervoor een geldboete van 750 euro.

Tot slot de schadevergoeding. Dat is het civielrechtelijk deel van het proces, maar om hiervoor alvast in het strafrechtelijk proces een eerste stap te zetten, heeft de advocaat van Diagnostiek voor U een symbolisch bedrag gevraagd: 1000 euro. De patiënten, waarvan er inmiddels nog negen over zijn ook: 100

euro per persoon. De rechter vindt het echter moeilijk vast te stellen wat de geleden immateriële schade dan is. Verder onderzoek hiernaar vindt hij bovendien “een onevenredige belasting op de strafzaak”. Hij stelt de schade daarom op nihil, oftewel geen vergoeding.

Krol komt er gezien de straf die hem boven het hoofd hing nog redelijk vanaf. Hij moet 750 euro en de proceskosten betalen en niet de schadevergoeding van 85.329 euro. Bovendien blijkt eens te meer dat rechters gevoelig zijn voor ethisch hacken, want het aantonen van de lekke site is in dit geval belangrijker dan de computervredebreuk. Alleen moet je dan niet meer dan nodig uit de kast halen. Hier dus een deeloverwinning voor verantwoord onthullen, die wellicht nog interessante jurisprudentie zal blijken voor toekomstige zaken. Bij het NCSC zien ze deze zaak zelfs als een eerste testcase voor hun leidraad responsible disclosure.

Diagnostiek voor U blijkt later ook de positieve kanten van de zaak in te zien. Directeur Van der Put vertelt 10 april 2013 op NU.nl dat hun beveiliging inderdaad tekort schoot en er nu meer aandacht voor is. “Dat systeem wordt ook door andere instellingen gebruikt. Opeens realiseerden veel partijen dat zij ook kwetsbaar waren (…) Je wilt niet weten hoeveel bestuurders van zorginstellingen naar mij toekwamen met vragen of opmerkingen.” Artsen moeten nu een betere inlognaam bedenken en inloggen met een extra code die ze via sms ontvangen, oftewel de gewenste tweefactor authenticatie. De Winter concludeert op NU.nl: “Hack Henk Krol vergroot bewustzijn zorgsector.”

Dit wordt, anderhalf jaar na dato bevestigd als ik mijn tekst naar Diagnostiek voor U stuur. Yvon van den Berg, manager relatiemanagement, marketing & communicatie schrijft in een reactie: “Deze zaak heeft een bijdrage geleverd ons bewustzijn ten aanzien van informatiebeveiliging te vergroten. Voorziene beveiligingsmaatregelen zijn versneld ingevoerd en hebben een positieve bijdrage geleverd aan onze organisatie.”

Mooi, dan is het allemaal toch nog ergens goed voor geweest. Maar wat in de periode na de rechtszaak toch vooral bleef hangen in de publieke opinie is dat Krol wel is veroordeeld en Diagnostiek voor U niet. Oftewel, ethisch hacken loont niet. Ook diverse

Kamerleden zijn hierover verontwaardigd. Een VVD-Kamerlid zou zelfs met de pet zijn rond gegaan om Krols boete te betalen. Intussen hebben politie, OM, NCSC, IGZ, CBP en de Kamer hun handen vol aan nog een zaak die dan al een tijdje speelt: de hacker van het Groene Hart Ziekenhuis, die nog veel meer uit de kast haalde. Met ook hier weer een hoofdrol voor Brenno de Winter.

14. Het crisisteam rond Verdier

Hacker Groene Hart Ziekenhuis wordt opgepakt

Zondag 7 oktober 2012. Monique Verdier is met een vriendin een weekendje weg in België. Ze zitten net op een terrasje te lunchen als ze wordt gebeld door haar werk. Het is Maarten Baaij, directeur Financiën en ICT van het Groene Hart Ziekenhuis. Er is een ernstig beveiligingslek gevonden en Brenno de Winter gaat er die dag over publiceren. De twee dames stappen meteen in de auto naar Gouda. Terwijl haar vriendin rijdt zit Verdier continu aan de telefoon. Ze is namelijk lid van de Raad van Bestuur van het GHZ en gaat direct een crisisteam samenstellen.

Het ziekenhuis heeft toevallig twee weken daarvoor nog een crisisoefening gedaan, met een zogenaamde aanslag en veel slachtoffers. Een groep studenten speelde de media en bestookte het team met nieuwsberichten. Het was een drama waarbij plannen niet werken omdat de situatie steeds veranderde. De bestuurders ervaren tijdens de training dat in crises de wereld buiten de vergaderkamer sneller gaat dan daarbinnen. Met die ervaring komen de bestuursleden weer bij elkaar in diezelfde vergaderkamer, maar nu voor een echte crisis.

Naast Verdier en Baaij zijn aanwezig: de voorzitter van de Raad van Bestuur Dirk Jan Verbeek, directeur Commerciële Eenheid Robin Alma, Manager Ammie Eleveld en senior adviseur Gelske Nederlof van de afdeling Marketing & Communicatie, Chief Information Security Officer André Beerten, de mannen van de ICT-afdeling en een juridisch medewerker. Een collega die ooit een hack bij een bank van dichtbij had meegemaakt, schuift ook aan. Ze spreken af dat Monique Verdier het team leidt en voorzitter Verbeek het woord voert naar de buitenwereld. Ze willen de problemen in kaart brengen en zo snel mogelijk een duidelijke boodschap naar buiten brengen, maar iedereen buitelt over elkaar heen.

Het belangrijkst is vooral alle feiten op tafel te krijgen over de veiligheidssituatie. Die blijkt niet zo best. Verdier: “Het was vooral een optelsom van veel kleine dingen die niet zo makkelijk op te lossen zijn. Veel wisten we al en daarom hadden we al jaren daarvoor een Chief Information Security Officer aangenomen. Er lag zelfs al een migratieplan, maar dat had een lange looptijd, die steeds weer werd opgerekt vanwege vertraging in de nieuwbouw, het budget en de continuïteit van de zorg.” Het bestuur realiseert zich op dat moment dat ze de ICT-afdeling tot dan toe eigenlijk alleen belden als ze zelf een probleem hadden, maar zich nooit hebben afgevraagd hoe het ervoor stond met de voortgang van het migratieplan en de veiligheid van hun systemen. Nu wel.

De ICT’ers doen hun verslag. Beveiligingsbedrijf Fox-IT is al maanden aan het werk in het ziekenhuis. Ze hebben een soort digitale veiligheidsring rond het ziekenhuis gelegd en monitoren al het internetverkeer. Ze hebben inderdaad verdachte activiteiten gezien die zouden kunnen wijzen op een inbraakpoging. Dat was enkele dagen daarvoor al gemeld, maar genegeerd door de betreffende GHZ-medewerker en niet doorgekomen bij het bestuur of de directeur Financiën & ICT. Nu wordt er wel snel gehandeld. Het interne netwerk wordt gescand op kwaadaardige software, de gehackte server is inmiddels offline gehaald en de veiligheidsring wordt gesloten. Rond 15.00 uur kan er geen data meer in of uit het ziekenhuis.

Om 15.32 die dag verschijnt het artikel van Brenno de Winter op NU.nl: **‘**Groene Hart Ziekenhuis lekt medische dossiers’. Het zou gaan om “brieven tussen artsen, röntgenfoto’s, echo’s, hartfilmpjes, medicatielijsten, recepten, diagnoses, diverse soorten scans, behandelplannen en laboratoriumuitslagen. Ook het volledige patiëntenbestand met de informatie van ruim 493.000 personen blijkt diverse malen op de computer te staan.”

Het lek zou zijn gevonden door ene Bonnie van het Nederlands Genootschap van Hackende Huisvrouwen, een pseudoniem dat in die tijd wel vaker door hackers wordt gebruikt. Ze zou een externe ftp-server hebben gevonden die makkelijk te kraken was. In het artikel wordt ook het wachtwoord genoemd: ‘groen2000’. Bonnie zou slechts vluchtig hebben gekeken en na

het aanleveren van het bewijsmateriaal alle gegevens direct hebben gewist. NU.nl heeft het lek voor publicatie gemeld bij het ziekenhuis, het National Cyber Security Center en de Inspectie voor de Gezondheidszorg.

Het crisisteam is intussen begonnen aan een reconstructie van de hack. Uit de Fox-monitor blijkt dat de dagen ervoor iemand zich toegang had verschaft tot een externe server, een HP-dataprotector. De server diende als doorgeefluik voor ingescande papieren dossiers uit 2008, maar deze dossiers waren na gebruik niet gewist. De hacker zou via die server ook het wachtwoord ‘groen2000’ hebben achterhaald. Dat werd op heel veel systemen door verschillende mensen van de ICT-afdeling gebruikt, dus daarmee kon hij zo’n beetje overal in. De monitor laat ook zien wat voor data er is gedownload en dat blijkt best veel. Het crisisteam besluit daar direct open over te zijn en zet de vondst op een vraag-en-antwoordpagina van hun website. Om die transparantie uit te dragen, noemen ze zeer precieze getallen:

- Pagina’s uit 47 patiëntendossiers, met daarin bijvoorbeeld medische diagnostiek, analyses, brieven en behandeling. Het betreft papieren dossiers van de afdeling Interne Geneeskunde van voor 2008 die daarna gedigitaliseerd zijn.
- Een bestand uit 2008 met NAW-gegevens en BSN-combinaties van 496.176 patiënten.
- Een databestand van 15.262 initialen, achternamen en patiëntnummers afkomstig van de afdeling Cardiologie en Kindergeneeskunde.

De volgende dag neemt het team contact op met de Inspectie voor de Gezondheidszorg, het College Bescherming Persoonsgegevens en het ministerie voor Volksgezondheid. Alles draait om direct en open zijn, want het team voelt zich verantwoordelijk voor de gegevens van hun patiënten. Degene van wie gegevens in die data stonden worden benaderd. Dat is op zich nog lastig, want daarvoor moeten ze eerst toestemming krijgen van het CBP. Uiteindelijk mag het en krijgen ze van twee patiënten een reactie.

Het team vertelt echter niet alles direct. Zo had Fox-IT gekeken vanaf welke IP-adressen de server was benaderd. Het

ging om een Zweeds Virtual Private Network. Dat is een verbinding waarmee iemand zijn eigen IP-adres kan afschermen, dus daar hadden ze niet zoveel aan. Echter, één keer was wel ingelogd vanaf een Nederlands IP-adres. Vanaf daar was er malware geïnstalleerd om de data te downloaden en crashte de server. Deze informatie houden ze nog achter de hand voor het forensisch onderzoek.

Dinsdag 9 oktober is het wekelijkse vragenuurtje in de Tweede Kamer en zien de parlementariërs de hack als een aanleiding vragen te stellen aan minister Schippers van Volksgezondheid, Welzijn en Sport. Het lid Bruins Slot (CDA) is de eerste die begint over het bericht op NU.nl: “Het gevonden lek is slechts het topje van de ijsberg. Heeft de minister zicht op hoe erg het gesteld is bij ziekenhuizen en monitoren de inspectiediensten, IGZ, wel goed genoeg?” Minister Schippers stelt dat dat de taak is van het CBP. Die heeft daarvoor de norm NEN 7510 om de informatiebeveiliging te toetsen. De discussie gaat vervolgens over het LSP, oftewel het landelijk schakelpunt, voor uitwisseling van patiëntengegevens. Met het EPD-drama nog vers in het geheugen, vragen Kamerleden of dat schakelpunt er wel moet komen als ziekenhuizen zo slordig met hun data omspringen. De minister ziet het LSP juist als de oplossing. Zo maken we een einde aan “de houtjetouwtjeoplossingen die elk ziekenhuis nu zelf invoert”.

Dan is Henk Krol aan het woord. Op dat moment denkt hij nog dat hij van de Diagnostiek voor U zaak af is, want pas de maand erna wordt hij vervolgd voor zijn hack. Hij vraagt, niet geheel zonder eigenbelang: “Ik zou zo graag van de minister willen weten of de hacker die dit naar voren heeft gebracht, een bloemetje of strafvervolging verdient?” Schippers: “Met de manier waarop dit is gegaan, namelijk vernietigen van wat je hebt ingezien, maar wel aantonen dat het niet deugt, ben ik als minister van Volksgezondheid blij. Hoe het verder juridisch zit, weet ik niet. Ik ben echter blij met dit signaal, want hierdoor weten wij dat het niet deugt.”

Hoe het juridisch zit, weet niemand op dat moment. Bij de zaken rondom de OV-chipkaart ging de vrijheid van meningsuiting

nog boven computervredebreuk, maar hier gaat het om gegevens van patiënten en die zijn toch wel wat gevoeliger dan reistegoeden. De zaken van Diagnostiek voor U en Habbo Hotel moeten dan nog voor de rechter komen, dus veel jurisprudentie is er niet. Maar er is bij het ziekenhuis wel malware geïnstalleerd en hun server is door de hack gecrasht. Bovenal gaat het hier om heel veel patiëntengegevens en wil het ziekenhuis graag weten wat ermee is gebeurd. Met het sporenonderzoek van Fox-IT is er een redelijk kans dat de dader ook gevonden kan worden. Het crisisteam van Verdier krijgt advies van politie, justitie en het NCSC toch aangifte te doen. Dat is wat bestuursvoorzitter Verbeek op 10 oktober ook doet.

Bonnie heet in het echt Jordy en is op het moment van de hack 26 jaar en woont in Nieuwerkerk aan den IJssel. Hij kent het Groene Hart Ziekenhuis omdat hij daar zelf wel eens patiënt is geweest. Als hij verneemt dat het ziekenhuis recent nog door de Inspectie voor de Volksgezondheid op de vingers is getikt vanwege gebreken in de beveiliging, is hij benieuwd hoe het er dan voor staat. Hij gaat 26 september het internet op via de Zweedse aanbieder VPN Tunnel en scant het netwerk van het ziekenhuis met behulp van het programma Nessus. Dit is volgens de bijbehorende site ‘The Most Widely Deployed Vulnerability Scanner in the World’ en bedoeld om te kijken of je netwerk goed beveiligd is. Voor hackers is het tegelijkertijd een handige tool om te kijken of je ergens in kunt.

Jordy ontdekt in het netwerk van het ziekenhuis een HP-dataprotector. Dat is een externe server die gebruikt wordt om backups of bestanden door te sturen en berucht is vanwege kwetsbaarheden. Zo was een half jaar daarvoor KPN gehackt via zo’n zelfde server, wat tot grote consternatie leidde. Dergelijke grootschalige kwetsbaarheden worden ook gedocumenteerd in de zogenaamde ‘common vulnerability and exposure’-database. Deze kwetsbaarheid staat bekend als CVE 2011:1866. Nu wordt het wel erg technisch, maar ik zal proberen uit te leggen hoe je in de HP-dataprotector komt.

Internetverkeer van en naar servers gaat via verschillende poorten met elk een uniek nummer. Zo worden bijvoorbeeld

mailverkeer en websurfen van elkaar gescheiden. Als hacker doe je vaak eerst een poortscan om te kijken of je ergens makkelijk in kunt om van daaruit het systeem te verkennen. De HP-dataprotector gebruikt poort 5550 om bestanden uit te wisselen via FTP, file transfer protocol. De kwetsbaarheid in deze server zit hem in een programma dat je via deze poort opdrachten kunt geven: omniinet.exe. Dat programma slaat opdrachten op in een tijdelijk schrijfruimte, de buffer. Maak je de opdracht echter groter dan de buffer aankan, dan wordt die code ergens anders opgeslagen en uitgevoerd. Dit is een zogenaamde buffer overflow en kan ervoor zorgen dat de server crasht, maar als je het goed doet, kun je hem op afstand besturen.

Jordy zorgt voor een buffer overflow door \Omniback\i386\instellservice.exe. naar de server te sturen. Dat is een programma waarmee je bestanden van de server kunt downloaden. Eerst gebeurt er niets en hij probeert het nog drie keer. Weer niets. Wellicht wordt de VPN Tunnel-verbinding gezien als onbetrouwbaar, dus probeert hij het nogmaals via zijn gewone internetverbinding. Dan lukt het wel en hij komt in de server. Daar ziet hij de gebruikersnaam en het wachtwoord van de systeembeheerder: ‘groen2000’. Hij logt in, ziet diverse bestanden en download twee zip-bestanden.

De volgende dag gaat hij zijn vangst analyseren. Als hij de zip-bestanden uitpakt blijken het één csv- en twee TIFF-bestanden te zijn. Een CSV-bestand (Comma Separated Value) is gewoon platte tekst in tabellen. Die zet hij om in een Excel sheet. Hij gaat door de kolommen en ziet namen, adressen, woonplaatsen en burgerservicenummers en telt in totaal 496.176 rijen. De twee TIFF-bestanden (Tagged Image File Format) blijken ingescande patiëntendossiers te zijn. Dan weet Jordy genoeg en neemt contact op met Brenno de Winter. Hij vertelt de journalist wat hij heeft gevonden, stuurt hem een screenshot van de mappenstructuur op de server en geeft hem het wachtwoord. Ze besluiten dat dit een interessante onthulling wordt voor NU.nl.

De dagen erna gaat Jordy verder met zijn onderzoek. Hij heeft weliswaar al aangetoond dat het ziekenhuis kwetsbaar is, maar wellicht komt hij nog wat interessante feiten tegen voor het artikel. Om zijn bevindingen concreet te maken zoekt hij op namen: die

van hemzelf, familieleden en een vriend. Ook die staan erin en hij neemt contact met hen op. De burgerservicenummers die hij bij hun namen heeft gevonden blijken te kloppen. Hij vertelt via de chat ook aan de vriend dat hij nog “500k personen” heeft. Daarnaast zoekt hij ook nog op de naam van een bekende Nederlander. Tot 6 oktober kijkt hij nog af en toe rond zonder bestanden te downloaden, maar dan is hij wel klaar. Hij wordt dan ziek, heeft geen zin meer in hacken en wacht op de onthulling.

Als op 7 oktober de rel eenmaal losbarst, schrikt hij van alle commotie die hij teweeg heeft gebracht. In de media wordt zelfs geroepen om aftreden van het bestuur. Als De Winter op 12 oktober verslag doet van de excuusbrieven die het ziekenhuis stuurt naar de patiënten van wie de dossiers zouden zijn ingezien, is dit voor Jordy een mooie gelegenheid om ook zijn mening te geven, wederom onder pseudoniem. NU.nl opent: ‘Groene Hart Ziekenhuis betuigt spijt voor lek’. Eronder staat dat volgens de hacker een lastercampagne wordt gevoerd tegen het Groene Hart Ziekenhuis. ‘Bonnie’ heeft juist bewondering voor het ziekenhuis: “Als je een fout maakt en je bent er zo open over dan snap je veel van beveiliging. Er zijn weinig bedrijven die durven te erkennen hoe lek ze eigenlijk zijn. Deze Raad van Bestuur geeft er juist blijk van beveiliging te begrijpen. Je erkent je fouten, je verhelpt ze en doet het beter.”

Het artikel besluit dat de hacker niet verwacht dat er aangifte tegen hem zal worden gedaan, want “De Tweede Kamer was duidelijk dat een probleem is aangetoond. Het ziekenhuis reageert beheerst en niemand had kwaad in de zin”. Wat hij dan niet weet, is dat de voorzitter van de raad van bestuur twee dagen ervoor al aangifte heeft gedaan. De politie start op 17 oktober met het onderzoek, identificeert Jordy op 23 oktober als de gebruiker van het door Fox-IT gevonden IP-adres en houdt hem aan op 27 november.

Jordy logeert op dat moment bij iemand in Amsterdam. Ze hebben de hele nacht doorgewerkt aan een nieuw softwareproduct dat ze op de markt willen brengen en liggen nog te slapen als de agenten naar binnen stormen. Jordy denkt eerst dat het een grap is, totdat hij hun wapens ziet. Hij wordt afgevoerd naar Houten,

waar hij drie dagen vastzit en verhoord wordt. Intussen is er ook een inval geweest in zijn huis in Nieuwerkerk aan den IJssel. Al zijn computerapparatuur is in beslag genomen: zijn laptop, pc en wat harde schijven.

Brenno de Winter meldt de dag van de aanhouding op NU.nl wat er is gebeurd. Twee dagen erna vragen Kamerleden aan Opstelten om hen te informeren over de situatie. De minister van Veiligheid en Justitie zegt toe dat hij binnen een week uitleg zal geven. De Winter doet die dag alvast een rondje langs de Kamerleden om hun meningen te peilen en op 29 november opent hij op NU.nl: ‘Kamer ontsteld over harde aanpak hacker’ en citeert hun uitspraken.

SP-kamerlid Sharon Gesthuizen: “Dit is schokkend en totaal onverwacht. De vraag is of het kabinet spreekt met één mond.” Ze snapt wel dat er onderzoek wordt gedaan, maar opsluiten vindt ze het andere uiterste. “Wat voor signaal is dit dan?”

Henk Krol: “Ik vind dit zo overtrokken. Volkomen onzin: hier gaat geen gevaar van uit. Mensen die gegevens onvoldoende beveiligen moeten we hard aanpakken.” En: “Als dit zo doorgaat dan word ik volgende week ook opgepakt”.

D66-kamerlid Gerard Schouw: “Wij willen heel snel opheldering hebben, want het is een bizarre zaak. Dit is ongelofelijk. (…) Daarom moeten we de feiten horen van de minister. Anders is het gek: een dataklokkenluider die in de gevangenis komt te zitten; dat kan nooit de bedoeling zijn. Wij zijn blij met klokkenluiders en zeker met dit soort onderwerpen. Daarom moet er vandaag helderheid komen.”

De opheldering van minister Opstelten volgt op 5 december per brief aan de Kamer. Over de aangifte zegt hij: “Indien er sprake is of lijkt te zijn van een grote hoeveelheid ontvreemde bestanden uit databases dan is het inderdaad het advies van het NCSC aan de betrokken partij om te overwegen om aangifte te doen. Middels een strafrechtelijk onderzoek kan dan onderzocht worden of er inderdaad sprake is van een strafbaar feit. Hierbij heeft het OM, gegeven de omstandigheden in de zaak, de mogelijkheid om vervolging in te stellen. Het is uiteindelijk aan de rechter om te beslissen of er daadwerkelijk sprake is van een strafbaar feit.”

Hij maakt van de gelegenheid gebruik om zijn beleid voor verantwoorde onthullingen uiteen te zetten want dat wordt eind 2012 bekend gemaakt. “Bij het melden van kwetsbaarheden in ICT is ‘responsible disclosure’, het op verantwoorde wijze melden van incidenten, van het grootste belang. Centraal bij het werken met responsible disclosure staat het verhelpen van de kwetsbaarheid en het verhogen van de veiligheid van informatiesystemen. Daarbij gelden een aantal algemene uitgangspunten, zo is het bijvoorbeeld niet gepast om onnodige schade aan te richten of verder te gaan dan het aantonen van de kwetsbaarheid. In een dergelijk geval is het niet gepast om onnodig grote databestanden te ontvreemden als al is aangetoond dat het databestand benaderbaar is. Tot slot speelt ook de proportionaliteit van de ingezette middelen een belangrijke rol, denk hierbij bijvoorbeeld aan het plaatsen van een eigen backdoor in een informatiesysteem om vervolgens daarmee de kwetsbaarheid aan te tonen.”

Over het Groene Hart Ziekenhuis zegt de minister dat de aangifte is gedaan op advies van het NCSC. Vervolgens bleek uit het onderzoek dat een verdachte kwaadaardige software had geïnstalleerd, er meerdere hacks hebben plaatsgevonden en grote hoeveelheden data zijn ontvreemd. Verder onderzoek richt zich op mogelijke andere verdachten.

Daarna wordt het voorlopig stil rondom de zaak en verschuift de media aandacht naar Henk Krol. De 50PLUS’er heeft namelijk de dag ervoor te horen gekregen dat hij voor de rechtbank moet verschijnen voor het hacken van Diagnostiek voor U. Het Openbaar Ministerie zal nog twee jaar nodig hebben voordat Jordy wordt veroordeeld, want in het onderzoek vangen ze veel meer dan ze in eerste instantie verwacht hadden. Net op dat moment zijn verschillende partijen druk bezig om nu eindelijk eens beleid te maken voor responsible disclosure. Een beter moment hadden ze niet kunnen kiezen…

15. @bl4sty en de tien miljoen modems

‘I hacked KPN, and all I got was this lousy T-shirt’

Begin 2013 was er dus nog veel onduidelijk over de status van ethisch hacken. Enerzijds zijn overheid en bedrijfsleven zichtbaar bezig met beleid voor responsible disclosure en zijn er veel bijeenkomsten van betrokkenen om draagvlak ervoor te creëren. Anderzijds zijn er steeds meer voorbeelden van hackers die ondanks hun ethische doelstellingen toch zijn opgepakt. De overheid wil de goedbedoelende hackers geen juridische garanties geven, vervolging blijft altijd mogelijk. Dit leidt tot debatten in de media, op conferenties en in het parlement. Minister Opstelten heeft intussen wel al een opzet voor een leidraad naar de Tweede Kamer gestuurd, maar die wordt pas op 29 mei besproken.

Het is in deze sfeer van tegenstrijdigheden dat twee jonge beveiligingsonderzoekers ontdekken hoe ze een ZyXEL-modem kunnen hacken. Ze gaan dan ook voorzichtig te werk als ze dit willen melden bij KPN, van wie ze hun modem hebben en doen hun melding onder pseudoniem. De hackers krijgen echter meteen een reactie met de garantie dat het telecombedrijf geen aangifte zal doen. Ze worden zelfs uitgenodigd om bij KPN in een besloten setting hun verhaal te doen. Hun verhaal verschijnt uiteindelijk ook op de website van KPN, onder de titel Guest Hacker Program. Daarin vertelt security officer Martijn van de Heide hoe belangrijk het is om dit soort meldingen te krijgen. Hij lijkt me een geschikte persoon om eens mee te gaan praten over hoe telco’s omgaan met responsible disclosure.

Als ik Van de Heide spreek op het KPN-hoofdkantoor in Den Haag is er taart voor iedereen. Zijn team is namelijk net derde geworden bij de Cyberlympics, een jaarlijkse hackcompetitie in Las Vegas waar Nederland altijd goed vertegenwoordigd is. Deze

ethisch hackers testen continu het netwerk van KPN en geven hun bevindingen door aan andere afdelingen. Dit is duidelijk een organisatie die begrijpt hoe hackers denken. Daarom is er ook een meldpunt responsible disclosure, waar direct op meldingen wordt gereageerd door het KPN Computer Emergency Response Team.

Volgens Van de Heide is er wat dat betreft veel veranderd sinds hij zes jaar geleden voor het eerst een melding binnenkreeg. Toen kwam de juridische afdeling direct in actie. Die wilde de identiteit van de hackers weten en een zaak beginnen. Zijn afdeling heeft toen hard moeten strijden om de melders te beschermen, maar gaandeweg ontwikkelde zich een responsible disclosure beleid. Nu krijgen ze gemiddeld één melding per week en die wordt meestal binnen een dag afgehandeld. Zo ging het ook bij de jongens die sindsdien bekend staan als de modemhackers.

De security officer vertelt hoe zijn afdeling in de eerste week van januari een voorzichtig e-mailtje krijgt. De exacte tekst weet hij niet meer, maar het bericht kwam neer op: “We hebben iets gevonden, maar zijn bang dat jullie ons oppakken.” Het was versleuteld en verzonden vanaf een generiek e-mailadres. Hij begrijpt hun voorzichtigheid wel. De hacker van het Groene Hart Ziekenhuis is de maand ervoor opgepakt en Opstelten heeft verkondigd dat het OM altijd alsnog onderzoek kan doen, ook als de betrokken organisatie geen aangifte doet. “Dat is jammer, want dat schrikt hackers af”, stelt Van de Heide. Hij gelooft ook niet in zoiets als een algemeen meldpunt, want meldingen moeten snel terechtkomen bij degene die er wat aan kan doen. Organisaties moeten zelf een meldpunt hebben voor wat hij noemt “gratis ogen”.

Hij spreekt dan ook met veel respect over de modemhackers. Als de twee jongens van nog geen twintig op het hoofdkantoor een powerpointpresentatie geven, blijkt dat ze hun hack heel gedetailleerd hebben vastgelegd. Ze laten zien wat ze hebben gedaan om de controle over de modem over te nemen, maar ook hoe het lek gedicht kan worden. Van de Heide begrijpt ook direct dat hun melding van grote waarde is, want deze ZyXEL-modem wordt wereldwijd door tientallen miljoenen mensen gebruikt. KPN

neemt daarom diezelfde dag nog contact op met de fabrikant en geeft die een termijn om de modems te patchen. De jongens willen namelijk begin april hun bevindingen presenteren op de hackersconferentie Hack in the Box. KPN zal in de tussentijd de modems op afstand updaten en zorgen dat ze allemaal voor eind maart gereset zijn. De gebruikers hebben er dan als het goed is niets van gemerkt.

Na wat zoekwerk vind ik ook de namen van de modemhackers. Het blijkt te gaan om @stevenketelaar en @bl4sty – ook wel Peter Geissler. Als ik Geissler spreek, hoor ik een bekend verhaal: een nieuwsgierige tiener voor wie school verre van interessant is. Hij deed MBO ICT, maar is vooral autodidact. Hij en Ketelaar vinden het vooral leuk om van alles uit te proberen en te kijken hoe iets werkt. Eind 2012 is hun modem aan de beurt, de ZyXEL P-260IHN-FI. Ze komen er bij toeval achter dat ze een hulppagina kunnen opvragen en daar tekst kunnen invoeren. Bij meer dan 58 tekens crasht de modem en start dan weer automatisch op.

Uit crashes kunnen ze afleiden hoe de modem werkt, dus schrijven ze een script om de crash te besturen. Ze zien dat poort 7676 is gereserveerd en je daar niet in mag. Dat is namelijk de management interface waarmee de aanbieder de modem op afstand voorziet van updates. Het lukt hen om er toch in te komen en via deze poort kunnen ze nu ook eigen software installeren tussen de gebruiker en het internet. Het hele onderzoek kost hen vijf dagen werk, maar de mogelijkheden zijn legio. Voor hun demo bij Hack in the Box kiezen ze ervoor een voice-over IP-telefoongesprek af te tappen.

Op 10 april staan beide heren bij Hack in the Box in een soort Star Trek-achtige overhemden op het podium, met voor zich een geïmproviseerd netwerk. De titel van hun presentatie is ‘How I met your Modem’. Na een technische verhandeling die ik jullie hier zal besparen, belt Ketelaar iemand via de VoIP en vraagt diegene een vooraf gegeven code te noemen. Geissler rommelt wat aan zijn laptop en jawel, hij tovert het gesprek tevoorschijn. De zaal applaudisseert. Vervolgens vertelt hij hoe KPN omging met de melding. Wederom klinkt applaus en spontaan verschijnt Jaya Baloo op het podium. De KPN Chief Information Security

Officer roept: “On behalf of KPN I would like to thank you for hacking our network.” Ze overhandigt beide heren een T-shirt met daarop de tekst ‘I hacked KPN, and all I got was this lousy T-shirt’. Nog meer applaus. Baloo zweept het enthousiasme nog maar eens op: “It shows responsible disclosure works!” Geissler mompelt wat verlegen: “Yes, sometimes it does” en gaat weer verder met zijn technische uitleg.

Dit alles klinkt als een succesverhaal en dat is het in zekere zin ook. Toch zit iets me nog niet helemaal lekker. De modems worden beheerd vanaf de providerkant via de beruchte poort 7676. Dus als je voor deze onthulling al gehackt bent, kan KPN het lek niet meer dichten. Dat klopt volgens Geissler, maar volgens hem zijn zij de eersten die dit ontdekt hebben. Maar zelfs dan nog: hoe zou het nu vergaan met die tien miljoen andere modems die niet van KPN zijn? Zou ZyXEL alle providers en individuele gebruikers hebben geïnformeerd? Of zou hun melding alsnog door velen misbruikt kunnen worden? Dat weten we niet, maar er zijn sindsdien geen gevallen bekend geworden...

Deze zaak laat zien dat responsible disclosure werkt en meldingen ook afgehandeld kunnen worden zonder tussenkomst van de media, overheid of rechtspraak. Maar het laat ook zien dat melder en eigenaar niet de enige betrokkenen zijn. Informatietechnologie is een keten van onveiligheden, waarvan het onmogelijk is te achterhalen of alle schakels gefixt worden. Uit die keten kan ook onverwachts een andere gedupeerde opduiken om de helpende hackers tegen te werken. Dat zien we in de volgende zaak.

16. De hash van Dismantling Megamos

Volkswagen houdt Radboudpublicatie over gekraakte autosleutels tegen

Ter illustratie van onze vorderende jurisprudentie en beleid voor responsible disclosure, hier een uitstapje naar een van onze buurlanden om te zien hoe het er daar aan toe gaat. De Digital Security Group van de Radboud Universiteit, die in 2008 door de rechter in het gelijk werd gesteld toen ze over de gekraakte Mifarechip wilde publiceren, krijgt hier een vergelijkbaar proces. Dit keer in Engeland, waar in 2013 hun publicatie over een gekraakte elektronische autosleutel wel door de rechter wordt tegengehouden. Dat terwijl de klager in deze zaak niet eens de eigenaar van de chip of het algoritme is, maar een gebruiker: Volkswagen. Hun miljoenen auto's zijn beveiligd met het Megamos-algoritme en de publicatie daarvan ziet de rechter als een onverantwoorde onthulling. Dat zou in Nederland waarschijnlijk niet zijn gebeurd.

Tegen die tijd is de Digital Security Group onder leiding van professor Bart Jacobs al meer dan tien jaar bezig met verantwoorde onthullingen. Onder de inmiddels veertig onderzoekers bevinden zich veel specialisten in RFID-systemen. Dit zijn chips die middels elektromagnetische golven op afstand zijn uit te lezen, zoals de Mifare Classic die wordt gebruikt in toegangspassen en de OV-chipkaart. Vanuit academische interesse en maatschappelijk belang, zijn al veel smartcards, tokens en e-readers onder hun handen geopend. Roel Verdult – die ook de Mifare Classic kraakte – richt zich eind 2012 op de Megamos Cryptochip. Die wordt gebruikt in de startsloten van Porsche, Audi, Bentley, Lamborghini en alle Volkswagens.

Zo'n slot werkt als volgt. Als je de fysieke sleutel in het slot steekt en omdraait, stuurt een lezer in dat slot een signaal naar een chip in de autosleutel. Eerst gaan er wat nummers heen en

weer om te kijken of de chip en lezer echt zijn, vervolgens geven ze elk een nummer dat uniek is voor dat specifieke slot en de sleutel van die auto. De berekening die op het getal wordt uitgevoerd, is het geheime algoritme. Als de uitkomst klopt, gaat het elektronische slot open en wordt de auto gestart. Dit slot voorkomt dat criminelen de auto handmatig kunnen starten door draden los te trekken en die tegen elkaar te houden.

Het gereedschap van Verdult is dit keer de Tango Programmer, waarmee hij een Megamossleutel en -slot kan programmeren. Het apparaat bevat zelf het geheime algoritme, waarmee de berekeningen worden uitgevoerd. Door steeds de input en output te variëren en te kijken wat er gebeurt, komt Verdult achter het algoritme. Dit is reverse enginering, net als bij de OV-chipkaart. Hij zou nu elke elektronische sleutel van auto's met Megamosstartonderbrekers kunnen namaken. Maar dat is natuurlijk niet zijn doel. Hij wil zijn bevindingen publiceren om te laten zien dat het kan en de beveiliging verbeterd wordt.

Deze publicatie schrijft hij samen met collega Barış Ege en Flavio Garcia, zijn voormalige begeleider die dan bij de Birmingham University werkt. De titel wordt: 'Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer' en ze willen het presenteren op de USENIX computer security-conferentie van de Advanced Computing Systems Association. De conferentie is in augustus 2013, maar het artikel moet voor die tijd wel door de peer review dus hun deadline is 25 juni. Ze hebben dus meer dan een half jaar om nog een reactie te krijgen van de eigenaar van het systeem, die vervolgens bijna een jaar heeft om maatregelen te nemen. Dat moet genoeg zijn.

Alleen, wie is die eigenaar? Het algoritme is van het bedrijf Thales. Die heeft een ander bedrijf - EM - toestemming gegeven het te gebruiken in hun RFID-chips. Weer een ander bedrijf - Delphi - gebruikt deze chips in hun sloten en sleutels en verkoopt dit systeem aan de fabrikanten die het in de auto's installeren. De onderzoekers gaan voor de chipleverancier en in november 2012 benaderen ze EM. Die reageert pas in februari. Delphi haakt intussen ook aan en op 6 juni hebben ze uiteindelijk een meeting. Daarin vragen de leveranciers van de chips en de sloten aan de onderzoekers of ze bepaalde delen van het algoritme niet willen

publiceren. Dat vinden Verdult en zijn collega's lastig, want zo kunnen ze niet bewijzen dat ze het algoritme ook werkelijk hebben achterhaald en laten zien waar het probleem precies zit. Ze besluiten dat ze de belangen van beide bedrijven nog wel in overweging willen nemen.

De onderzoekers gaan na de meeting weer naar hun werkplek en zien daar dat ze een e-mail hebben ontvangen van een advocaat van Volkswagen. De autofabrikant heeft de High Court of England and Wales gevraagd een rechtelijk bevel uit te voeren en hun publicatie tegen te houden. Dat verzoek blijkt de dag ervoor te zijn ingewilligd. De zitting is 25 juni 2013, de dag van de deadline van hun artikel.

Net als bij de voorgaande rechtszaken, kunnen we ook deze teruglezen in het rechtbankverslag. Dat is maar goed ook, want de onderzoekers mogen er nog steeds niets over zeggen, dus dit is onze enige bron. We lezen hier dat de klager zich niet beroept op computervredebreuk of auteursrecht, maar juist die hogere wet waar de verdediging zich normaal op beroept: de Universele Verklaring van de Rechten van de Mens, of in het geval van Engeland, the Human Rights Act. In artikel 12, over de vrijheid van meningsuiting, staat namelijk dat die vrijheid gepaard gaat met een zekere maatschappelijke verantwoordelijkheid. Een rechter mag daarom een publicatie tegenhouden als mogelijke gedupeerden daar overtuigende argumenten voor hebben.

Volgens de klager zijn die argumenten er wel degelijk. Het algoritme is vertrouwelijke informatie en het onthullen ervan faciliteert diefstal van miljoenen Volkswagens. Het algoritme moet onrechtmatig verkregen zijn door de maker van de Tango Programmer. Wie de Bulgaarse site van de verkoper Scorpio bezoekt, ziet meteen dat dit illegale software is, aldus de advocaat van Volkswagen.

De advocaat van de onderzoekers vindt deze argumenten niet overtuigend. Het algoritme is juist achterhaald middels legale apparatuur en methoden. Een slechte site hoeft niet te betekenen dat de aanbieder crimineel is. De Tango Programmer wordt ook door veel anderen gebruikt, bijvoorbeeld autogarages. Hun methode is ook legaal: reverse enginering is erkend, zie de OV-

chipkaart. Maar bovenal: onthulling van het beveiligingslek is geen risico, maar juist in het publieke belang, want ook criminelen zouden het slot kunnen kraken en daarom moet ook het publiek ervan op de hoogte zijn.

Interessant is dat in de verdediging hier ook de leidraad responsible disclosure van het NCSC wordt aangehaald. De advocaat van de onderzoekers stelt dat deze leidraad in Nederland staat voor de geëigende manier waarop beveiligingslekken op een verantwoorde manier onthuld worden. Geheel in lijn met de leidraad, hebben de onderzoekers EM minstens zes maanden de tijd gegeven maatregelen te nemen. Dat Volkswagen als mogelijke gedupeerde pas later op de hoogte werd gebracht is niet hun schuld. Bovendien: hoe kan het dat Volkswagen hen aanklaagt? Zij zijn immers niet de eigenaar, maar een van de gebruikers van het algoritme.

Hier zien we een duidelijk verschil met de Engelse rechtspraak. Rechter Justice Birss vindt namelijk dat Volkswagen zeker gezien kan worden als klager en wijst op jurisprudentie uit de zogenaamde Cream Holdings zaak. Daar kwam namelijk uit naar voren dat als de eigenlijke gedupeerde van een publicatie een sterke zaak zou hebben, een andere ook in diens plek kan aanklagen als dat nodig is. Maar eigenlijk is Volkswagen volgens hem ook gedupeerde: “Their products depend on the secrecy of the Megamos Crypto algorithm.” Hij vindt de onthulling dan ook niet verantwoord, want met deze publicatie wordt een nieuwe manier om auto’s te stelen publiekelijk bekend. Academische vrijheid is dan wel een groot goed, maar “I think the defendants’ mantra of ‘responsible disclosure’ is no such thing. It is a self-justification by defendants for the conduct they have already decided to undertake and it is not the action of responsible academics.” Hij verbiedt de onderzoekers hun artikel te publiceren.

Verdult, Garcia en Ege kunnen het artikel ook niet meer aanpassen, want de deadline is die dag. Typisch voor cryptografen publiceren ze in plaats daarvan de hashfunctie van hun tekst. Dat is een algoritmische bewerking die de hele tekst van het artikel terugbrengt tot een unieke code van 128 tekens. Mocht later nog eens iemand de Megamos kraken en daarover

publiceren, dan kunnen zij alsnog hun artikel laten zien en met de hash aantonen dat zij dat al eerder hebben gedaan.

Verdult is uiteindelijk in augustus 2013 nog wel naar de USENIX Security Conference geweest. Zonder artikel, maar wel met een presentatie erover. Zijn verhaal is vooraf gecheckt door juristen en begint met disclaimers. Hij zegt in zijn inleiding dat hij geen technische details mag geven of vragen mag beantwoorden. Vervolgens vertelt hij hoe ze andere elektronische autosleutels hebben gekraakt en wat over responsible disclosure en reverse engineering. Tussendoor laat hij af en toe vallen dat het met Megamos ook zo ging. Op de laatste slide staat de SHA-512-hash van het artikel dat hij daar had willen presenteren. Dit is zijn “Historical claim” die natuurlijk ook hier niet mag ontbreken:

9d05ba88740499eecea3d8609174b444
43683da139f78b783666954ccc605da8
4601888134bf0c23ba46fb4a88c056bf
bbb629e1ddffcf60fa91880b4d5b4aca

In Nederland zou deze zaak naar mijn inschatting anders zijn afgelopen. Met de jurisprudentie van de voorgaande zaken zou de rechter veel positiever tegenover responsible disclosure hebben gestaan. Vooral de zaak OV-chipkaart kan één op één vertaald worden naar deze en dan had de Digital Security Group gewoon mogen publiceren. Maar omdat Garcia nu niet meer in Nederland, maar bij de Birmingham University werkt en het een internationale publicatie betreft, kan Volkswagen de zaak uitvechten voor de High Court of England and Wales. Of ze ook bewust die strategie hebben gehanteerd blijft gissen, maar het geeft ons wel een doorkijkje van hoe het elders anders kan verlopen.

Ik neem daarom contact op met Volkswagen. We zijn intussen alweer een half jaar verder. Het artikel is nog steeds niet gepubliceerd en ik ben benieuwd of ze inmiddels iets hebben gedaan met het gratis advies. Na veel heen en weer mailen met de Nederlandse pr-afdeling krijg ik uiteindelijk een reactie van ene Ralf Dennissen. Hij is PR-manager Volkswagen en heeft zelf een autohandel in Leusden. Ik stuur hem de bovenstaande tekst en vraag of Volkswagen nog concrete maatregelen heeft genomen,

zoals het terugroepen van auto’s naar de garage om hun slot te vervangen.

Dennissen schrijft: “Aan Volkswagen en Thales is een voorlopige gerechtelijke bevel toegewezen dat publicatie verbiedt van het betreffende algoritme en wat andere informatie. Deze zaak loopt nog altijd en er zal door de rechtbank een definitief oordeel geveld worden als de betrokken partijen er voor die tijd niet onderling uitkomen.” Ik mail terug of ik hieruit kan afleiden dat er geen concrete veiligheidsmaatregelen zijn genomen. Helaas, meer dan dit kan hij mij niet vertellen. Security by obscurity, zucht…

17. Tijd voor beleid

Verantwoorde onthullingen in het digitale polderlandschap

In de voorgaande hoofdstukken hebben we al aardig wat onthullingen gehad met rechtszaken en Tweede Kamerdebatten. Specifieke gevallen leidden telkens weer tot meer algemene discussies over de grenzen van het ethisch hacken en verantwoordelijkheden in informatiebeveiliging. Begin 2013 is het daarom tijd voor beleid. Het NCSC publiceert de ‘Leidraad om te komen tot een praktijk van Responsible Disclosure’ en het CBP haar ‘Richtsnoeren van beveiliging persoonsgegevens’. Bij de overheid en daarbuiten ontstaan initiatieven voor meldpunten waar ethisch hackers terecht kunnen. Maar, er komt geen nieuwe wetgeving. Als direct betrokken het niet eens worden, zullen ze het nog steeds moeten uitvechten in de rechtszaal. Om de rechtsgang daartoe te begeleiden, stuurt het College van procureurs-generaal hierover een brief aan alle parkethoofden met de aanhef: “Hoe te handelen bij ‘ethisch’ hackers?”

Typisch aan het Nederlandse polderlandschap is dat niet één partij het voor het zeggen heeft, maar alle betrokkenen meedoen. Discussies monden uit in patstellingen of een compromis waar iedereen zich wel een beetje in kan vinden, maar uiteindelijk niemand echt helemaal. Wellicht past dat ook juist wel bij informatiebeveiliging. Want in de lange keten van digitale schakels is iedereen een beetje en uiteindelijk niemand helemaal verantwoordelijk. Kennis over kwetsbaarheden verandert ook continu. Dan kun je maar beter met elkaar erover blijven praten dan dat één partij zegt hoe het moet.

Volgens Barend Sluijter van het NCSC was het Kamerdebat van 10 april 2012, waarover we al lazen in het hoofdstuk over @legosteentje, het politieke startsein voor responsible disclosure. Minister Opstelten zei tijdens het debat toe dat er een eenduidige

procedure moest komen om beveiligingslekken openbaar te maken. Zijn ministerie was daar toen al achter de schermen mee bezig, maar hij bleef terughoudend. Hij wilde vooral ook geen hoge verwachtingen scheppen: het NCSC bemiddelt alleen en wordt geen toezichthouder, want dan gaat iedereen maar achteroverleunen. De procedure zou ook zeker geen vrijbrief worden voor hackers om hun gang te gaan, want computervredebreuk blijft strafbaar. Daarna kregen we de zaken van Diagnostiek voor U en het Groene Hart Ziekenhuis die de boel op scherp zetten.

Opstelten stuurt uiteindelijk op 3 januari 2013 een brief aan de kamer waarin hij zijn belofte nakomt. De minister stelt voorop dat verantwoord onthullen primair de verantwoordelijkheid is van organisaties zelf. Hij noemt als voorbeelden de telecomsector en de financiële sector waar veel bedrijven op dat moment een procedure op hun website hebben gezet voor meldingen. Het NCSC handelt alleen meldingen af die betrekking hebben op de Rijksoverheid en de vitale sectoren. Daarnaast heeft het centrum een tekst opgesteld die organisaties kunnen gebruiken als bouwstenen voor een eigen meldpunt. Opstelten waarschuwt via de brief de hackers: “Deze leidraad laat de geldende strafrechtelijke kaders onverlet en beperkt niet de bevoegdheid van het Openbaar Ministerie om in bepaalde gevallen ambtshalve te vervolgen.”

Eigenlijk verandert er dus niet veel aan de juridische status van ethisch hacken: het blijft computervredebreuk en of de vrijheid van meningsuiting zwaarder telt, is aan de rechter om te beoordelen, zelfs als de ethisch hacker en de organisatie er samen uit zijn gekomen. Wat wel verandert, is wat je zou kunnen noemen de bewustwording rondom verantwoord onthullen: er zijn nu eenmaal mensen die ongevraagd lekken vinden en dat willen melden, dus laten we er met z’n allen het beste van maken. Als hacker en organisatie elkaar weten te vinden, wordt de informatietechnologie veiliger en krijgt de melder de eer. Deze leidraad kan daarbij helpen. De tekst zit in de bijlage van de Kamerbrief, wordt 22 januari gepresenteerd op de NCSC One conferentie en verschijnt 28 januari op ncsc.nl.

De titel van het lang verwachte stuk had niet veel minder spannend kunnen zijn: ‘Leidraad om te komen tot een praktijk van Responsible Disclosure’. Maar, voor een ambtelijk document is het een opvallend praktische handleiding. De nog geen zes pagina’s bestaan vooral uit instructies voor de organisatie en de melder. Het gaat immers vooral om hen. Komen ze er niet uit, of hebben ze een kwetsbaarheid gevonden die ook interessant is voor anderen, kunnen ze altijd nog besluiten het NCSC erbij te betrekken.

Responsible disclosure begint volgens de leidraad bij de organisatie waar het systeem draait. Die stelt een procedure op over hoe om te gaan met meldingen en heeft voldoende capaciteit om adequaat te kunnen reageren. Ze kan daarvoor instructies op de site zetten, met een e-mailadres waar de melder terechtkan, al dan niet anoniem. Als iemand dan iets meldt, volgt een ontvangstbevestiging, die bij voorkeur digitaal is ondertekend om zo de prioriteit te benadrukken. De melding moet dan snel naar de juiste afdeling om te beoordelen wat voor kwetsbaarheid het is en wat eraan gedaan kan worden. De melder wordt bij elke stap op de hoogte gehouden. Het is aan de organisatie of zij al bij voorbaat zegt af te zien van juridische vervolgstappen, maar dat heeft blijkbaar wel de voorkeur.

De organisatie en melder beslissen gezamenlijk wat een redelijke termijn is voor de onthulling en hoe ze dat doen. Voor kwetsbaarheden in software vindt het centrum zestig dagen redelijk. Hardware problemen duren over het algemeen wat langer om op te lossen: zes maanden. Het kan zijn dat de kwetsbaarheid ook bij andere organisaties zit en die eerst betrokken moeten worden. Is het probleem helemaal niet op te lossen of is de oplossing te duur, dan kunnen ze besluiten de kwetsbaarheid niet te onthullen. Lukt het wel, dan krijgt de melder de credits voor zijn ontdekking en wellicht ook een beloning.

Bij de instructies voor de melder staat vooral wat hij *niet* moet doen: kwetsbaarheden verder benutten dan noodzakelijk is om ze vast te stellen; gegevens van het systeem kopiëren, wijzigen of verwijderen; veranderingen in het systeem aanbrengen; herhaaldelijk toegang verkrijgen; de kwetsbaarheid of toegang delen met anderen; social engineering; brute forcen of een

backdoor plaatsen. Oftewel: ontdek je dat je in het systeem kan, maak een screenshot van wat je ziet, log meteen uit en meld het bij de organisatie.

De leidraad is dus vooral een stappenplan over wat de organisatie kan doen en wat de melder moet laten. Dat klinkt wellicht voor de organisatie wel logisch, maar niet voor hackers. Wel of geen social engineering? Als je met een beetje praten wachtwoorden kunt afvangen bij personeel, dan is dat ook een kwetsbaarheid. Maar hoever mag je daarin gaan en creëer je dan eigenlijk niet alleen maar meer kwetsbaarheden? Hetzelfde geldt voor brute forcing: als je maar lang genoeg wachtwoorden blijft proberen, kom je uiteindelijk overal wel in, dus dat is geen kunst. Aan de andere kant zou de inlogprocedure zo moeten zijn ingericht dat teveel herhaling wordt tegengegaan.

Een ander probleem voor melders is dat de leidraad stelt dat de melding direct moet worden gedaan bij de eigenaar van het systeem, maar niet altijd duidelijk is wie die eigenaar dan is. Informatietechnologie is vaak een keten van onveiligheden. Ga je dan naar de maker of de gebruiker ervan, of een derde partij die het als dienst aanbiedt? Vervolgens is het maar afwachten of die partij dan beleid heeft voor onthullingen. Is dat niet het geval, heb je als melder dus niets om op terug te vallen. Je zou hen hooguit de leidraad kunnen mailen en hopen dat ze er voor open staan. Of dan toch maar voor de veiligheid melden via een journalist? Die zal vervolgens de gevonden kwetsbaarheid eerst willen toetsen bij andere hackers voordat hij het naar buiten brengt.

Om organisaties die aan responsible disclosure willen doen tegemoet te komen, maakt Floor Terra (die van de ING-app) een voorbeeldbrief (zie bijlage). Deze kunnen ze op hun site zetten om hackers uit te nodigen hun systemen te testen. De punten in de tekst komen grotendeels overeen met de leidraad, maar met een belangrijk verschil: er wordt niets gezegd over de mogelijkheid dat je als hacker alsnog vervolgd wordt. De leidraad is daar wel helder over: “Het melden van de kwetsbaarheid vrijwaart de melder, indien hij bij het aantonen van de kwetsbaarheid een strafbaar feit heeft gepleegd, niet van de mogelijkheid van een strafrechtelijk onderzoek en vervolging.” Het OM kan dat ook ‘ambtshalve’ doen, oftewel zonder dat er aangifte is gedaan.

Is nu elke ethisch hacker vogelvrij? Om hier enige duidelijkheid in te krijgen, stuurt het College van procureurs-generaal, oftewel de leiding van het OM, op 18 maart een brief aan alle parkethoofden. Onderwerp: ‘responsible disclosure (hoe te handelen bij ‘ethisch’ hackers?)’. Ook hier lezen we: “Het verantwoord melden van een kwetsbaarheid vrijwaart de melder, indien hij bij het aantonen van de kwetsbaarheid een strafbaar feit heeft gepleegd, geenszins van de mogelijkheid dat de politie, op gezag van het OM, een strafrechtelijk onderzoek instelt en/of dat wordt overgegaan tot vervolging.” Wat volgt, is een aantal uitgangspunten die een officier van justitie kan betrekken in de afweging om wel of niet te vervolgen.

In de brief wordt onderscheid gemaakt tussen ethisch hacken en responsible disclosure. Het begrip ‘ethisch hacken’ kent het Wetboek van Strafrecht niet, alleen computervredebreuk. Dat is strafbaar en er zijn geen specifieke uitsluitingsgronden voor goede bedoelingen. Responsible disclosure is wat anders, want dat gaat over het naar buiten brengen van een lek en niet over het vinden ervan. Of de onthulling verantwoord is, hangt niet alleen af van de melder, maar vooral ook van de organisatie waar gemeld wordt. Heeft die er geen beleid voor, dan is er ook geen sprake van verantwoord onthullen. Wel kunnen bij de beoordeling ervan wat algemene principes worden gehanteerd:

“Als een hacker direct en veilig communiceert met de eigenaar van het ICT-systeem over een getroffen lek in de beveiliging en er geen gegevens zijn verwijderd of gemanipuleerd, kan er sprake zijn van RD en is er geen aanleiding om verder strafrechtelijk onderzoek in te stellen. Daar waar wel gegevens zijn verwijderd, gemanipuleerd of gekopieerd, dan wel op onevenredige wijze is gehandeld bij het toegang verschaffen tot een ICT-systeem, is er geen sprake van RD en is verder strafrechtelijk onderzoek en eventuele strafvervolging geïndiceerd.”

Ook als de melder en organisatie er onderling uitkomen, kan de hacker vervolgd worden, want als er “aanwijzingen zijn dat de hacker bewust dan wel onbewust meer heeft gedaan dan alleen melden van het beveiligingslek aan het betreffende bedrijf, dan dient dat weldegelijk verder te worden onderzocht. Te denken valt aan het overnemen van gevoelige (persoons-) gegevens of het

achterlaten van ‘malware’ op het systeem.” In de brief wordt een vergelijking getrokken met journalisten die strafbare feiten plegen met het oog op nieuwsgaring. De officier van justitie kan daarom bij zijn afweging de volgende vragen stellen:

1. Was het handelen van de verdachte noodzakelijk binnen een democratische samenleving (was er een zwaarwegend algemeen belang)?
2. Heeft de verdachte bij zijn handelen proportioneel gehandeld (stond het gekozen middel in verhouding tot het te bereiken doel)?
3. Heeft de verdachte subsidiair gehandeld (waren er andere mogelijkheden om te handelen)?

Deze vragen kwamen we al eerder tegen bij Krol en zullen we straks weer zien bij de hacker van het Groene Hart Ziekenhuis. Als deze met ‘ja’ beantwoord kunnen worden, kan de officier van justitie afzien van vervolging, maar om ze te beantwoorden zal hij dus wel de hacker eerst als verdachte moeten aanmerken. Dat is bizar, want dan moet de hacker vervolgens een advocaat regelen en lange tijd in onzekerheid zitten, terwijl volgens hem de organisatie degene is die iets verkeerd heeft gedaan. Ik vraag me af waarom het OM zo te werk gaat en ga daarom op bezoek bij het landelijk parket in Rotterdam. Daar zit openbaar aanklager Lodewijk van Zwieten, die al aardig wat cybercrime zaken heeft gedraaid. Hij vertelt:

“De leidraad is een handreiking en geen richtlijn. De minister wilde niet dwingend opleggen, want hij kan niet in één richtlijn de wereld een kleur geven in alle tinten die er zijn. Maximale wat hij kan doen is sectoren stimuleren spelregels op te stellen. Good practice. Welke rechten kun je hieraan ontlenen? Geen. Ethisch hacken kent de wet niet. Civielrechtelijk ben je bezig met het onrechtmatig betreden van een computer. Ik weet dat jij persoonsgegevens hebt en dat niet veilig doet en wil het verantwoord naar buiten brengen. Is er RD-beleid en zijn we eruit, dan staat het morgen in de krant. Als je dan alsnog naar de civiele rechter gaat, heb je geen zaak. Voor ons is er dan ook geen aanleiding voor opsporingsonderzoek. Maar wel als er een database is met gevoelige persoonsgegevens. Je bent dan wel

verwerker, maar geen eigenaar persoonsgegevens. Die mensen hebben nog steeds te maken met inbreuk op hun privacy en kunnen de systeemeigenaar aanspreken vanwege onrechtmatige daad, dus hij kan ook niet de hacker vrijwaren."

Volgens Van Zwieten neemt het OM het hier dus op voor mogelijke derden van wie persoonlijke gegevens zijn gebruikt om de onthulling te doen. "Als je het bekijkt vanuit responsible disclosure, is het uiteindelijk aan de rechter om te oordelen of een onthulling verantwoord is. Het gaat bijvoorbeeld niet alleen om het ziekenhuis, maar om de patiënten." Wie ga je dan vervolgen? Van Zwieten: "De hacker, want die heeft computervredebreuk gepleegd. De eigenaar heeft geen strafbaar feit gepleegd. Misschien nalatigheid, maar daar kun je alleen iets mee als gezondheid of levens van mensen gevaar lopen, bijvoorbeeld dood door schuld. Je hebt een verdenking nodig, dus moet ik de hacker verdachte maken om te onderzoeken wat er met de database aan de hand is. We hebben vaak onderzoeken gehad waarin gaandeweg meer bleek te zijn. De enige mogelijkheid die we hebben om objectief vast te stellen wat er gebeurd is, is het strafrecht."

Vanuit het perspectief van het OM is het vervolgen van de hacker dus de enige manier om erachter te komen of belangen van burgers zijn geschaad. Dat is op zich begrijpelijk, maar het gevolg is dan wel dat dit veel hackers afschrikt. Zelfs als hij denkt dat de organisatie geen aangifte zal doen, zou hij alsnog vervolgd kunnen worden. Dan maar liever weer anoniem onthullen via een journalist. Dan is die de melder en blijft de hacker buiten schot.

De journalistiek heeft echter weer zo haar eigen regels. Een onthulling moet wel nieuws zijn: feitelijk, hard en snel. Het veiligheidslek komt dan wel direct onder de aandacht, maar deze weg leidt ook vaak weer tot conflicten die voor het brede publiek worden uitgevochten. Die zouden voorkomen kunnen worden door een onafhankelijk meldpunt waar ethisch hackers anoniem terechtkunnen en meldingen achter de schermen afgehandeld worden. Hiervoor ontstaan in die periode dan ook verschillende initiatieven.

Een daarvan komt van drie beveiligingsexperts: Andre Koot (@meneer die we al eerder tegenkwamen in de zaak Krol), Alf Moens (@alfmoens van SURF, de club die de ICT doet in het hoger onderwijs) en Hans van Looy (@quux_nl van beveiligingsbedrijf Madison Gurkha). Op 20 maart beleggen de heren een bijeenkomst op het SURF-hoofdkantoor in Utrecht. Ze hebben een gemêleerd gezelschap bijeengebracht: hackers, ambtenaren, bedrijven en onderzoekers. Doel van de bijeenkomst is te kijken of mensen mee willen werken aan het oprichten van een meldpunt waar ethisch hackers terecht kunnen met hun meldingen.

Koot begint met een presentatie. Hij maakt zich zorgen om de informatiebeveiliging in Nederland en geeft overzicht van zaken die dan spelen: Groene Hart Ziekenhuis, Diagnostiek voor U, de pompen van Veere, etc. Hackers die hun vondsten direct melden bij de organisatie die verantwoordelijk is voor het systeem worden volgens hem meestal niet serieus genomen. Bij wie kunnen ze dan terecht? Bij de toezichthouders, zoals CBP, IGZ, ACM, maar die doen niet zoveel. Bij NCSC? Dan word je volgens hem “onder een vergrootglas gelegd”. Of anders bij hackmeldpunt.nl van de Haagse hackerspace Revspace. Maar meestal gaan ze naar een journalist zoals Brenno de Winter. Elk van deze partijen vertegenwoordigt echter een belang. Daarom moet er een onafhankelijk meldpunt komen dat wordt ondergebracht in een stichting. Hackers en organisaties kunnen daar terecht bij een ‘hackersgilde’, een groep gecertificeerde experts die hen begeleiden bij de onthulling.

De aanwezigen zien wel de noodzaak dat er iets moet gebeuren, maar hebben zo hun twijfels bij een nieuw meldpunt. Zelf zie ik vooral een pr-probleem in deze constructie: hoe breng je zo’n meldpunt onder de aandacht? Zullen jongeren die op hun zolderkamer zitten te knutselen überhaupt wel op het idee komen naar een meldpunt op zoek te gaan? En zo’n organisatie die dan op een dag een melding krijgt van zo’n meldpunt, neemt die het wel serieus? Of is het meldpunt alleen bedoeld om de hacker te anonimiseren, zodat hij snel iets over de schutting kan gooien en niet vervolgd kan worden? Dan roept iemand: “Er zijn al zoveel meldpunten, misschien moet er een meldpunt voor meldpunten

komen…” De stemming in de groep is in ieder geval dat er niet nog een meldpunt moet komen.

Dat wordt bevestigd door student David van Es. Hij zit naast zijn begeleider van de Haagse Hogeschool en doet op dat moment voor zijn vrije minor Information Security Management onderzoek naar responsible disclosure. Van Es heeft opdracht gekregen van SURF om te onderzoeken of er voldoende maatregelen zijn om het te laten werken, of dat er mogelijk nieuwe initiatieven nodig zijn. Zijn uiteindelijke verslag is een mooi overzicht van wetgeving en enkele cases die ook hier aan bod zijn gekomen. Daarnaast heeft hij interviews gedaan met diverse betrokkenen uit het veld.

Over zijn conclusies kunnen we kort zijn: meer organisaties zouden aan responsible disclosure moeten doen, maar een onafhankelijk meldpunt is niet de oplossing. Het zou te weinig daadkracht hebben en geen toegevoegde bescherming kunnen bieden aan melder of organisatie. Het gilde als certificerende instantie blijkt voor de meerderheid van de ondervraagden niet wenselijk. Die zouden een soort certificaat moeten geven aan de melding, maar aan de waarde daarvan wordt getwijfeld. Ethiek is nu eenmaal niet te meten. Voorlichting en uitwisseling van informatie zijn volgens Van Es wel wenselijk.

Nu, twee jaar later, is er nog steeds geen onafhankelijk meldpunt. In de tussentijd word ik nog benaderd door iemand van Stichting M, die onder andere achter Meld Misdaad Anoniem zit. De medewerkster is aan het verkennen of haar stichting misschien ook een hackersmeldpunt kan inrichten. Als we elkaar spreken over de telefoon doe ik me, zo goed als ik kan, voor als een hacker die op enigszins chaotische wijze een kwetsbaarheid meldt. Dan blijft het lang stil aan de andere kant van de lijn, waarop ze besluit dat zij hiervoor misschien niet de juiste expertise in huis hebben.

De site hackmeldpunt.nl is nog wel bemand en daar zitten wel beveiligingsexperts achter. Als ik daar een mailtje naartoe stuur, krijg ik meteen een reactie van Revspace bestuurslid Mark Janssen. Meldingen zijn welkom. Ze worden geanonimiseerd doorgezet naar de organisatie waar het lek is gevonden en verder wordt er niet gecorrespondeerd. Dat is jammer, want of zo’n over-

de-schuttingmodel werkt, is achteraf dan niet echt vast te stellen. Ik kan me ook voorstellen dat ethisch hackers graag horen wat er uiteindelijk gebeurt met hun melding en er ook iets van waardering voor willen krijgen.

Terug naar begin 2013, want er kwam nog meer beleid aan. Het CBP werd al vaker aangeroepen als mogelijke handhaver bij verantwoorde onthullingen. Illustratief daarvoor was het handhavingverzoek van Koot en consorten naar aanleiding van Krols onthulling. In februari komt het college zelf met een positiestuk: ‘Richtsnoeren van beveiliging persoonsgegevens’. Dit document is een stuk uitgebreider dan de leidraad en vooral een uitleg van hoe WBP-artikelen 13 en 16 moeten worden toegepast. Van belang is dat hier niet de hacker, maar de beheerder van de gegevens de maat wordt genomen.

Artikel 13 gaat over beveiliging van gegevens: “De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. (…) In het begrip ‘passend’ ligt besloten dat de beveiliging in overeenstemming is met de stand van de techniek. (...) Het begrip ‘passend’ duidt mede op een proportionaliteit tussen de beveiligingsmaatregelen en de te beschermen gegevens. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens.”

Artikel 16 gaat over bijzondere gegevens, waarbij je dus wat meer beveiliging mag verwachten. “Het gaat daarbij om persoonsgegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging en om strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.”

In deze richtsnoeren is te lezen dat informatiebeveiliging niet alleen gaat over techniek, maar vooral ook de organisatie er omheen. Het CBP adviseert: doe vooraf een risicoanalyse, pas

beveiligingsstandaarden toe en neem die mee in een plan-do-check-act-cyclus. Verder in het rapport lezen we dat informatiebeveiliging gaat om preventieve, detectieve, repressieve en herstelmaatregelen. Dat is allemaal wat abstract, maar gelukkig staan er ook wat voorbeelden bij, zoals waar je encryptie moet toepassen en hoe je moet omgaan met oude apparatuur. Toch zal het lastig zijn voor organisaties om te bepalen of ze aan de WBP voldoen en zo niet, wat voor maatregelen ze dan kunnen verwachten van het college.

Hoe handelde het college bij de cases in dit boek? Bij de OV-chipkaart werd duidelijk opgetreden toen vervoerders reisgedrag gingen volgen, maar niet toen de kaart gekraakt werd. Het college let blijkbaar op gebruik van persoonsgegevens en niet op fraude. Dat gold ook voor de SCADA-systemen: heel gevaarlijk voor de fysieke veiligheid, maar niet voor de persoonlijke levenssfeer. In de zaak Krol ging het wel om persoonsgegevens, zelfs gevoelige. Toen hij met vijf cijfers toegang kreeg tot medische dossiers bleek de beveiliging ervan niet echt passend bij de stand van de techniek, maar het CBP greep niet in. Dat is wellicht omdat Diagnostiek voor U zelf vrij snel handelde; de site uit de lucht haalde en een wachtwoordenbeleid met twee-factor authenticatie invoerde. Dat gold ook voor de Lektober zaken waar gevoelige gegevens vrij kwamen. Naast veel medische gegevens, zagen we daar ook gegevens over kredietwaardigheid, rechtszaken en seksuele voorkeuren. De techniek was dan wel niet ‘passend’, maar er werd wel direct gehandeld. Het Groene Hart Ziekenhuis staat op het moment dat deze richtsnoeren verschijnen onder toezicht van CBP, dus daar lezen we later nog over.

Deze cases werden het college aangereikt via de media, maar ze krijgt ook veel directe meldingen van burgers. Dat kan via mijnprivacy.nl, het telefonisch spreekuur en per post. Deze meldingen hoeven niet altijd te leiden tot actie. Volgens de richtsnoeren geven ze vooral “een beeld van de naleving van de wettelijke regels die toezien op de bescherming van persoonsgegevens en kunnen voor het CBP aanleiding zijn om een onderzoek in te stellen”. Het is een kwestie van prioritering van beperkte capaciteit: “Het aantal aangedragen zaken en de complexiteit daarvan neemt echter voortdurend toe, terwijl de

middelen die het CBP ter beschikking staan begrensd zijn. Het CBP kan derhalve niet alle zaken die worden aangebracht in behandeling nemen en moet keuzes maken. Het CBP geeft prioriteit aan zaken waarbij het een vermoeden heeft van ernstige, structurele overtredingen die veel mensen treffen en waarbij het CBP door de inzet van handhavingsinstrumenten effectief verschil kan maken."

Heeft het CBP het vermoeden dat een organisatie de Wbp onvoldoende naleeft, dan kan het college toezichthoudende bevoegdheden inzetten: inlichtingen en zakelijke gegevens vorderen, zaken en middelen onderzoeken (waaronder computerapparatuur) en ruimtes betreden, waaronder woningen. De overtreder moet dan volledige openheid van zaken geven en is verplicht mee te werken. Blijkt dan dat de organisatie handelt in strijd met de Wbp, dan kan het college bestuursdwang toepassen met een zogenaamde 'last onder dwangsom'. De verantwoordelijke krijgt dan te horen dat hij bepaalde beveiligingsmaatregelen moet treffen binnen een vastgestelde termijn. Doet hij dat niet, dan moet hij een bepaald bedrag betalen per dag dat de overtreding blijft voortbestaan. Dat kan oplopen tot een vooraf vastgesteld maximumbedrag.

Hoe hoog die bedragen kunnen of moeten zijn, is tot op de dag van vandaag onderwerp van discussie. Laatste stand van zaken (eind 2014) is dat de Kamer een wetsvoorstel bespreekt van staatssecretaris Fred Teeven van Veiligheid en Justitie. Daarin krijgt het CBP uitgebreidere boetebevoegdheden: maximaal 20.250 euro voor lichtere overtredingen en maximaal 810.000 euro voor de zwaardere. Daarnaast introduceert het wetsvoorstel een meldplicht voor ernstige beveiligingsinbreuken waarbij persoonsgegevens in het geding komen. Het voorstel voor een meldplicht datalekken rouleert echter al jaren tussen de Tweede Kamer, ministerraad, Raad van Staten en wie er nog meer betrokken zijn bij wetgeving. Inmiddels is er wel een meldplicht gekomen voor datalekken in de telecomsector, die lekken nu moeten melden bij de ACM. Ook organisaties die systemen beheren die behoren tot de vitale sectoren hebben nu een meldplicht en moeten dat doen bij het NCSC. Het CBP zal hier nog even op moeten wachten.

Na het verschijnen van de leidraad, deze richtsnoeren, de brief van het OM en reacties hierover in de media, is het op 29 mei 2013 weer tijd voor een Kamerdebat. Dat vindt dit keer plaats in de vaste commissie voor Veiligheid en Justitie met minister Opstelten. Zijn brief met leidraad, die de aanleiding is voor dit debat, is dan al bijna vijf maanden bekend. De minister en Kamerleden hebben dus ruim de tijd gehad om te kijken wat de rest van Nederland ervan vindt. Ook hier is het voornaamste punt van discussie dat ethisch hackers geen garanties krijgen met de leidraad en alsnog strafrechtelijk kunnen worden vervolgd. Verder is het interessant om te lezen hoe de deelnemers aan het debat elkaar proberen te overtuigen dat zij weten wat er leeft in de hackers scene.

Dijkhoff (VVD) begint en neemt het vooral op voor zijn partijgenoot: “Mijn fractie kan zich vinden in die richtlijn. Het lijkt mij goed dat mensen die goedwillend kwetsbaarheden blootleggen, daarvoor niet per se gestraft worden. Er moet wel altijd iemand zijn die beoordeelt of er inderdaad binnen de lijntjes of daarbuiten is gekleurd. Dit lijkt mij een aangewezen taak voor het OM. Als ik de stukken zo lees, lijkt het erop dat beide zijden echt moeten meewerken aan het systeem, dus ook de partijen bij wie de kwetsbaarheid geconstateerd wordt.”

Oosenbrug (PvdA) kiest duidelijk partij voor de helpende hackers: “Ik vind dat de ethisch hacker – wij spreken namelijk niet over de kwaadwillende hacker, maar over de beveiligingsexpert – te weinig beschermd is in responsible disclosure. Ik ga deze zomer naar een hackcongres in Nederland en zal daar via crowd sourcing – het klinkt allemaal heel interessant – bekijken of ik een initiatiefwetsvoorstel kan maken om de ethisch hacker te beschermen. Dit heeft wel te maken met het fenomeen ‘klokkenluiders’, maar valt daar net buiten. In deze tijd zijn wij heel erg bezig met het beschermen van bedrijven. Een bedrijf wil bekijken wat er misgaat en waar de kwetsbaarheden zitten, ook al heeft het geen geld om constant beveiligingsexperts in te huren. Iemand die voor zijn hobby of beroep hackt, zou dit kunnen doen, maar dan wel goed beschermd. Wij zouden daar allemaal veel meer over moeten nadenken. Ik denk dat een initiatiefwetsvoorstel de beste weg hiervoor is en kondig dat bij

dezen aan.” Dat voorstel is er niet gekomen, maar haar stelling is duidelijk.

Gesthuizen (SP): “Overal waar je komt, bij welke club met ICT-experts je ook je licht opsteekt, er wordt steeds gehamerd op samenwerking, publiekprivate samenwerking, samenwerking met de hackerscommunity of met mensen die al dan niet toevallig lekken in de beveiliging tegenkomen. Steeds wordt daarop gehamerd. Ik spreek mijn zorg hierover uit, omdat ik van diverse bronnen begrijp dat er in de hackerscommunity grote zorgen zijn over de leidraad voor responsible disclosure. Ik vraag mij dus ook af of en hoe intensief er overleg en samenwerking is geweest met die hackersgemeenschap bij het opstellen van deze richtlijn.”

Opstelten benadrukt in zijn beantwoording van deze vragen vooral hoe ver we inmiddels zijn gekomen: “Je kunt zeggen dat wij met het publiceren van de leidraad om te komen tot de praktijk van responsible disclosure wereldwijd tot de koplopers behoren. Dank voor de support daarbij. (…) Zoals ik al eerder zei, juich ik de samenwerking met de ICT-community toe. Bij het uitwerken van het kader voor responsible disclosure is dan ook met diverse partijen en potentiële melders gesproken.”

De minister bekent zelf ook wel een beetje ethisch hacker te zijn: “Hierbij moet opgemerkt worden dat er binnen de overheid al ervaring is opgedaan met het werken met hackmethodes. Ik had twee jaar geleden niet kunnen vermoeden dat ik die nu ook een beetje zou kunnen hanteren. Ik heb het zien gebeuren, zo snel gaan die ontwikkelingen, ook bij mijzelf. Ik zie blikken van herkenning bij u allen, dus ik hoop dat u, als u die methode wilt hanteren, dat te goeder trouw doet.”

Opstelten houdt wel vast aan zijn positie over computervredebreuk: “Hackers zijn in de kern, als zij kwade bedoelingen hebben, natuurlijk inbrekers. Er moet dus een scheiding worden gemaakt tussen hackers die te goeder trouw zijn en hackers die dat niet zijn. Dit heb ik altijd al gezegd en herhaal ik vandaag. Hackers dienen binnen de juridische kaders te vallen.” Dat betekent niet dat ze zomaar worden opgepakt, sterker nog: “Er zijn overigens geen gevallen bekend waarin het OM is overgegaan tot vervolging terwijl het betreffende bedrijf en de melder op basis van responsible disclosure met elkaar overeen

waren gekomen dat er geen aangifte zou plaatsvinden. Ik ga er dus van uit dat dit de lijn is van het OM."

Kern van de zaak is dat hij als minister het nut ziet van ethisch hacken, maar niet in de weg wil lopen van het Openbaar Ministerie: "Het OM beslist zelf. Ik breng de interne richtlijn van het OM ter informatie aan de Kamer. Ik ben natuurlijk verantwoordelijk voor het OM, maar dit bepaalt het OM zelf. Ik neem aan dat de criteria uit de leidraad worden meegenomen om de proportionaliteit te beoordelen, ook als er geen beleid is. Jurisprudentie zal dit moeten bevestigen."

Daar neemt Oosenbrug geen genoegen me: "Wat ik hoor, is hetzelfde als waar ik me zorgen over maak: de vrijblijvendheid. Een bedrijf kan kiezen om zelf iemand te vragen om eens naar de systemen te kijken. Als een ethisch hacker vervolgens een kwetsbaarheid tegenkomt in de software of in het systeem en dat bedrijf is chagrijnig omdat die kwetsbaarheid is ontdekt, kan het dan besluiten om alsnog die ethisch hacker te vervolgen, die verder helemaal niets stuk maakt maar alleen het probleem aantoont? Kan hij in een dergelijk geval alsnog vervolgd worden ook al vindt het OM eigenlijk van niet? Ik ben echt op zoek naar bescherming voor de ethisch hacker. In de richtlijn lijkt het namelijk alsof de bedrijven heel erg beschermd zijn en de ethisch hackers helemaal niet."

We moeten dus nog maar zien hoe deze leidraad gaat uitwerken in de praktijk. Gesthuizen vraagt daarom of er ook een evaluatiemoment komt. Opstelten: "De hele wereld komt naar ons kijken omdat wij de eerste overheid zijn die een richtlijn heeft ontwikkeld. Ik denk dat een evaluatie vanzelfsprekend is." Hij stelt voor dat ze na twee jaar kijken hoe het ervoor staat. Gesthuizen vindt dat te lang duren en wil liefst jaarlijks evalueren. Dat is volgens Opstelten geen evaluatie, maar een monitor. Die kan ze krijgen. Verder krijgt de Kamer jaarlijks het Cyber Security Beeld Nederland, met daarin ook een verkenning van "de rol van hackers bij het op verantwoorde wijze inventariseren van kwetsbaarheden en het voorgenomen gebruik van de input van hackers". Geen wetswijziging dus, maar wel veel kennisuitwisseling en goede intenties.

In juni 2013 verschijnt CSBN 3, waarin nog bescheiden wordt gemeld dat nu de leidraad is gepubliceerd, het aan organisaties is hun eigen beleid te formuleren. Verder meldt het rapport dat bij het NCSC de eerste meldingen binnenkomen, vooral over hun eigen site en enkele over anderen, maar het is nog te vroeg om daar conclusies uit te trekken. De CSBN 4 van september 2014 gaat veel uitgebreider in op responsible disclosure. Er zijn dan al bijna honderd meldingen binnengekomen, met sterke aanwijzingen dat dit komend jaar zal toenemen. Driekwart van de kwetsbaarheden gaat over websites, in het bijzonder Cross Site Scripting. De exacte getallen zijn wat lastig, want sommige meldingen blijken geen echte kwetsbaarheid te onthullen en soms komen verschillende melders met eenzelfde kwetsbaarheid.

Op 18 december 2014 krijgt de Tweede Kamer weer een brief van Opstelten over de voortgang van responsible disclosure. Het staat er volgens de minister goed voor. De Rijksoverheid heeft nu beleid voor meldingen over hun eigen websites. De Rijksdienst en de Belastingdienst hebben hun eigen meldpunten ingericht en capaciteit gereserveerd om tot snelle oplossing van kwetsbaarheden te komen. Ook de private partijen doen mee. De telecomsector en de banken waren er als eersten bij om te werken volgens de leidraad. Nu hebben ook de verzekeraars en hosting providers als sectoren responsible disclosure ingevoerd.

Bij NCSC staat de teller inmiddels op 136 meldingen: 66 voor diensten van de overheid, 34 voor NCSC zelf en 36 waarbij het centrum bemiddelde tussen de melder en een private partij. Bij de Rijksdienst kwamen er nog eens 55 binnen en bij de Belastingdienst 22. Kortom: “De cijfers laten zien dat met responsible disclosure in de afgelopen twee jaar aanmerkelijke stappen zijn gezet. Twee jaar geleden was Nederland het eerste land in de wereld dat de stap van het actief uitdragen van responsible disclosure heeft gezet. Deze stap is gezet in een gezamenlijke beweging van overheid, private partijen en spelers binnen de bredere ICT-community”, aldus Opstelten.

Over het vervolgen van ethisch hackers schrijft hij kort: “Het OM heeft in 2013 en 2014 geen vervolging ingesteld naar melders die conform het RD-beleid van de desbetreffende organisaties handelden.” In die periode speelde ook het Groene Hart

Ziekenhuis. Het uiteindelijke vonnis van de rechter verschijnt vrijwel tegelijkertijd met deze brief van Opstelten. In de volgende hoofdstukken zullen we zien of dit meer duidelijkheid geeft over wat wel en niet mag bij ethisch hacken.

18. De achterkant van het Groene Hart

Hacker en gehackten twee jaar in onzekerheid

Terwijl begin 2013 veel betrokkenen uit dit verhaal druk aan het discussiëren zijn over de zojuist verschenen leidraad, is Team High Tech Crime van de Nederlandse politie aan de slag gegaan met Jordy's computer. De digitaal rechercheur die zich ontfermt over de apparatuur weet zich toegang te verschaffen middels brute forcing: na behoorlijk wat willekeurige wachtwoorden te proberen komt hij erin. De rechercheur vindt een chatgesprek van 1 oktober 2012 tussen Jordy en een familielid. Jordy vraagt in die chat of de gevonden gegevens van hem zijn. Het gesprek gaat ook over een bekende Nederlander die in de bestanden van het Groene Hart Ziekenhuis zou staan. In een andere chat wordt gesproken over een bestand met 500k gegevens. Sporen wijzen uit dat Jordy ook gebruik heeft gemaakt van de Zweedse VPN-dienst, 'VPN Tunnel'. De rechercheur vindt slechts één bestandje dat van het GHZ zou kunnen zijn, verder niets. Jordy had alles namelijk opgeslagen op een virtuele machine en die later verwijderd.

Volgens de Fox-IT-monitor was er op 5 en 6 oktober maar liefst 7,5 GB aan data vanaf de server van het ziekenhuis gedownload via een andere VPN-dienst, maar hier vindt de rechercheur geen sporen van. Juist daar was het OM naar op zoek. De zaak draaide niet alleen om computervredebreuk, maar ook om de vele mogelijk gedupeerde patiënten wiens gegeven op straat lagen. Jordy had in het verhoor al aangegeven daar niets van te weten. Ook van de gebruikte VPN-dienst waren op zijn computer geen sporen terug te vinden. Er was dus geen enkel bewijs dat Jordy ook achter de tweede hack zou kunnen zitten.

De rechercheur zoekt verder, want hij wil weten of er misschien bestanden verborgen zijn en gokt dat Jordy gebruik heeft gemaakt van het programma Truecrypt. Met Truecrypt kun je bestanden versleuteld opslaan in een afgebakend gedeelte van

een harde schijf, een container. De versleutelde bestanden komen pas tevoorschijn wanneer je het juiste wachtwoord intypt. Na lang zoeken vindt de rechercheur inderdaad een Truecryptcontainer op Jordy's computer. Deze container laat na het openen echter slechts een paar kleine bestanden zien, terwijl de totale omvang ervan behoorlijk groot is. Er zouden dus nog meer verborgen bestanden kunnen zijn. Na een maand lang regelmatig wachtwoorden uitproberen, raadt de rechercheur uiteindelijk een tweede wachtwoord, dat een variatie is op het eerste wachtwoord.

Het tweede wachtwoord biedt toegang tot een verborgen gedeelte van de Truecryptcontainer. Nadat de rechercheur dit gedeelte opent, treft hij bestanden aan met vreemde bestandsextensies, zoals .kpv en .kpi. Het lukt hem uiteindelijk om die bestanden te openen. Het blijken foto's en video's te zijn. De rechercheur schrikt als hij de beelden ziet: de verdachte blijkt kinderporno op zijn computer te hebben staan. Hij draagt de bestanden daarom direct over aan het team Bestrijding Kinderporno en Kindersekstoerisme van de Landelijke Eenheid. Uit hun collectiescan, oftewel het geautomatiseerd analyseren van de beelden, blijkt dat het gaat om grote hoeveelheden grove kinderporno. De zaak, die de naam 'Magneto' meekrijgt, zal daardoor flink wat langer gaan duren. De hack van het ziekenhuis wordt daarin aangeduid als 'feit 1', het bezit van de kinderporno als 'feit 2'.

Het Openbaar Ministerie brengt het nieuws 21 maart 2013 naar buiten, wellicht om aan te geven dat de zaak wat gecompliceerder ligt dan eerder gedacht en het daarom wat langer gaat duren. De meeste betrokkenen die tot dan toe een duidelijke mening hadden over de zaak raken hierdoor in verlegenheid. Kan iemand die dergelijke verschrikkelijke beelden bezit en dus waarschijnlijk ook met plezier bekijkt, wel voldoende moreel besef hebben om ethisch hacker te zijn? Of gaat het hier om twee zulk verschillende handelingen dat je die ook echt als afzonderlijke zaken moet behandelen?

Zelf ben ik daar nog steeds niet helemaal uit, maar ik besluit na anderhalf jaar wikken en wegen dat het voor mijn onderzoek toch van belang is om ook het verhaal van de verdachte te horen.

In de media is niet meer over hem bekend dan zijn leeftijd en waar hij woont. Brenno de Winter wil niets over hem kwijt, want hij kan als journalist zijn bronnen niet prijs geven. Het OM wil me natuurlijk ook niet in contact brengen met de verdachte, want het onderzoek loopt nog. Dan hoor ik tijdens een borrel na een bijeenkomst iemand de naam Jordy noemen en dat “die hacker nu nota bene een eigen IT-securitybedrijfje runt”. Na lang zoeken vind ik een bedrijf dat voldoet aan het profiel. Via de Kamer van Koophandel krijg ik een telefoonnummer en besluit te bellen.

“Hallo met Jordy”, hoor ik aan de andere kant van de lijn. Ik vertel hem over mijn onderzoek en dat ik graag ook zijn kant van het verhaal hoor. Dat vindt hij prima, maar hij wil wel eerst met zijn advocaat overleggen. De zitting van de zaak is namelijk over drie weken en hij vraagt zich af wat het effect van zo’n interview is op de zaak. Ik stel voor hem te mailen wat ik tot nu toe heb en welke vragen ik aan hem wil stellen. Dan verneem ik later wel of het interview doorgaat of niet. Dat is goed. In mijn mail vertel ik wie ik allemaal nog meer interview voor de zaak Groene Hart Ziekenhuis en dat betrokkenen altijd de gelegenheid krijgen de citaten te controleren en aan te passen. Mocht hij het interview liever na de rechtszaak doen, dan is dat ook goed.

De volgende dag reageert hij en schrijft: “Mijn advocaat is donderdag weer in Nederland, dan kan ik vragen of het een goed idee is, maar ik denk van wel. Er zijn wel een paar dingen die ik graag wel duidelijk wil hebben. Ik wil graag meewerken, maar wel anoniem of anders alleen met mijn voornaam. Tijdens de rechtszaak in december zal ik tegelijkertijd ook voor iets anders (veel ergers) terecht staan en wil daar geen of zo minder mogelijk ‘pers’ bij hebben. Het zou fijn zijn als hier verder niets over in de publicatie wordt vermeld. En nog een vraag waar je als onderzoeker geen antwoord op hoeft te geven, maar hoe kom je aan m’n naam en nummer?” Als ik na een paar dagen nog geen reactie heb, besluit ik weer te bellen. Helaas, zijn advocaat vindt het toch niet zo’n goed idee. Ik moet het dus voorlopig doen met het verhaal van de andere betrokkenen.

Op 18 november 2014 bezoek ik het Groene Hart Ziekenhuis. Het is een groot, deels nieuw gebouw in het centrum van Gouda. Bij

de receptie word ik ontvangen door Gelske Nederlof, de Manager Marketing en Communicatie en een van de leden van het crisisteam van destijds. We gaan naar de kamer van de leider van het crisisteam: Monique Verdier, lid van de Raad van Bestuur, dan acht jaar werkzaam bij het Groene Hart Ziekenhuis en daarvoor tien jaar manager bij diverse andere ziekenhuizen. Opvallend is haar technische achtergrond. Na haar opleiding aan de Technische Universiteit Eindhoven was ze namelijk tien jaar fabrieksdirecteur.

We zitten in dezelfde kamer waar het team destijds bijeen kwam. Als ik de dames vertel over mijn onderzoek en boek ‘Helpende hackers’, word ik meteen gecorrigeerd. “Nou, dit was geen helpende hacker hoor”, roept Verdier. “Inderdaad”, beken ik, “deze was ook zeker te ver gegaan. Daarom staat hij 3 december in de rechtbank. Maar de vraag is vooral of het heeft geholpen jullie securitybeleid te verbeteren.” “Dat wel, maar ten koste van wat?”, zeggen de dames tegelijk. Ze wisten destijds inderdaad dat de veiligheid niet helemaal op orde was. Er liep ook al een traject om dat in fasen te verbeteren. Nu moest alles ineens versneld en dat heeft veel geld gekost. Verdier: “Het heeft ook invloed op al het werk hier. Alles gaat langzamer. We hebben bijvoorbeeld nog steeds geen online afsprakensysteem.”

Verdier vertelt over 7 oktober, zoals beschreven in hoofdstuk 14 en hoe ze daarna te werk zijn gegaan. Het was een hectische tijd, waarin ze veel hadden aan de crisisoefening die ze twee weken daarvoor hadden gehad. Nederlof: “Echt een drama waarbij plannen niet werkten omdat de situatie steeds veranderde. Dat hielp in de bewustwording dat de wereld buiten sneller gaat dan die binnen. Dat is de redding geweest voor de echte crisis twee weken later.” Verdier: “De eerste vergadering na de digitale inbraak die zondag was heel rommelig. Hoe gaan we om met dingen? Ik ging daarom structureren, overzicht maken en problemen afhandelen. Heb geprobeerd het heel strak te leiden, terwijl Dirk Jan, onze bestuursvoorzitter destijds, naar buiten toe het woord voerde.” De kroon op haar werk vond Verdier de vierde vergadering, op de donderdag na de melding. “De ICT-jongens hadden een slagroomtaart voor de afdeling communicatie, omdat ze vonden dat zij het zo goed hadden gedaan. Klinkt misschien

als iets onbelangrijks, maar het gaf aan dat we niet elkaar de schuld gaven en het met elkaar wilden oplossen."

In de periode erna moesten ze niet alleen snel de beveiliging op orde brengen, maar alles werd ook nog eens nauwlettend in de gaten gehouden door het College Bescherming Persoonsgegevens. Er werd ook flink geïnvesteerd. Fox-IT was al voor de hack aan de slag om de beveiliging te verbeteren. PricewaterhouseCoopers werd ingeschakeld door het bestuur om de organisatie door te lichten. Deloitte leverde een groep ICT'ers om de vorderingen aan het CBP te rapporteren. In totaal heeft het beveiligingstraject vijf miljoen euro gekost. Dit had het ziekenhuis anders ook wel uitgegeven, maar minder snel. De extra kosten, die direct te relateren zijn aan de hack, schat het GHZ op 300.000 euro, met name kosten voor beveiliging en juridisch advies. Verdier: "Dat is dus geld dat we anders niet hadden uitgegeven. Dit staat gelijk aan zes verpleegkundigen een jaar in dienst hebben. De gevolgen van de hack zijn dus zeker maatschappelijk onverantwoord te noemen."

Het CBP-traject dat erop volgde, bleek behoorlijk zwaar voor het ziekenhuis. Verdier: "Elk antwoord roept weer tien vragen op. Alles ging zes keer heen en weer. In januari is de wet aangepast, dus kwamen er meer vragen. Alles ging door elkaar lopen: privacy, veiligheid, projectmanagement. Natuurlijk begon het in het GHZ. We hadden het 'badkamerraampje' niet open mogen laten staan!" Maar, "Het CBP vroeg ook dingen die onacceptabel waren. Bijvoorbeeld over de end-of-life software. Het kwam er uiteindelijk op neer dat we naar de VS moesten, naar Microsoft, omdat er daar iets moest veranderen. Dit is natuurlijk geen reële verwachting. We zitten hier met end-of-life systemen, waar ook de leverancier niks mee kan. CBP heeft dit uiteindelijk ingezien, waardoor we vooralsnog geen boete krijgen. Voor eind 2014 moeten we nog twee of drie dingen doen die marginaal zijn. Dan voldoen we volledig aan artikel 13."

Enkele van de meer specifieke systemen bij het ziekenhuis draaien dan nog op Windows XP of Windows 2000. Beide worden inmiddels niet meer geüpdate door Microsoft en zijn zoals dat heet 'end-of-life'. Gebruikers wordt dan geadviseerd over te stappen op een hogere Windows versie, maar dat kan niet altijd

omdat de applicaties die erop draaien dat niet trekken. Je kunt dan als individuele gebruiker nog wel een update van Microsoft kopen, maar dat is natuurlijk niet de bedoeling. Verdier is daarom ook kritisch naar het CBP: “Ik krijg er pijn in mijn buik van dat CBP drie plaatsen achter de komma kijkt, terwijl de overheid zelf de end-of-life van XP kan afkopen.”

Maar Verdier is een optimistisch mens en kan al terugkijkend toch ook nog wel inzien dat ze er als organisatie wat van geleerd hebben. Security is niet alleen doorgedrongen tot het bestuur en managementteam, maar ook bij de artsen in het ziekenhuis: “Vroeger kwamen ze leuren om elk nieuw ICT-speeltje geïmplementeerd te krijgen. Nu komen ze vragen: mag dit?” Het netwerk van het ziekenhuis wordt zoals dat heet gesegmenteerd: niet een systeem waar iedereen van alles op kan doen, maar elk zijn eigen omgeving. De artsen kunnen nu met hun eigen pasje op verschillende computers inloggen en komen zo in hun eigen digitale werkplek, waar alleen de programma’s draaien die zij gebruiken. Bijkomend voordeel was dat het ziekenhuis daarmee ook het aantal softwarepakketten kon schrappen van 900 naar 287.

Het GHZ heeft later ook nog een congres georganiseerd waar Verdier beschreef wat er allemaal gebeurd was. Een soort lessons learned voor andere zorginstellingen. Die openheid moest wel gepaard gaan met een zekere beslotenheid. Deelnemers werden gecontroleerd aan de deur en alleen toegelaten als ze zich konden identificeren en de uitnodiging van de Raad van Bestuur lieten zien. Verdier: “We hadden geen zin meer in nog een keer Brenno.”

Na dit gesprek lijkt het me goed om eens de kant te horen van het CBP. Waarom duurt het traject zo lang? We zijn immers twee jaar verder en er is nog steeds geen eindrapport. Het hoofd communicatie aldaar, Koosje Verhaar, vertelt me dat het CBP in zo’n geval niet in één keer een definitief oordeel opstelt. Eerst komt er een rapport met de voorlopige bevindingen, waar de onderzochte organisatie op kan reageren en maatregelen kan nemen, die ook weer onderzocht moeten worden. Pas daarna worden de definitieve bevindingen opgesteld.

Op 27 november 2014 komt eindelijk het CBP-rapport uit en Verhaar mailt het me die dag nog. Er zit ook een linkje bij naar NU.nl. Daar schrijft Brenno de Winter: “Het Groene Hart Ziekenhuis in Gouda had lang de beveiliging van computersystemen niet op orde en overtrad daarmee de wet.” Ik verwacht een spannend rapport, maar het blijkt een nogal warrig verhaal, waarschijnlijk omdat het zo vaak is herschreven na elke feedbackronde. Op zich is het doel van het CBP duidelijk: “te onderzoeken of het GHZ voldoende passende technische en organisatorische maatregelen ten uitvoer brengt om de (medische) persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking.” Het is ook helder wat voor hen de aanleiding was: het bericht op NU.nl van 7 oktober 2012 – al had het ziekenhuis ook zelf het lek gemeld bij het CBP. Maar wat er nu precies mis was bij het ziekenhuis en wanneer dat opgelost is, blijft onduidelijk.

In het rapport is te lezen dat er veel contactmomenten zijn geweest en hoe telkens de wederzijdse beweringen worden bijgesteld. Zo was er onenigheid over waar het ziekenhuis aan moest voldoen. Het onderzoekstraject startte eind 2012, terwijl begin 2013 de ‘richtsnoeren beveiliging persoonsgegevens’ van het CBP uitkwamen. Het ziekenhuis is van mening dat gaandeweg het traject de eisen worden aangescherpt, terwijl het CBP de richtsnoeren slechts ziet als een verduidelijking van normen die al eerder van kracht waren, te weten artikelen uit de WBP en de NEN-7510, die aanwijzingen geeft voor het toepassen van de Code voor informatiebeveiliging NEN-ISO/IEC 27002.

Het rapport is gebaseerd op de bevindingen van het CBP tot en met begin 2014. Inmiddels is het november en is het beveiligingsproces in het GHZ al weer vele fasen verder. Hoe dan ook, in het rapport stelt het college dat het ziekenhuis tekort schiet omdat nog steeds niet alle oude systemen zijn uitgefaseerd. De term ‘end-of-life’ komt maar liefst veertig keer voor in het rapport. Bovendien stelt het CBP dat het netwerk nog niet volledig is gesegmenteerd, waardoor veiligheidsrisico’s snel kunnen overslaan van een deel naar een ander. De vraag is wanneer dat verholpen zal zijn en welke organisatorische maatregelen in de tussentijd ervoor zorgen dat het niet weer misgaat. Die vraag

wordt in het rapport niet eenduidig beantwoord, maar het GHZ geeft in een reactie aan het CBP aan dat eind 2014 alle maatregelen geïmplementeerd zullen zijn.

In het rapport bevestigt het CBP dat er al veel maatregelen genomen zijn sinds de hack in 2012, maar dat pas na een paar jaar alles echt klaar is. Sinds de hack wordt wel al het digitale verkeer gemonitord op verdachte handelingen. Pentesten hebben geen zin: het GHZ en de digitale adviseurs van Fox-IT weten waar de kwetsbaarheden zitten en ze willen de boel niet nog onveiliger maken. Het CBP besluit in haar oordeel “dat het GHZ in elk geval tot april 2016 in strijd handelt met artikel 13 Wbp door gebruik te maken van een niet gesegmenteerd netwerk waarop apparatuur met end-of-life (besturings)software is aangesloten. Het GHZ heeft onvoldoende aanvullende maatregelen getroffen om de risico’s te beperken of weg te nemen.”

Maar, krijgen ze nu een boete of niet? Ik mail daarom weer met Verhaar. Ze schrijft: “Het CBP zal de komende tijd controleren of het ziekenhuis de overtredingen heeft beëindigd en kan zo nodig handhavende maatregelen inzetten. We kunnen dus nog geen uitspraken doen over een eventuele sanctie. Zodra we daarover wel wat kunnen openbaar maken, zullen we je dat laten weten. Overigens kunnen we tot op heden nog geen directe boetes opleggen, wel een last onder dwangsom. Dan krijgt de verantwoordelijke een periode om de geconstateerde overtredingen te beëindigen en als dat niet gebeurt, moet de verantwoordelijke een bedrag betalen.” Veel is dus nog onzeker, eind november 2014. Niettemin was de timing van het rapport, toevallig of niet, perfect. Want de week erna is de rechtszaak.

19. Bonnie van de hackende niet-zo-huisvrouwen

Zware rechtszaak leidt tot heldere jurisprudentie

In de voorgaande hoofdstukken zijn al aardig wat rechtszaken uitgebreid beschreven, op basis van rechtbankverslagen. Nu kon ik er één in het echt meemaken. Op 3 december 2014 loop ik het Paleis van Justitie binnen en vraag ik aan de balie waar ik moet zijn voor rechter Frenkel, die volgens de afdeling voorlichting de zaak van Jordy zal behandelen. Vervolgens moet ik door een metaaldetector en word ik gefouilleerd. Gelukkig mag mijn laptop mee, want ik wil wel aantekeningen maken. Na nog een paar balies kom ik uiteindelijk uit op een publieke tribune. De zaak is net begonnen. Ik ben de enige op de tribune en zie door het glas zes mensen in toga achter bureaus zitten. De vrouw in het midden is iets aan het voorlezen. De rest van de mensen zie ik van achter. Wie Jordy is, is wel duidelijk. Hij zit in het beklaagdenbankje.

De vrouw in het midden blijkt rechter Frenkel en ze is bezig met wat heet de ‘behandeling feiten’. Ze begint met feit 1 en na een opsomming van alles wat ook in het nieuws te lezen was, vraagt ze aan Jordy: “Hoe bent u te werk gegaan?” Hij vertelt dat hij ook zelf bij het ziekenhuis stond ingeschreven en wilde testen of hun beveiliging in orde was. Ik hoor in de manier waarop hij de technische details beschrijft enige twijfel of het wel overkomt bij de zittende magistratuur. Maar uit de ondervraging van Frenkel maak ik op dat zij in ieder geval behoorlijk op de hoogte is.

Ze wil vooral duidelijkheid over wat, wanneer is gedownload. Het csv-bestand met de half miljoen namen en adressen van patiënten blijkt op 6 oktober te zijn gedownload. Jordy moet daar dus ook verantwoordelijk voor zijn geweest, want het is ook genoemd in het artikel op NU.nl, maar hij ontkent. Na wat gerommel in de verslagen blijkt dat het twee keer is gedownload,

namelijk ook een keer op 26 september. Dat was hij wel en dat kan hij onderbouwen, want hij noemt de 500k in de chat van 1 oktober. Waarom zou hij het daarna nog een keer downloaden? Die tweede keer moet iemand anders zijn geweest. De rechter lijkt voorlopig overtuigd.

Vervolgens krijgen ze een discussie over malware. Volgens Jordy is het bestand dat hij stuurde om de data te downloaden geen malware, volgens haar wel. Ze vertelt dat er ook een Trojan Horse was gedetecteerd. Was die ook van hem? Nee, maar wat volgens Jordy gebeurd kan zijn, is dat zijn hack een virusscanner heeft geactiveerd die vervolgens een Trojan detecteerde die er al op stond. Frenken vraagt ook waarom hij, als hij toch geen kwaad in de zin had, zich verborg achter een VPN-verbinding. Jordy antwoordt dat hij liever de politie voor de deur heeft dan een knokploeg van het ziekenhuis. Er volgt rumoer in de zaal.

Dan vraagt ze waarom hij zijn vondst op deze manier heeft onthuld, via een journalist en niet bijvoorbeeld via de politie of het CBP. “Nou, het heeft wel geholpen”, zegt hij laconiek, waarop de rechter vraagt: “Zou u het zo weer doen?” Als hij “ja” zegt, schrikt ze zichtbaar en waarschuwt ze Jordy dat hij hier wel op zitting zit voor een misdrijf. “Maar nu zou ik het wel via het NCSC doen”, mompelt hij er snel achteraan. Frenken lijkt weer gerustgesteld.

Ik probeer zo snel als ik kan te typen en het gesprek bij te houden, maar mis de helft. De rechter zegt iets over een schade en ineens zie ik een lange man opstaan die begint te praten. Ik hoor hem nauwelijks en probeer toch nog iets op te vangen door mijn oor tegen het glas te drukken. De rechter onderbreekt hem: “Sorry, kunt u in de microfoon spreken? Ik zie iemand op de tribune die u blijkbaar niet kan verstaan.” Ik schaam me rot dat ik het al zo beladen proces verstoor en verschuil me weer snel achter mijn laptop.

De man blijkt Maarten Baaij te zijn, de directeur financiën en ICT van het Groene Hart Ziekenhuis die destijds ook in het crisisteam zat. Hij dient een schadevergoeding in van 300.000 euro. De rechter protesteert dat zij en ook de verdediging nog geen stukken hebben ontvangen waarin het bedrag wordt onderbouwd. Ze vraagt aan de collega’s links en rechts van haar of de zitting hierom geschorst moet worden. Nee, we kunnen door

en Baaij wordt gevraagd uit te leggen hoe hij aan het bedrag komt. Het zou gaan om de kosten die direct gemoeid zijn met de hack: de uren van personeel van het ziekenhuis en de extra uren van Fox-IT, PWC en Deloitte. De rechter is niet geheel overtuigd, want ze vraagt zich af waar die uren dan precies aan besteedt zijn, maar laat het hier verder even bij.

Daarna volgt behandeling van feit 2, dat ik hier terzijde laat. Wel is te merken dat hiermee de stemming in de zaal omslaat. Zeker als hierna het onderdeel ‘achtergronden’ volgt waarin uitgebreid Jordy’s privéleven uit de doeken wordt gedaan. Ook daar zal ik verder niet over uitwijden. Daarna is het pauze en verlaat iedereen de zaal.

In de hal zie ik een stuk of vijftien mensen de rechtszaal uitkomen. De stemming is bedrukt en iedereen kijkt wat verdwaald om zich heen. Ik besluit op Jordy af te gaan en stel me aan hem voor. Naast hem staat een jonge vrouw. Het blijkt zijn zus te zijn die daar is om hem te steunen in dit proces. Zijn advocaat komt er ook bij staan. Ik voel me behoorlijk opgelaten om tijdens zo’n zware zaak (feit 2) te beginnen over ethisch hacken (feit 1), maar merk al snel dat de omstanders het eigenlijk wel prettig vinden om het over iets luchtigers te hebben. Ik vertel snel iets over andere zaken, zoals de OV-chipkaart en Henk Krol en vraag de advocaat welke jurisprudentie hij gaat aanhalen. Inderdaad, Krol is de juiste zaak, want het gaat hier om vrijheid van meningsuiting. Dan loopt het drietal weg voor overleg.

Ik kijk om me heen wie er nog meer zijn. De mensen van het Groene Hart Ziekenhuis zijn helaas weg. Graag had ik even met Baaij gesproken om zijn kant van de zaak te horen. Dan word ik herkend door drie mannen van Team High Tech Crime, die ik nog ken van mijn praatprogramma en verwonderd vragen ze wat ik als presentator hier doe. Ik begin enthousiast over mijn boek te vertellen en dat zij er ook in voor komen, maar dan gaat de bel. We moeten weer naar binnen. Een van de mensen in toga roept dat ik ook best beneden mag komen zitten, dus loop ik met iedereen mee.

In de zaal gaat iedereen om de een of andere reden links zitten. Dus ga ik rechts zitten, want daar is de meeste plek. Als de

rechter vanaf achter de zaal betreedt, gaat iedereen ineens weer staan. Een van de agenten gebaart me dat ik dat ook moet doen. Blijkbaar hoort dat in een rechtszaal. Dan pas zie ik dat iedereen achter de medewerkers van het Groene Hart Ziekenhuis zit en ik, als enige, achter Jordy en zijn zus. Hopelijk is dit niet ook een van de gewoonten in een rechtszaak, want het laatste wat ik hier wil is partij kiezen. Hoe dan ook, de zaak wordt hervat en iedereen gaat weer zitten. De rechter meldt eerst kort dat het Groene Hart Ziekenhuis de schadeclaim laat vallen. Daarna geeft ze het teken aan de officieren van justitie om hun aanklacht toe te lichten. Er zijn er twee, één voor elk feit.

Danielle Laheij, landelijk officier van justitie cybercrime, behandelt feit 1 en ze begint met het voorlezen van haar requisitoir. “Het is zondag 7 oktober 2012 als een van de moderne nachtmerries van een ziekenhuis waarheid lijkt te worden. Er wordt publiekelijk bekend gemaakt dat het Groene Hart Ziekenhuis is gehackt en dat er mogelijk gegevens van talloze patiënten via het internet toegankelijk waren.” Dan volgt een samenvatting van het artikel in NU.nl, waarbij ze de naam “Bonnie” telkens uitspreekt met duidelijk cynisme en Jordy aankijkt als ze vervolgt: “van de hackende niet-zo-huisvrouwen”.

Laheij schetst vervolgens de maatschappelijke context: “De hack en publicaties erover zorgen voor veel onrust, uiteraard met name bij patiënten van het Groene Hart ziekenhuis, maar ook in de maatschappij als geheel. Een algehele discussie barst los, over veiligheid van medische gegevens, maar vooral ook over de rol van de hacker.” Ze erkent dat er zowel begrip als verontwaardiging was voor het onderzoek en de aanhouding door het OM. De berichtgeving varieerde van ‘hackende held’ tot ‘cybercrimineel’. Ook politiek was er bemoeienis en er werden door Kamerleden en een enkele minister uitspraken gedaan over de zaak. Maar, relativeert ze, die waren toen natuurlijk nog niet op de hoogte van wat er allemaal aan de hand was.

Volgens haar is in de eerste plaats van belang te achterhalen wat er was gebeurd met de gedownloade gegevens van de patiënten. Zekerheid hierover kan alleen worden verkregen door aanhouding van de dader. Daarom deed het ziekenhuis aangifte,

mede op advies van Fox-IT, politie, justitie en het NCSC. Dan stopt ze met voorlezen en richt ze zich weer tot Jordy: “An sich heeft het Groene Hart Ziekenhuis het volste recht de schade te verhalen, dus je mag van geluk spreken dat zij hun vordering van drie ton laten vallen.”

De zaak dient volgens de officier ook een hoger doel, namelijk helderheid krijgen over ethisch hacken. Ze stelt: “Het is goed wanneer kwetsbaarheden bij zorggerelateerde instellingen aan het licht worden gebracht. Dat neemt niet weg dat, indien het aantonen van kwetsbaarheden gepaard gaat met een strafbaar feit, dit strafrechtelijk kan worden onderzocht door het OM. Dit vloeit voort uit het zeer zwaarwegend maatschappelijk belang dat gemoeid is met de bescherming van gevoelige persoonsgegevens zoals medische informatie.” Het Openbaar Ministerie had volgens haar niet kunnen optreden tegen het Groene Hart Ziekenhuis zelf, want dat heeft geen strafbare feiten gepleegd die aanleiding zouden kunnen zijn voor vervolging. Bovendien wordt al tegen het ziekenhuis opgetreden door het CBP, waarvan de rechter het rapport als het goed is ook heeft ontvangen. Het gaat dus nu alleen om Jordy, die ook als hij alleen feit 1 zou hebben gepleegd, zich voor de rechtbank moet verantwoorden.

Laheij twijfelt aan Jordy’s ethische motieven. De grenzen die hiervoor zouden kunnen gelden zijn volgens haar in ernstige mate overschreden. Hij heeft zich namelijk te vaak toegang verschaft tot de server, zeer grote hoeveelheden gegevens gedownload, deze besproken en soms zelfs gedeeld met derden en meerdere keren kwaadaardige software achtergelaten. Dat heeft volgens haar op geen enkele wijze meer met ideologische motieven te maken. Daarna volgt een opsomming van alles wat volgens de Fox-IT-monitor is gedownload. Alles van ‘hack 1’, oftewel het csv-bestand met de 500k patiëntgegevens en een paar ingescande dossier had Jordy al bekend. Dan komt ze bij de gegevens die op 6 en 7 oktober zijn gedownload. Naast het csv-bestand, dat voor de tweede keer is gedownload ook 1243 TIFF-bestanden met volledig ingescande medische gegevens en adviezen van 47 patiënten en nog een csv-bestand met gegevens van 56.690 patiënten (naam, adres, woonplaats, patiëntnummer,

telefoonnummer, geboorteplaats, geslacht, taal en religie). Dat is de verloren 7,5 GB aan gevoelige informatie.

Laheij erkent dat ze geen hard technisch bewijs heeft dat Jordy ook dit heeft gedownload, maar wil het wel aannemelijk maken: “Vast staat dat op 6 en 7 oktober 2012 rechtstreeks is ingelogd met de gebruikersnaam/wachtwoord combinatie die ook door Jordy bij de initiële hack is achterhaald. Er zijn geen aanwijzingen aangetroffen dat er een nieuwe hack heeft plaatsgevonden waarbij deze combinatie door anderen is achterhaald.” De inloggegevens zouden ook bekend zijn bij medewerkers van het ziekenhuis, maar ze vindt het niet aannemelijk dat een van hen, of een oud-medewerker dan net die dag inlogt en ook nog eens een VPN-dienst daarbij gebruikt. Bovendien werd in het artikel van 7 oktober ook naar deze gegevens verwezen, dus moet De Winter ervan hebben geweten. De journalist gaf Jordy bovendien later nog de gelegenheid in een artikel te reageren op alle commotie. Waarom heeft Jordy die gelegenheid niet aangegrepen om te vertellen dat hij die gegevens niet heeft gedownload? Ze besluit: “Gelet op het voorgaande is een alternatief scenario niet aannemelijk geworden. Het OM houdt verdachte aldus ook verantwoordelijk voor het tweede deel van de hack.”

Volgens haar had dat allemaal niet gehoeven om kwetsbaarheden in het netwerk aan te tonen. “Verdachte had zich kunnen en moeten beperken tot het raadplegen en/of downloaden van zijn eigen gegevens dan wel het maken van screenshots van deze gegevens. Tot slot had verdachte het lek zelf kunnen melden bij het ziekenhuis en afspraken kunnen maken over de wijze en het moment waarop hij daarmee naar buiten zou treden. Verdachte heeft de grenzen van het noodzakelijke ruimschoots overtreden en volkomen disproportioneel en niet subsidiair gehandeld. Verdachte kan dan ook geen beroep doen op artikel 10 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de fundamentele vrijheden”, aldus officier van justitie Laheij.

Ze vervolgt: “In de onderhavige zaak was het recht op privacy van derden in het geding. Van belang daarbij is bovendien dat het gevoelige, medische gegevens van derden betrof, die zonder hun

goedvinden, zelfs buiten hun medeweten om, zijn geraadpleegd en zelfs gekopieerd. Ik vind hierbij extra bezwarend dat verdachte aangeeft dat hij ook meermalen is teruggekeerd op de server uit nieuwsgierigheid. Hiermee is door verdachte heel bewust inbreuk gemaakt op de privacy van deze derden en is hun privacy kennelijk niet zozeer, of in ieder geval niet alléén, opgeofferd voor zijn beweerde ideologische motieven maar aan zijn private nieuwsgierigheid! (…) Een slechte beveiliging is geen open uitnodiging om binnen te treden. Dat de beveiliging niet op orde was, betekent geenszins dat het reeds daarmee een gegeven is dat verdachte zijn 'gang kon gaan' op de server. Een slechte beveiliging ontslaat verdachte niet van zijn eigen verantwoordelijkheden of de verplichting juiste belangen af te wegen. Indien ik vergeet mijn deur op slot te doen, betekent dat immers niet dat ik inbrekers daarmee toestemming geef om mijn huis te betreden en spullen mee te nemen."

"Het openbaar ministerie is dan ook van mening dat in dit specifieke geval het recht op de bescherming van de integriteit van het geautomatiseerde systeem waar de website op draaide (het belang dat primair wordt beoogd te beschermen in artikel 138ab Sr), alsmede het recht op privacy van de betrokken derden, zwaarder dienen te wegen dan het recht op de vrijheid van meningsuiting en nieuwsgaring van verdachte. Artikel 10 van het EVRM staat mijns inziens dan ook strafvervolging, noch een strafoplegging van verdachte in de weg."

Daarnaast verwacht ze "dat een veroordelend vonnis en een daarbij passende strafoplegging zal bijdragen aan duidelijkheid over de grenzen die gelden bij het plegen van strafbare feiten in het digitale domein en schenden van rechten van derden onder het mom van de datalekken en het hacken uit ideologische motieven en daaraan paal en perk te stellen en meer in het bijzonder richting kunnen geven aan de discussie waar de grenzen van 'ethisch hacken' liggen. Maar vooral ook dat er een signaal wordt afgegeven dat wanneer men, zoals verdachte, de grenzen ernstig overschrijdt, daar ook zware straffen passend bij zijn."

Dan is de beurt aan de tweede openbare aanklager, die haar deel van het requisitoir voorleest, oftewel feit 2. Ze beschrijft het

gevonden beeldmateriaal zo minutieus en expliciet, dat ik verschillende mensen onpasselijk zie worden. Daarna volgt haar strafeis: een jaar gevangenisstraf. Laheij mag vervolgens daar haar eis aan toevoegen. Ze begint te zeggen dat het bijna ondoenlijk is na het voorgaande over te gaan op de zaak Groene Hart Ziekenhuis en doet er daarom nog een schepje bovenop. Ze gaat daarbij zodanig tekeer tegen Jordy dat zijn zus, die weer naast hem zit, in huilen uitbarst. Dan pas begint ze weer over de hack en doet ze iets wat ik niet begrijp. Ze spreekt een strafeis uit voor beide feiten tegelijk: twee jaar gevangenisstraf, waarvan acht maanden voorwaardelijk en een proeftijd van drie jaar waarin Jordy onder behandeling komt te staan. Wat wordt er nu precies geëist voor de hack? Ik weet het niet en hoop hier later duidelijkheid over te krijgen.

Daarna is de verdediging aan de beurt. Het woord is aan Bob Kaarls, een strafrechtadvocaat die vooral bekend is van moord-, drugs-, zeden- en cybercrimezaken. Nu is hij Jordy's raadsman en hij begint met een samenvatting: "De verdediging is van oordeel dat er sprake is van een ethische hack, reden waarom er geen sprake is geweest van strafwaardig handelen door cliënt. Immers, cliënt heeft op verantwoorde wijze een misstand aan het licht gebracht. Cliënt heeft onze maatschappij duidelijk gemaakt dat persoonlijke medische gegevens van patiënten niet in veilige handen zijn van een ziekenhuis indien de netwerkbeveiliging niet op orde is."

De hack was noodzakelijk, want andere manieren om de beveiliging te testen hadden gefaald. Zo blijkt uit het verslag van de rechter-commissaris dat Fox-IT ook al eens pentests had gedaan bij het ziekenhuis, maar die waren niet gelukt. De audits die de Inspectie voor de Gezondheidszorg had gedaan waren volgens bestuursvoorzitter Verbeek niet meer dan papieren-audits. De hack van Jordy was daarom nodig om de kwetsbaarheden aan te tonen. De digitale recherche oordeelde dan ook over zijn cliënt dat hij 'computer technisch begaafd' lijkt. De Winter noemde cliënt zelfs 'materiaal voor de inlichtingsdiensten'. Het was daarom onbegrijpelijk dat het OM haar strafrechtelijke vervolging had doorgezet na dit onderzoek.

Het is dus het Groene Hart Ziekenhuis dat hier de fout in is gegaan en niet Jordy. “GHZ overtrad/overtreedt de wet: computersystemen waren zo oud dat ze niet meer werden onderhouden, antivirussoftware was soms niet in gebruik en alles draaide op één netwerk.” Hij onderbouwt dit met het rapport van het CBP, dat dan net uit is. Daarin staat immers dat de publicatie over de hack de directe aanleiding was voor het onderzoek. “Indien cliënt deze kwetsbaarheid van het netwerk niet had aangetoond, had het CBP-onderzoek niet gevolgd.” Aldus: “Duidelijker kan het niet; indien cliënt niet de kwetsbaarheid zou hebben aangetoond, zou niet alleen het GHZ, maar ook andere ziekenhuizen momenteel ernstige veiligheidslekken kennen.”

Net als Laheij gaat ook Kaarls in op het maatschappelijke belang van de zaak. “Onderhavige zaak, het handelen van cliënt, heeft dan ook onder andere geleid tot het stellen van Kamervragen, actie door ziekenhuizen op eigen ICT-gebruik, aandacht en onderzoek door de Inspectie (IGZ), adviezen en aanpassingen door Fox-IT en andere computerbeveiligingsbedrijven, onderzoek door het CBP, bewustwording van instellingen in de gezondheidszorg van veiligheidsrisico’s en een handvat van het ministerie over hoe om te gaan met responsible disclosure.” De raadsman citeert de minister van Volksgezondheid: “Met de manier waarop dit is gedaan, namelijk vernietigen van wat je hebt gezien, maar wel aantonen dat het niet deugd, ben ik als minister van Volksgezondheid blij.” Kamerlid Gesthuizen was verbolgen en geschokt en Schouw noemde het bizar toen Jordy werd opgepakt. En: “Een ander Tweede Kamerlid heeft gezegd dat cliënt juist een bloemetje verdiend.” Dat was Krol, maar dat zegt hij er om de een of andere reden niet bij.

De leidraad van het NCSC zou volgens Kaarls ook door Jordy’s ethische hack versneld tot stand zijn gekomen en ook die spreekt in zijn voordeel. “De leidraad gaat er vanuit dat het aantonen van de kwetsbaarheden veelal zal geschieden middels het plegen van strafbare feiten door hackers, te weten computervredebreuk.” De leidraad laat helaas onbeantwoord wat te doen in geval van aangifte, dus zal de rechtbank nu in dat antwoord moeten voorzien. Dat Jordy een algemeen

maatschappelijk belang diende moge inmiddels duidelijk zijn. Nu nog de vraag of hij voldoet aan de eisen van subsidiariteit en proportionaliteit.

Zijn cliënt heeft geen kwaadaardige software geïnstalleerd, alleen de omniback en dat was nodig om de bestanden te kunnen downloaden. Die heeft hij bekeken en vervolgens gesloten. “Hij heeft geen wetenschap van concrete patiëntgegevens van derden en die ook niet gedeeld met derden.” De screenshot die hij aan De Winter heeft getoond, bevatte alleen zijn eigen gegevens en het wachtwoord. Alles wat gezien wordt als hack 2 wordt door zijn cliënt ontkend. Hij had ook geen reden om nogmaals het netwerk binnen te dringen. Bij het downloaden op deze dagen is ook een andere VPN-dienst gebruikt en op de inbeslaggenomen computerapparatuur zijn geen aanwijzingen gevonden die duiden op betrokkenheid van verdachte bij de hack op 6 en 7 oktober 2012. “Gezien de gebeurtenissen na bekend worden van het lek bij derden, waaronder GHZ, Fox-IT en De Winter, valt niet uit te sluiten, sterker is het reëel te veronderstellen, dat een ander dan cliënt verantwoordelijk is voor de tweede hack.”

Jordy is volgens de raadsman ‘ethisch hacker’ en kan, zoals al eerder was gebeurd in de zaak Krol versus Diagnostiek voor U, een beroep doen op artikel 10 van het EVRM. Hij heeft daarbij voldaan aan de eis van proportionaliteit, door “uiterst zorgvuldig en prudent te werk te gaan, geen schade aan het netwerk van het GHZ toe te brengen, geen medische dossiers van derden in te kijken of naar buiten te brengen en bovendien een ziekenhuis uit te kiezen waar hij zelf patiënt is.” Ook aan de eis van subsidiariteit heeft verdachte voldaan, omdat het niet mogelijk was om het beveiligingslek op een andere manier aan te tonen dan op de wijze waarop hij dit heeft gedaan. Advocaat Kaarls besluit: “Gezien het voormelde komt de verdediging tot het primaire oordeel dat het Openbaar Ministerie niet ontvankelijk dient te worden verklaard in de vervolging van cliënt.” Hierna volgt zijn verdediging ten aanzien van feit 2. Vervolgens is er een lunchpauze en gaat iedereen weer naar buiten.

Dit is voor mij een goede gelegenheid de mensen van het Groene Hart Ziekenhuis te ontmoeten. De directeur financiën en ICT

Maarten Baaij had ik nog niet gesproken, dus ik stel me meteen aan hem voor. Gelukkig is Gelske Nederlof van communicatie er ook en ze vertelt Baaij over mijn onderzoek. Baaij stelt voor te gaan lunchen. Ik vraag of ik mee mag en dat vindt hij goed. Als we later in een broodjeszaak om de hoek wachten op onze bestelling, vertelt hij kort zijn kant van het verhaal. Het hele ICT-traject heeft voor hem ook een belangrijke fysieke dimensie: er moeten nieuwe serverruimten komen en door het hele gebouw nieuwe draden worden getrokken en dat kost veel tijd en geld. Geld dat dus niet besteed kan worden aan de primaire taak van een ziekenhuis: de zorg. De buitenwereld zal zich dat misschien niet realiseren bij een zaak als deze, maar voor hem is het de dagelijkse realiteit.

Verder vertelt hij waarom hij de schadevergoeding heeft ingetrokken. Na de behandeling van feit 2 realiseerde hij zich dat Jordy waarschijnlijk de gevangenis in gaat en de kans dat hij de drie ton kan betalen wel erg klein wordt. Dan zien we door de ruit van de broodjeszaak de rechtelijke macht voorbijkomen, zonder toga, maar wel met broodjes en koffie in de hand. Het is alweer bijna tijd, dus we moeten snel weer terug. Onze lunch wordt haastig ingepakt en we rennen naar het Paleis voor Justitie om nogmaals door de beveiligingspoorten te gaan.

Terug in de rechtszaal is het tijd voor repliek en dupliek, oftewel de aanklager reageert op het verweer, waar de gedaagde dan weer op reageert. Het gaat weer vooral over feit 2 en ik hoop meer duidelijkheid te krijgen over de strafeis ten aanzien van feit 1, maar die komt er niet. Tot dan toe kon ik precies alle waardevolle elementen voor responsible disclosure uit het proces destilleren en de rest laten voor wat het was. Nu beide feiten toch door elkaar lopen, overweeg ik zelfs de hele case te laten vallen, want dit wordt nu wel erg rommelige jurisprudentie.

NU.nl heeft blijkbaar minder moeite met deze vaagheid en kopt diezelfde dag: ‘Twee jaar geëist tegen hacker Groene Hart Ziekenhuis’. Het artikel beschrijft uitgebreid de melding van twee jaar terug, wat erna gebeurde en het rapport van het CBP. Feit 2 wordt kort tussendoor vermeld, waardoor de suggestie wordt gewekt dat de eis van twee jaar vooral is vanwege de hack.

Op 17 december volgt het vonnis. Dit keer is het een stuk minder druk in de rechtszaal. Naast Jordy en zijn advocaat is er alleen iemand van Team High Tech Crime. We moeten lang wachten en de stemming is bedrukt, want wat zeg je tegen iemand die een flinke gevangenisstraf boven zijn hoofd heeft hangen? Ik knoop daarom maar een praatje aan met de agent. Die mag natuurlijk niets vertellen over de zaak, want hij zal wel een van de mannen zijn die Jordy heeft opgepakt, maar over cybercrime in het algemeen kun je toch een redelijke stilte vullen. Als we dan eindelijk naar binnen mogen, vraagt rechter Frenkel wie we zijn. Ik weet eigenlijk niet zo goed wat ik moet zeggen, dus ik roep: “Ik ben journalist”. “Oh, voor wie schrijft u dan?”, vraagt ze. “Ik schrijf hier een boek over”. Dan kunnen we gaan zitten en begint ze het vonnis voor te lezen, waarvan ik hieronder de belangrijkste fragmenten citeer:

“Hoewel de rechtbank wil aannemen dat de hacker geen kwade bedoelingen heeft gehad en een misstand aan de kaak heeft willen stellen – namelijk een lek in de beveiliging – heeft hij door na de initiële hack meermalen in te loggen en te zoeken naar privacygevoelige gegevens van derden strafrechtelijk laakbaar gehandeld. (…) De enkele omstandigheid dat verdachte stelt een ‘ethisch hacker’ te zijn en ten behoeve van de maatschappij te hebben gehandeld, is onvoldoende, alleen al omdat het handelen van verdachte ook steeds moet worden getoetst aan de eisen van proportionaliteit en subsidiariteit. De rechtbank zal derhalve het verweer verwerpen. Het openbaar ministerie is ontvankelijk in de vervolging van verdachte.”

Ze geeft vervolgens een opsomming van wat Jordy aantoonbaar heeft gedaan in de bekende computervredebreukformulering: “een kwetsbaarheid van op een of meerdere server(s) aanwezige software (HP Data Protector) uitgebuit en/of beheerdersrechten (onder meer inloggegeven(s) en wachtwoord(en)) verkregen en/of (vervolgens) ingelogd op die (FTP)server(s), met gebruikmaking van inloggegevens en wachtwoord, tot welk gebruik hij en/of zijn mededader(s) niet gerechtigd was/waren, waarna verdachte en/of zijn mededader(s) vervolgens meermalen, althans eenmaal, gegevens, die waren opgeslagen, werden verwerkt of werden overgedragen door

middel van dat/die geautomatiseerde werk.” Dit is dus de eerste hack.

Over de tweede hack zegt ze: “Anders dan de officieren van justitie, is de rechtbank van oordeel dat niet kan worden bewezen dat verdachte zich ook in de periode van 4 oktober 2012 tot en met 7 oktober 2012 hieraan schuldig heeft gemaakt (‘tweede hack’). De rechtbank overweegt hiertoe dat verdachte ter terechtzitting heeft ontkend dat hij in deze periode heeft ingelogd en bestanden heeft gedownload van de server van het GHZ, dat in deze periode gebruik is gemaakt van een VPN-dienst waarvan uit onderzoek niet is gebleken dat verdachte hierover de beschikking heeft gehad, en dat op de in beslag genomen computerapparatuur van verdachte wel bestanden zijn aangetroffen die in verband met de ‘eerste hack’ kunnen worden gebracht, maar geen bestanden die in verband met de ‘tweede hack’ kunnen worden gebracht. Gelet hierop kan niet worden uitgesloten dat een ander dan verdachte in de periode van 4 oktober 2012 tot en met 7 oktober 2012 op de server van het GHZ heeft ingelogd en bestanden (waaronder de 1243 medische dossiers) heeft gedownload, mede in aanmerking genomen dat verdachte met derden over de ‘eerste hack’ heeft gecommuniceerd waarbij ook het wachtwoord en de gebruikersnaam zijn uitgewisseld.”

Jordy wordt dus alleen de eerste hack ten laste gelegd. De vraag is nu of hij daarbij ethisch heeft gehandeld. Volgens de rechter diende hij een algemeen belang en heeft hij daarbij gehandeld volgens het subsidiariteitsbeginsel. “Naar het oordeel van de rechtbank levert dergelijk hacken op zichzelf bezien een belangrijke bijdrage aan de beveiliging van vertrouwelijke gegevens in de gezondheidszorg en de maatschappelijke discussie daarover. De rechtbank is voorts van oordeel dat er voor verdachte geen andere, minder vergaande manieren waren om zijn doel te bereiken en dat verdachte derhalve heeft voldaan aan de eis van subsidiariteit. De rechtbank overweegt daartoe dat verdachte zijn bevindingen heeft gemeld bij een journalist bij wie hij eerder bevindingen had gemeld, met wie hij een vertrouwensrelatie had opgebouwd en van wie hij wist dat deze, voordat hij de bevindingen zou publiceren, het GHZ eerst de

gelegenheid zou bieden adequate maatregelen te treffen om te voorkomen dat gevoelige gegevens in de openbaarheid terecht zouden komen.”

Maar was de hack ook proportioneel? “De rechtbank overweegt evenwel dat verdachte vervolgens gedurende een week meermalen opnieuw zonder toestemming in het systeem van het GHZ heeft ingelogd en bestanden heeft gedownload, terwijl verdachte heeft verklaard dat hij reeds op 26 september 2012 aan de journalist had gemeld dat de beveiliging van het GHZ niet op orde was en hij dus kennelijk op die datum al voldoende informatie had verzameld. Bovendien heeft verdachte verklaard dat hij in de door hem aangetroffen patiëntgegevens heeft gezocht naar informatie over derden, niet alleen familieleden en een vriend, maar ook een ‘bekende Nederlander’.” Daar ging hij dus te ver.

Kortom, dat Jordy malware heeft geplaatst, daarmee op de server kwam en toen enkele bestanden heeft gedownload, kan nog gezien worden als vrijheid van nieuwsgaring en hoeft niet bestraft te worden. Dit was nodig om de misstand aan te tonen. Maar, toen hij de dagen daarna doorging met zoeken en heeft gezocht op de namen van anderen en zelfs een van een bekende Nederlander, daarmee overschreed hij de grenzen van proportionaliteit en krijgt hij wel straf. De tweede hack, waarbij 7,5 GB werd gedownload, kan volgens de rechter niet aan hem worden toegeschreven dus daarvan wordt hij vrijgesproken.

Frenkel behandelt uiteraard eerst nog feit 2. Dan volgt het vonnis: twaalf maanden gevangenisstraf, waarvan acht maanden voorwaardelijk. Een van de voorwaarden is dat hij zich de komende drie jaar laat behandelen bij een psycholoog. Daarnaast krijgt hij 240 uur taakstraf. De in beslag genomen computerapparatuur wordt vrijwel geheel verbeurd verklaard. Ook de rechter maakt dus in haar uitspraak geen onderscheid tussen feit 1 en 2. Zwaar teleurgesteld verlaat ik de zaal en twijfel zelfs even om naar haar toe te gaan voor uitleg. Maar het lijkt me volkomen ongepast om hierover te beginnen, als hier net iemand te horen krijgt dat hij de gevangenis in moet. De zaak hier draait vooral om feit 2.

Die avond krijg ik een bericht van Jordy: “Uit het vonnis blijkt dat ik 120 uur taakstraf krijg voor de hack en de rest voor dat andere.” En inderdaad, als het vonnis online staat, lees ik daarin dat de rechter wel duidelijk onderscheid heeft gemaakt tussen feit 1 en 2. Nu hebben we eindelijk een heldere uitspraak over de grenzen bij verantwoorde onthullingen, al doet de rechtbank tegelijk zelf een onverantwoorde onthulling. In het vonnis staan namelijk nog allemaal namen van betrokkenen. Gelukkig meldt iemand dat bij de rechtbank en snel wordt de tekst vervangen.

Wat vindt het OM van de uitspraak? Laheij reageert via de mail: “Met de uitspraak heeft de rechtbank duidelijk gemaakt dat verdachte de proportionaliteitsgrenzen hier inderdaad heeft overschreden en daarom niet van een ethische hack kan worden gesproken. Daarmee is de door ons verzochte duidelijkheid voor deze casus ook door de rechtbank gegeven. Uiteraard is beantwoording van de vraag of een hack als ‘ethisch’ kan worden aangemerkt bijzonder casuïstisch en zal dit van geval tot geval bekeken moeten worden. De uitspraak van de rechtbank geeft, samen met de uitspraak in de zaak van Krol, wel een duidelijke richting, waar naar mijn mening alle partijen in de wereld van beveiliging in het digitale domein iets aan kunnen hebben. Zeker gezien in combinatie met de huidige leidraad voor responsible disclosure.”

“Al met al zijn wij dan ook niet ontevreden met de uitspraak. De strafmaat van 120 uur taakstraf voor de hack is in het licht van het feit dat een deel van de hack wel acceptabel wordt geacht en voor een zwaar deel van de handelingen, te weten het downloaden van de 47 patiëntendossiers, hij is vrijgesproken, wel te begrijpen. Ik vind de straf aan de lage kant en had uiteraard liever meer gezien, maar kan deze gelet op het voorgaande wel plaatsen. Uiteraard ben ik enigszins teleurgesteld in de vrijspraak voor het deel van de hack op 6 en 7 oktober, maar gelet op de inhoud van het dossier hebben wij besloten daar geen hoger beroep tegen in te stellen. Voor het OM was voor het hack-deel van de zaak het meest belangrijk om duidelijkheid van de rechtbank te krijgen en daar voldoet de uitspraak aan.” Aldus de officier van justitie.

Zelf vind ik het ook een goede uitspraak van de rechter, want ze geeft vrij duidelijk aan waar de grenzen liggen. Ethisch hacken dient een hoger maatschappelijk doel en het is te verwachten dat je digitale schade aanricht bij het aantonen van kwetsbaarheden, maar wees je er wel van bewust dat je handelt met de persoonsgegevens van anderen. Dit is belangrijke jurisprudentie waar we in toekomstige zaken nog veel aan zullen hebben. De timing van de uitspraak viel mooi samen met de brief van Opstelten aan de Tweede Kamer, over de voortgang van responsible disclosure. Het Groene Hart Ziekenhuis kreeg ook een brief, van het CBP. Daarin staat dat het ziekenhuis inmiddels voldoet aan artikel 13 en ze dus geen boete zal krijgen. Begin 2015 kunnen we naar mijn oordeel wel stellen dat responsible disclosure werkt.

Zijn we nu klaar? Is het verhaal nu verteld? Nee, want ik heb mijn punt nog niet gemaakt. Het is verleidelijk om vooral te kijken naar de spectaculaire zaken, waar grote ophef over is in de media en politiek en waar rechtszaken op volgen. De echte helpende hackers hebben dat niet nodig. Zij werken achter de schermen. Daarom besluit ik met een reeks portretten van ethisch hackers die vooral buiten de media opereren en elk op hun eigen manier bijdragen aan onze digitale veiligheid.

20. Gratis boeken voor @iliaselmatani

Uitgeverij erkent lek, maar komt traag in actie

Een van de aspecten die vaak onbelicht blijft bij verantwoorde onthullingen is dat de ethisch hacker veel geduld moet opbrengen. Zo ook @iliaselmatani die maar liefst een jaar moest wachten totdat een ogenschijnlijk eenvoudig lek in de site van Noordhoff Uitgevers werd gedicht. Waarom? De journalistiek had geen interesse in zijn meldingen en de uitgeverij zelf had het al zo druk met andere dingen. Dat terwijl El Matani had ontdekt dat hij al hun boeken gratis kon downloaden.

In de herfst van 2013 zie ik op Twitter een uitnodiging voorbijkomen van een zogenaamde #fristileaks. Dat is de jongerenvariant van #wiskyleaks, een open informele bijeenkomst waar hackers onder Chatham House rules hun geheimen delen. Oftewel: je mag alles doorvertellen, als je maar niet zegt van wie je het hebt. Het is ook wel interessant om te zien hoe zoiets georganiseerd wordt. Eerst roept iemand of het niet weer eens tijd wordt voor een bijeenkomst. Als er voldoende respons is, komt er een linkje naar een online document waar iedereen aangeeft wanneer en waar zij kunnen, net zolang tot er een datum en plek is besloten. Dat, terwijl de meesten elkaar alleen virtueel kennen. Na een paar weken heen en weer gechat, spreken we af op 12 oktober in een café in Utrecht. Het lijkt me leuk om op deze manier jonge hackers te ontmoeten en verhalen te horen die je normaal niet in de media leest. Wellicht houd ik er een goede casestudie aan over voor mijn onderzoek.

We zijn met een stuk of twaalf deelnemers en betrekken een rustige bovenverdieping van de kroeg. De meesten kijken een beetje verlegen om zich heen, wellicht bang dat ik opschrijf wat ze vertellen, dus begin ik zelf maar over mijn onderzoek. Aan het einde van de avond realiseer ik me dat ik vooral zelf aan het woord ben geweest, vanachter een groot glas Triple. Ik weet niet of de verlegen jongens – en een meisje – met hun Fristi's zich

hadden vermaakt met de praatgrage onderzoeker, maar ik had gefaald: geen interessante onthulling, helaas.

Onderweg naar de trein praat ik nog wat na met enkele van de hackers die meelopen, totdat er nog maar eentje over is: @iliaselmatani. Hij vertelt dat hij nog wel een onthulling heeft. Hij heeft namelijk ontdekt hoe je alle boeken van Noordhoff Uitgevers zomaar kunt downloaden. El Matani had dit al eerder willen onthullen via Webwereld, maar de journalisten bleken niet geïnteresseerd. Hij vraagt me of ik wil bemiddelen tussen hem en de uitgever. Ik zeg toe, want dit lijkt me een uitgelezen kans om zelf ook eens een onthulling te doen, maar dan wel op een verantwoorde manier. El Matani lijkt me een integere jongen en het lijkt me een zaak die niet zo snel uit de hand kan lopen. Het gaat immers om boeken en niet om persoonsgegevens die gelekt worden. Als het lek gefikst is, kan ik er mooi een stukje over schrijven voor het tijdschrift Informatiebeveiliging om te laten zien dat het zo ook kan.

De volgende dag krijg ik een mail met uitgebreide documentatie. El Matani schrijft dat hij voor zijn studie een online boek had aangeschaft bij Noordhoff. Je logt dan in met een vouchercode en kan er dan online in bladeren. Pagina's opslaan kan niet. Dat vindt hij eigenlijk best lastig, want zo kan hij het boek bijvoorbeeld niet lezen als hij in de trein zit. Hij ontdekt echter dat de pagina's steeds geladen worden vanaf een url die eindigt op 'page' met een nummer erachter. Als hij het nummer handmatig aanpast, krijgt hij een foutmelding. Hm, dat zou ook te eenvoudig zijn. Maar als hij in de cache van zijn Firefoxbrowser bekijkt, ziet hij dat de inhoud van de pagina steeds geladen wordt vanaf een andere url. Als hij hier een van de nummers verandert, komt hij wel gewoon uit bij de gevraagde pagina.

Hij ziet aan de url dat het boek ook een nummer heeft. Als hij dat nummer verandert, komt er een ander boek tevoorschijn waar hij ook in kan bladeren. Hij probeert wat nummers uit en komt er zo achter dat hij maar liefst 1643 boeken zou kunnen downloaden. Dat is zo'n beetje de hele collectie van de uitgeverij. El Matani laat zijn bevinding zien aan @sander2121. Samen schrijven ze een script in Python dat de urls automatisch aanpast,

de pagina’s download, netjes in de juiste volgorde zet en opslaat als pdf. Het werkt. Ze zouden nu al deze boeken gratis kunnen downloaden.

Wat zou jij doen als je zoiets ontdekt? Ikzelf zou het meteen aan mijn medestudenten doorgeven en zo iedereen trakteren op gratis boeken. @iliaselmatani en @sander2121 niet. Ze willen de slechte beveiliging op een verantwoorde manier melden. Maar hoe zal die uitgever reageren? Zal hij aangifte doen? Ze besluiten het via de media te doen en sturen hun melding op 21 april naar Webwereld. Daar wordt het echter niet opgepakt en daarom komt El Matani nu met zijn melding bij mij.

Ook al is dit niet zo’n heel zware zaak, vind ik het nog best spannend om zo’n uitgever te melden dat hun site lek is. Er zijn dan wel geen persoonsgegevens gelekt en je zou zelfs kunnen stellen dat systematisch urls afgaan niet gezien kan worden als hacken. Maar toch, ze zouden een rechtzaak kunnen starten - alleen al om ons af te schrikken. De uitgever kan immers een flinke reputatieschade oplopen door deze onthulling. Als ik ze opzoek op internet, zie ik dat achter deze uitgever het miljarden investeringsbedrijf Bridgepoint zit. Die hebben hoogstwaarschijnlijk een flinke batterij aan advocaten klaarstaan om ons het leven zuur te maken - ook als ze geen zaak hebben. Ik begin daarom met een voorzichtig mailtje waarin ik het lek meld en me aanbied als bemiddelaar tussen hen en de hacker.

Binnen een dag krijg ik een reactie van Jean Pierre Miani, Technology Officer bij Infinitas Learning. In de cc zie ik nog drie mensen van de technische afdeling. Mooi. Hij zegt de melding zeer serieus te nemen en vraagt met spoed om aanvullende informatie. Even bellen dan maar. Als ik Miani vertel over de urls en de boeken, reageert hij laconiek: “Oh, dat. Nou, dat is geen hacken toch? Hebben we in april al gehoord en dat is nu gefikst. Is dit nu weer diezelfde jongen?” Dat wil ik natuurlijk niet zeggen. Infinitas kan alle details krijgen, maar eerst moeten ze via een PGP-gesigneerde mail beloven niet tot vervolging over te gaan. Miani reageert geërgerd: “Nee, ik ga geen vrijbrief geven.”

Als ik El Matani verslag doe van het gesprek is hij onaangenaam verrast. “Tsja, hier gaan mijn nekharen van

overeind staan. Het is inderdaad geen hacken, eerder ongeautoriseerde toegang. Maar als je dit op Twitter gooit, kunnen ze de tent wel sluiten. Dat scriptje heeft me twee uur gekost en zelfs met een gewone verbinding kun je in een nachtje alle boeken downloaden. Kun je je eigen uitgeverij beginnen." Hij begrijpt ook niet hoe de melding al bij hun is gekomen. Ze hebben dit nog met niemand gedeeld, ook niet bij #fristileaks. Vervolgens kijkt hij even op de site van Noordhoff. Nee, het lek is nog niet gedicht. Wat volgt is een langdurige woordenwisseling tussen El Matani en Miani, via mij. Als we er niet uitkomen, besluit ik voor te stellen elkaar dan maar te ontmoeten zonder vrijwaring. El Matani is gelukkig bereid het risico te lopen. Ook Miani draait bij: "Ik vind dat white hat hackers beloond moeten worden, want ik kan er zelf ook van leren."

Op 6 januari 2014 ga ik samen met El Matani naar het kantoor van Infinitas in Houten. Als we de Technology Officer ontmoeten in zijn kantoor, steekt hij direct van wal. Security is zijn hoogste prioriteit. Als educatieve uitgever hebben ze vaak aanvallen te verduren van scholieren die vanuit school proberen te hacken en DDoS-aanvallen lanceren. Ze verzamelen daarom een minimum aan persoonsgegevens met het idee: als je ze niet hebt, kun je ze ook niet kwijtraken. Het abonnement waarmee je de boeken kunt inzien, is dan ook alleen maar een nummer.

Ze hadden dus al in april gehoord van het lek via een leverancier. Maar om het te dichten moest wel het hele systeem op de schop, terwijl bij een educatieve uitgever alles in juni goed moet draaien, want dan schaffen de scholen de nieuwe uitgaven aan. Je kunt dan niet het hele systeem omgooien. De aanpassing zou worden meegenomen in het groot onderhoud, maar toen werd het druk en verdween het probleem weer naar de achtergrond. Zo spannend is het niet, dat iemand een pagina kan downloaden, vindt de uitgever. En nee, er is daarom geen enkele reden om een rechtszaak tegen ons te beginnen.

Ik opper dat Ilias ook zijn programma aan andere studenten had kunnen geven en er dan veel meer boeken gratis zouden worden gedownload. De auteurs lopen dan hun royalty's mis en zouden die op Infinitas willen verhalen. Volgens Miani krijgen niet

al hun zesduizend auteurs royalty's, maar er zouden inderdaad een paar een zaak kunnen starten. "Hoe dan ook", stelt hij trots, "er wordt aan gewerkt en de nieuwe versie wordt binnenkort uitgerold." "Mag Ilias het dan testen?" opper ik enthousiast. Miani twijfelt: "Eh, nu nog niet, we zijn er nog mee bezig. Geef ons nog een paar weken. Ik zal wat documentatie sturen waar hij naar kan kijken."

De weken worden maanden, zonder bericht van Infinitas. El Matani heeft het inmiddels helemaal gehad met de trage uitgever. Ikzelf ook en wil uiteindelijk wel mijn artikel publiceren. Ik besluit dan toch maar te wachten tot de truuk met de urls niet meer werkt, want anders zou deze onthulling ook niet erg verantwoord zijn. Een paar maanden later probeer ik het nog eens en jawel: de geconstrueerde links leiden slechts naar dode pagina's. Blijkbaar is het Jean Pierre Miani uiteindelijk gelukt.

Het is dan juni 2014 en ik lees op de homepage van de uitgever: "Infinitas Learning re-affirms market leadership by launching e-book platform Classmate". And what's new? De inmiddels tweeduizend boeken zijn nu eindelijk ook te downloaden - mits je een voucher hebt gekocht natuurlijk - zodat je ze offline kunt lezen. Niet dat @iliaselmatani daar nu nog wat aan heeft, want hij is inmiddels klaar met zijn opleiding. Hij werkt nu als security specialist bij Securelabs en krijgt, net als de uitgever, eindelijk gewoon betaald voor zijn werk.

Zo gaat het dus meestal: een goedbedoelende hacker vindt een lek, pas na lang zeuren wordt het gedicht en er is geen enkele waardering voor het gratis advies. Je moet dus als ethisch hacker het nodige geduld kunnen opbrengen en omgaan met teleurstellingen. Je kunt je afvragen waarom ze het nog doen. Die vraag zal ik later beantwoorden. Eerst nog een case die ongeveer net zo verloopt.

21. De ethische commissie van @1sand0s

Youfone te goedkoop voor goede security

De meeste onthullingen van beveiligingsproblemen worden niet gedaan in de media, maar op Twitter. Dat is snel, open en als je wilt, anoniem. Zo heb ik al aardig wat spannende verhalen voorbij zien komen, maar vraag ik me vaak af wie er achter de wonderlijke pseudoniemen schuilgaan. Daarom gooi ik er vaak nog even een tweet uit als ik naar een bijeenkomst ga waar ook hackers zijn: “Nog tweeps aanwezig?” Op 28 april was er weer zo’n bijeenkomst: #hackdetoekomst @De_Zwijger. Diverse bekende hackers reageren op mijn tweet. Zo ook @1sand0s.

Die avond zie ik hem in de bar van Pakhuis de Zwijger. Hij heeft een zwart T-shirt aan met de tekst “I hacked my ISP and all I got was this lousy T-shirt”. Dat zou weer een mooie casestudie kunnen zijn, dus ik roep: “Ah, je hebt een ethische hack op je naam!” Inderdaad. Hij kon vrij eenvoudig bij zijn telecomprovider Youfone accounts overnemen en heeft dit gemeld. Niet dat hij van hen dit T-shirt kreeg. Het is van het NCSC, zoals te zien is aan het logo op zijn mouw.

@1sand0s is volgens zijn Twitterprofiel “researcher and teacher on the arts of moving 1s and 0s (preferably securely and privately)”. Het blijkt te gaan om Jeroen van der Ham van de UvA. Hij studeerde en promoveerde daar en was er vier jaar Post Doc. Nu is hij onderzoeker en docent System and Network Engineering. Niet dat de onderzoekers aldaar het lek bij de telco hadden gevonden. Deze ethische hack kwam uit zijn persoonlijke omgeving.

Zijn vriendin heeft namelijk een mobiel abonnement bij Youfone. Als ze op haar persoonlijke pagina wil inloggen lukt dat niet. Ze probeert een nieuw wachtwoord aan te vragen, maar de site herkent haar e-mailadres niet en ze vraagt aan Van der Ham of hij er even naar wil kijken. Dat is goed, want dit is zijn werk, maar het lukt hem ook niet het wachtwoord aan te passen. Dat is

vreemd. Hij heeft zelf ook een Youfone-abonnement, dus probeert hij het bij zijn eigen account. Daar lukt het wel om een nieuw wachtwoord in te stellen. Tot zijn verbazing ziet hij dat hij zijn e-mail niet hoeft te verifiëren en er een wachtwoord wordt gegenereerd dat bestaat uit zijn postcode en huisnummer.

Dit is een wel heel klungelig lek. Als je dus het e-mailadres en de postcode van een andere Youfonegebruiker hebt, kun je daarmee dus zijn account overnemen door een nieuw wachtwoord aan te vragen. Vervolgens kun je het abonnement aanpassen, het rekeningnummer zien, hoeveel er gebeld is en ook met wie en wanneer… Hij graaft wat dieper in de browser en ziet dat de communicatie ook nog eens niet versleuteld is en de interactie plaatsvindt met een sessie cookie. Dat betekent dat je er tussen kunt gaan zitten en wachtwoorden afvangen. Dit is wel een hele reeks standaard securityfouten.

Van der Ham stuurt daarom meteen een mailtje naar de Youfoneklantenservice. Hij doet dit vanaf zijn werkadres, want dan weten ze meteen dat ze hier te maken hebben met iemand die er verstand van heeft. Als hij geen reactie krijgt, doet hij zijn melding maar openbaar. @1sand0s tweet aan @youfone: “Ik heb via contactformulier een bericht gestuurd, maar nog geen reactie. Het is best ernstig en zou z.s.m. antwoord willen zien!”. Dan volgt wel een reactie: “Beste Jeroen, je krijgt binnen maximaal vijf werkdagen een reactie op je ticket. Stuur je 06-nummer in een pb, dan kijken wij alvast wat er aan de hand is. Groet, Youfone” In de discussie die volgt via de DM, stelt de helpdeskmedewerker dat het lek niet echt een probleem is. Van der Ham vraagt of hij het aan de media kan melden. Dat vindt de medewerker OK.

Van der Ham wil echter wel dat het lek eerst gedicht wordt voordat hij erover publiceert, dus neemt hij contact op met het NCSC. Het is inmiddels vrijdagavond en hij weet dat hun responseteam ook in het weekend werkt, maar dan alleen op de meest urgente meldingen reageert. Maandag krijgt hij een reactie. Het centrum ziet dit niet als haar primaire verantwoordelijkheid, maar omdat er ook burgers getroffen kunnen worden willen ze wel helpen. Een medewerker meldt dat Van der Ham het beste contact kan opnemen met de directiesecretaresse en geeft haar e-mailadres.

De secretaresse reageert op de mail dat ze ernaar zullen kijken. Als hij woensdag nog geen reactie heeft, mailt hij nogmaals, weer zonder reactie.

Intussen benadert Van der Ham de bouwer van de site, maar die reageert geïrriteerd en zegt: “Je moet ons niet lastig vallen, dit is iets wat Youfone zelf moet oplossen”. Dan benadert hij uiteindelijk verschillende journalisten die wel eens onthullingen hebben gedaan, maar die tonen helaas ook geen interesse. Dan maar weer wachten. Anderhalve week later heeft hij nog steeds geen reactie van Youfone. Hij blijft via de mail aandringen om een belafspraak met de directeur. Die belt na een paar dagen zowaar zelf terug en vraagt: “Hoe erg is dit nou? Hoe zou je dit kunnen uitbuiten?” De directeur luistert vervolgens geïnteresseerd naar wat kwaadaardigen met dit lek zouden kunnen en belooft dat de site gefikst wordt.

Dat gebeurt inderdaad. Van der Ham moet het vernemen via de Youfonenieuwsbrief, waarin staat dat de site vernieuwd is, zonder vermelding van het incident of zijn melding. Als hij de site checkt blijkt er nog steeds geen e-mailverificatie te zijn. Er wordt gelukkig nu wel een random wachtwoord gegenereerd en niet een postcode. Ook de encryptie en de sessie cookie is aangepast. Vreemd is wel dat het certificaat dat erachter hangt dateert van drie maanden voor zijn melding. Ze hadden dus al een oplossing klaar liggen, maar die om een of andere reden niet ingevoerd.

Voor Van der Ham was dit al met al erg frustrerend. Hij is er drie weken mee bezig geweest, zonder enige reactie van hun kant. “Er moet begrip zijn voor de persoon die de melding doet, want die doet dat vrijwillig, zonder belang. Je zou snel afspraken moeten maken met de melder over vrijwaring van vervolg en hem op de hoogte houden van de voortgang” Hij is ook teleurgesteld in de journalisten die het nieuws niet oppakten en concludeert: “Zo’n melding is blijkbaar niet sexy meer.” Hij stuurt Youfone tot slot nog een mailtje waarin hij schrijft blij te zijn dat het nu is opgelost en krijgt een kort bedankje. Dan stuurt @1sand0s 7 november zijn laatste tweet over de zaak: “Na een responsible disclosure procedure (met dank aan @ncsc_nl) heeft @youfone nu een veiliger klantenportal.”

Deze zaak speelde eind 2013. Alle grote telecombedrijven hebben tegen die tijd beleid voor responsible disclosure en een meldpunt waar ethisch hackers terecht kunnen. Youfone blijkbaar niet. Op www.youfone.nl staan vooral “superrrrr goedkope aanbiedingen”, maar nog steeds geen e-mailadres waar je veiligheidsproblemen kunt melden, laat staan een richtlijn. Wel is er een algemeen e-mailadres. Als ik daar de bovenstaande tekst naartoe stuur, krijg ik de bekende automatische melding dat ik binnen vijf dagen een reactie kan verwachten. Die volgt: “Wij hebben het artikel doorgezet naar de desbetreffende afdeling en willen u bedanken voor het voorleggen van het artikel.” Verder niets meer van gehoord.

Voor Van der Ham was het tegelijkertijd ook wel weer een leerzame ervaring, want de ongeveer 35 studenten die hij aan de UvA begeleidt, moeten dit ook vaak meemaken. Zij doen onderzoek naar beveiligingslekken en ook hun vondsten moeten op een en of andere manier verantwoord onthuld worden. Van der Ham heeft daarom met twee collega’s een ethische commissie opgericht die de onderzoeken toetst. Ze kijken al bij de opzet van het onderzoek hoe de studenten omgaan met gevoelige persoonsgegevens en of hun onthulling verantwoord is. Elk onderzoek wordt voorzien van een risicoclassificatie voor adequate begeleiding. Dat gaat over het algemeen goed en er zitten af en toe pikante vondsten bij. Zo ontdekten zijn studenten bijvoorbeeld lekken in de beveiliging van de datingapps Tinder en Grindr. In beide gevallen hadden de studenten manieren gevonden om veel verborgen data over de deelnemers tevoorschijn te toveren, dat gemeld bij de aanbieder en er pas over gepubliceerd toen het lek gedicht was.

Tinder is een datingapp waar je profielfoto’s swiped: niet leuk naar links, wel leuk naar rechts. De profielfoto’s komen uit het Facebookprofiel waarmee iemand inlogt en eronder staat hoe ver diegene op dat moment van je vandaan is. Als twee mensen elkaar allebei naar rechts hebben geveegd, hebben ze een match en kunnen ze met elkaar chatten en wellicht tot een afspraakje komen. Studenten Joey Dreijer en Eric van den Haak hadden ontdekt dat ze met een zelfgemaakte interface voor de app en

nepprofielen vrij nauwkeurig de locatie konden bepalen van Tinderaars. Dat deden ze door de drie nepprofielen elk een andere locatie te geven en met driehoeksmeting de drie afstanden van een profiel om te rekenen tot een geografisch punt. Vervolgens konden ze de Tinderprofielen ook linken aan de oorspronkelijke Facebookprofielen, omdat die meer informatie gebruikten dan alleen de foto's. Dat zal niet de bedoeling zijn geweest van de datingapp, maar is wel handig voor stalkers bijvoorbeeld.

Deze truuk was het jaar daarvoor ook al toegepast op Grindr door studenten Tobias Fiebig en Wouter Katz. Dat is ook een datingapp, maar dan speciaal voor homoseksuele mannen. Die kunnen een profiel aanmaken, met foto's en seksuele wensen en krijgen dan de 24 mannen gepresenteerd die het dichts in de buurt zijn. De studenten hadden ook hier met nepprofielen vrij exact achterhaald waar andere gebruikers zich bevinden. Bovendien ontdekten ze dat ze met diezelfde locatiegegevens ook makkelijk iemands account en chatsessies konden overnemen. Dat kan niet alleen leiden tot gênante situaties, maar is ook gevaarlijk omdat Grindr ook gebruikt wordt in landen waar men wat minder tolerant is ten aanzien van homoseksualiteit.

In beide gevallen ging het om beveiligingslekken die op zich al bekend waren, maar nog steeds bestonden, ook al waren ze volgens de aanbieders gedicht. Blijkbaar niet dus. De studenten gingen daarom, onder begeleiding van de ethische commissie, zeer voorzichtig te werk. Ze zorgden ervoor dat ze in hun onderzoek geen persoonsgegevens gebruikten van echte mensen, alleen nepprofielen. Vervolgens meldden ze hun vondst eerst bij de eigenaren van de systemen en gingen ze pas over tot publicatie als het lek weer gedicht was.

Zo zijn er nog enkele tientallen beveiligingslekken door de UvA-studenten achter de schermen afgehaald. Hun publicaties verschijnen uiteindelijk als academisch onderzoeksverslag op de website van de vakgroep en niet als kort en krachtig artikel op een nieuwssite. Het gaat hen om de erkenning van hun vondst, niet om het publiekelijk aanklagen van organisaties die de beveiliging niet op orde hebben. Net als de onderzoekers van de Radboud Universiteit hebben deze jonge hackers een plek gevonden waar

ze legitiem hun werk kunnen doen, daarin begeleid worden en de credits krijgen, zonder dat het meteen uitloopt op een rel.

Het zou mooi zijn als we veel van de responsible disclosures konden overlaten aan de universiteiten. Dat zorgt voor goede kennisuitwisseling, methodeontwikkeling en erkenning voor vondsten. De meeste ethisch hackers zitten echter niet op de universiteit. Vaak zijn ze al vrij jong ergens vastgelopen in het onderwijssysteem en moeten ze elders hun onderzoek onderbrengen, zoals we zien in het geval van @rickgeex.

22. @rickgeex komt er wel

Een plek voor helpende hackers

Terug naar de NCSC One conferentie van juni 2014. Daar stonden we dus twee dagen lang met onze Tek Tok Studio interviews te doen voor ons Youtubekanaal. Enkele personages uit dit boek verschijnen ook voor de camera. Jeroen van der Ham vertelt over zijn ethische commissie aan de UvA. Oscar Koeroo doet het SCADA-verhaal nog even kort over en vertelt over Operation Cyberpaint, waar hackers en cyber security experts van bedrijven en overheid elkaar te lijf gaan met paintball. Lodewijk van Zwieten van het OM lanceert samen met de politie een nieuw plan om cybercriminaliteit aan te pakken. Melanie Rieback heeft samen met modemhacker Pieter Geissler een non-profit security consultancy opgericht: Radically Open Security. En wie achter het alias @XS4me2all zit, zal de oplettende lezer inmiddels wel doorhebben.

Verder hadden we nog wat internationale gasten aan tafel. Jon Callas vertelt over zijn bedrijf Silent Circle, dat versleutelde communicatie aanbiedt voor de gewone gebruiker, inclusief een “black phone” die niet is af te luisteren. Een groepje jonge cryptografen vertelt dat uiteindelijk alles te hacken is en voorspelt het einde van de versleuteling met de onheilspellende woorden: “Cryptopocalypse is near.” Joshua Cornwell is als filosoof een tijdje opgetrokken met Anonymous en waarschuwt dat de gevaren uit de cyberwereld steeds meer de fysieke wereld gaan bepalen. Enkele managers van grote bedrijven zien vooral kansen in cyber security, als we allemaal maar goed samenwerken. En de mensen van het NCSC, die de conferentie organiseren, komen natuurlijk ook aan het woord. Erg gezellig allemaal, maar hierdoor heb ik zelf wel zo ongeveer het hele event gemist.

Tussen de items door loop ik daarom de trap op naar de grote zaal, om toch nog even iets van de keynotesprekers te zien. Helaas, de deur is dicht. Dan ontdek ik een jongen die daar ook

staat te wachten. Hij heeft geen pak aan, maar gewoon een zwarte spijkerbroek en T-shirt. Hij is een stuk jonger en langer dan ik en zijn lijf lijkt enigszins uit verhouding. Ik had hem al eerder voorbij zien lopen, met nog vier jongens. Dan denk ik aan mijn onderzoek en spreek hem aan: “Hee, ik zag je net met die andere jonge gasten. Wat doen jullie hier? Zijn jullie hackers ofzo?”

De jongen begint meteen te vertellen: “Ja, ik heb al T-shirts gekregen van het NCSC. Veel Cross Site Scripting gedaan. Zij hebben er maar één, ik heb er vijf, maar er zit er ook eentje bij die heeft er al acht…” Ik vraag hoe oud hij is. “Ik ben veertien jaar, maar heb al veel ervaring met computerbeveiliging. Werd vroeger ook wel gepest, heb ADHD, of autisme ofzo, maar ze weten nog niet precies wat ik heb, want dat moet nog uitgezocht worden en daarom krijg ik nu medicatie.” Deze jongen praat, zonder me aan te kijken, over zichzelf alsof hij een computer is waar nog een bug gefikst moet worden.

Hij heet Mischa van Geelen en het liefst zou ik meteen een interview met hem doen, maar ik moet weer terug naar de studio. Daar zou ik hem voor de camera kunnen zetten om zijn verhaal te doen, maar dat lijkt me ongepast gezien zijn persoonlijke ontboezemingen. Bovendien ben ik hier niet voor mijn onderzoek, maar voor het NCSC. Ik moet nog een aantal kopstukken interviewen en dan is de conferentie alweer bijna voorbij. Ik vertel hem daarom kort waar ik zo al mee bezig ben en stel voor elkaar later nog eens te spreken. We wisselen telefoonnummers uit en gaan elkaar volgen op Twitter.

Als de laatste interviews zijn gedaan, is ook de conferentie al voorbij en zien we de laatste gasten vertrekken. Tijdens het opruimen volgt nog een laatste onverwachte ontmoeting. Het is @0xDUDE, die op Twitter vaak vertelt over beveiligingsproblemen. Ook hem had ik graag willen interviewen, want hij schijnt al veel verantwoorde onthullingen te hebben gedaan. “Ja, dat zijn er nu 3645”, vertelt hij, “maar niets daarvan is in de media verschenen. Ik werk het liefst achter de schermen.” Ik ben onder de indruk van deze leeftijdsgenoot, die al vijftien jaar verantwoorde onthullingen blijkt te doen. Maar ik ben tegelijkertijd ook doodmoe van de twee dagen interviewen en maak ook met hem de afspraak elkaar later eens uitgebreid te spreken.

We hebben tijdens NCSC One in twee dagen tijd zestien items geschoten, waarbij we de gasten telkens de keuze gaven of we hun video ook op Youtube mogen zetten. Ze vonden het allemaal meteen prima. Het NCSC zelf ook, zonder enige controle of redactieslag op wat we daar met de experts hebben besproken. Cyber security is dan wel een technische wereld die draait om geheimen, maar de mensen in deze wereld houden vooral van openheid. Kennis delen, om bij te blijven en anderen te laten zien dat wat we doen belangrijk is, daar gaat het hier om. Gesterkt door deze ervaring en met een paar nieuwe contacten, ga ik daarna weer verder met mijn onderzoek.

Een week later zie ik een tweet voorbij komen van @rickgeex. Het is Mischa en hij heeft een kwetsbaarheid gevonden op mijn website. In een DM-bericht staat een url naar mijn site, met erachter “alsjeblieft”. Verder geen uitleg. Ik klik erop en zie onze nieuwsbrief verschijnen, maar niets bijzonders. Als ik hem vraag wat er aan de hand is, vertelt hij dat hij een Cross Site Scripting zou kunnen doen en zo bezoekers naar een andere site kan loodsen. Dat zou natuurlijk wel vervelend zijn, denk ik, als ik straks iedereen mail dat de video’s online staan en ze onbewust naar een site met malware stuur.

Ik begrijp niet helemaal hoe iemand de nieuwsbrief zou kunnen aanpassen, dus stuur ik zijn melding door naar de provider die mijn site beheert. Die reageert gelukkig meteen en zegt dat wat Mischa doet alleen kan op zijn eigen computer en niet op de site. Volgens Mischa zelf kan dat wel en er ontstaat een discussie, die eindigt als de provider toch iets aanpast. Wat er precies gebeurd is, weet ik niet, maar het is op zich wel interessant om zelf eens een melding af te handelen. Mischa heeft intussen zijn tweet verwijderd, want hij realiseert zich dat je kwetsbaarheden beter niet openlijk kan melden en ik bedank hem hartelijk voor zijn hulp.

Mischa wijst me ook op zijn blog, waar hij een verslag heeft gepubliceerd over kwetsbaarheden in Truecrypt. Dat is het programma waarmee de hacker van het Groene Hart Ziekenhuis zijn bestanden had verborgen en dat wel vaker wordt gebruikt door hackers om hun data af te schermen. Hij zou een lek hebben

gevonden waarmee je de encryptie kunt omzeilen. Hoe het precies werkt, snap ik niet, maar ik besluit het op Twitter te zetten. Ik heb inmiddels al aardig wat ethisch hackers onder mijn volgers, dus wellicht kan ik hem zo helpen aan interessante contacten, dus ik tweet: “Hee techies, anyone understand this report? Did @rickgeex found a gov backdoor in #truecrypt?”

Iemand die ik nog ken van de #fristileaks reageert, maar schrijft dat hij niet begrijpt waarom de kwetsbaarheid die @rickgeex heeft gevonden interessant zou moeten zijn. Ik uiteraard ook niet, dus ik bemoei me er even niet mee en hoop op wat positievere reacties. Als hij vervolgens schrijft: “It’s clearly bullshit” kan ik het niet laten hem via de DM een beetje respect te vragen voor de nog jonge hacker. Hij schrijft dat hij misschien wat minder grof had moeten zijn, maar zijn bevindingen negeren zou pas echt respectloos zijn. Daar heeft hij ook wel weer gelijk in. Daarna stopt de Twitterdiscussie. Blijkbaar was het toch niet zo interessant, maar @rickgeex heeft er wel weer wat volgers bij, onder andere de ervaren @0xDUDE.

Enkele maanden later word ik midden in de nacht wakker gebeld. Ik negeer het eerst, maar als mijn telefoon blijft gaan, ga ik toch even kijken wat er aan de hand is. Het is Mischa weer, dit keer met een hele reeks Whatsappberichten:

0.41: “Hi Chris”
0.47: “Ik zoek hulp…bij het blootleggen van een reeks vulnerabilities”
1.23: “Hallo”
1.24: “Sorry, het is verschrikkelijk belangrijk en krijg geen vat op het bedrijf”
1.24: “Excuus voor het late telefoontje”
1.24: “Mischa”
1.25: “Ik krijg waarschijnlijk een aanklacht anders.”
1.27: “Anyway, hoop op je hulp. Groeten”

Ik besluit het te negeren, want ik wil graag verder slapen. Die dag moet ik namelijk weer een congres leiden en ik kan mijn rust goed gebruiken. Voor het College Bescherming Persoonsgegevens nota bene. “Over bescherming van de persoonlijke levenssfeer gesproken”, mompel ik tegen mijn vriendin, die ook niet echt blij is

met de plotselinge nachtelijke activiteiten. Ik denk ook niet dat ik hem kan helpen met zijn vulnerability report. Wellicht kan hij hiermee beter naar het NCSC. Dat schrijf ik ook de volgende ochtend aan hem terug, met het verzoek mij niet meer ’s nachts te bellen.

Toch blijft het aan me knagen: doe ik een onderzoek naar responsible disclosure, komt zo’n jonge hacker naar me toe en kan ik niets voor hem betekenen. Maar wat zou ik kunnen doen? Ik heb zelf onvoldoende verstand van computers om in te schatten of een gevonden kwetsbaarheid ook echt iets is. Ik wil ook zeker geen Brenno de Winter worden en in allerlei conflicten belanden. Ik wil een boek schrijven waarin ik achteraf alle kanten belicht, om zo toekomstige conflicten juist te voorkomen. Bovendien ben ik op dat moment vooral druk bezig met congressen, want die zijn om de een of andere reden bijna allemaal in het najaar en ligt de vordering van dit boek even stil.

Dan neemt Mischa weer contact met me op. Dit keer via de mail en hij vraagt of hij nog iets voor mij kan betekenen. Blijkbaar zijn de verhoudingen omgekeerd. Ik zoek inderdaad nog een echte hacker voor een sessie bij het ECP-jaarcongres van 20 november. Dat is elk jaar weer een groot feest en lijkt me een perfecte plek om alvast dit boek te pitchen. Niet met een saaie presentatie, maar met een levendige discussie. Ik heb al Astrid Oosenbrug, die het in de Tweede Kamer vaak heeft opgenomen voor ethisch hackers, Jeroen van der Ham, met zijn ethische commissie aan de UvA en niemand minder dan Brenno de Winter om de kant van de journalistiek te belichten. @rickgeex is perfect getypecast binnen dit gezelschap. Stiekem hoop ik ook dat hij dan na dit congres met zijn meldingen terecht kan bij Brenno of Jeroen.

Om me voor te bereiden op ons gesprek google ik wat op zijn naam. Hij is dan nog maar vijftien jaar, maar heeft wel al een LinkedIn-profiel en een mooie site. Hier lees ik dat hij een gepassioneerde security researcher is, met zeven jaar ervaring. Hij heeft veertien Awards en tachtig responsible disclosures op zijn naam staan vanwege kwetsbaarheden die hij heeft gemeld bij ABN AMRO, SNS, ING, eBay, Marktplaats, Vakantieveilingen,

Microsoft, Google, Apple, Firefox, Belastingdienst, Rijksoverheid, Rijkshuisstijl, NCSC, Defensie en Sony. Indrukwekkend.

Daarna bellen we nog even om de sessie door te nemen. Ik vertel hem dat ik dan zal vragen hoe hij te werk gaat bij het vinden van kwetsbaarheden, hoe hij dit meldt en wat voor reacties hij dan krijgt. Daar wil hij wel wat over vertellen. Ik vraag hem wat voor opleiding hij doet en hij vertelt dat hij nu in het eerst jaar zit van een mbo, maar dat gaat niet zo goed vanwege gedragsproblematiek. Dat kwam volgens hem vooral vanwege de medicatie die hij kreeg en daar is hij nu vanaf. Ik moet nog wel binnenkort op zijn website kijken want die is hij net aan het vernieuwen. Hij heeft dan inmiddels honderd responsible disclosures op zijn naam en staat nummer één op de NCSC ranglijst van melders. Ook bij andere organisaties prijkt zijn naam in de Hall of Fame.

ECP is een platform dat mensen in de informatiesamenleving met elkaar verbindt. Het is volgens mij ook de enige club in de ICT die voornamelijk bestaat uit vrouwen. Die organiseren veel bijeenkomsten waar vervolgens vooral mannen op af komen: consultants, ambtenaren en zelfstandigen. Dit jaar is het congres in de Fokker Terminal en als ik de hal binnenkom gonst het van de grijze pakken die druk aan het netwerken zijn. Al zwaaiend en handenschuddend werk ik me door de menigte, op zoek naar mijn panelleden. Pas als het hoofdprogramma begint, zie ik dat Mischa al klaar zit in de grote zaal. Hij valt met zijn zwarte haardos meteen op tussen de grijze en kale mannen. Als hij gaat staan en mij een hand geeft, valt me vooral op hoezeer hij is veranderd. Hij staat rechtop, is behoorlijk afgevallen en kijkt me nu wel aan.

“Jeeh, wat is er met jou gebeurd!” roep ik uit. “Nu ik ben gestopt met medicatie, ben ik 37 kilo afgevallen en voel me een stuk beter”, zegt hij terwijl hij blij zijn armen in de lucht steekt. We willen liefst meteen bespreken wat we straks gaan doen in de sessie, maar het hoofdprogramma begint en we moeten stilzitten. Dat blijkt nog niet zo makkelijk voor hem. Hij zit druk te draaien op zijn stoel en vertelt bij elke organisatie die op het podium verschijnt wat voor kwetsbaarheden hij heeft gevonden op hun websites. Gelukkig hebben de oudere heren om ons heen niet

echt veel last van de praatgrage jongen en vinden ze het volgens mij wel vermakelijk wat ze horen.

Wel vraag ik me af hoe ik hem straks tijdens de sessie een beetje kort kan houden. We hebben met z'n vijven maar veertig minuten en ik wil ook het publiek nog aan het woord laten. Maar ook daarin onderschat ik hem want elk antwoord dat hij geeft op mijn vragen is kort en helder en in nog geen vijf minuten geeft hij het publiek een duidelijk beeld van hoe hij als ethisch hacker te werk gaat. Als ik vraag naar zijn toekomst, vertelt hij dat hij zo snel mogelijk het mbo wil afmaken om naar de UvA te gaan. Naar de opleiding van Jeroen van der Ham dus. Die vertelt vervolgens over zijn studenten en hoe hun onderzoek naar beveiligingslekken wordt begeleid door een ethische commissie. Hij hoopt dat jongens als Mischa de weg zullen vinden naar de universitaire wereld.

Dat is aardig van Jeroen, maar de rest van het panel vindt vooral dat er ook wel wat mag veranderen in het onderwijs, want veel hacktalent haalt het gewoon niet naar de universiteit. Ze zijn heel slim, maar denken gewoon anders en daar kunnen leraren niet mee omgaan. We spreken daarbij ook wel een beetje uit eigen ervaring. Brenno, Astrid en ik liepen ook tegen van alles aan op de middelbare school: moeite met lezen, te eigenwijs, andere interesses. Ikzelf las gewoon helemaal niet, maar kon wel heel goed rekenen en werd daarom maar naar de lagere technische school gestuurd. Dat was het toenmalige vmbo en pas later ging ik lezen en zelfs studeren. Uiteindelijk hebben we elk op onze eigen manier een weg gevonden in de informatiesamenleving. Die weg is voor Mischa net begonnen en daarom nemen we het voor hem op.

Na de sessie hebben we ook nog een fotoshoot. Tobias Groenland wil namelijk portretten maken van mensen in de ICT. Hij ziet hen als voorboden van een nieuwe tijd in de informatiesamenleving en heeft mij gevraagd of ik nog geschikte personen ken. Ik stel voor mijn hele panel stuk voor stuk voor de camera te halen en dat vindt hij een goed idee. Hij heeft ook een studio ingericht: een koud kamertje achterin de Fokker Terminal met veel felle lampen en een mooie witte achtergrond. Hij wil

indringende, rauw realistische portretten. Die zal hij levensgroot gaan tentoonstellen, met opgenomen geluidsfragmenten.

Als Mischa aan de beurt is, blijf ik erbij en zie ik hoe hij zich al de aanwijzingen voor poses van de fotograaf en het geflits laat welgevallen. Als Tobias na afloop een interview met hem doet, hoor ik hem vertellen over zijn medicijngebruik. Al die pillen waren eigenlijk niet nodig geweest en daar is hij best boos over. Maar, omdat hij in die jaren bijna niet met anderen omging, heeft hij wel de computer goed leren kennen. Dat is dus hoe hij al op jonge leeftijd security expert is geworden. Na de shoot moet Mischa er meteen weer vandoor. Hij heeft namelijk een afspraak bij het NCSC. Later hoor ik dat hij inmiddels regelmatig bij het NCSC over de zwaarbewaakte vloer van het Ministerie van Veiligheid en Justitie komt om zijn meldingen toe te lichten en zo met het NCSC samen te werken. Wie weet wat hem en het NCSC nog te wachten staat.

Dat geldt ook voor Jeroen van der Ham, die dezelfde dag ook op gesprek ging bij NCSC. Hij is daar nu aan de slag als security onderzoeker. Zelf heb ik intussen contact opgenomen met de andere jongen van het clubje dat tijdens de NCSC One conferentie rondliep: Olivier Beg, de jongen die niet alleen acht NCSC T-shirts, maar ook een aardig inkomen bij elkaar heeft gehackt.

23. Beg en de Bug Bounties

0md4t H4ck3rs d3 d1ng3N v44k g3w00N N3t 13ts 4Nd3rs z13N d4N 4Nd3r3N

Op 12 oktober 2014 gaat het VPRO-programma Tegenlicht over zero days, met als ondertitel: ‘veiligheidslekken te koop’. De voice-over schetst in de opening een onheilspellend beeld: “Terwijl wij rustig over het internet surfen, scant een elite van de slimste hackers dag en nacht naar onbekende veiligheidslekken. Ze toveren deze lekken om tot bouwstenen voor cyberwapens en verkopen deze voor astronomische bedragen aan criminele organisaties. Maar ook aan veiligheidsdiensten en cyberlegers, die hiermee ongemerkt kunnen binnendringen in uw computer, bij banken of zelfs kerncentrales. Onder hackers is een gold rush gaande naar veiligheidslekken, ze noemen dit goud zero days.”

Zero days zijn kwetsbaarheden in software die nog niet eerder gevonden zijn. Als jij die vindt, heb je een voorsprong op anderen die de kwetsbaarheid nog niet kennen. Dit wordt in het programma ondersteund met een interessante beeldretoriek. Normaal gesproken is het moeilijk om ICT op tv in beeld te brengen, want alleen pratende hoofden en schermen met code zijn saai, maar deze journalisten hebben er iets moois van gemaakt. Fox-IT-directeur Ronald Prins wordt aangekondigd als “de machtigste nerd van Nederland” en helpt hen een handje door met zijn drone zichzelf te filmen op het dak van hun kantoor. Cyberkolonel Hans Folmer spreekt een groep mannen in uniform toe alsof de cyberoorlog al is begonnen, maar als hij wordt gevraagd of Nederland ook een cyberwapen heeft, zwijgt hij veelbetekenend. Tussen de interviews door zien we telkens hackers in een woestijn machinegeweren afvuren. Zelfs tijdens de interviews knallen ze door. De boodschap is duidelijk: virtuele wapens zijn ook echte wapens.

Na al dit geweld zien we iemand die een cheque van 200.000 dollar in handen krijgt en overladen wordt met confetti. De voice-

over vermeldt: “Een succesvolle white hat hacker is de 17-jarige Olivier Beg die duizenden euro’s heeft verdiend aan het vinden van zero days bij Yahoo. Ook hackte Olivier met enige regelmaat de Nederlandse banken. En hij hackte de Belastingdienst.” We zien een jongen in een kamer met alleen een bed, bureau en twee computerschermen. Hij toont een beker met de tekst: “I hacked the Dutch Taks Administration and never got a refund”.

Beg vertelt waarom hij hackt: “Ik denk vanuit een interesse voor computers en toen programmeren en vanuit programmeren ook lekken vinden in codes.” Hij laat nog wel een handboek zien, maar vertelt dat hij het vooral zichzelf heeft aangeleerd. Op een video zien we hoe hij op de site van Yahoo ‘1=1’ invoert in een text box die eigenlijk bedoeld is om kortingscodes in te vullen. Het bedrag van zijn aanbesteding schiet vervolgens op nul. “Een zero day waarmee hij gratis kon winkelen”, meldt de voice-over enthousiast, “maar in plaats van dat te doen, stuurde hij dit filmpje naar Yahoo om ze te helpen deze kwetsbaarheid op te lossen.”

De documentaire is misschien wat tendentieus door hacken gelijk te stellen aan wapenwedloop, maar zo gaat dat met televisie. De makers wijzen ons wel op een dimensie die tot nog toe onbelicht is gebleven: hacken kan ook veel geld opleveren. Beg kreeg overigens niet die twee ton, maar 16.000 dollar voor alle bugs die hij vond bij Yahoo. Dat lees ik in een artikel op Webwereld, met de titel: ‘Nederland karig met belonen white hat hackers’. Het is een pleidooi voor betere bug bounties, zoals ook de grote Amerikaanse bedrijven doen. Hier in Nederland is er weliswaar responsible disclosure beleid, maar de melder krijgt meestal alleen maar een T-shirt of een paar cadeaubonnen. Het artikel laat in het midden of dit nu gierigheid is, of dat we gewoon bang zijn voor hackers.

Beg is te vinden via zijn site olivierbeg.nl en op Twitter als @smiegles. Op 22 oktober 2014 hebben we een belafspraak. Hij is net achttien jaar geworden en loopt op dat moment stage voor zijn mbo-opleiding. En ja, hij is nog steeds nummer één in de Hall of Fame van Yahoo. Als ik begin te vertellen over mijn onderzoek, zegt hij dat hij er al vanaf weet. Hij blijkt een van de jongeren te zijn die tijdens de NCSC One conferentie daar rondliep. Dus roep

ik enthousiast: “Ah, dan ben jij die met die acht NCSC T-shirts!” Ja, het is hem: “Maar ik heb inmiddels al een hele kast vol. Ik weet ook niet waarom ze me die blijven sturen.”

Tijdens ons gesprek kom ik erachter dat hij ook een van de melders was tijdens Lektober, de maand oktober 2011 waarin Webwereld elke dag een lek meldde. Ik zal niet zeggen welke onthulling, want hij bleef toen, net als de meeste melders, liever anoniem. Hij was dus nog maar veertien jaar toen hij het lek vond. Twee jaar daarna had hij nog een onthulling voor Webwereld, maar die ging over hun eigen content management systeem. Hij ontdekte namelijk een manier om in de account van een journalist te komen. Het zou best grappig zijn geweest als hij dan had geprobeerd zelf een artikel op de site te zetten, maar hij was volwassen genoeg om dat niet te doen.

Ondanks zijn bijzondere begaafdheid, bleek school niet makkelijk voor hem. Of misschien juist wel daarom. Op de lagere school ontdekten ze dat hij dyslectisch is. De lesstof interesseerde hem ook niet zo, dus werd hij naar het vmbo gestuurd. Daar ging hij tijdens de les zitten hacken, vooral uit verveling en omdat de school een snelle internetverbinding had. Als Olivier beveiligingsproblemen in het schoolnetwerk vond, meldde hij dat netjes. Verder zei niemand er wat van als hij tijdens de les op zijn laptop werkte. Ook zijn ouders begrepen niet echt wat hij deed, maar lieten hem zijn gang gaan.

In de jaren daarna trad Olivier steeds meer naar buiten met zijn meldingen en dat zijn er behoorlijk wat. Zo’n beetje alle grote Nederlandse banken: ABNAmro, ING, SNS, RABO, ASN, Regiobank en Van Lanschot Bank. Soms kreeg hij wat VVV-bonnen, maar vaak ook een spreekverbod omdat de organisaties liever niet wilden dat anderen hoorden over hun kwetsbaarheden. Ook bij de grote telecombedrijven vond hij veel kwetsbaarheden. UPC, Ziggo en KPN namen zijn meldingen netjes in ontvangst, zonder beloningen te geven. Bij XS4all kreeg hij nog wel een appeltaart. Zijn melding bij T-mobile is echter nog steeds onbeantwoord.

Hij ontdekte ook lekken bij de Nederlandse overheid, bijvoorbeeld op de site van de Belastingdienst. Daar bleek een oude Adobe Flash Player te draaien waar hij een Cross Site

Scripting zou kunnen doen. Deze videoapplicatie werd bovendien gebruikt bij verschillende andere overheidssites, waaronder ook het NCSC. Hij meldde het daarom bij het centrum. Het was zondagavond 22.50 uur. Hij kreeg al om 23.10 uur een reactie en zag twintig minuten later dat het gefikst was, ook bij de Belastingdienst. Opmerkelijk, want zo'n vlotte reactie verwacht je niet van de overheid. Als dank kreeg Beg de beker die hij liet zien in de aflevering van Tegenlicht.

Beg vertelt dat hij best verbaasd was toen hij bij Yahoo geen VVV-bon, T-shirt of beker kreeg, maar gewoon keiharde cash: bijna duizend dollar per melding. Hij deed er zeventien, dus tel uit je winst. Het Parool kopte toen trots: '17-jarige Amsterdammer voert hackerslijsten aan'. Bovendien staat hij niet alleen bij Yahoo in de Hall of Fame, maar ook bij Google, Microsoft, Nokia, Apple, Adobe, AT&T, eBay… Als ik hem vraag of hij liever gaat voor de bounties of zich ook nog wel wil inzetten voor het Hollandse vrijwilligerswerk, zegt hij me dat het hem eigenlijk niet zoveel uitmaakt. Hij doet het vooral voor de erkenning. Hij wil de puzzel oplossen en dat aan anderen laten zien.

Op het moment van ons interview heeft hij overigens nog maar weinig tijd voor ethisch hacken, want hij doet al de hele dag aan informatiebeveiliging op zijn stage. Nog een paar maanden en dan is hij klaar met het mbo. Als dit boek verschijnt, is hij waarschijnlijk op reis door de VS om wat hackerscongressen te bezoeken. Daarna ziet hij wel verder. Ik vraag me daarom af hoe we jongens als Olivier in Nederland houden. Hun werk is blijkbaar belangrijk, maar wordt nog onvoldoende gewaardeerd.

Vooral in het onderwijs blijkt men nogal moeite te hebben met jonge hackers. Wellicht was je dat al opgevallen in voorgaande hoofdstukken. Er zitten er een paar bij die uiteindelijk wel de universiteit halen. Verdult, die de OV-chipkaart kraakte, is ondanks zijn dyslexie en mavo uiteindelijk zelfs gepromoveerd aan de universiteit, maar hij is wel een uitzondering. De meesten die ik heb gesproken blijven ergens steken in het middelbaar beroepsonderwijs. Dat, terwijl ze naar mijn mening wel buitengewoon intelligent zijn. Nu weet ik vrij weinig van onderwijs - dus kan ik daar niet echt over oordelen - maar ik hoor wel vaak

vanuit de cyber security dat hier nog veel te winnen valt. Zo ook op 23 juni 2014, tijdens een ‘Ronde Tafel bijeenkomst Cyber Onderwijs’ op het ministerie van OCW.

Het initiatief komt van de Cyber Security Raad. Dat is een club experts die de taak hebben om “de regering en private partijen gevraagd en ongevraagd adviezen te geven over relevante ontwikkelingen op het gebied van digitale veiligheid”. Voor 2014 is het thema onderwijs één van de speerpunten van de raad en hebben ze hiervoor een werkgroep in het leven geroepen. Deze groep stelt vast dat “vanwege de enorme opmars van ICT in ons werk en dagelijks leven, digitale veiligheid een bijzonder belangrijk aandachtspunt is. In het onderwijs blijft dit tot op heden onderbelicht, met als gevolg een tekort aan opgeleide deskundigen, een te laag algemeen bewustzijn van de noodzaak van digitale veiligheid en daardoor mogelijk negatieve gevolgen voor de Nederlandse samenleving en economie. De werkgroep is van mening dat investeren in cyber security in het hoger onderwijs vooral bij kan dragen aan het beschikbaar krijgen van meer deskundigheid.”

Het is een redelijk gemêleerd gezelschap dat bijeenkomt in de caféruimte van het ministerie: jong, oud, man, vrouw, bedrijfsleven, onderwijs, overheid en verder nog wat zelfstandige consultants. Ik zie echter maar één hacker: Melanie Rieback van Radically Open Security. De inleiding wordt verzorgd door hoogleraar cyber security Jan van den Berg. Hij begint met een opsomming van de problemen in zijn sector: te weinig studenten, leraren te oud en verkokering van academische specialismen. De oplossing: meer samenwerking met bedrijven, multidisciplinair en iets leuks met jongeren.

Ik vraag daarom wat we kunnen doen voor briljante jonge hackers, die op de een of andere manier het vwo zijn misgelopen en de sector zeker veel te bieden hebben. Waarom geen mbo cyber security of een soort zij-instroomprogramma? Nee, dergelijke moeilijke materie moet je wel op niveau behandelen volgens de hoogleraar. Liefst universitair. Aan het hbo wordt gewerkt, maar dat loopt nog wat moeilijk. Dan roept Rieback enthousiast: “Doe iets met hackerspaces, daar ligt zoveel kennis

en dat vinden jongeren leuk!” De deelnemers kijken haar glazig aan. Iemand vraagt: “Hackerspaces, waar zijn die dan?” Zucht.

Beste mensen: H4ck3rs z13N d3 d1ng3N v44k g3w00N N3t 13ts 4Nd3rs d4N 4Nd3r3N. Als het goed is, heb je moeite met het lezen van de voorgaande zin. Zo niet, dan ben je er waarschijnlijk ook zo een en heb je in het verleden juist veel moeite gehad met het lezen van gewone tekst. Respect dat je zover bent gekomen in dit boek.

In mijn onderzoek naar ethisch hackers kom ik vaak dit levensverhaal tegen: slechte cijfers ondanks uitzonderlijke intelligentie, dan maar naar het vmbo, misschien nog een mbo-certificaat of een cursusje erachteraan, gevolgd door een stage. De meesten zijn erg leergierig, maar hebben moeite met teksten stampen. De één vindt het leuk om zich lange tijd te focussen op een heel specifiek probleem, de ander heeft de gave om bij een complex systeem direct te zien wat afwijkt en een derde heeft er vooral lol in van alles uit te proberen tot een systeem vastloopt. Waarom doen ze dit? Antwoorden die ik dan vaak krijg zijn: “Ik wil weten hoe iets werkt”, “de puzzel oplossen” of “de kick ergens in te kunnen”. Dat is de hackersmentaliteit.

Informatietechnologie wordt gemaakt met een gebruiker op het oog die zo ongeveer doet wat de makers verwachten: klik op A of op B, vul hier gewone tekst in, upload hier je video en vind dit leuk. De software wordt eerst intern getest op bugs en vervolgens net zo lang op gewone mensen uitgeprobeerd totdat alles redelijk naar tevredenheid werkt. In dat proces worden continu fouten gemaakt die de makers en gebruikers niet zien en hackers wel.

De buitenwereld en met name het onderwijs, heeft de neiging de aparte leerlingen te behangen met labels zoals dyslexie, ADHD of autisme, die vooral aangeven wat ze niet kunnen. Dit is naar mijn idee vooral een reactie van een samenleving die niet goed weet wat ze aan moet met mensen die anders denken en hen daarom maar pathologiseert. Ik denk dat iedereen wel de neiging heeft om tegenover de rauwe rommelige werkelijkheid een eigen wereld te creëren waarin de dingen wel kloppen, alleen doen hackers dat anders dan anderen. Dat zie je ook bij schrijvers, kunstenaars en muzikanten. Dat de buitenwereld niet

direct begrijpt wat er allemaal in hen omgaat, is dan ook niet zo erg, maar eerder een bevestiging van hun eigen wereld.

Dat hackers anders denken dan anderen ziet Peter van Hofweegen vooral als een nieuwe kans voor de detacheringsmarkt. Samen met IT'er Frans de Bie heeft hij het bedrijf ITVitae opgericht. Hun site meldt: "Wij werken met bijzondere professionals, die bijzondere resultaten boeken. Dat maakt ons bijzonder krachtig." Hun missie: "Het creëren van maatschappelijke impact door mensen uit het Autisme Spectrum op te leiden tot IT-professional en hen aan het werk te helpen." Als ik Van Hofweegen spreek, vertelt hij dat ITVitae inmiddels tien cyber security-experts begeleidt die allemaal wel een beetje apart zijn en beschikken over bijzondere vaardigheden die heel nuttig zijn. Zeker in de ICT, waar een groot tekort is aan geschikt personeel. Hij regelt de detachering en De Bie training, zodat hun jongens zich volledig kunnen richten op waar ze goed in zijn: software testen en hacken.

Beide heren halen hun motivatie vooral uit hun privéleven. Van Hofweegen heeft een zoon met Asperger. Dat is een milde vorm van autisme gepaard met een bijzonder hoge intelligentie. Deze mensen kunnen heel goed denken in logische structuren en zien sneller dan anderen afwijkende details. Van Facebookbaas Mark Zuckerberg wordt bijvoorbeeld beweerd dat hij ook Asperger heeft. De Bie heeft twee kinderen met dyslexie en dat is iets wat ook veel voorkomt onder ICT-talenten. Maar ondanks de uitzonderlijke talenten van hun kinderen, liepen ze aan tegen de beperkingen van het reguliere onderwijs.

Dat herken ik, want zo'n vader ben ik ook. Mijn dochter moest in groep drie een jaar overdoen vanwege een leerachterstand, terwijl ze wel de namen en eigenschappen van bijna alle bekende dinosaurussen kon opnoemen. Lena is dyslectisch en heeft een enorme fantasiewereld. Het stampen van rijtjes woorden kwam niet over bij haar. Ik heb inmiddels begrepen dat bij dyslexie tekst ook anders bij je binnenkomt: niet lineair van links naar rechts, maar door elkaar, waardoor het brein continue zoekt naar structuur en daar betekenis aan geeft. Met lange, ingewikkelde woorden heeft ze bijvoorbeeld minder moeite dan de korte, want

de afwijkingen zijn makkelijker te herkennen. Nadat ze op een andere manier leerde lezen en schrijven, schoten haar cijfers omhoog en kon ze naar een klas voor hoogbegaafden. Nu is ze vooral trots op haar anders zijn. Ik begrijp daarom de motivatie van Van Hofweegen en De Bie, al is mijn dochter helaas niet geïnteresseerd in computers.

Als ik vertel over mijn onderzoek is Van Hofweegen meteen enthousiast. Hij zoekt nog meer hackers en organisaties waar ze aan de slag kunnen, dus wellicht kan ik hem nog hier en daar introduceren. Dan vertelt Van Hofweegen dat hij geïnspireerd was door een presentatie met de titel: ‘Hire the hackers!’. Daarin zegt onderzoeker Misha Glenny dat veel hackers Asperger hebben en daarom zo goed met computers zijn. Ze zijn alleen niet zo goed met mensen en zijn daarom ergens in het leven vastgelopen, het slechte pad op gegaan en uiteindelijk in de gevangenis beland. Van Hofweegen: “Voor deze jongens geldt wit is wit en zwart is zwart. Je wilt voorkomen dat ze in handen van criminelen vallen.” Hij overweegt zelfs bij de reclassering langs te gaan, op zoek naar veroordeelde cybercriminelen die zij onder hun hoede kunnen nemen. Dit hoorde ik ook tijdens mijn gesprekken met de politie en het openbaar ministerie. Jonge hackers zijn technisch begaafd, maar hun morele kompas is nog onderontwikkeld. Lodewijk van Zwieten, de landelijke aanklager Cybercrime, wordt ook wel eens gekscherend de jongerenafdeling van het OM genoemd.

Ik begrijp hun punt, maar moet hen hier toch even corrigeren. Bij de ethisch hackers die ik heb ontmoet in mijn onderzoek zie ik juist een bijzonder groot verantwoordelijkheidsgevoel. Hun morele kompas lijkt prima in orde. Ze zouden veel schade kunnen aanrichten bij anderen, zonder dat iemand het doorheeft, maar ze doen dat juist niet. Dat is wat hen onderscheidt van de black hats. Soms ontketenen ze weliswaar een rel met hun onthullingen, maar dat is eerder te wijten aan de journalistiek en de politiek die dingen opblazen. Er zitten volgens mij ook geen echte autisten bij, hooguit wat aparte types met een eigen kijk op de wereld, die wat meer gedreven zijn dan anderen. Van Hofweegen zegt dat dat ook wel geldt voor zijn jongens, maar autisme blijft wel zijn interesse houden.

Het is dus vooral de buitenwereld die zal moeten wennen aan de andersdenkenden en niet andersom. Meer wederzijds begrip zou fijn zijn, maar ook zonder hulp zullen de helpende hackers wel een plek vinden in onze samenleving. Olivier Beg in ieder geval wel, want als ik deze tekst op 27 januari 2015 naar hem toestuur voor een laatste controle, krijg ik een update: “Het bedrag en aantal lekken is niet meer 16.000 dollar en 17 lekken maar zo’n 40.000 dollar en 45 lekken.” Hopelijk worden dit spoedig ook euro’s. Niet vanwege het geld, maar wel vanwege de erkening.

24. @0xDUDE, the biggest dude of ’em all

De man achter bijna vierduizend verantwoorde onthullingen

Na onze korte ontmoeting tijdens de NCSC One conferentie lukt het me maar niet om @0xDUDE te spreken. We mailen nog wel wat over zijn database met duizenden meldingen, maar daar wil hij niet al teveel over kwijt. Hij heeft ze immers achter de schermen afgehandeld. Wel heeft hij een lijstje gestuurd met het type beveiligingslekken en webdiensten waar het om ging. Zo’n beetje alles wat in dit boek voorkomt zit er wel bij. Maar om te duiden wat dit alles betekent, moet ik hem toch echt even spreken. Ik zie zijn naam vaak op de gastenlijsten van de vele conferenties en seminars die in het najaar van 2014 spelen, maar telkens lopen we elkaar mis.

Van 28 oktober tot en met 6 november is de landelijke campagne Alert online waarin zo’n beetje heel cyber security Nederland bij elkaar komt. Met ons team hebben we op 28 oktober een Tek Tok Studio bij KPN, om via Youtube te laten zien wat het grootste telecombedrijf van Nederland doet aan cyber security. Op 4 november hebben we met ECP weer een aflevering van Tek Tok late night in het Paard van Troje, om de site veiliginternetten.nl te lanceren. Daar omheen probeer ik zoveel mogelijk bijenkomsten van anderen te bezoeken. De slotbijeenkomst van Alert online is op 6 november in Rotterdam en die is alleen voor de belangrijkste mensen en bestuurders. Ik ben niet uitgenodigd, @0xDUDE wel. Dat is voor mij een mooie gelegenheid om even op mijn fiets te springen en hem uit de menigte te halen voor een interview.

De statige hal van het Hulstkampgebouw aan de Maaskade is vol wit marmer met rood pluche. Terwijl bestuurders voorbij komen met jassen, tassen en zakenkaartjes in handen, ontmoet ik @0xDUDE weer. Hij heet Victor en met zijn kleurrijke pak, zwarte

baard en kuif lijkt hij meer op een kunstenaar dan een hacker. Ik vraag of hij op dat moment niet nog iets belangrijkers te doen heeft nu al die mensen hier zijn, maar op de manier waarop hij ‘nee’ schudt, merk ik dat hij het eigenlijk wel best vindt de conferentie eventjes te verlaten. Een interview hier zou niet lukken, dus ik moet een rustig plekje vinden. Onderweg hier naartoe zag ik een broodjeszaak die er wel relaxt uitzag, dus ik stel voor daar te gaan lunchen.

Eenmaal in de lunchroom vraag ik me af of deze plek eigenlijk wel geschikt is voor een interview. Twee ongure types hangen op een bank en kijken ons wantrouwend aan terwijl er harde hiphopmuziek klinkt. Met de pasteltinten en namaak palmboompjes lijkt dit eerder een coffeeshop, dus ik vraag voor de zekerheid of ze ook lunch hebben. Een charmante dame achter de bar geeft ons een lunchkaart, maar zegt dat het wel even gaat duren. Geen probleem, we hebben tijd genoeg. Ik klap mijn laptop open en lees de laatste tweet van @0xDUDE voor: “Responsible Disclosure case #3,840 has just been archived. Retirement is imminent or is it? When is it really done? And what will be next..?” Vanwaar dit bericht en hoe komt hij aan zijn pseudoniem?

De ‘0’ in de naam is een eerbetoon aan een personage uit de cultfilm ‘Hackers’. Zero Cool is daarin een mysterieuze elfjarige die allerlei systemen heeft platgelegd. Victor heeft daar ‘0x’ van gemaakt omdat computers dat gebruiken om aan te geven dat een getal in het hexadecimale stelsel is. Dat is ‘Hexspeak’, net als die vreemde zin in het vorige hoofdstuk. En ‘DUDE’ is omdat hij ook zomaar een gast is die liever op de achtergrond opereert. Victor leeft namelijk met een sociale fobie. Ik realiseer me dan pas dat dit gesprek in deze omgeving best een opgave moet zijn voor hem, maar hij verzekert me dat het wel gaat zo.

Ik vertel dat ik veel hackers tegenkom die allemaal wel iets aparts hebben. Ze kijken anders en vinden daarom dingen die anderen niet zien, maar lopen vaak ook tegen problemen aan in het onderwijs. Hoe was zijn schooltijd? Hij vertelt dat hij het Tinbergen college heeft gedaan, richting economie en daarna wat losse cursussen in IT-beveiliging en management. Maar eigenlijk is hij, zoals zoveel ethisch hackers, autodidact: “Gewoon netjes

de opleiding afmaken, maar intussen wel je eigen plan trekken.” Eigenlijk wilde hij computergames gaan ontwikkelen, maar dat vonden ze thuis niet zo’n goed idee. Daarom heeft hij op de middelbare school een economieprofiel gekozen, maar hij is nooit gaan studeren.

Na wat werkervaring en deelcertificaten in project- en programmamanagement kwam hij terecht bij diverse overheidsorganisaties, ver weg van de IT-afdeling, maar wel dicht bij de directie en het management. Als hij zich dan veilig voelde gaf hij gaandeweg steeds meer vrij over zijn technische kennis om uiteindelijk bezig te gaan met de beveiliging. “Een soort dekmantel, want als je zegt dat je ethisch hacker bent schrikt dat af.” Al die tijd heeft hij zijn activiteiten als de ethisch hacker @0xDUDE en zijn werk strikt gescheiden gehouden. Nu is hij ambtenaar bij een ICT-dienstverlener binnen de Rijksoverheid. Victor: “Ik ga daar niet zelf graven, ik ben daar Security Architect en geen pentester.” Gelukkig heeft hij goed contact met directies en andere kanalen. Als hij toch iets vindt kan hij het via hen melden, al telt dat natuurlijk niet mee bij de 3840 meldingen van @0xDUDE.

Wat staat er dan in de beruchte database? Hij wil het niet hebben over specifieke meldingen, dat is een van zijn ethische codes, maar kan wel een soort samenvatting geven van hoe hij te werk gaat. Naast de meldingen houdt hij bijvoorbeeld ook alle correspondentie er over bij. In het begin was dat vooral als bewijsvoering, voor het geval er onenigheid zou komen. Maar dat is eigenlijk nooit gebeurd. Nu gebruikt hij zijn database vooral om overzicht te houden van zijn werk en het te verbeteren, bijvoorbeeld hoeveel tijd hij bezig is met een lek en wat hij beter kan doen.

Hij ziet in zijn database ook dat zijn vroegere meldingen veel uitgebreider waren. Nu stuurt hij een kort berichtje dat hij iets heeft gevonden met een stukje bewijs erbij, voornamelijk screenshots van directories waar hij in zou kunnen. Dat blijkt vaak genoeg. Hij merkt ook bij zichzelf dat hij anders meldt. Vroeger lag het tempo veel hoger en wilde hij dat een lek snel gedicht werd. Dit veranderde vooral doordat hij meer inzicht kreeg in wat de

organisatorische impact kan zijn van een onthulling: “De meesten beschouwen zo’n melding als een security incident, met alle capriolen die daarbij komen kijken.”

Verder ziet hij dat kleine bedrijven sneller reageren dan de grote. Vooral grote, oude organisaties blijken soms moeite te hebben met zijn meldingen. Hij ziet ook wie de meeste beveiligingsfouten maken. Wetenschappers en onderzoekers zijn volgens hem nog de slechtste systeembeheerders. Ze delen heel makkelijk veel informatie met elkaar, maar lijken zich er niet altijd van bewust hoe gevoelig patiëntendata is. Als hij een lek ziet, maar zij zien het probleem niet, dan kan ‘dreigen’ het CBP in te lichten wel eens helpen. Het is wel vaak lastig de juiste ingang te vinden. De officiële weg is de afdeling communicatie of een persvoorlichter, maar liever handelt hij het af via de CIO of de CEO, die hij dan via LinkedIn opspoort. Als hij de juiste persoon vindt, reageert die meestal wel goed op zijn meldingen en krijgt hij een bevestiging van ontvangst, met soms ook de termijn waarin ze het lek gaan dichten.

Victor komt ook veel lekken tegen van mensen die thuis willen verder werken aan documenten. Die sturen ze dan door via een Network-attached storage, oftewel een NAS. Dat is een opslagmedium dat op het netwerk is aangesloten en gebruik maakt van het ftp-protocol voor dataoverdracht. Zo’n NAS staat soms gewoon open en is dan eigenlijk een soort online usb-stick. Af en toe zoekt hij daarom op internet naar bestanden op dit soort apparaten met trefwoorden als: ‘patiënt’, ‘klant’, ‘dossier’, ‘belangrijk’, ‘onderzoek’, ‘vertrouwelijk’, ‘confidentieel’, ‘paspoort’, ‘geheim’, ‘creditcard’, ‘testament’, ‘medisch’, ‘letselschade’, etc. Dan komt hij uit bij bijvoorbeeld managers of CEO’s die kopietjes van legitimatiebewijzen, belastingaangiftes en andere gevoelige bedrijfsinformatie opslaan.

Als hij zo’n open NAS vindt, gaat hij niet in de bestanden kijken, maar maakt hij een screenshot van de mappenstructuur. Daarna zoekt hij via LinkedIn of de bedrijfswebsite de betrokken persoon. Als hij die dan belt of mailt, wordt er meestal wel positief gereageerd, al schrikken de meeste mensen natuurlijk wel van zo’n melding. Een maand geleden had hij ook weer zo’n scan gedaan. Hij vond 47.394 gebruikers die via een open NAS

vertrouwelijke informatie aan het delen waren, waarschijnlijk onbewust. Hij heeft in de weken erna 177 van hen benaderd via sms en e-mail. Deze meldingen tellen overigens ook niet mee in de 3840, want dat zou te makkelijk zijn.

Behalve wat algemeenheden op Twitter, is er dus niets terug te vinden in de media van zijn meldingen. Sindskort geeft hij wel presentaties op congressen over ethisch hacken. In een powerpoint die hij me later stuurt zie ik hoe hij te werk gaat. De titel is: ‘SCAnDAlousness-Cakewalking in Critical Infrastructures’. Deze gaat dus over SCADA-systemen die we ook tegen kwamen in hoofdstuk zeven. Alleen vindt hij ze niet vanuit huis via internet met de zoekmachine Shodan en de IP-adressen die daar te vinden zijn, maar door met eigen apparatuur in de buurt te komen van de installaties. Zijn presentatie begint met de gedragscode van de ethisch hacker. Naast de gebruikelijke ‘Leidraad responsibsible disclosure’ illustreert hij die met Japanse tekens van de Bushido, oftewel de erecode van de samurai. Daarna komen wat waarschuwingsborden: ‘Don’t try this at home, or at work!’

Wat volgt is een reeks hackingdemo’s. Tijdens de Nuclear Summit liep hij met een apparaat in de beveiligde zone om het wifinetwerk te testen op veiligheid. Met zijn Android smartphone weet hij een afvalwaterzuiveringsinstallatie binnen te komen terwijl hij onopvallend met zijn hond langs de hoge hekken loopt. Hij maakt dan onder andere gebruik van open-source intelligence, waaronder Wigle: de Wireless Geographic Logging Database. Zijn applicatie stuurt dan de gps-coördinaten naar een online database met wireless accesspoints en dan ziet hij de kwetsbaarheden van die locatie. In de presentatie laat hij ook zien hoe hij via een richtantenne uiteindelijk bij een SCADA-systeem terechtkomt. Tijdens de demo rollen wat onbegrijpelijke afkortingen over het scherm, maar met de beelden van hoe hij praktisch te werk gaat, maakt hij security ook voor de leek heel inzichtelijk.

Als hij me tijdens ons interview vertelt over deze presentaties, vraag ik enthousiast waarom hij niet voor zichzelf gaat beginnen, want dat is leuk: pentesten en mensen wakker schudden. Daar is ook veel behoefte aan. Maar dan realiseer ik me dat het voor

iemand met een sociale fobie al een hele opgave is zo'n presentatie te doen, laat staan klanten te gaan werven. Is dat de reden dat hij pas na zestien jaar ethisch hacken naar buiten treedt met zijn verhaal? Nee, het is meer dat het voor hem geen werk is, maar gewoon iets wat hij moet doen, een missie. Niet dat het een verslaving is, maar eerder een geloofsovertuiging. In de afgelopen vijf jaar heeft hij in totaal 9000 uur van zijn vrije tijd hieraan besteed en maakte hij dagen van twintig uur. Dit jaar heeft hij besloten het rustiger aan te doen. Hij gaat richting de veertig jaar en vindt het tijd dat hij het ethisch hacken gaat overlaten aan de volgende generatie. Vandaar de tweet 'Retirement is imminent or is it?'

Hij wil zich in de toekomst meer gaan inzetten om jonge hackers te enthousiasmeren voor responsible disclosure. Ze kunnen bijvoorbeeld veel lekken vinden bij de energievoorziening, elektriciteitsnetwerken, vervoersbedrijven en watervoorziening, oftewel de grote, oude organisaties. Daar zitten nog veel securityproblemen, terwijl het wel de slagaders van ons land zijn en juist daar nog veel weerstand is tegen verantwoorde onthullingen. Hij wil jonge hackers leren hoe ze om moeten gaan met bedrijven en overheden die hier nog aan moeten wennen en ze laten zien hoe ze contact kunnen leggen als ze een lek vinden. De hackers moeten er ook voor waken dat ze anderen niet ondersneeuwen met zinloze meldingen. Hij voorziet dan ook meer samenwerking met andere hackers door bijvoorbeeld peer reviewing van bevindingen en oplossingen.

Heeft hij zelf kinderen? Ja: twee dochters van elf en een zoon van zestien. Die leren nu ook programmeren en onderzoek doen naar beveiliging. Een van zijn dochters ontdekte bijvoorbeeld veiligheidslekken bij haar favoriete game Movie Star Planet. De app verstuurde chats en privéberichten onversleuteld. De inlogpagina op de website deed dat ook. Vader Victor meldt trots op Twitter: "Teaching my kids how to Wireshark their @MSP_world password from MovieStarPlanet. They're shocked nothing is encrypted", met een foto erbij van zijn dochter achter de computer.

Hoe ziet zijn toekomst als ambtenaar er verder uit? De organisatie waar hij nu werkt gaat namelijk flink uitbreiden: van

120 man naar 800 man en ze gaan hun ICT-diensten ook aan andere departementen van de Rijksoverheid verlenen. Hij hoopt dat hij ook daar goede contacten zal vinden, mocht hij veiligheidslekken langs zien komen. Dat blijkt het geval. Want als ik hem 29 januari 2015 mijn concepttekst stuur, schrijft hij terug dat hij ook betrokken is bij het begeleiden van pentestopdrachten en security assessments. Niet alleen voor de organisatie zelf, maar ook bij de klanten. Hij zal het dus nog flink drukker krijgen met ethisch hacken, maar dan als ambtenaar. En ook al komen die meldingen natuurlijk niet in de database, staat de teller bij 0xDUDE inmiddels wel op 3993.

Zo zien we dus dat elke helpende hacker wel zijn plek vindt in het digitale polderlandschap. 0xDUDE is naar mijn inschatting de biggest dude of ’em all met zijn bijna vierduizend meldingen en drukke baan, maar er zullen er veel meer zijn die net als hij achter de schermen opereren. De jongeren zoals Beg en Van Geelen, die momenteel wel in de spotlights komen, zullen hopelijk uitgroeien tot goede voorbeelden voor de nieuwe generatie ethisch hackers. De vele andere helpende hackers in dit boek hebben hun plek gevonden in het bedrijfsleven, bij de overheid of blijven gewoon lekker zelfstandig. Zij hebben ons niet nodig, maar wij hen wel. Ze hacken en ze helpen. Ze hebben in ieder geval mij enorm geholpen. Want in de jaren dat ik hen heb mogen leren kennen, heb ik niet alleen veel geleerd over cyber security, maar vooral ook een geweldig leuke tijd gehad met deze bijzondere mensen.

25. Achter de schermen

Onderzoek doen naar de Nederlandse cyber security

De oorspronkelijke titel van dit boek was ‘Verantwoorde onthullingen’, net als mijn column in het tijdschrift Informatiebeveiliging. Die column was een manier om mijn werk enigszins te structureren: telkens een casestudie kort beschrijven, reacties vangen en er tot slot een hoofdstuk van maken. Dat werkte goed. Onder de kenners van het dossier leek ‘verantwoorde onthullingen’ een voor de hand liggende titel, gewoon de Nederlandse vertaling van ‘responsible disclosure’.

Toen ik deze titel ook uitprobeerde bij een wat breder publiek van werk en vrienden, viel die wat minder goed. Ze vonden het een moeilijke woordencombinatie met een onduidelijke betekenis. Ik moest dus wat anders bedenken. ‘Helpende hackers’ kwam al snel bovendrijven als de meest voor de hand liggende nieuwe titel. Lekker, zo’n alliteratie met twee h’s en ook een statement: hacken wordt vaak gezien als iets wat niet mag, terwijl het gebruikt kan worden voor goede zaken. Hacken en helpen lijken twee tegengestelden en die wilde ik in dit boek samenbrengen.

Het eerste wat je dan doet is natuurlijk even kijken of helpendehackers.nl nog beschikbaar is. En jawel, die kon ik meteen aanvragen. Maar eerst nog even googlen of niet iemand anders deze titel al heeft bedacht. Dat bleek het geval. Karin Spaink had op 21 september 2011 een blog geschreven op hackerspaces.nl met precies dezelfde titel. Het Diginotardrama was net begonnen en ze betoogde dat de Nederlandse overheid best wat meer gebruik kon maken van de skills in deze scene. De hacker spaces hadden ook net een brandbrief geschreven aan de regering hierover en hun vrijwillige diensten aangeboden. We hadden hetzelfde doel en dezelfde titel, dus kon ik haar best vragen of ze het goed vond als ik haar titel ging gebruiken.

Spaink trof ik op 16 december 2014 tijdens de uitreiking van de Big Brother Awards. Ze vond het gelukkig prima als ik de titel gebruikte. We praatten nog wat na over haar ervaringen met verantwoorde onthullingen en ik realiseerde me dat ik hier toch wel een interessant verhaal ben misgelopen. Ze was er vroeg bij, toen ze al in 2005 een groep hackers losliet op het toenmalige EPD en er een boek over schreef. Net als Brenno de Winter is ze een actievoerende journalist die zich op vernieuwende wijze inzet voor een veiligere informatiesamenleving. Eigenlijk had ik haar verhaal hier ook willen verwerken. Dan had ik ook meer aandacht kunnen besteden aan de hacker spaces, maar had ik wel op het laatste moment mijn boek flink moeten omgooien. Bijkomend voordeel zou dan wel zijn geweest dat ik dan ook een vrouwelijke hoofdpersoon erbij had, want daar zijn er nu veel te weinig van.

Wellicht was het je al opgevallen: er zijn geen cases van vrouwelijke hackers in dit boek. Dat vind ik jammer, want het is toch eigenlijk best raar dat iedereen informatietechnologie gebruikt, terwijl de mannelijke helft van de bevolking bepaalt hoe het werkt. Dat het Nederlandse Genootschap van Hackende Huisvrouwen geen echte huisvrouwen zijn zal je wellicht zelf ook wel bedacht hebben. Maar het leek me niet al te moeilijk om op z’n minst één vrouw te vinden die ergens een beveiligingslek heeft onthuld.

Een bekende was Shirley de Jong, die tijdens Lektober als een van de weinige hackers ook bij naam werd genoemd. De Jong kon een SQL-injection doen bij het Amstelland Ziekenhuis en had dit via De Winter gemeld. Als ik haar opzoek op internet blijkt ze webdeveloper te zijn en heeft ze een eigen site. Daar lees ik: “Krijg nou tieten?!” Shirley is transseksueel. Ik besluit dat ze wat mij betreft ook meetelt als vrouwelijke hacker, maar uit onze e-mailwisseling blijkt toch dat het niet echt een heel spannend verhaal is: lek gevonden, gemeld, opgelost, bedankt.

Vervolgens heb ik rondgevraagd via Twitter, LinkedIn en tijdens bijeenkomsten. Daar kwam slechts één tip uit, over een dame die een Cross Site Scripting zou hebben gemeld, nota bene bij de 50PLUSpartij van Henk Krol. De contactpersoon zei echter dat de meldster er verder niet over wilde uitweiden en ze bleef

dus onbekend voor me. Misschien is het toch een mannending om meteen een heel verhaal te maken van een onthulling… Dat geldt natuurlijk ook voor mij als schrijver. Bovendien: ik had al zoveel goede verhalen gekregen van al die jongemannen en het tekort aan vrouwen in de hackersscene wordt ruimschoots gecompenseerd door goede verhalen van dames in juridische, bestuurlijke of politieke functies.

Mijn onderzoek kwam in een stroomversnelling toen ik Brenno de Winter leerde kennen. We hadden elkaar al eens gesproken toen ik in 2010 onderzoek deed naar de OV-chipkaart. In 2012 begon ik met mijn eigen praatprogramma Tek Tok late night en vroeg ik hem om elke aflevering een onthulling te doen onder de titel: ‘Kraak van de maand’. Dat wilde hij wel: gratis, als hij maar wel de vrijheid behield zijn column zelf in te vullen. Prima deal.

Zijn eerste column op 2 oktober 2012 was meteen een hit. Hij gaf een live demonstratie met een hotspot die het verkeer van mobieltjes in de zaal kon onderscheppen. Hij had het namelijk ‘KPN’ genoemd en dat was voor de meeste mobieltjes genoeg om in te loggen. Vanaf het podium kon hij bij sommigen zelfs aanwijzen wie het waren en wat ze deden: de een was aan het Whatsappen, de ander checkte Buienradar en er had zelfs iemand Spotify opgestart. Erg hilarisch allemaal. Bij de volgende afleveringen kwam hij met de onthullingen over Diagnostiek voor U en het Groene Hart Ziekenhuis.

Bij de aflevering van 5 maart 2013 ging het mis. Tek Tok late night heeft elke aflevering een andere partner die het thema bepaalt en de show betaalt. Pim Takkenberg, teamleider van Team High Tech Crime was al eerder in het programma te gast geweest en zijn team wilde nu zelf een aflevering. De Nederlandse politie ging namelijk een wervingscampagne lanceren voor nieuwe digitale rechercheurs. Het leek mij en de rest van mijn team geweldig om zoiets op het publiekelijk toegankelijk poppodium te zetten, dus we gingen meteen aan de slag. Halverwege kwam echter van hogere hand het bericht dat het op zich prima was om dit publiekelijk te doen, maar dan wel zonder Brenno de Winter.

De reden die ik kreeg van Pim was dat het hun feestje was en ze geen gedoe wilden. Eerst was het argument dat Brenno te kritisch was naar de overheid. Ik probeerde nog uit te leggen dat het juist leuk is met Brenno erbij, maar na lang doorzeuren kwam het hoge woord eruit: hij is betrokken in een zaak. Dat was voor mij genoeg, maar wel onder een voorwaarde: hij mocht het hem zelf gaan uitleggen. Dat deed Pim en ik dacht dat ik er daarmee vanaf was, maar daarin onderschatte ik Brenno. Toen hij te horen kreeg dat hij niet op het podium mocht bij de campagne schreef hij een artikel in HP de Tijd dat de overheid een kritische journalist censureert. Hij zette ook een transcript van hun telefoongesprek op Geenstijl.

Dit alles zorgde voor veel negatieve publiciteit rondom de werving. Brenno legde me nog wel uit in een uitgebreide mail dat hij het mij niet kwalijk nam, maar dat hij onder deze omstandigheden niet meer mee kon werken aan mijn programma. Hij wilde als journalist zijn neutraliteit bewaken. THTC heeft hem nog wel uitgenodigd om als schrijvende pers het event te bezoeken. Operation High Tech Crime was met 623 bezoekers een geweldig succes, maar Brenno was er die avond niet bij.

Pas later realiseerde ik me dat de zaak waar Pim aan refereerde de hack van het Groene Hart Ziekenhuis was, maar daar kon hij natuurlijk niets over zeggen omdat het onderzoek nog liep. Brenno was gevraagd te getuigen, maar wilde daar niet aan mee werken. Als journalist wilde hij zijn bronnen beschermen. Al bij de aflevering van 4 december 2012, toen Lodewijk van Zwieten van het OM en Pim Takkenberg te gast waren om te praten over digitale veiligheid, merkte ik spanningen achter de schermen. Nu weet ik waarom. Ik wist wel al dat de hacker de week daarvoor was opgepakt, maar realiseerde me toen niet wat het betekende voor deze drie heren om op hetzelfde podium te staan.

Ik heb getwijfeld of ik dit verhaal wel moest verwerken in de hoofdstukken over deze zaak, omdat de meeste betrokkenen er wel iets van hebben meegekregen. Uiteindelijk heeft het weinig invloed gehad op het verloop van de zaak, maar wel op het verloop van mijn onderzoek. Daarom staat het hier. Gelukkig hebben we het weer bijgelegd en hebben Brenno, Pim en

Lodewijk me alle drie enorm geholpen met informatie en het aanscherpen mijn casestudies.

Het is me sowieso enorm meegevallen hoe open alle betrokkenen hebben verteld over hun ervaringen. Niet alleen de hackers, maar ook de organisaties die gehackt waren en de betrokkenen vanuit de overheid. Je zou verwachten dat de wereld van cyber security er één is van geheimen. Dat is in zekere zin ook zo, maar het is vooral ook een wereld waarin mensen graag kennis uitwisselen omdat die zo snel veroudert. Niet alleen om bij te blijven, maar ook om te laten zien wat ze weten en zo hun positie te versterken. Het werkt veelal volgens een ‘web of trust’: als iemand die ik vertrouw zegt dat jij te vertrouwen bent, ben ik ook geneigd jou te vertrouwen – een soort sociaal certificatensysteem.

Juist daarom zijn er ook een aantal verhalen niet in dit boek gekomen. Vooral tijdens borrels op bijeenkomsten wordt er nogal eens geheime informatie uitgewisseld. Het is geven en nemen, waarbij je ook afspreekt wat je wel en niet mag doorvertellen. Sommige dingen die ik hoorde, maar niet kon verwerken in het boek omdat ik er geen bron bij kon noemen, hebben me wel weer geleid naar anderen die er wel over mochten vertellen.

Een geïnterviewde wil ik hier uitlichten, juist omdat hij niet in het boek is gekomen. Het gaat om een Chief Information Security Officer die een zware hack bij zijn organisatie had afgehandeld. Hij had een prachtig verhaal, waar ik tweeëneenhalf uur druk typend naar heb zitten luisteren. Toen ik het verslag ter controle naar hem stuurde kreeg ik een paar dagen later een mail terug met de boodschap alsjeblieft niets tegen iemand te zeggen over ons gesprek. Ik belde hem op en kreeg te horen dat hij op non-actief was gesteld. Later werd hij ontslagen, want hij had over de zaak gesproken zonder toestemming van de directie en veel teveel verteld. Zijn verhaal staat hier dus niet beschreven en ik hoop dat hij weer ergens anders zijn plek heeft gevonden. Gelukkig is er veel behoefte aan bijzondere cyber security experts. Hij is ‘een witte raaf’, zoals een van de directieleden tegen me zei en hij mag best weten dat ze hem daar erg missen.

De code bij elk interview was dat ik het gesprek eerst helemaal uitschreef en met de geïnterviewden heen en weer mailde tot het

klopte. Dat deed ik vervolgens ook met de column en het uiteindelijke hoofdstuk waarin ze terechtkwamen. Dat was best ingewikkeld als er meerdere mensen tegelijk in voorkwamen, die dan de on-affe teksten over elkaar te lezen kregen. Soms leidde het tot een welles-nietes tussen antagonisten, maar gaandeweg leidde dat meestal juist tot meer wederzijds begrip.

Dat was ook het voornaamste doel van dit boek: om al deze betrokkenen, die elk een andere kant van de cyber security doen, inzicht te geven in elkaars belevingswereld. Zelfs als dit boek niet wordt gelezen, is dat dus voor een deel al gelukt. Dat had ik niet gekund zonder hun medewerking en daarom veel dank aan hen.

I. Dank

Een dankwoord in een boek begint meestal met lof voor de uitgever die de auteur heeft bijgestaan in het zware schrijfproces en ondanks alles in hem bleef geloven. Dit keer niet, want die uitgever ben ik zelf. ‘Helpende hackers’ is een eerste in een reeks publicaties van mijn bedrijfje Tek Tok, waarmee ik wil laten zien dat media maken ook anders kan. Hopelijk volgen er nog veel meer, ook met andere auteurs. Schrijven is uiteraard een zwaar proces, vooral als je alles moet checken met iedereen die in het verhaal voorkomt, maar ik heb er elk moment van genoten, juist dankzij al deze betrokkenen. Mijn dank gaat dan ook op de eerste plaats uit naar al deze mensen, die ik bij wijze van naslag in de volgende bijlage opsom. Dat jullie je bijzondere kennis en betrokkenheid in de cyber security zo openhartig met me hebben gedeeld, maakte dit project tot een bijzondere levenservaring. Hartelijk dank daarvoor.

Enkele van de respondenten wil ik hier in het bijzonder uitlichten omdat ze niet alleen hebben verteld over de zaken waar ze zelf bij betrokken waren, maar me ook hebben geholpen om de wereld van cyber security te begrijpen. Allereerst de hackers, sorry, ‘computer beveiligingsdeskundigen’: Bart Jacobs, Floor Terra, Rickey Gevers, Oskar Koeroo en Jeroen van der Ham. Zonder jullie zou het internet een stuk minder veilig zijn en dit boek een stuk saaier. Ik heb ook veel gehad aan de mensen van het NCSC, met name Barend Sluijter. Vaak ben ik op bezoek geweest in de toren van Veiligheid en Justitie en ook over de mail heeft hij veel van mijn casestudies van commentaar voorzien. Lodewijk van Zwieten van het Openbaar Ministerie heeft ook veel van de hoofdstukken doorgenomen en daarbij mijn juridisch begrip aangescherpt. Brenno de Winter heeft ook een groot deel van dit boek vooraf doorgenomen en van commentaar voorzien. Dat moest ook wel, want hij komt er nog het meeste in voor. Pim Takkenberg heeft me vooral veel aanwijzingen gegeven waar ik moest zoeken om de juiste mensen en feiten boven tafel te

krijgen. Dat juist deze heren tegelijkertijd bij het hele onderzoek betrokken zijn gebleven is op zich al bijzonder. Dank daarvoor.

Het eerste idee voor dit onderzoek kreeg ik toen ik nog bij het Rathenau Instituut werkte. Ik noemde het toen ‘handboek hackersethiek’, maar ging daar weg nog voordat we er iets mee konden doen. Veel Rathenauers zijn betrokken gebleven bij dit project en ik ben hen daar bijzonder dankbaar voor. Ik ben blij dat ik de eerste casestudies heb kunnen doornemen met mijn vaste onderzoeksmaatjes Jelte Timmer en Rinie van Est. Afdelingshoofd en hoogleraar Ethiek Frans Brom had mijn eerste ideeën en morele kompas al aardig aangescherpt. Later heeft hij een halve versie van dit boek helemaal gelezen en uitgebreid met me doorgenomen. Toen hij zei: “Je hebt met dit onderwerp goud in handen”, heeft me dat enorm gesterkt. Het grootste goud kwam van Pascal Messers. Als redacteur heeft ze in mijn tijd bij Rathenau mijn teksten enorm verbeterd en ook nu weer heeft ze met een stapel bekrast papier mooie lijnen in dit boek aangebracht.

Toch is dit boek geen Rathenauboek geworden, eerder een boek van het Platform Informatiebeveiliging, want de mensen aldaar hebben de eindredactie gedaan. Elke zes weken leverde ik een casestudie af in de vorm van een column, die door Lex Borger werd geredigeerd. Dat gaf een prettig ritme aan het project en een gelegenheid om via dit publiek mijn bevindingen te testen. Voor de eindredactie van dit boek heeft PvIB Anna Teresa Bellinzis ingehuurd. Lex en Anna, hartelijk dank voor jullie geduld en scherpe pennen, die dit boek hebben gemaakt tot wat het nu is.

Een dankwoord eindigt meestal met excuses aan het gezin dat zo te lijden heeft gehad onder het zware schrijfproces. Ook dat zal ik hier laten. Mijn dochter vond het geloof ik wel fijn dat ik al die tijd veel meer thuis was en ze heeft in die tijd ook zelf een boek geschreven, over draken. Haar anders-denken is een belangrijke inspiratie voor me geweest, niet alleen om weer te gaan schrijven, maar ook om hackers beter te begrijpen. Daarom, tot slot ook dank aan jou Lena. Je bent dan wel geen hacker, maar ook jij zal later, net als zij, anderen helpen vanuit jouw bijzondere kijk op de wereld.

II. Cast: de personages in dit boek

De respondenten in dit onderzoek zijn veelal live geïnterviewd, maar soms ook via Skype, telefoon of e-mail. Al deze personen hebben ook de teksten waarin ze voor komen van commentaar voorzien. Hun functietitel is die uit de periode waarin de casestudie speelde. Daar waar het relevant is, staat hun huidige positie erbij. De politici die geciteerd zijn uit Kamerstukken, staan hier ook vermeld. Personages die geciteerd zijn uit andere bronnen, staan alleen in de hoofdstukken.

Respondenten

- 0xDUDE, @0xDUDE, ethisch hacker en Victor, ambtenaar bij een ICT-dienstverlener binnen de Rijksoverheid
- Bas Anneveld, @basanneveld, Manager Site Operations Marktplaats
- Maarten Baaij, directeur Financiën en ICT van het Groene Hart Ziekenhuis
- Jaya Baloo, Chief Information Security Officer KPN
- Vincent Beerends, countrymanager bij Sulake, het bedrijf achter Habbo Hotel
- Olivier Beg, @smiegles, ethisch hacker en mbo-scholier
- Yvon van den Berg, manager Relatiemanagement, Marketing & Communicatie bij Diagnostiek voor U
- Joost Blokzijl, @jblokzijl, redacteur bij het tv-programma EenVandaag
- Frank Brokken, Security Manager van de Rijksuniversiteit Groningen
- Ralf Dennissen, PR-manager Volkswagen
- Peter van Dijk, directeur Mcomm
- Beau van Doorn, Habbo helpdeskmedewerkster
- Wouter van Dongen, ethisch hacker en eigenaar Dong-IT
- David van Es, student Information Security Management aan de Haagse Hogeschool

- Mischa van Geelen, @rickgeex, ethisch hacker
- Peter Geissler, ethisch hacker @bl4sty en medeoprichter Radically Open Security
- Arda Gerkens, directeur HCC
- Rickey Gevers, @UID_, ethisch hacker en security researcher bij Digital Investigation
- Jeroen van der Ham, @1sand0s, ethisch hacker, onderzoeker en docent System and Network Engineering aan de UvA en Security Researcher bij NCSC
- Martijn van de Heide, Security Officer KPN
- Maarten Hilbrandie, perswoordvoerder Ministerie van Defensie
- Anita Hilhorst, perswoordvoerster TLS
- Jaap-Henk Hoepman, @xotoxot, onderzoeker Radboud Universiteit en TNO en Scientific Director Privacy and Identity Laboratory
- Peter van Hofweegen, oprichter ITVitae detachering
- Bart Jacobs, hoogleraar Security & Software Correctness van de Digital Security Group bij de Radboud Universiteit
- Mark Janssen, bestuurlid Revspace
- Shirley de Jong, webdeveloper
- Jordy, ethisch hacker als Bonnie van het Nederlands Genootschap van Hackende Huisvrouwen
- Oscar Koeroo, @okoeroo, Nikhef, het nationale instituut voor subatomaire fysica en Identity and Access Officer bij KPN.
- Gerard de Koning Gans, onderzoeker Radboud Universiteit en digitaal rechercheur bij THTC
- Andre Koot, @meneer, zelfstandig beveiligingsexpert
- Steven Kroesbergen, strafrechtadvocaat
- Bob Kaarls, strafrechtadvocaat
- Danielle Laheij, landelijk officier van justitie cybercrime
- Frank Linde, directeur Nikhef
- Ilias el Matani, @iliaselmatani, ethisch hacker en Security Specialist bij Securelabs
- Jean Pierre Miani, Technology Officer bij Infinitas Learning
- Gelske Nederlof, Manager Marketing & Communicatie bij het Groene Hart Ziekenhuis
- Astrid van der Put, directrice bij Diagnostiek voor U
- Ntisec, @ntisec, ethisch hacker

- Melanie Rieback, onderzoeker VU en oprichter Radically Open Security
- Hans Schröder, @jmSchroder, ethisch hacker en hbo-student
- Robin Schuil, @schuilr, medeoprichter en Innovation Program Manager Marktplaats
- Barend Sluijter, beleidsmedewerker NCSC
- Pim Takkenberg, @Pim_Takkenberg, teamleider Team High Tech Crime van de Nederlandse Politie
- Wouter Teepe, onderzoeker Radboud Universiteit en lid van het team dat de OV-chipkaart kraakte
- Floor Terra, @floorter, ethisch hacker en Technoloog bij CBP
- Roel Verdult, onderzoeker Radboud Universiteit en lid van het team dat de OV-chipkaart kraakte
- Pieter Vlasblom, @legosteentje, ethisch hacker en @ChunkrGames
- Monique Verdier, lid van de Raad van Bestuur van het Groene Hart Ziekenhuis
- Koosje Verhaar, hoofd Communicatie College Bescherming Persoonsgegevens
- Arjen de Waard, kolonel en directeur Marinebedrijf
- Robert-Jan Willems, Principal Consultant Security bij KZA
- Brenno de Winter, ICT journalist o.a. bij Webwereld en NU.nl
- Inge Witteman, perswoordvoerster ING
- Tarik El Yassem, medewerker NCSC
- Lodewijk van Zwieten, openbaar aanklager cybercrime bij het landelijk parket

Ministers en staatsecretarissen

- Piet Hein Donner, CDA, van 1 oktober 2010 tot 16 december 2011 Minister van Binnenlandse Zaken
- Tineke Huizinga, CU, van 22 februari 2007 tot 23 februari 2010 staatssecretaris van Verkeer & Waterstaat
- Ivo Opstelten, VVD, van 14 oktober 2010 tot 9 maart 2015 Minister van Veiligheid en Justitie
- Melanie Schultz Van Haegen, VVD, sinds 14 oktober 2010 Minister van Infrastructuur en Milieu

- Hans Hillen, CDA, van 14 oktober 2010 tot 5 november 2012 Minister van Defensie
- Liesbeth Spies, CDA, van 16 december 2011 tot 5 november 2012 Minister van Binnenlandse Zaken en Koninkrijksrelaties
- Edith Schippers, VVD, sinds 14 oktober 2010 Minister van Volksgezondheid

Tweede Kamerleden

- Farshad Bashir, SP
- Hanke Bruins Slot, CDA
- Klaas Dijkhoff, VVD
- Wijnand Duijvendak, Groen Links
- Arjan El Fassed, Groen Links
- Andre Elissen, PVV
- Ineke van Gent, Groen Links
- Sharon Gesthuizen, SP
- Maarten Haverkamp, CDA
- Wassile Hachchi, D66
- Pierre Heijnen, PvdA
- Janine Hennis-Plasschaert, VVD, later minister van Defensie
- Leon de Jong, PVV
- Ger Koopmans, CDA
- Henk Krol, 50PLUS
- Attje Kuiken, PvdA
- Jacques Monash, PvdA
- Astrid Oosenbrug, PvdA
- Jeroen Recourt, PvdA
- Gerard Schouw, D66

III. Bronnen

1. Intro

Interview met Frank Brokken (28 maart 2014) en Rickey Gevers (5 augustus 2013). Zie de video van hun ontmoeting terug op www.tektok.nl

Dijk, W. van, (2007, 7 maart) ‘Hackers breken in bij Groningse universiteit’ *NU.nl*

Nieuwenhuizen, M. (2007, 18 juli) ‘Computerkaping RUG heeft positieve kant’ *Computable*

2. Radboud opent de poorten

Interview met Bart Jacobs (11 september 2013) en Jannemiek Zandee (17 september 2009).

Broek, P. van den, (2008) ‘De schokgolf na de ontmanteling’. In: *VOX*, jaargang 8, nr 15, pp.14-18

Broek, S. van den, Radewalt, N. (2009, 26 maart) *Evaluatie OV-chipkaart* Roelofarendsveen: DocAdvies

CBP (2005) *Privacy en de OV-chipkaart. De visie van het College bescherming persoonsgegevens*

CBP (2007) *Verwerking van persoonsgegevens ten behoeve van de OV-chipkaart bij het GVB te Amsterdam.*

Couvreur, N. (2007, 11 januari) *Onderzoek OV-chipkaart* Presentatie Media Test bij het Rathenau Instituut

Garcia, Flavio D., De Koning Gans, G., Muijrers, R., Van Rossum, p. Verdult, R., Wichers Schreur, R. en Jacobs, B. (2008) *Dismantling MIFARE Classic* Institute for Computing and Information Sciences, Radboud Universiteit Nijmegen

Garcia, Flavio D. en Jacobs, B. (2011) *The Fall of a Tiny Star* Institute for Computing and Information Sciences, Digital Security Group, Radboud University Nijmegen

Govcert (2008, 9 mei) *Kwetsbaarheden Myfare Classic in toegangspassen.* Govcert Factsheet, FS-2008-03

Heuvel, E. van den, Nagel, K., Hof, C. van ’t en Schermer, B. (2007) *RFID-bewustzijn van consumenten: Hoe denken Nederlanders over Radio Frequency Identification?* Rathenau Instituut, de Consumentenbond en ECP.nl

Hof, C. van ‘t, Est, R. van en Daemen, F. (2010) *Check in / check uit. Digitalisering van de openbare ruimte.* Rathenau Instituut, NAi Uitgevers Rotterdam

‘Nerdy momenten bij een wegwerpkaart’ In: *Science Guide* (2008, 10 november)

‘So what?’ In: *Science Guide* (2008, 13 november)

Udo de Haes, A. (2010, 11 februari) ‘Miljoenen voor nieuwe OV-chip Mifare SmartMX’ *Webwereld*

Verdult, R. (2008, 25 juni) *Security analysis of RFID tags* Masterthesis Radboud Universiteit

Wichers Schreur, R., P. van Rossum, F. Garcia, W. Teepe, J. Hoepman, B. Jacobs, G. de Koning Gans, R. Verdult, R. Muijrers, R. Kali, & V. Kali (2008, 12 maart) *Security Flaw in MIFARE Classic* Persbericht Institute for Computing and Information Sciences, Digital Security Group, Radboud University Nijmegen.

3. Crypto is geen cultuuruiting, onthullen wel

Interview met Bart Jacobs (11 september 2013), Pedro Peters (28 mei 2008), Peter van Dijk (12 juni 2009), Michael van der Vlies (19 mei 2008), Wouter Teepe (19 mei 2008), Wijnand Duyvendak (19 mei 2008) en Jannemiek Zandee (17 september 2009).

Huizinga, T. (2008, 29 februari) *Aanvalsplan OV-chipkaart* Tweede Kamer

Huizinga, T. (2008, 28 november) *Actualisatie Aanvalsplan OV-chipkaart* Tweede Kamer

Rechtbank Arnhem, sector Civiel recht (2008) *Vonnis kort geding van 18 juli 2008*, zaak 171900 / KG ZA 08-415

Tweede Kamer (2011, 27 januari) *Verslag Algemeen Overleg van de vaste commissie voor Infrastructuur en Milieu, met minister Schultz van Haegen-Maas Geesteranus van Infrastructuur en Milieu.*

Udo de Haes, A. (2010, 11 februari) ‘Miljoenen voor nieuwe OV-chip Mifare SmartMX’ *Webwereld.nl*

4. Zo lek als een mandje

Interview met Brenno de Winter (5 augustus 2014) en e-mailcorrespondentie met Anita Hilhorst.

Fox-IT (2011, 3 september) *Operation Black Tulip* Fox-IT

Geenstijl (2011, 8 oktober) ‘Deze gemeentesites zijn allemaal LEK!’ geenstijl.nl

Tweede Kamer (2011), *Verslag Algemeen Overleg van de vaste commissie voor Infrastructuur en Milieu, met minister Schultz van Haegen-Maas Geesteranus van Infrastructuur en Milieu van 27 januari.*

Rechtbank Utrecht (2011, 5 september) *Afdoeningsbeslissing in de zaak 09Device.*

5. @Brenno en de superknallers

Interview met Brenno de Winter (5 augustus 2014).

Bakker, J. (2011, 4 oktober) ‘Lek 3: psychologensite loopt leeg door SQL-injectie’ *Webwereld.nl*

Bakker, J. (2011, 6 oktober) ‘Lek 5: SQL-injectie bij Erasmus MC’ *Webwereld.nl*

Bakker, J. (2011, 11 oktober) ‘Lek 9: diabetici-site druppelt data’ *Webwereld.nl*

Bakker, J. (2011, 17 oktober) ‘Lek 13: psychiatrische site lekt beheer en forum’ *Webwereld.nl*

Bakker, J. (2011, 19 oktober) ‘Lek 15: woningzoekers in de Bijlmer’ *Webwereld.nl*

Bakker, J. (2011, 31 oktober) ‘Lek 29: UU lekt privédata tienduizenden studenten’ *Webwereld.nl*

Bareman, B. (2011, 11 oktober) ‘Politiek witheet door Lektober, wil actie Donner’ *Webwereld.nl*

Marten, K. (2011, 17 september), ‘Brandbrief van nationale hackergemeenschap inzake ICT-beveiliging overheid’. Hack42 te Arnhem, ACKspace te Heerlen, TkkrLab te Enschede, Bitlair te Amersfoort, Randomdata te Utrecht, Frack te Leeuwarden, Sk1llz te Almere, eth0, 2600nl.net, HXX en Revelation Space te Den Haag.

Meijs, S. Van der (2011, 7 oktober) ‘Lek 6: Escortservice lekt e-mailadressen’ *Webwereld.nl*

Tweede Kamer (2011) *Diginotar en ICT problemen bij de overheid*. Verslag debat van 13 oktober. Kamerstuk 12-26-105

Udo de Haes, A. (2011, 26 oktober) ‘Lek 20: database BOVAG wagenwijd open’ *Webwereld.nl*

Winter, B. de (2011, 1 oktober) ‘Lek 1: Blunder Logius maakt DigiD-fraude kinderspel’ *Webwereld.nl*

Winter, B. de (2011, 3 oktober) ‘Lek 2: 7 gemeenten kwetsbaar voor DigiD-lek’ *Webwereld.nl*

Winter, B. de (2011, 5 oktober) ‘Lek 4: Ziekenhuis lekt data via beterschapskaartjes’ *Webwereld.nl*

Winter, B. de (2011, 8 oktober) ‘Lek 7: Lektober superknaller: Megalek treft 50 gemeenten’ *Webwereld.nl*

Winter, B. de (2011, 10 oktober) ‘Lek 8: Horst aan de Maas lekt ook mail’ *Webwereld.nl*

Winter, B. de (2011, 12 oktober) ‘Lek 10: Zeewolde lekt wachtwoorden van journalisten’ *Webwereld.nl*

Winter, B. de (2011, 13 oktober) ‘Lek 11: Hackers neuzen in wachtwoorden gemeente’ *Webwereld.nl*

Winter, B. de (2011, 14 oktober) ‘Lek 12: overheid lekt wachtwoorden Raad van State’ *Webwereld.nl*

Winter, B. de (2011, 18 oktober) ‘Lek 14: Privédata patiënten af te luisteren’ *Webwereld.nl*

Winter, B. de (2011, 20 oktober) ‘Lek 16: Davilex meervoudig en langdurig gehackt’ *Webwereld.nl*

Winter, B. de (2011, 21 oktober) ‘Lek 17: accounts ov-chipkaart.nl volledig te kapen’ *Webwereld.nl*

Winter, B. de (2011, 24 oktober) ‘Lek 18: 715.000 klanten van CheapTickets.nl’ *Webwereld.nl*

Winter, B. de (2011, 25 oktober) ‘Lek 19: Administrator toegang tot een webshop’ *Webwereld.nl*

Winter, B. de (2011, 26 oktober) ‘Lek 21-27: Eindhoven Lektober Lekkenkampioen’ *Webwereld.nl*

Winter, B. de (2011, 28 oktober) ‘Lek 28: Vliegschool lekt BKR-gegevens en strafblad’ *Webwereld.nl*

6. DongIT en het DigID Debacle

Interview met Wouter van Dongen (14 oktober 2013 en 11 december 2014) en e-mailcorrespondentie met Sonja Kok en Michiel Groeneveld.

Dongen, W. van en K. Vahl (2013, 4 februari) *Softwareversies van gemeentelijke websystemen in kaart gebracht* Leiden: DongIT

Hoek, C. van de (2011, 16 september) 'Vertrouwelijke raadsstukken openbaar door lek' *NU.nl*

NOS (2011, 1 oktober) 'De veiligheid van overheids-websites ligt onder vuur. Kunnen hackers een rol spelen bij het beveiligen?' *Nieuwsuur*

Winter, B. de (2011, 16 september) 'Hoster lekt honderden gemeentedatabases' *Webwereld.nl*

Winter, B. de (2011, 3 oktober) 'Lek 1: Blunder Logius maakt DigiD fraude kinderspel' *Webwereld.nl*

7. @okoeroo en de pompen van Veere

Interview met Oscar Koeroo (19 februari 2014) en Joost Blokzijl (8 april 2014) en e-mailcorrespondentie met Frank Linde.

Opstelten, I.W. (2012, 16 maart) *Beantwoording vragen van de leden Hachi en Schouw (beiden D'66) over de risico's van software voor het op afstand besturen van industriële processen (ingezonden 1 februari 2012)* Brief aan de Kamer

Opstelten, I.W. (2012, 19 maart) *Beveiliging van SCADA-systemen* Brief aan de Kamer

Schultz van Haegen, M.H. (2012, 12 maart) *Beantwoording Kamervragen van de leden Bashir en Gesthuizen over sluizen, gemalen en bruggen die slecht beveiligd zijn* Brief aan de Kamer

Schellevis, J. (2012, 20 januari) 'Scadabeveiliging: een structureel probleem'. *Tweakers.nl*

Tweede Kamer (2012) *Veiligheidsregio's Verslag Algemeen Overleg Tweede Kamer 15 februari 2012*, kamerstuk nr. 29517

Tweede Kamer (2012) *Cyber Security en veiligheid overheidswebsites. Verslag Algemeen Overleg Tweede Kamer 10 april 2012*, kamerstuk nr. 26643

8. Dan gaan we nat

Interview met Barend Sluijter en Tarik el Yassem (30 april 2014) en correspondentie met Ntisec

FBI, (2012, 23 juli) *Vulnerabilities in Tridium Niagara Framework Result in Unauthorized Acces to a New Jersey Company's Industrial Control System* Situational Information Report

NCSC (2012, 7 maart) *Beveiligingsrisico's van on-line SCADA systemen* Factsheet FS-2012-01 versie 2.0

9. @UID_ belt de kazerne

Interview met Rickey Gevers (5 augustus 2013).

Brusselmans (2012, 24 februari) 'Communicatiesysteem Defensie gehacked' *Geenstijl.nl*

Kok, V. de (2012, 24 februari) 'Communicatie Defensie eenvoudig te kraken' *de Volkskrant*

Tweede Kamer (2012, 28 februari) *Vragen van het lid Hachchi aan de minister van Defensie over het bericht dat vergaderingen van de Defensietop gemakkelijk af te luisteren zijn.* Kamerstuk 2012Z03576

10. @floorter: a man in the middle

Interview met Floor Terra (20 maart 2013) en Joost Blokzijl (8 april 2014).

Berg, R. van den (2011, 8 november) 'ING mobiel bankieren authenticatie' *Mountknowledge.nl*

Blokzijl, J. (2012, 21 maart) 'Mobiel Bankieren ING maandenlang onveilig' *EenVandaag*

Terra, F. (2012, 15 januari) 'Verantwoordelijkheid voor beveiliging' *floort.net*

11. @legosteentje verdient een witte hoed

Interview met Pieter Vlasblom (5 augustus 2013 en 20 december 2014) en e-mail correspondentie met Bas Anneveld en Robin Schuil.

Tweede Kamer (2012, 24 mei), *Verslag van een algemeen overleg Informatie- en Communicatietechnologie van 10 april 2012* Kamerstuk 26643

12. @jmschroder belt de Habbohelpdesk

Interview met Hans Schröder (8 april 2014) en e-mail correspondentie met Brenno de Winter, Vincent Beerends en Beau van Doorn.

Bakhuys Roozeboom, F. (2013, 6 maart) 'TMG verkoopt aandelen Habbo' *Adformatie.nl*

Gerechtshof Amsterdam, beklagkamer (2013, 25 april) *Beschikking van 25 april 2013 op het beklag met het rekestnummer K12/0126 van TTG Sulake B.V.*

Winter, B. de (2013, 14 juni) ‘Online game sleepte minderjarige voor rechter om tonen lek’ *Webwereld.nl*

13. Hacker Krol haalt net iets teveel uit de kast

E-mail correspondentie met Brenno de Winter, Andre Koot, Arda Gerkens, Oscar Koeroo, Henk Krol en Yvon van den Berg.

NOS, (2013, 31 januari) ‘Henk Krol voor de rechter’ *EenVandaag*

Omroep Brabant (2012, 19 april) ‘Medische gegevens duizenden Brabanders op straat’

Omroep Brabant (2012, 19 april) ‘Brenno de Winter: “Medische gegevens op straat mogelijk overtreding wet”’

Omroep Brabant (2012, 20 april) ‘Diagnostiek voor U wijst vooral naar anderen na lekke website’

Omroep Brabant (2012, 20 april) ‘Diagnostiek voor U doet aangifte van diefstal’

Omroep Brabant (2012, 4 december) ‘Henk Krol vervolgd voor hacken medische gegevens’

Omroep Brabant (2012, 5 december) ‘Brenno de Winter over rechtszaak hackende Henk Krol: “Deze rechtszaak zou niet nodig moeten zijn”’

Omroep Brabant (2013, 30 januari) ‘Psychiater schendt beroepsgeheim in hackerszaak Henk Krol’

Omroep Brabant (2013, 15 februari) ‘Diagnostiek voor U laat schadeclaim tegen Henk Krol vallen’

Omroep Brabant, (2013, 26 februari) ‘VVD Kamerlid ‘met de pet rond’ om boete Henk Krol te betalen’

Rechtbank Oost-Brabant (2013, 15 februari) *Vonnis, Parketnummer: 01/820892-12*

Schoemaker, R. (2013, 14 januari) ‘‘Gehackt’ medisch centrum eist 85.000 euro van Krol’ *Webwereld.nl*

Winter, B. de (2013, 16 december) ‘Kamer wil controle IGZ op beveiliging medische dossiers’ *NU.nl*

Winter, B. de (2013, 3 februari) ‘Beveiligingsexperts eisen CBP-onderzoek gehackte kliniek’ *NU.nl*

Winter, B. de (2013, 9 februari) ‘GGZ Eindhoven stuurt medische gegevens aan ICT-bedrijf’ *NU.nl*

Winter, B. de (2013, 10 april) ‘Hack Henk Krol vergroot bewustzijn zorgsector’ *NU.nl*

14. Het crisisteam rond Verdier

Interview met Jordy (17 november 2014), Monique Verdier (18 november 2014) en Gelske Nederlof (18 november 2014).

Opstelten, I.W. (2012, 5 december) *Brief van de Minister van Veiligheid en Justitie* Kamerstuk 27529

Rechtbank Den Haag (2014, 18 december) ‘Celstraf voor hacken en kinderporno’ ECLI:NL:RBDHA:2014:15611 *Rechtspraak.nl*

Winter, B. de (2012, 7 oktober) ‘Groene Hart Ziekenhuis lekt medische dossiers’ *NU.nl*

Winter, B. de (2012, 12 oktober) ‘Groene Hart Ziekenhuis betuigt spijt voor lek’ *NU.nl*

Winter, B. de (2012, 29 november) ‘Kamer ontsteld over harde aanpak hacker’ *NU.nl*

Tweede Kamer (2012, 9 oktober) *Vragen van het lid Bruins Slot aan de minister van Volks- gezondheid, Welzijn en Sport over het bericht “Groene Hart Ziekenhuis lekt medische dossiers”.*

15. @bl4sty en de tien miljoen modems

Interview met Martijn van der Heide (24 september 2013) en Peter Geissler (19 november 2013).

16. De hash van Dismantling Megamos

E-mail correspondentie met Ralf Dennissen.

High Court of England and Wales (2013, 25 juni) *Chancery Division Decisions* Neutral Citation Number: [2013] EWHC 1832 (Ch) Case No. HC13C02168

17. Tijd voor beleid

Interview met Barend Sluijter (23 september 2013) en Lodewijk van Zwieten (29 september 2014) en e-mail correspondentie met Andre Koot, David van Es, Mark Janssen en Koosje Verhaar.

Bolhaar, H.J. (2013, 18 maart) *Hoe te handelen bij ‘ethisch’ hackers?* brief College van procureurs-generaal aan alle parkethoofden

CBP (2013, februari) *Richtsnoeren van beveiliging persoonsgegevens*

NCSC (2013, januari) *Leidraad om te komen tot een praktijk van Responsible Disclosure*

NCSC (2013, juni) *Cyber Security Beeld Nederland 3*

NCSC (2014, september) *Cyber Security Beeld Nederland 4*

Opstelten, I.W. (2012, 28 december) *Brief van de Minister van Veiligheid en Justitie* Kamerstuk 26643-264

Opstelten, I.W. (2013, 18 december) *Voortgang responsible disclosure* Brief aan de Kamer

Tweede Kamer (2012, 24 mei), *Verslag van een algemeen overleg Informatie- en Communicatietechnologie van 10 april 2012* Kamerstuk 26643-240

Tweede Kamer (2012, 21 juni), *Verslag van een algemeen overleg Informatie- en Communicatietechnologie van 29 mei 2012* Kamerstuk 26643-286

Tweede Kamer (2012, 24 september), *Verslag van een schriftelijk overleg Informatie-en Communicatietechnologie van 21 september 2012* Kamerstuk 26643-253

18. De achterkant van het Groene Hart

Interview met Pim Takkenberg (15 september 2014), Jordy (17 november 2014), Monique Verdier (18 november 2014) en Gelske Nederlof (18 november 2014) en e-mail correspondentie met Brenno de Winter, Danielle Laheij en Bob Kaarls.

CBP (2014, oktober) *Onderzoek naar de beveiliging van het netwerk van het Groene Hart Ziekenhuis*

Winter, B. de (2014, 27 november) ‘Het Groene Hart Ziekenhuis in Gouda had lang de beveiliging van computersystemen niet op orde, en overtrad daarmee de wet’ *NU.nl*

19. Bonnie van de hackende niet-zo-huisvrouwen

Interview met Pim Takkenberg (15 september 2014), Jordy (17 november 2014), Monique Verdier (18 november 2014), Gelske Nederlof (18 november 2014) en Maarten Baaij (3 december 2014) en e-mail correspondentie met Brenno de Winter, Danielle Laheij en Bob Kaarls.

Rechtbank Den Haag (2014, 18 december) ‘Celstraf voor hacken en kinderporno’ ECLI:NL:RBDHA:2014:15611 *Rechtspraak.nl*

20. Gratis boeken voor @iliaselmatani
Interview met Ilias el Matani (6 januari 2014) en Piere Miani (6 januari 2014)

21. De ethische commissie van @1sand0s
Interview met Jeroen van der Ham (15 mei 2014)

Dreyer, J. en Haak, E. Van den (2014, 1 juni) *Tinder Privacy Revised* Project report UvA

Fiebig, T. en Katz, W. (2013, 27 mei) *Grindr Application Security Evaluation* Project report UvA

22. @rickgeex komt er wel
Interview met Mischa van Geelen (6 en 20 november 2014)

23. Beg en de Bug Bounties
Interview met Olivier Beg (22 oktober 2014) en Peter van Hofweegen (7 januari 2015)

Klein-Baltink, G. (2014, 23 juni) *Overwegingen ronde tafel onderwijs* uitnodigingsbrief

Kruyswijk, M. (2014, 22 februari) ‘17-jarige Amsterdammer voert hackerslijsten aan’ *Het Parool*

Udo de Haes, A. (2014, 21 februari) ‘Nederland karig met belonen white hat hackers’ *Webwereld.nl*

VPRO (2014, 12 oktober) ‘Zero-days. Veiligheidslekken te koop’ *Tegenlicht*

24. @0xDUDE, the biggest dude of ’em all
Interview met 0xDUDE/Victor (6 november 2014)

25. Achter de Schermen
Interview met Karin Spaink (16 december 2014)

IV. Voorbeeldtekst meldpunt

Bij Acme Corporation vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is.

Als u een zwakke plek in een van onze systemen heeft gevonden horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar cert@example.com. Versleutel uw bevindingen met onze PGP key om te voorkomen dat de informatie in verkeerde handen valt,
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of gegevens van derden in te kijken, verwijderen of aanpassen,
- Het probleem niet met anderen te delen totdat het is opgelost en alle vertrouwelijke gegevens die zijn verkregen via het lek direct na het dichten van het lek te wissen,
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden, en
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

Wat wij beloven:

- Wij reageren binnen 3 dagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing,

- Als u zich aan bovenstaande voorwaarden heeft gehouden, zullen wij geen juridische stappen tegen u ondernemen betreffende de melding,
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk,
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem,
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker, en
- Als dank voor uw hulp bieden wij een beloning aan voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van de lek en de kwaliteit van de melding met een minimum van een waardebon van 50,- euro.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

Bron: Floor Terra, *www.responsibledisclosure.nl*, Creative Commons

V. RTFM: verklarende woordenlijst

ACM: Autoriteit Consument & Markt

Admin: standaard gebruikersnaam van de administrator, wordt helaas te vaak niet aangepast naar een minder voor de hand liggende naam.

AIVD: Algemene Inlichtingen- en Veiligheidsdienst.

ASCII-art: American Standard Code for Information Interchange is een standaard voor letters, cijfers en leestekens. Zet je die op een artistieke manier bij elkaar, dan vormen ze samen een afbeelding.

Black hat hacker: een hacker met slechte motieven.

Brute forcing: net zo lang wachtwoorden uitproberen tot je erin kan.

Bug bounty: geldbedrag dat door organisaties wordt uitgekeerd als je een fout in hun software ontdekt en op een verantwoorde manier bij hen meldt.

Buffer overflow: opdrachten geven aan een server die te groot zijn voor de tijdelijke schrijfruimte, de buffer, waardoor de code elders wordt opgeslagen en uitgevoerd. Dit kan ervoor zorgen dat de server crasht, maar als je het goed doet, kun je hem op afstand besturen.

CBP: College Bescherming Persoonsgegevens, toezichthouder die namens de Wet Bescherming Persoonsgegevens optreedt.

Certificaat: code die door een derde partij wordt afgegeven en daarmee bevestigt dat de partij is wie die zegt te zijn.

Chatham House rules: afspraak bij bijeenkomsten dat je alles mag doorvertellen wat je hoort, als je maar niet zegt van wie je het

hebt.

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CMS: Content Management Systeem, een online systeem waar je moet inloggen en op basis van je identiteit voorbestemde delen van de inhoud van een website kunt aanpassen.

Cross Site Scripting (XSS): Een hacktechniek waarbij je code invoert waar die niet hoort, bijvoorbeeld in de adresbalk of de cookies die vanuit je browser naar de site worden gestuurd. Je kunt dan een sessie die een andere gebruiker op de site doet overnemen en je naar die site voordoen als die gebruiker en andersom. Deze kwetsbaarheden zijn al langer bekend en de website moet zo worden ingesteld dat de kwalijke codes worden afgevangen, maar dat wordt dus niet altijd goed gedaan. Dit is nog steeds de meest voorkomende kwetsbaarheid bij websites.

Crypto-1: het algoritme waarmee de Mifare Classic en de oude OV-chipkaart is versleuteld.

CSV: Een Comma Separated Value bestand is platte tekst in tabellen, gescheiden door een teken. Dat kan een komma zijn, maar ook een ander teken zoals een tab.

CVE: Common Vulnerability and Exposure. De CVE-database bevat bekende kwetsbaarheden en archiveert ze onder jaartal met een uniek nummer, bijvoorbeeld CVE 2011:1866.

DDoS: Distrubuted Denial of Service attack, een aanval waarbij een site bewust heel veel wordt opgevraagd en daardoor crasht.

Diginotar: een Nederlands bedrijf dat certificaten uitreikte aan websites over de hele wereld. Als je zo'n site bezocht, checkte je browser dat certificaat bij Diginotar. Klopte alles, dan verscheen het bekende slotje links boven in de browser. Totdat het bedrijf zelf gehackt werd.

ECP: platform voor de informatiesamenleving, waar bedrijven, overheden en non-profits elkaar ontmoeten.

End-of-life: aanduiding dat software niet meer wordt geüpdate, zoals bijvoorbeeld Windows XP.

FTP: File Transfer Protocol, een reeks afspraken waardoor de uitwisseling van bestanden tussen computers wordt vergemakkelijkt.

Govcert: het Governmental Emergency Response Team van de Nederlandse overheid, dat nu is ondergebracht bij het NCSC.

Hall of Fame: een lijst van verantwoorde onthullingen die een organisatie op haar site zet om de melders de credits te geven voor hun vondst.

Hashfunctie: een algoritmische bewerking die tekst of getallen terugbrengt tot een korte, unieke code. Dit wordt bijvoorbeeld gebruikt om wachtwoorden te controleren zonder ze te op te slaan of als echtheidskenmerk van een tekst.

Cookie: een klein bestandje dat door een website op je computer wordt geplaatst zodat de site kan zien of je die al eerder hebt bezocht.

IBD: Informatiebeveiligingsdienst voor gemeenten, werd 1 januari 2013 opgericht door VNG en KING.

IGZ: Inspectie voor de Gezondheidszorg.

Kamermotie: een uitspraak van één of meer Tweede Kamerleden om aan te geven dat een onderwerp belangrijk is, met een oproep aan de regering om actie te ondernemen.

Keylogger: programma waarmee je toetsaanslagen vastlegt en bijvoorbeeld wachtwoorden kunt afvangen.

KING: Kwaliteits Instituut Nederlandse Gemeenten.

Man in the middle attack: communicatie tussen twee partijen afvangen en je zo als een van beiden voordoen.

NEN 7510: norm voor informatiebeveiliging.

LAN: Local Area Network, meerdere computers die met elkaar verbonden zijn.

Megamos: algoritme dat gebruikt wordt om RFID-communicatie te versleutelen

Mifare Classic: een RFID-chip van NXP, die veel gebruikt wordt in toegangs- en betaalsystemen.

NAS: Network-attached storage, een opslagmedium dat op het netwerk is aangesloten en gebruik maakt van het ftp-protocol voor dataoverdracht.

NCSC: Nationaal Cyber Security Centrum.

Nikhef: het nationale instituut voor subatomaire fysica.

Officier van justitie: vertegenwoordiger van het Openbaar Ministerie, verantwoordelijk voor het opsporen en vervolgen van strafbare feiten.

Opta: Onafhankelijke Post en Telecommunicatie Autoriteit.

OTR: off the record.

Pastebin: website waar iedereen anoniem informatie op kan zetten en die populair is onder hackers. Zoek hier bijvoorbeeld eens op een van je wachtwoorden of gebruikersnamen…

Pentest/penetratietest: testen of je in een systeem kunt.

PGP: Pretty Good Privacy, een versleuteling op basis van een bekende code en een privé gedeelde code, waardoor derden de communicatie niet kunnen onderscheppen.

Poortscan: het op afstand analyseren van de poorten van een server. Internetverkeer van en naar servers gaat via verschillende poorten met elk een uniek nummer. Zo wordt bijvoorbeeld mailverkeer en websurfen van elkaar gescheiden. Als hacker doe je vaak eerst een poortscan om te kijken of je ergens makkelijk in kunt om van daaruit het systeem te verkennen.

Raadsman: advocaat die de verdachte bijstaat.

Rechter Commissaris: een rechter die aangewezen is door de president van de rechtbank om tijdens het opsporingsonderzoek, dat door de politie plaats vindt, beslissingen te nemen over zaken waarvoor de officier van justitie geen bevoegdheden heeft.

Rainbow table: een tabel met de versleutelde waarden (hashes) van wachtwoorden. Deze wordt gebruikt om te kijken hoe veilig wachtwoorden zijn, maar ook om ze te kraken.

Rathenau Instituut: onafhankelijk instituut dat de publieke en politieke meningsvorming over wetenschap en technologie stimuleert door middel van onderzoek en debat.

RFID: Radio Frequency Identitification, chips die communiceren via radiogolven en bijvoorbeeld gebruikt worden in toegangs- en betaalpasjes.

RTFM: Read The Fucking Manual, bekende reactie van hackers als iemand een te eenvoudige vraag stelt over een computerprobleem.

SCADA: Supervisory Control and Data Acquisition, een systeem dat meet- en regelsignalen van machines online doorgeeft en waarmee ze soms ook bestuurd kunnen worden, bijvoorbeeld pompen, verkeersseinen, vliegtuigen, straatverlichting of generatoren.

Shodan: online zoekmachine die alle apparaten weergeeft die aan het internet verbonden zijn.

Social engineering: hacktactiek waarbij eerst vertrouwen wordt gewonnen met mensen binnen een organisatie en hen vertrouwelijke informatie wordt ontlokt om uiteindelijk ook de systemen binnen te dringen. Bijvoorbeeld je als collega voordoen en een wachtwoord opvragen.

SQL injection: Structured Query Language invullen in een tekst box of de adresbalk van een website, om zo direct met de achterliggende database te communiceren. Je kunt bijvoorbeeld zoeken op een naam van een persoon en daar gegevens over opvragen. Je kunt die gegevens ook aanpassen, of de database opdracht geven een beheerdersaccount voor je aan te maken.

SSL: Secure Socket Layer: een encryptieprotocol dat werkt met certificaten om wederzijds te bewijzen dat je bent wie je zegt dat je bent.

Stuxnet: een worm, een zichzelf vermenigvuldigend computerprogramma dat onder andere is gebruikt om Iraanse kerncentrales onbruikbaar te maken.

Tango Programmer: apparaat van het Bulgaarse bedrijf Scorpio, waarmee je RFID-chips kunt programmeren.

THTC: Team High Tech Crime van de Nederlandse politie.

TIFF: Tagged Image File Format, een bestandformaat om beelden op te slaan.

Trans Link Systems: consortium van Nederlandse vervoersbedrijven dat het OV-chipkaart systeem beheert.

Truecrypt: programma waarmee je bestanden versleuteld kunt opslaan in een afgebakend gedeelte van een harde schijf, een container, die alleen zichtbaar wordt bij het juiste wachtwoord.

Twee/meerfactor authenticatie: inloggen in meerdere stappen, bijvoorbeeld gebruikersnaam met wachtwoord en vervolgens een pasje laten scannen of sms-verificatie invoeren.

TYPO3: een open source content management systeem.

VNG: Vereniging Nederlandse Gemeenten.

VPN: Virtual Private Netwerk, een internetverbinding via een derde partij die jouw IP-adres afschermt, waardoor je niet te traceren bent.

VPS: Virtual Private Server, ook wel Virtual Machine, een deel van een server dat je huurt bij een provider en gebruikt alsof het je eigen server is en ook weer makkelijk kan laten verdwijnen.

VNG: Vereniging Nederlandse Gemeenten.

White hat hacker: een hacker met ethische motieven.

Wigle: de Wireless Geographic Logging Database, een site waar je gps-coördinaten naar toe stuurt en dan ziet wat voor draadloze verbindingen daar zijn, met bijbehorende kwetsbaarheden.

Zero Day: een beveiligingslek dat nog niet eerder door anderen is gevonden.

Chris van 't Hof is onderzoeker en presentator in wetenschap en technologie. *Helpende hackers* is zijn achtste boek. In zijn tijd bij het Rathenau Instituut verschenen o.a. van hem: *Voorgeprogrammeerd. Hoe internet ons leven leidt*, *Check in / Check out. The Public Space as an Internet of Things* en *RFID and Identity Management in Everyday Life*. Nu organiseert en modereert hij met zijn bedrijf Tek Tok congressen en heeft hij een eigen talkshow: Tek Tok late night.

'Ziekenhuis lekt patiëntengegevens', 'OV-chipkaart zo lek als een mandje', 'Bankieren App onbetrouwbaar' – het lijkt wel of tegenwoordig alles te hacken is. Gelukkig is de persoon die dat doet niet altijd een cybercrimineel, maar juist iemand die wil helpen de digitale beveiliging te verbeteren.

Wie zijn deze ethisch hackers? Hoe ver mogen ze gaan? En wat moeten we doen als zij een beveiligingslek onthullen?

In dit boek komen hackers, gehackten, ICT-ers, journalisten, managers, politici en juristen aan het woord die betrokken zijn geweest bij een ethische hack. Ze schetsen een digitaal polderlandschap waarin iedereen een beetje, maar uiteindelijk niemand volledig verantwoordelijk is voor de informatiebeveiliging.

De persoonlijke verhalen geven een kijkje in de mysterieuze wereld van cyber security en laten zien hoe hackers ons kunnen helpen.

www.helpendehackers.nl

TEK TOK