CYBERELLENDE WAS NOG NOOIT ZO LEUK

Onthullende verhalen uit de wereld van informatiebeveiligers en hackers

Chris van 't Hof

TEK TOK


CYBERELLENDE
WAS NOG NOOIT ZO LEUK
Onthullende verhalen uit de wereld van informatiebeveiligers en hackers
Chris van 't Hof
TEK TOK

Cyberellende was nog nooit zo leuk

Onthullende verhalen uit de wereld van informatiebeveiligers en hackers

Chris van ’t Hof

Cyberellende was nog nooit zo leuk
Onthullende verhalen uit de wereld van informatiebeveiligers en hackers

Nederlandstalige uitgave onder Creative Commons, 2021 Tek Tok
Uitgeverij, www.tektok.nl
Auteur: Chris van ‘t Hof
Eindredactie: Bianca Kroon, www.auteurscollege.nl
Afbeelding voorkant: Hack Talk aflevering “Hacksters” van Simone van Lent
Afbeelding achterkant: Hack Talk aflevering “Het einde van het internet” van Jan Piet Barthel
Druk: Pumbo

Non-fictie
ISBN: 9789082346251
NUR: 958 - Computertechniek

www.cyberellende.nl

Inhoud

Intro

De afgelopen vier jaar heb ik meer dan honderd mensen gesproken aan tafel bij mijn praatprogramma Hack Talk. Het doel was gewone mensen te laten zien dat hackers best heel aardig kunnen zijn en de hackers te laten zien dat gewone mensen ook best interessant zijn. Daarnaast sprak ik meer dan honderd mensen tijdens cybersecuritycongressen, hackerevents en cybercrisisoefeningen. De meest interessante gesprekken heb ik geselecteerd voor dit boek en samengevat in een verhaal dat is opgebouwd uit zestien thema's.

Voor de meeste mensen is cybersecurity vooral lastig: weer dat f*ckingW4CH7W00rD! vergeten, opdringerige updates op het moment dat je het druk hebt en altijd weer die spam met phishingmails en andere malware in je inbox. Vraag je er een expert bij, dan wordt het ook al niet veel leuker. Die jast er een PowerPoint met horrorverhalen doorheen, doorspekt met afkortingen van technische termen, om tot de slotconclusie te komen dat als ze je willen hacken, dat altijd wel lukt. De wereld van cybersecurity, informatiebeveiliging en hackers wordt daarom vaak gezien als geheimzinnig en ondoorgrondelijk, en betekent vooral veel ellende.

Mijn ervaring is juist dat de wereld van cybersecurity een heel open wereld is, waarin mensen veel over hebben voor elkaar en daar veel lol aan beleven. In dit boek ontmoet je hackers die je willen helpen de beveiliging te verbeteren, een overheid die begrijpt dat je voor betere beveiliging af en toe de regels moet overtreden, organisaties die ervoor openstaan gehackt te worden en nerds die de beste feestjes organiseren. Cybersecurity kan, naast ellende, namelijk ook ontzettend leuk zijn. Onze reis in de cyberwereld begint daarom met een vette cybercrisis.

Chris van 't Hof

Rotterdam, februari 2021

1. Cybercrisis

Donderdag 4 oktober 2018, 9.30 uur. Bij de IT-helpdesk van de universiteit verschijnt een onderzoeker van de universiteit met een opengeklapte laptop. “Hij doet raar”, zegt de man en hij draait het scherm naar de helpdeskmedewerker. “Toen ik vanochtend opstartte, kreeg ik ineens dit te zien.” Het scherm is zwart en gevuld met witte letters: “Files encrypted”, “Pay now” en “Terminating this application or disconnecting from the network will result in the LOSS OF ALL DATA. More info? Go to http://nlnetneutrality.nl.” Leestekens naast de tekst vormen een doodshoofd. De laptop van de onderzoeker is besmet met ransomware.

“Geen probleem”, stelt de helpdeskmedewerker, “Ik zal hem effe schoonvegen en dan zet ik de laatste versie van de shared drive terug.” Hij probeert de laptop van de man over te nemen, maar die trekt hem weer terug. “Nee! Ik heb al mijn onderzoeksdata hierop staan. Erg gevoelig. Ik vertrouw die gedeelde schijf van jullie niet.” De helpdeskmedewerker zucht: “Momentje, ben zo terug” en hij loopt naar zijn leidinggevende in de andere kamer.

De man wil net gaan zitten als de volgende helpdeskmedewerker verschijnt. “Kan ik u helpen?” De man draait weer zijn laptop naar de medewerker. Die klikt de afbeelding met doodshoofd weg, zet de wifi aan en bladert wat door de bestandenmappen. “Nee hoor. Niks aan het handje. Hij doet het gewoon. Succes!”

De eerste medewerker treft in de kamer ernaast de leidinggevende van de helpdesk achter zijn scherm. Drie collega’s kijken mee en praten op hem in. “Check waar die webbeheerder allemaal toegang toe had!” roept één. “Trek de site uit de lucht!” roept een andere. Het hoofd schrijft een mail: “Doodshoofd op scherm” en voegt een bijlage toe met een screenshot van

hun website, met ook daar het doodshoofd met dreigende tekst van NLNetneutrality. Een van de medewerkers draait zich om: “Onze site is gedefaced. Het account van de webbeheerder is gehackt en we zijn die aan het resetten.” Een andere roept: “En ik heb iemand aan de balie met ransomware.” Het hoofd draait zich om: “Ik stuur wel een mail naar het CERT” en duikt weer op zijn toetsenbord. Een van zijn medewerkers zegt: “Misschien kun je ze beter even bellen…”

Het Computer Emergency Response Team (CERT) blijkt die dag zwaar onderbezet. De meesten zijn op training bij SURF, de ICT-samenwerkingsorganisatie van het onderwijs en onderzoek in Nederland. De presentielijst meldt slechts een CERT-er, maar die neemt niet op. De lijn is bezet. Bij andere helpdeskmedewerkers druppelen nu ook meldingen binnen. Er zijn inmiddels vier laptops vergrendeld met dezelfde doodshoofdtekst. Een van de medewerkers begint de tekst voor te lezen die op hun gehackte site staat:

“Netneutraliteit en academische vrijheden staan op de tocht! Mailhaus blokkeert onder de vlag van ‘een veiliger netwerk’ legitieme bedrijven en ontzegt individuen die hen niet aanstaan effectief toegang tot het internet. Hierdoor wordt het internet, wat de vrijplaats van meningsuiting zou moeten zijn, gecensureerd. SURFnet, de coöperatie van onderwijs, onderzoek en zorg in Nederland, is hoofdsponsor van Mailhaus. Het sponsoren van dergelijke organisaties is in strijd met de doelstellingen en beperkingen die SURFnet zijn opgelegd. Belastinggeld is er niet om internetmaffia te sponsoren.

Hieronder staat een lijst van leden van SURF die aan deze maffiapraktijken meedoen. Ik heb bij deze organisaties een groot aantal machines onder controle. Ik houd deze in gijzeling tot de maffiapraktijken stoppen!

Ik ben geen crimineel en ik wil docenten en onderzoekers niet duperen. Omdat ik onderwijs een groot hart toedraag is er daarom een clementieregeling: tegen betaling van een schadevergoeding…”

“Ja, ja”, onderbreekt het hoofd hem, “ze willen geld. Maar dat gaan we natuurlijk niet doen. Neem al die laptops maar in en breng ze naar het CERT. Ik bel de Incident Manager. We gaan opschalen.”

De universiteit heeft sinds de recente reorganisatie haar crisismanagementproces gestroomlijnd met nieuwe bemensing en protocollen. Binnen enkele minuten gaan op verschillende afdelingen mobieltjes af. Er worden twee Crisis Management Teams geformeerd: één van de afdeling Communicatie en één van de afdeling ICT. De teams worden geleid door hun afdelingshoofden en samengesteld op basis van een oproeplijst van mensen die zich hiervoor hebben opgegeven. De meesten blijken afwezig, waardoor vervangers uit vergelijkbare posities worden opgeroepen. Dat zijn vooral nieuwe medewerkers. Volgens protocol krijgt elk team een observator toegewezen die het proces documenteert en evalueert. Ik ben de observator van team ICT.

De formatie van het team verloopt chaotisch. Verschillende medewerkers die de oproep van de Incident Manager hebben gekregen, dwalen over de gang. Hun afdelingshoofd blijkt vandaag afwezig en is niet oproepbaar. Tweede in lijn blijkt clustermanager Frits, een ervaren techneut met wie de universiteit wel vaker IT-brandjes heeft geblust. Nu, in deze crisis, ziet hij zijn kans schoon om zijn waarde voor zijn afdeling te bewijzen. Met ferme tred baant hij zich een weg door de volle gang en sleurt onderweg zoveel mogelijk dwalende collega's mee naar vergaderkamer 101.

Frits loopt direct naar de flip-over, trekt er drie vellen af en plakt die naast elkaar op een lege zijwand. De medewerkers druppelen één voor één binnen, nemen een plek aan tafel en klappen hun laptops open. Zelf stel ik me verdekt op in een hoek. Als externe observator mag ik het proces niet beïnvloeden. Wel heb ik goed zicht op de vellen van Frits, die hij markeert met 'feit', 'waarneming' en 'veronderstelling'. Zichtbaar tevreden draait hij zich om.

Iedereen kijkt nu naar de Incident Manager die op een whiteboard aan een andere muur noteert: 'phishingmail via SURF-nieuwsbrief', 'encryptie bestanden', 'powershellscript met doodskop'. Hij licht toe: "Het CERT is inmiddels gealarmeerd en buigt zich over de geïnfecteerde laptops. Er zijn ook bestanden op de shared drive geraakt." Richard, adjunct-afdelingshoofd en de derde in lijn als crisismanager, vult aan: "De geraakte webbeheerder heeft zijn wachtwoord gereset. SURF meldt dat er inderdaad phishingmails namens hen verstuurd worden met een link naar de ransomware. We zijn

die mails van de server aan het wissen. Moeten we het College van Bestuur informeren?"

"Nee", zegt Frits, "nog niet" en hij wijst naar Gerda: "Houd jij de media bij." In het dagelijks leven is ze Hoofd van de afdeling Inkoop, maar omdat daar vandaag geen behoefte aan is, doet ze nu de communicatie. Een andere vrouw is van het functionele beheer van SharePoint, de Microsoft werkomgeving van de universiteit. Nu monitort ze het onlineverkeer van en naar hun gedeelde werkomgeving. Verder zitten er nog twee afdelingshoofden, één van Infrastructuur en één van Identity & Access, maar zij krijgen geen taak toegewezen. Frits heeft dus als clusterhoofd vooral de hoofden verzameld die onder hem de verschillende afdelingen leiden. Hij vertrouwt erop dat ieder zijn taak kent in tijden van calamiteiten, zoals ze altijd al hebben gedaan.

Dit is de groep mensen die ik deze dag observeer. Tenminste, als ze in deze ruimte zijn, want het grootste deel loopt continu in en uit. De communicatie verloopt chaotisch en ik heb de grootste moeite om uit de flarden van feiten en veronderstellingen enig overzicht te krijgen van wat er gebeurt. Wat mij als observator wel enorm helpt, is dat de universiteit me een e-mailaccount heeft toegewezen, waarmee ik kan meelezen in een groot deel van de mailgroepen die de leden van dit team en de andere teams gebruiken.

Zo zie ik een mail voorbijkomen van het team Communicatie. Het is een concepttekst om alle medewerkers te waarschuwen voor de nepmail van SURF. Aangeraden wordt die te negeren en te verwijderen. Het concept gaat als een pingpongbal van de één naar de andere, met wijzigingen die de tekst er niet leesbaarder op maken. Telkens als iemand van het team hier vraagt waar die mail blijft, lijkt die weer een zetje te krijgen in een andere richting. Het zal nog tot in de middag duren voordat de mail eindelijk verstuurd wordt.

Frits pakt regelmatig zijn telefoon en loopt dan zonder enige toelichting naar buiten. Op die momenten valt de discussie aan tafel stil en duikt iedereen in zijn laptop. Ik ook en ik check Twitter, Facebook en Nu.nl. Daar lees ik dat ook andere onderwijsinstellingen geraakt zijn door ransomware. Studenten en medewerkers klagen dat hun accounts uit de lucht zijn. Speculaties over de dader doen de ronde. Iemand vraagt: "Internetmaffia of

helden?" Ik kijk op de site NLNetneutrality.nl en lees daar dezelfde tekst die we net van onze eigen site hebben verwijderd. Eronder staat een lijst met alle universiteiten en hogescholen van Nederland. Een teller geeft aan hoeveel bestanden zijn versleuteld. Onze universiteit zou vier besmettingen hebben. Dat klopt dus. Er zouden 19.134 bestanden versleuteld zijn en we hebben nog 13 uur en 14 minuten om te betalen. Op Twitter haalt een van onze onderzoekers uit naar onze universiteit: "Waardeloos IT-beheer. Daarom bewaar ik mijn bestanden zelf." Dit is volgens mij de man van de laptop. Maar ik zeg niets. Ik ben slechts observator.

Frits is weer terug en roept triomfantelijk: "Er wordt een mail verspreid dat mensen een malafide mail hebben gekregen van SURF en dat ze die direct moeten weggooien." Niemand reageert. Hij geeft de Incident Manager opdracht hierover een WhatsApp te versturen. Die vraagt: "Prio 1?" Frits: "Uiteraard!" Ik lees in onze WhatsAppgroep: "Update: Prio verhoogd naar 1. Geïnfecteerde werkstations zijn veroorzaakt door een nieuwsbrief die afkomstig leek van SURF. Links hierin kunnen zorgen voor versleuteling van bestanden, lokaal en op netwerkschrijven." Degene die normaal SharePoint beheert en nu het netwerk monitort roept: "Ik zie dat 68 werkstations de mail hebben ontvangen en geopend. Die zouden geïnfecteerd kunnen zijn."

Er komen twee mannen binnen. Het zijn onze Chief Information Officer en Chief Information Security Officer: "We komen voor een update." Frits raast door zijn flip-overs: "Veronderstelling: Mailhouse hack. Feit: mail met login. Waarneming: bod met doodshoofd. Medewerkers worden via een mail gewaarschuwd." Gerda corrigeert hem: "Nee, die is nog in concept. We zijn wel al mails aan het verwijderen van de server. Andere universiteiten hebben ook een doodshoofd." De CISO heeft ook nieuws: "Er is net iemand betrapt die ergens een USB-stick in stak en wegrende. De man is niet gepakt, maar de stick wel." Gerda: "Is in Eindhoven ook gebeurd."

Iedereen begint nu door elkaar te praten. "CERT meldt dat er een besmetting is geconstateerd bij de centrale server, door een laptop die weer van het netwerk is getrokken. – Is dat niet die zwarte laptop van die onderzoeker, die hem niet wilde afgeven? – Is dat die man die ons ook

online beschuldigt? – Of was dat die stick? – Wat voor data? – Moeten we de Autoriteit Persoonsgegevens niet bellen? – Kunnen we alles uitzetten of zijn er toetsen gaande? – Heeft er wel datatransfer plaatsgevonden? – Kan nog steeds bluf zijn. Gewoon uitzitten en hard uitlachen. – Ja, we isoleren het besmette deel en zetten de back-up weer terug. – Moeten we alle wachtwoorden resetten? Nee dan krijg je paniek. – Stuur die USB-stick op voor analyse…"

De CIO maant tot stilte: "Hier is duidelijk sprake van een gecoördineerde aanval op verschillende universiteiten. We zijn inmiddels opgeschaald. Het Crisis Management Team van het College van Bestuur is geactiveerd." Als de CIO en de CISO naar buiten lopen, stelt Frits voor om even pauze te nemen. Het team verlaat de kamer en ik ren achter de CISO en CIO aan. We gaan naar een andere verdieping, waar het College van Bestuur samenkomt.

De sfeer in de grote bestuurskamer voelt meteen anders aan. De voorzitter van het College van Bestuur kijkt rustig de tafel rond en wijst verschillende rollen toe. Ze introduceert de net binnengekomen CISO en CIO aan de rest van haar team als de verbindingslijn met het ICT-team. Beiden zijn blijkbaar nog niet zo lang in functie. Het hoofd Communicatie verdeelt de rollen binnen haar team. Een teamlid wordt aangewezen om het woord te voeren met de buitenwereld en een andere om de media te analyseren. De voorzitter knikt instemmend naar de secretaris, die opstaat en drie flip-overvellen ophangt met: 'Beeld', 'Oordeel' en 'Besluit'. Ze gaat de tafel rond voor ieders input en leidt het gesprek zonder zelf te oordelen. De hoofden van de collega's aan tafel draaien in een vast ritme van de voorzitter die de discussie leidt naar de collega's en de vellen met het overzicht. Mijn collegaobservator zit rustig te typen en maakt een foto van de flip-overvellen.

In nog geen halfuur komen ze tot een reeks besluiten over acties die moeten worden uitgezet. De universiteit zal geen losgeld betalen. Het CERT neemt besmette computers in om ze schoon te maken. De waarschuwingsmail is klaar en mag verzonden worden. Communicatie stelt een Q&A op, voor het geval studenten en collega's met vragen komen. De woordvoerder heeft ook een Q&A, mochten er journalisten gaan bellen.

ICT moet het internetverkeer monitoren en uitzoeken wat er versleuteld of gelekt is. Daarna kan de Autoriteit Persoonsgegevens worden ingelicht. “Verder nog iets?” vraagt ze. Nee. “Mooi. Dan zie ik jullie hier weer over twee uur.”

Terwijl we naar buiten lopen, steek ik mijn duim op naar mijn collega-observator. Ze glimlacht, maar we zeggen niets. Het team mag niet beïnvloed worden en wij moeten doen alsof wij er niet zijn. Zij mag nu even pauze nemen. Ik niet, want terug in kamer 101 blijkt ICT op volle stoom te zijn. Er staan gelukkig wel broodjes op tafel. Maar als ik er een pak, roept Frits: “Hee, jij bent hier toch niet?!” Iemand lacht. Zwijgend trek ik me terug in mijn observatiepost in de hoek.

Frits gaat zijn krabbels op de flip-over bijwerken, terwijl de rest rond een laptop staat. Eén mompelt: “Hm, video’s, een Excel-sheet met namen en adressen, bonnetjes van de decaan en een bestand ‘Aanstellingen Hoogleraren’.” De bestanden zouden van de gedeelde schijf naar een verdacht IP-adres zijn gegaan – hetzelfde adres dat de ransomware oproept als die geïnstalleerd is. Frits lijkt niet geïnteresseerd en wijst naar de flip-overvellen: “Vier geïnfecteerde laptops. Daar kunnen we wat aan doen, dus dat is onze prioriteit!”

Klokslag 17.00 uur klapt iedereen zijn laptop dicht en verlaat kamer 101. In de tussentijd heeft de universiteitskrant een artikel gepubliceerd, waarin een boze medewerker meldt dat de universiteit data heeft gelekt. Het betreft een medisch onderzoek naar verstandelijk gehandicapte kinderen, compleet met video’s en contactgegevens van de ouders. Een woordvoerder meldt dat de universiteit geraakt is door een grootschalige cyberaanval en zij er alles aan doet om de slachtoffers te informeren.

De volgende dag komen om 9.00 uur de drie Crisis Management Teams weer bijeen. Het College van Bestuur zit op de bovenste verdieping. Communicatie en wij eronder. Frits zit naast Richard, die als adjunctafdelingshoofd de derde in lijn is als crisismanager. De CIO en CISO staan aan weerszijden met hun handen achter hun rug te glimlachen. Frits zit wat onderuitgezakt en kijkt de groep rond: “Ik draag even over. Vier besmette laptops. Verschillende bestanden versleuteld. Data gelekt

over baby's. Succes ermee!" Hij staat op en gaat in een hoek zitten. De CISO en CIO vertrekken naar het College van Bestuur.

Richard mag blijkbaar nu de voorzitter zijn van ons crisisteam. Hij knikt naar Eva, zijn secretaresse, die blijkbaar aan het team is toegevoegd. Ze staat op, verwijdert de vellen met de krabbels van Frits en hangt, duidelijk in het zicht, een vel op. Richard kijkt de groep rond: "Goed, wat weten we? En welke acties zijn daarop uitgezet?" Eén voor één leggen de medewerkers hun feiten en acties op tafel. Eva pakt een stift en noteert:

- ransomware aanval NLnetneutrality op alle universiteiten – SURF coördineert
- 4 laptops besmet: 2 veiliggesteld, 1 vermoedelijk bij onderzoeker, 1 zoek
- datalek: onderzoek kinderen, declaraties decaan en aanstellingsbeleid – onderzoeker wordt opgespoord, getroffenen worden gecontacteerd door Communicatie, CvB informeert AP
- phishingmail: 68 ontvangen – we monitoren het verkeer
- verdachte USB-stick gevonden – ligt bij CERT voor analyse.

Richard: "Mooi. Dit is dus wat we weten. Maar wat weten we niet? Waar zitten de blinde vlekken?" De SharePointmedewerkster kijkt op van haar monitor en roept: "Of die 68 mensen die op die phishingmail hebben geklikt, ook besmet zijn. Van vier weten we het zeker, maar van 64 dus niet. Als ze die ransomware hebben, komen ze vanzelf bij de helpdesk. Maar als ze gebruikt worden om data van ons netwerk te halen, zien we dat dus niet." Iemand suggereert: "Dan maar gewoon hun wachtwoorden resetten. Komen ze vanzelf naar ons toe." Frits springt op: "Moet je nooit doen. Je weet niet wat er dan gebeurt!" Een reeks vernietigende ogen vermaant hem weer te gaan zitten.

Richard rent naar buiten en komt even later binnen met een verbaasd kijkende man. Het is het Hoofd van de IT-helpdesk. "Ga zitten. Stel dat er binnen een paar uur 64 mensen aan de servicebalie komen om hun wachtwoord te resetten, kunnen jullie dat aan?" De man grijnst: "Ja hoor, we maken wel ergere dingen mee." "Mooi. Hebben jullie een protocol voor wat te doen bij ransomware?" "Ja, laptop innemen, wissen en back-up terugzetten. We hebben er nog een staan, maar weten niet van wie die is."

“Ah, dat is die ene die we kwijt waren. Dankjewel, heb je verder nog nieuws? Nee, dan was dat het.”

Net als het Hoofd Helpdesk vertrekt, komen de CISO en CIO binnen. Richard neemt de lijst door met de heren en vraagt: “Zijn wij bevoegd om een harde-wachtwoordreset te laten uitvoeren?” De CIO glimlacht: “Nee, maar ik wel. Waarom zijn jullie daar niet eerder op gekomen?” Iedereen kijkt wat schaapachtig om zich heen. “Kan de helpdesk dat wel aan? “Ja, die hebben we net ingelicht.” “Doen! SURF heeft overigens de sleutels gevonden van de ransomware, dus we kunnen gaan ontsleutelen. Prioriteit is nu kijken wat wel en niet gelekt is, dan kunnen we dat melden aan de Autoriteit Persoonsgegevens en getroffenen.”

Het crisisteam werkt die middag hard aan een totaaloverzicht van al het netwerkverkeer van en naar de universiteit. De analyse van de USB-stick komt terug, maar blijkt weinig spannends te bevatten. Waarschijnlijk een afleidingsmanoeuvre. De klok op NLnetneutrality.nl blijft onverbiddelijk aftellen. Nog een uur en dan zouden al onze 19.134 versleutelde bestanden online gepubliceerd worden, maar ons team vermoedt dat dat alleen maar bluf is. De teamleden rapporteren alles netjes via de mail. Die komt echter niet aan. De wachtwoorden van de laptops van de andere crisisteams zijn namelijk ook gereset…

Langzaam maar zeker begint de energie weg te vloeien uit ons team. Hier en daar komen mobieltjes tevoorschijn voor berichtjes aan het thuisfront. Ik zie op Twitter een bericht: “Mogelijke dader cyberaanval opgepakt”. Dan komt de spelleiding binnen: “Einde oefening”.

OZON is een landelijke cybercrisisoefening waar op 4 en 5 oktober 2018 in totaal vijftig Nederlandse kennisinstellingen aan deelnamen: alle universiteiten, vele hogescholen en roc’s en enkele ziekenhuizen, medische centra, bibliotheken en onderzoeksinstituten. Ook de politie, mbo-raad, VSNU en de Autoriteit Persoonsgegevens deden mee. De in totaal meer dan 2.500 deelnemers wisten alleen dat er een oefening zou zijn en niet wat hen zou overkomen – met uitzondering van de spelleiders. OZON staat voor Oefening Zonder Officiële Naam en is bedacht en wordt geleid door SURF. De eerdergenoemde gebeurtenissen heb ik geconstrueerd uit ervaringen bij

verschillende kennisinstellingen, van mezelf als observator en uit de verhalen die ik hoorde tijdens de evaluatie bij SURF. Die vond plaats op 9 oktober op hun kantoor in Utrecht.

De bijeenkomst zou 10.00 uur beginnen. Als ik netjes op tijd binnenkom, is de vergaderzaal al helemaal afgeladen. Alle spelleiders van de deelnemende instituten zijn aanwezig. De sfeer is uitbundig, er wordt flink gelachen. Remon Klein Tank, bij SURF de projectleider van OZON, trapt af met een bedankje aan ene Mr. Malware. Het is iemand van het Nederlands Forensisch Instituut die de ransomware heeft geschreven. De universiteiten waren dus ook echt besmet, uiteraard zonder daadwerkelijk bestanden te gijzelen of weg te sluizen. Hij krijgt veel applaus. Remon geeft een samenvatting van de oefening in de vorm van een kennisquiz, die vervolgens wordt gewonnen door Mr. Malware. Hij krijgt een sjaal.

De deelnemers blijken op verschillende niveaus mee te hebben gespeeld. Het merendeel deed het volledige spel, niveau ‘goud’. Een van hen doet verslag: ze hadden gerekend op vijftig deelnemers, vijfenzeventig meldden zich aan, maar op de dag zelf werden het er meer dan honderd. Van alles ging mis – dus veel geleerd. Een andere ‘goudspeler’ vult aan: “Alles wat we vooraf hadden bedacht, viel weg, dus we hebben het puur op adrenaline gedaan.” Een zilverspeler meldt dat haar team juist heel veel heeft aan de draaiboeken en ze door de oefening hun rollen beter kunnen definiëren: “Het crisisteam moet minder zelf uitvoeren, daar hebben we nu een flexibele schil van specialisten omheen”. Overigens hadden ze wel hun firewall moeten uitzetten, omdat de ransomware er anders niet doorheen kwam. Ook niveau brons komt aan het woord. In hun scenario waren mobieltjes met gevoelige data kwijt, wat uitmondde in een wilde speurtocht. Volgende keer doen ze ook mee met goud.

Dan komt ene Koen op en de zaal ontploft zowat van gelach en geklap. Hij blijkt de man op de foto te zijn met een zwart balkje voor zijn ogen, bij het bericht “Dader cyberaanval opgepakt”. Hij zwaait wat verlegen en toont statistieken van de evaluatie:

“Algeheel rapportcijfer: 8,2”

“Zou je de oefening aanraden bij je collega’s: 99%”

Koen licht toe: “Die 1% bleek een persoon te zijn die er niet eens bij was.” De spelleiders hadden elk gemiddeld 210 uur besteed aan de

voorbereidingen. Hebben zij hun oefendoelen bereikt? De helft zei ‘ja’, de andere helft ‘deels’ en niemand antwoordde ‘nee’. Links en rechts gaan vingers omhoog om aanvullingen te geven, waarbij Koen hen een microfoon in catchbox toewerpt. De sponzen kubus gaat steeds sneller door de zaal en vangt veel grappige anekdotes. Hier en daar worden laptops omgegooid. Is iedereen er in de volgende keer ook weer bij? Jazeker.

Cybersecurity is gewoonlijk taaie materie. Voorlichtingen over online veiligheid staan bol van onpraktische handelingen, technische termen en zware waarschuwingen. Dat is niet leuk en daarom luisteren mensen misschien nog wel, maar passen ze hun onlinegedrag nauwelijks aan. Bij een oefening gaat het niet om luisteren, maar doe je ook echt iets. Je leert jezelf en je collega’s beter kennen, vanuit welke veronderstellingen we onze IT-systemen gebruiken, hoe we reageren in crisissituaties, welke communicatielijnen er zijn en wat er beter kan. Bovenal maakt een goeie crisisoefening cyberellende niet alleen leerzaam, maar vooral ook leuk.

Het kan zijn dat je zelf een cybersecurity expert bent. Je weet dat je een goede passwordmanager moet gebruiken, je installeert updates altijd zo snel mogelijk en klikt nooit op iets wat je niet vertrouwt. Je weet wat een CISO of pentester doet, waar ik het over heb als ik er een CVE of XSS in gooi en denkt wellicht: kom maar op met die bugs die we moeten fixen. Die krijg je zeker, maar dit boek gaat vooral ook over mensen. Gewone mensen, die zoiets bijzonders hebben meegemaakt, zoals de OZON-oefening hierboven, waardoor ze anders zijn gaan kijken naar hun dagelijks gebruik van IT. En bijzondere mensen, die op eigen wijze omgaan met IT en net dat ontdekken waardoor het stuk kan, anders gebruikt kan worden of juist verbeterd kan worden. Dat zijn de helpende hackers: mensen die technologie maken, breken en bespreken.

Voeg je de twee samen, mens en technologie, dan gebeurt er iets magisch. Je leert de mensen kennen door hoe ze technologie gebruiken en je leert de technologie kennen door wat mensen ermee doen. Die twee komen samen in het woord ‘cyber’ en daar hebben we inmiddels aardig wat van in Nederland.

We hebben een Nationaal Cyber Security Centrum, dat jaarlijks een Cyber Security Beeld Nederland uitbrengt, gevolgd door een Cyber

Security Agenda, die wordt opgesteld samen met de Cyber Security Raad en uitgevoerd door een Cyber Security Alliantie. Onderzoekers komen samen in dcypher, het Dutch Cyber Security Platform for Higher Education and Research, om een Nationale Cyber Security Research Agenda en een Nationale Cyber Security Educational Agenda op te stellen. Onze gemeenten hebben een Handreiking Cyber Gevolg Bestrijding om cybercrises te lijf te gaan. Defensie bereidt zich voor op een cyberoorlog en heeft hiervoor cyberrekruten en een Dutch Cyber Command. Deze soldaten zien cyber als hun vijfde slagveld, naast land, lucht, water en ruimte. Onze geheime diensten hebben een Joint Cyber Strike Unit. Onze securitybedrijven hebben zich verenigd in Cyber Veilig Nederland. En op tv zien we programma's als Opgelicht Cyber en CSI cyber…

Maar wat is nou 'cyber'? Volgens criticasters op Twitter is cyber vooral een buzzword om IT-beveiliging mysterieus en sexy te maken. Ik geef toe dat mensen eerder enthousiast worden van een Cyber Security Awareness Session, dan wanneer je iets aankondigt als een informatiebeveiligingsbewustwordingsbijeenkomst. Volgens het nieuwe *Cybersecurity Woordenboek* van Cyberveilig Nederland is cyber niets bijzonders, gewoon "iets wat te maken heeft met digitale informatie en systemen die verbonden zijn met het internet".

Cyber is echter meer dan dat. Het woord heeft immers zijn oorsprong in de klassieke oudheid: Kubernetis, wat zoveel betekent als 'stuurman'. Plato gebruikte de term vervolgens als 'bestuur' in een democratische samenleving. Ampère nam het woord en de betekenis over en vertaalde het in 1834 in het Frans naar 'cybernétique'. De link met technologie werd in 1948 gelegd door Norbert Wiener in zijn boek *Cybernetics* als "control and communication whether in the machine or in the animal". Cyber werd echter pas echt populair door het boek *Neuromancer* uit 1984, waarin William Gibson het heeft over 'cyberspace', de digitale belevingswereld waarin de hoofdpersonages zich begeven. Onbedoeld zet hij een nieuw literair genre in gang, 'cyberpunk'. Schrijvende hackers die zich afzetten tegen de macht van bedrijven en overheidsorganisaties, die op hun beurt gretig alles wat met digitaal te maken heeft, voorzien van het woord 'cyber'.

Wat al deze werken gemeen hebben, is dat ze beschrijven hoe technologie het handelingsvermogen en de belevingswereld van mensen vergroot. Gevolgd door de vraag: wie bestuurt wie, de mens de technologie of andersom? Ik denk dat het daarom een zeer bruikbaar woord is. Zeg je ‘digitaal’ of ‘informatietechnologie’, dan denken mensen dat het alleen over de apparaten gaat en niet over henzelf. Cyber is beide: wat wij doen met technologie en wat technologie doet met ons.

Niet alleen het woord cyber, maar ook cyberellende vinden we al terug in de Klassieke Oudheid. Dat is te lezen in *The Code Book. The Secret History of Codes and Code-Breaking* van Simon Singh uit 1999. Toen de Spartanen grote delen van het huidige Griekenland koloniseerden, kregen de soldaten instructies mee voor wie wanneer waar moest aanvallen. Nadat die instructies een paar keer in de handen van de vijand vielen, bedachten ze een vorm van versleuteling. De riem van een soldaat werd een paar keer om een cilinder gerold, de zogenoemde scytale en de tekst overdwars geschreven. Rol je de riem uit, dan lijkt het een tekst die je van boven naar beneden moet lezen, maar dan met alle letters door elkaar. Je kunt de boodschap alleen lezen als je het trucje kent en een cilinder hebt met de juiste diameter. Briljant, want met tweeëntwintig verschillende letters in het Griekse alfabet heb je bij een zin van slechts tien letters al biljoenen mogelijke uitkomsten. Tenzij je weet hoe het werkt natuurlijk. Zo wist Lysander in 404 v.Chr. een slag tegen Pharnabazus te winnen omdat hij de riem van een van zijn soldaten had bemachtigd en wel wist hoe hij de boodschap kon ontsleutelen. Zie hier een voorbeeld van antieke cyberspionage.

In diezelfde tijd kwam *Kama Sutra* uit, een boek waar veel meer in staat dan de erotische posities waarvan het bekend is geworden. In de lijst van 64 kunsten die een vrouw volgens deze leer moet beheersen, staat op nummer 45 het geheimschrift. Deze cryptografie is even simpel als doeltreffend voor die tijd: maak een tabelletje waarmee je elke afzonderlijke letter vervangt door een willekeurige andere en geef alleen een kopie aan de ontvanger. Mocht iemand jullie tekst onderscheppen, dan zal die het aantal tekens tot de macht het aantal letters in je alfabet moeten afgaan om het te ontsleutelen. Dat is niet te doen.

Een ander voorbeeld van beroemde crypto volgt een kleine 300 jaar later: de Caesar Cipher. Als Julius Caesar een geheime boodschap wilde versturen, verplaatste hij simpelweg elke letter een paar plaatsen in het alfabet, dus: a=d, b=e, etc. Dat is natuurlijk barslechte versleuteling, maar niemand durfde dat toentertijd te zeggen tegen de bloeddorstige dictator. Had hij de *Kama Sutra* maar gelezen…

Niet alleen het maken, maar ook het kraken van encryptie kent een rijke geschiedenis. Wellicht een van eerste grote codekrakers is de Arabische filosoof Al-Kindi, geboren in 801. Om versleuteling te kraken, paste hij onder andere frequentieanalyse toe: kijk hoe vaak een letter gemiddeld voorkomt in een taal en vergelijk dat met de versleutelde tekst. Je begint met de meest voorkomende letter. In het Nederlands is dat de ‘e’. Komt de X het vaakst voor in de sleuteltekst, dan staat die waarschijnlijk voor de ‘e’. Al-Kindi stond aan het begin van een rijke traditie van Arabische cryptoanalisten. Deze vrije intellectuelen hielden zich, grofweg van de jaren 800 tot 1200, bezig met taal, wiskunde, filosofie en codekraken. Ze deden dit vooral als intellectuele uitdaging en om versleuteling te verbeteren. Deze Arabieren waren dus eigenlijk de eerste helpende hackers.

De vroege geschiedenis van versleuteling in Europa is vooral ingegeven door conflicten tussen landen, zowel in tijden van oorlog als vrede. Vanaf de 16e eeuw had elk zichzelf respecterend land wel een zogenoemde Zwarte Kamer, waar voor spionagedoeleinden codes werden gekraakt. In de 19e eeuw deden de eerste machines voor versleuteling en ontsleuteling hun intrede, wat in de 20e eeuw evolueerde tot de epische machine Enigma. Dit van oorsprong Poolse ontwerp werd door de Duitse nazi’s geperfectioneerd tot een kluwen van bewegende schijven die bij elke toetsaanslag letters op een andere manier verving. Enigma was niet te kraken, volgens de Duitsers.

Wel volgens Alan Turing. Deze Britse wiskundige was al voor de oorlog bezig een machine te bouwen om algoritmes uit te voeren, zijn Turing Machine. Turing was niet echt geschikt voor op het slagveld, dus ging hij aan de slag bij de Government Code and Cypher School. Toen de Britten enkele Enigma-machines en een handboek in handen hadden gekregen, wilde Turing wel proberen de Duitse code te kraken. Hij bouwde met zijn team de Bombe, een elektromechanisch beest van vele

relaisschakelingen. Het ding had maar één doel: zoveel mogelijk combinaties van versleuteling uitproberen tot er iets logisch uitkwam, een techniek die we vandaag de dag ‘brute forcing’ noemen. Eén bleek niet genoeg, dus bouwden ze een hele reeks Bombes, die net zolang bleven draaien tot ze de code kraakten. De rest is geschiedenis.

Eigenlijk waren er dus eerst hackers en daarna pas de computer, die we mede te danken hebben aan een van de grootste hackers aller tijden. Turing was ook een bijzondere persoonlijkheid: geniaal, geobsedeerd, moeilijk in de persoonlijke omgang, maar wel met de beste bedoelingen voor de mensheid. Die eigenschappen zie ik wel vaker bij helpende hackers. De geschiedenis van hacken is er vooral een van de andersdenkenden die meer begrip verdienen. Dat is ook mijn motivatie voor het schrijven van dit boek.

De informatietechnologieën die we dagelijks gebruiken, of het nu gaat om websites, apps, smartphones of slimme deurbellen, worden over het algemeen geproduceerd door mensen die dit ook maar gewoon doen voor hun werk. Ze kopiëren en plakken code en componenten aan elkaar, net zolang totdat het naar behoren werkt. Dan wordt het product getest op de gebruikers. Bijvoorbeeld een website: dit is het internetadres, klik daar op a, b, c of d, vul hier je naam in, betaal, klik op ‘like’ en vertel ons wat je ervan vindt… Ook dat wordt herhaald, net zolang totdat het naar behoren werkt. Op naar de volgende site.

Hackers doen dat niet. Die vullen niet achteloos het internetadres in, maar typen er meteen wat code achter. Ze klikken niet op a, b, c of d, maar zoeken of er ook een optie x, y of z is. En ze drukken dan niet één keer op die knop, maar wel 100.000 keer. Ze schrijven niet hun naam in het tekstvakje, maar een computercommando. Waarom? Omdat het kan.

En als er dan iets gebeurt wat niet de bedoeling is, dan worden hackers enthousiast en gaan ze kijken wat er nog meer kan. Net zolang tot ze de puzzel hebben opgelost. Dat is de kick van het hacken. De een doet dat heel systematisch, de andere gaat juist alle kanten op. De een wil vooral kijken hoe iets werkt, de ander wil gewoon slimmer zijn dan de maker. Hackers zijn er in alle soorten en maten, maar ze hebben een ding gemeen, namelijk:

H4CK3R5Z13ND1NGEN4ND3R5D4N4ND3R3N

Voor ons gewone mensen is het dan van belang dat iemand die anders kijkt naar de apparaten die we dagelijks gebruiken, aan onze kant staat. Alleen dan kunnen kwetsbaarheden opgelost worden voordat ze worden misbruikt. In de versleuteling zit overigens bewust een fout. Zag je hem meteen? Dan heb jij wellicht ook een hackersgave. Zo niet, hij zit in het midden, een ‘E’ in plaats van ‘3’. In dit boek laat ik op vergelijkbare wijze zien dat hacken soms ingewikkeld is, soms een simpel trucje dat je vaak moet herhalen, maar vaak toch neerkomt op net even anders naar de dingen kijken dan de bedoeling is.

Ik neem je mee in de wereld van cybersecurity, die weliswaar draait om geheimen, maar juist heel erg open blijkt te zijn. Iedereen deelt en doet van alles met elkaar, zowel online als in real life. Je leert hackers kennen die zich meer dan wie dan ook onbaatzuchtig inzetten om onze beveiliging te verbeteren. Dan leer je dat je pas echt veilig bent als je een keer goed gehackt bent. Sterker nog: wellicht zullen we deze hackers nog hard nodig hebben voor de eerstvolgende oorlog. Laten we ze daarom helpen in hun missie, zodat zij ons kunnen helpen. Zo maken we samen de digitale wereld een stuk veiliger.

2. Hackers verbeteren beveiliging

Stel je ontvangt op een dag deze e mail:

“Dear madam, sir,
Could you please forward this message to your client / the owner of this server?
Thank you very much!
I want to inform you that your website is running a MongoDB instance which appears not to be correctly configured or protected by a firewall allowing connections via port 27017 from anywhere and anyone without any form of authentication and grants full admin access (Create, Read, Update and Delete records). But also allows replication to other remote servers and shell (admin) access to the server which is a security risk.”

Wat volgt is een serie screenshots van directories op je server, enkele scenario’s met wat criminelen met de database zouden kunnen doen en hoe je het lek kunt dichten. De mail is ondertekend door Victor Gevers. Wat zou jij doen met deze mail?

a. Meteen onderzoeken wat er aan de hand is.
b. Doorsturen naar afdeling IT.
c. Antwoorden: WTF is dit?
d. Negeren. Zal wel spam zijn.

De meeste mensen doen d, sommigen b en dat is het dan wel. Zo niet Peter Beverloo van Las Venturas Playground, die dit bericht ontvangt op 26 mei 2016. Las Venturas Playground is een online community rondom het spel *Grand Theft Auto, San Andreas* met maar liefst 117.000 leden. Die zijn

uiteraard het beschermen waard. Bovendien is Peter in het dagelijks leven software engineer bij Google, dus hij weet wel hoe om te gaan met security issues. Hij gaat meteen onderzoeken wat er aan de hand is.

Wat blijkt? Inderdaad, op de server staat een Mongo-database gewoon open online. Gelukkig bevat die geen gegevens van gebruikers. Dat scheelt een melding naar de Autoriteit Persoonsgegevens. Volgens melder Victor zou de database door criminelen gebruikt kunnen worden om illegale content te hosten, malware te verspreiden, DDoSsen uit te voeren… Dat blijkt volgens de logfiles gelukkig nog niet het geval. Maar het had dus wel gekund en dan had het bedrijf van Peter Beverloo toch wel een groot probleem gehad.

Hoe heeft dit kunnen gebeuren? Als ik Beverloo hierover mail, schrijft hij: “De groei van de community naar meer dan 117k gebruikers stond absoluut niet in de planning; het begon als een server voor een klein groepje vrienden. Hierdoor hebben we, met name op het gebied van security, zeker de nodige groeipijnen meegemaakt. (Gelukkig niets met verlies en/of uitgave van persoonsgegevens.) Eén van de consequenties hiervan is dat de server beheerd werd door vier mensen die af en toe ook voor eigen redenen software installeerden. MongoDB is hier een voorbeeld van: iemand wilde er meer over leren, heeft het een week of twee gebruikt en heeft er daarna niet meer aan gedacht.”

Totdat de database dus opdook in een van de scans van Victor Gevers, alias @0xDUDE. Dergelijke slecht geconfigureerde Mongodatabases zijn volgens hem op dat moment verantwoordelijk voor 72% van zijn meldingen over potentiële datalekken. MongoDB is open source en gratis, en wordt veel gebruikt, maar heeft blijkbaar nogal wat kwetsbare standaardinstellingen. Zoals het standaard openzetten van poort 27017 en automatisch admin-rechten toekennen aan elke bezoeker. Eind 2015 komt er een update uit voor veiligere standaardinstellingen, maar die is niet compatible met de oudere versies. Veel organisaties blijven daarom de oude versie gebruiken. Hun cloudproviders gaan daarin mee en leveren nog steeds de oude kwetsbare versie, wat zorgt voor een constante stroom van nieuwe datalekken.

Als ik Victor spreek, demonstreert hij hoe hij te werk gaat. Hij maakt gebruik van wat hij noemt ‘Open Source Intelligence’ (OSINT), oftewel onderzoek naar kwetsbaarheden dat al door anderen is gedaan en gewoon online staat. Zoals Zmap, een tool van Michigan University waar je een scan kunt uitvoeren op alle beschikbare websites die IPv4 gebruiken. Dan kun je bijvoorbeeld vragen welke diensten daar worden aangeboden. Daar selecteert hij sites die MongoDB draaien. Vervolgens laat hij er een Nmap (‘network map’) scanner op los waarmee hij opdrachten kan sturen naar de beruchte poort 27017. Krijgt hij de reactie: “It looks like you are trying to access MongoDB over HTTP on the native driver port”, dan weet hij dat hij beet heeft. Met de opdrachten ‘db.serverStatus();’ ziet hij welke versies er draaien en met ‘show dbs’ welke databases. Vervolgens ziet hij wat voor soort informatie erin staat met de opdrachten ‘use [dbname]’ en ‘show collections’. Tot slot is van belang of de database ook wel gebruikt wordt. Dat ziet hij door er ‘show log global’ naartoe te sturen.

Dat is genoeg om te weten of hier sprake is van een mogelijk lek. Hij hoeft niet te weten wat er in de database staat. Dat mag ook niet, volgens zijn ethische code als helpende hacker. Omdat deze informatie vrij opvraagbaar is, hackt hij niet in de strikte zin van het woord. Hij kijkt niet welke informatie er staat, alleen maar dat er informatie staat.

Zo komt hij dus op een dag terecht in de database van Las Venturas Playground. En nog in die van vele honderdduizenden andere sites. Die kan hij niet allemaal melden, dus filtert hij op de gevallen waar sprake lijkt te zijn van misbruik en meldt hij die als bulk bij de Internet Service Providers waar de sites gehost worden. In dit geval niet, want hij kan zien dat de site heel veel gebruikers heeft en dat dit een gaming platform is. Dat maakt het naar zijn inschatting waarschijnlijker dat er mensen achter zitten die zijn melding wel op waarde kunnen schatten.

Inderdaad, de database wordt binnen een dag offline gehaald. Op 1 juni post @beverloo op Twitter: “Received a ‘responsible disclosure’ from @0xDUDE about a security vulnerability on one of my servers—that’s super awesome, thank you! :-)”. Hij stuurt ook een mail naar Victor, met “Thank you *so much* for sharing this issue in a friendly manner with us!”, uitleg over wat er aan de hand was en de vraag of hij nog iets kan overmaken aan een goed doel. Dit lijkt een kleinigheid, maar de meeste

meldingen van kwetsbaarheden worden stilletjes afgehandeld, vaak ook nog zonder enige reactie. In Nederland krijgt Victor meestal wel een positieve reactie, maar blijft dit onder de melder en ontvanger en tweet @0xDUDE er niet over. Dit keer verschijnt het bedankje wel online en daarom kan ik erover schrijven.

Victor zoekt online niet alleen naar MongoDB. Ook de beruchte kwetsbaarheid Heartbleed waart op dat moment nog rond over het internet. Dit is een kwetsbaarheid in de veelgebruikte versleutelingssoftware OpenSSL. Draai je hier een verouderde versie van, dan kan iedereen zich met je gelekte sleutel voordoen als jou of de ontvanger en zo jullie internetverkeer onderscheppen. Kwaadwillenden kunnen dan wachtwoorden afvangen, banktransacties overnemen of zelfs volledige beheerdersrechten krijgen over systemen. Als Victor wereldwijd zoekt naar eigenaren van websites waar het woord ‘bank’ in voorkomt, vindt hij al 852.612 systemen die mogelijk kwetsbaar zijn voor Heartbleed. Hier zitten ook vals-positieven bij, dus moet hij een bewerkelijke schifting maken om alleen de serieuze gevallen te vinden en die te melden.

Dit alles doet hij dus ongevraagd, onbetaald en vaak zonder enige reactie van de ontvanger van zijn meldingen, puur om te helpen het internet veiliger te maken. Victor is een van de centrale personen in dit boek. Mijn boek *Helpende hackers* sloot ik met hem af. De teller van het aantal afgehandelde meldingen stond toen op 4.000. In het jaar erna ging hij al snel over de 5.000 omdat hij heel 2016, alle 366 dagen 15 uur per dag lekken is gaan zoeken en melden. Een soort hacksabbatical. Inmiddels heeft zich een hele groep hackers rondom hem geformeerd die hetzelfde doen of hem op een andere manier helpen. Hierover meer in het slothoofdstuk.

Victor is zeker niet de enige die zo massaal het internet scant op kwetsbaarheden. We zijn in Nederland inmiddels flink aan het opschalen met het scannen en melden van kwetsbaarheden. Individuele lekken worden sneller gemeld en opgelost, zonder de media te bereiken. Het massaal scannen van hele IP-reeksen wordt steeds populairder. Echter, hoe benader je duizenden internetgebruikers met de boodschap dat ze lek zijn? En wat moet je doen als ze reageren? Of als ze juist niet reageren? Dit probleem

ondervond Remco Verhoef, die het hele internet scande op een ogenschijnlijk simpele code van vier tekens: '.git'.

Remco is net als velen in dit boek een IT'er die graag naast zijn werk projecten opzet om het internet veiliger te maken. Dat kan een online platform zijn om kennis te delen, een tool die door vrijwilligers verder wordt ontwikkeld of een project dat uitmondt in een goed lopend cybersecurity bedrijf. Uiteraard met wonderlijke namen, zoals: Ephorius, Red5, Myjour, Honeycast, Hackercafe, Dutchcoders en Kennisplatforms.nl. In 2017 richtte hij samen met andere IT'ers Dutchsec op en daar werkt hij nu nog steeds.

Het bijzondere project waar het hier om draait, begint in 2015 als Remco bij toeval ontdekt dat veel sites op een onverwacht makkelijke manier kwetsbaar blijken te zijn. Door '/.git/' achter een internetadres te typen, kom je in de broncode van de site. Dat vindt hij vreemd, want via die verborgen bronnen kun je veel te weten komen over de site. Feitelijk is hij niet aan het hacken, de bron is immers gewoon open, maar via deze open deur wordt het wel erg makkelijk de site helemaal over te nemen. Hij gaat op onderzoek uit om te kijken hoe vaak deze kwetsbaarheid voorkomt en vindt 15.000 sites van zeker niet de minste partijen…

Git is in 2005 ontwikkeld door Linus Torvalds, de man achter het besturingssysteem Linux. Vandaag de dag is het vooral bekend door het Github-platform van Microsoft. Het is een handig systeem waarmee je vanaf meerdere plekken aan software kunt werken. Elke verandering die in de broncode wordt aangebracht – een commit – krijgt een unieke identiteit die voortbouwt op de vorige, zodat de hele geschiedenis aan wijzigingen voor jou duidelijk is en je kunt kiezen welke wijzigen je wel of niet accepteert. Wikipedia meldt: "As a distributed revision control system it is aimed at speed, data integrity and support for distributed, non-linear workflows." Git is daarom ook handig als je samen aan een website werkt en wilt dat iedereen snel dezelfde versie heeft.

De software kent geen inlogprocedure. Die moet je er zelf voor zetten en dat blijkt dus niet iedereen te doen. Upload je dan de nieuwe versie van de site, dan kan iedereen die bekijken – inclusief de broncode – door simpelweg '/.git' achter de URL te typen. Verhoef ontdekt ook sites waar gewoonweg de gebruikersnaam en het wachtwoord in het

configuratiebestand staan. Daar kun je in door '/.git/config' achter de URL te zetten. En dan heb je meteen de rechten om de site aan te passen. Ook interessant is '/.git/logs', waarmee je kunt terugbladeren in de geschiedenis van de applicatie. Je kunt ook alles downloaden en op je gemak de code doorpluizen.

Verhoef informeert hier en daar of anderen deze kwetsbaarheid ook al eens zijn tegengekomen. De eerste reacties zijn vooral in de trant van: "Ja, dat gebeurt weleens, open deur". Het had voor hem weinig zin om de makers van de software in te lichten. Deze kwetsbaarheid is immers geen fout in de software, maar hoe de gebruikers het systeem configureren. Wil hij dit probleem oplossen, dan moet hij dus die eindgebruikers zien te bereiken.

Juni 2015 neemt Remco contact op met het Nationaal Cyber Security Center. Ik vraag Security Researcher Jeroen van der Ham hoe er destijds werd gereageerd: "We zagen dit als een ernstige kwetsbaarheid. Daarom hebben we actief met Remco Verhoef samengewerkt om een aantal partijen uit onze doelgroep te benaderen. Daarnaast hebben we regelmatig contact met hem gehad over het verder onderzoeken van deze kwetsbaarheid en het inlichten van andere partijen onder responsible disclosure. Aangezien het hier vooral om een configuratiefout gaat en niet om een kwetsbaarheid in een softwarepakket hebben wij hier geen beveiligingsadvies over uitgebracht. In onze beveiligingsrichtlijn voor webapplicaties wordt het instellen van de juiste toegangsrestricties behandeld."

Het NCSC geeft wat bekendheid aan de configuratiefout en benadert enkele eigenaren van Nederlandse sites. Maar meer dan dat kan het centrum niet doen. Intussen ziet Verhoef dat steeds meer webdevelopers git gaan gebruiken en vraagt hij zich af hoeveel sites wereldwijd hierdoor kwetsbaar zijn.

Begin september 2016 ontwikkelt hij daarom een tool die de /.gittruuk automatisch uitvoert en noemt die: ANAM, Automated Network Analysis en Mass. Die laat hij los op het internet en de teller loopt meteen op. De vraag is wel wat voor sites je dan vangt. Alleen verlaten hobbysites of ook echt belangrijke? Het aantal kwetsbare sites moet wel iets betekenen. Hij gaat daarom voor de miljoen meestbezochte sites. De adressen krijgt hij via

Alexa.com, een bedrijf van Amazon dat internetverkeer meet. Met zo'n omvangrijke steekproef kan hij dus wel uitspraken doen over het hele internet.

Op 26 september laat hij zijn ANAM een nacht lang alle miljoen URL's uitproberen. De scanner meldt de volgende ochtend dat 15.000 sites, met hier en daar wat onderliggende sites, git open hebben staan. Vervolgens mailt hij de eigenaren van de sites. Eerst handmatig en vervolgens geautomatiseerd. In de header staat 'Responsible Disclosure', gevolgd door deze boodschap:

Hi,

During our campaign to clean the internet from common vulnerabilities, we've encountered that <site> is vulnerable to information disclosure, by allowing public download of the .git repository. This allows everyone to download the source code of your website and application. You can read more about us and this campaign at http://internetsecure.today/campaign/sourcecode-access-through-public-available-git-repository/.

The URL https://<site>/.git/HEAD contains the repository configuration, as this is proof that it is possible as well to download the complete repository itself. See the attached files, the git config, head and commit log. Currently we are in progress to disclose our discoveries, and we're aiming to publish the article within two weeks. We are sending our findings to info, security and abuse e-mail addresses of the vulnerable domain. We are sending this e-mail in an automated way, and we are aware that in some cases this is expected behavior. If that is the case, you can ignore this message. We believe that this issue endangers your site, application and data and that we needed to inform you.

About InternetSecure.today: there are a lot of common vulnerabilities that are being exploited often. Our mission is to scan the internet and notify owners about the dangers of these vulnerabilities. You can read more about us at: https://internetsecure.today/.

Let me know if you've got any questions,

Remco Verhoef

remco@internetsecure.today
@remco_verhoef

In deze boodschap lezen we ook het dilemma bij een dergelijke omvangrijke onthulling van kwetsbaarheden. Een van de regels van responsible disclosure is dat je de kwetsbaarheid pas bekendmaakt als die gefixt is. Bij 15.000 sites zullen er echter altijd partijen zijn die niet reageren, terwijl je wel meer bekendheid wilt geven aan de kwetsbaarheid zodat anderen het ook kunnen oppakken. Remco bedenkt een tussenoplossing: van 27 september tot en met 21 oktober mailt hij alle sites en kondigt daarin alvast de datum van de onthulling aan: 31 oktober.

Wat begon als een hobbyproject groeit uit tot een mondiale reddingsactie. Dat kan Verhoef niet alleen. Bas Eikelenboom, met wie hij samen Dutchsec heeft opgericht, haakt aan als organisator en mobiliseert hulptroepen. Het Threat Intell Center van Ernst & Young is bereid de meldingen met telefoontjes op te volgen. Niet alleen met de eigenaren van de websites, maar bijvoorbeeld ook met Computer Emergency Response Teams in verschillende landen. De IT-consultants van Considerati haken aan als juridisch adviseurs, want het zou immers kunnen gaan om privacygevoelige gegevens. De website internetsecure.today gaat in de lucht zodat iedereen de voortgang kan volgen en Eikelenboom vraagt mij en enkele andere journalisten te schrijven over deze bijzondere zaak.

De oogst na twee maanden open deuren intrappen: 300 tot 400 positieve reacties, met de erkenning dat de ontvangers kwetsbaar waren voor het probleem en ze het inmiddels hebben opgelost. Hieronder ook grote namen als Akzo Nobel. Drie andere bedrijven sturen Remco als bedankje een T-shirt: Vice, Sony en Knewton. Een melding naar MIT gaat via bug-bountyplatform HackerOne, waardoor ze er ook nog een beloning voor krijgen van 150 dollar. Een bedrijf, dat niet bij naam genoemd wil worden, heeft zelfs becijferd dat ze dankzij de melding een schade hebben voorkomen van acht ton.

Is dit een goede score voor een dergelijk grote online veegactie? Dat is lastig te zeggen. Veel organisaties zullen namelijk de configuratiefout verhelpen zonder daar al te veel ruchtbaarheid aan te geven. Remco blijft

daarom periodiek scannen met ANAM en ziet dat nog duizenden sites kwetsbaar zijn omdat er geen enkele actie is ondernomen. Hieronder vallen bijvoorbeeld websites van politieke partijen, stichtingen, multinationals en heel veel kleinere sites. Ook een grote internationale hulporganisatie blijkt nog lange tijd kwetsbaar.

De site die hier destijds voor werd gelanceerd, internetsecure.today, staat anno 2020 nog steeds online. De teller met ‘numbers resulting from our work’ staat nog op dezelfde score als toen: 1,1 miljoen sites gescand, 15.943 disclosures en drie T-shirts ontvangen. Dat zien we wel vaker bij hackersprojecten. Iemand vindt iets kleins dat veel impact blijkt te hebben, iedereen duikt erop om het op te lossen en voor je het weet zijn ze alweer bezig met het volgende. Uiteindelijk is het Remco Verhoef ook niet te doen om in zijn eentje het hele internet te redden. Hij vindt het vooral interessant deze tool te ontwikkelen, die te delen met andere onderzoekers en zo samen het internet een stukje veiliger te maken. Dat gebeurt, ironisch genoeg, open source op Github… Maar, we kunnen ervan uitgaan dat de configuratie daar wel goed is ingesteld.

Straks meer heldenverhalen van helpende hackers die belangeloos kwetsbaarheden zoeken, vinden en melden. Maar eerst de vraag: mag dat allemaal zo maar? Of in juridische termen: is hier sprake van computervredebreuk, oftewel, volgens het Wetboek van Strafrecht artikel 138ab: “het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk, door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid”. Soms wel, maar meestal niet. We hebben momenteel in Nederland een cultuur gecreëerd waarin het goed toeven is voor hackers die willen helpen. Daarvoor moest het natuurlijk wel eerst een paar keer flink fout gaan.

3. Beetje computervredebreuk moet kunnen

Dit hoofdstuk is een korte samenvatting van de ontstaansgeschiedenis van responsible disclosure in Nederland, oftewel hoe het verantwoord onthullen van digitale kwetsbaarheden eraan toegaat in ons digitale polderlandschap. Voor responsible disclosure bestaat inmiddels een goede richtlijn, die door veel organisaties wordt gebruikt om te voorkomen dat hackers te enthousiast lekken naar buiten brengen en iedereen optimaal kan profiteren van hun vrijwilligerswerk. Hackers voelen zich inmiddels meer dan ooit gevrijwaard van vervolging als ze een klein beetje computervredebreuk plegen om aan te tonen dat iets lek is. Hiervoor hebben we jurisprudentie, die voortkomt uit drie rechtszaken.

Voor de eerste zaak gaan we terug naar januari 2008. De onderzoekers van de Digital Security Group van de Radboud Universiteit, onder leiding van professor Bart Jacobs, zijn er op vernuftige manier achter gekomen hoe de Myfare Classic-chip versleuteling afhandelt. Deze chip zit in toegangs- en betaalsystemen, zoals de OV-chipkaart. Als je de kaart bij een lezer houdt, worden er codes uitgewisseld. De versleuteling vindt plaats door middel van het Crypto1-algoritme, dat tot dan toe geheim was. Studenten Roel Verdult en Gerhard de Koning-Gans hebben met een stapeltje kaarten en een leesapparaat net zo lang in- en uitgecheckt, tot ze erachter komen hoe het versleutelingsalgoritme werkt. Reverse engineering noemen we dat. Hiermee hebben ze een mooi onderzoek om af te studeren en een wetenschappelijk artikel te schrijven. Bovenal maken ze hiermee de digitale wereld veiliger door de makers en gebruikers van de chipkaart te informeren over de gevonden kwetsbaarheid.

Bart Jacobs realiseert zich dat ze de vondst niet zomaar kunnen publiceren, want de chipkaart wordt op dat moment wereldwijd veel gebruikt. Ze zullen dan niet alleen ov-fraudeurs helpen, maar ook criminelen die toegangspasjes van gebouwen willen namaken. Hij licht daarom eerst het ministerie van Binnenlandse Zaken in en krijgt vervolgens het Nationale Bureau voor Verbindingsbeveiliging van de AIVD op bezoek. Deze rijkscryptografen zijn onder de indruk van de bevindingen en bevestigen dat de chip te kraken is. De dag erna worden de overige betrokkenen geïnformeerd: chipfabrikant NXP, Translink Systems die de ov-transacties afhandelt, het ministerie van Verkeer en Waterstaat en de rest van de Rijksoverheid waar de chip wordt gebruikt in toegangspassen.

NXP lijkt aanvankelijk nog dankbaar voor het aantonen van kwetsbaarheden in hun product. Hun directeur komt Jacobs zelfs een fles wijn brengen als bedankje. Maar als hij verneemt dat de onderzoekers hun vondsten willen publiceren, start hij een rechtszaak. Niet alleen tegen de Radboud Universiteit, maar ook tegen Bart persoonlijk. De inzet: een dwangsom van een miljoen euro als de onderzoekers overgaan tot publicatie.

De zaak komt voor de rechter op 10 juli 2008. De advocaat van NXP heeft een hele reeks wetsartikelen in stelling gebracht over diefstal van intellectueel eigendom en bedrijfsgeheimen en schade die aan het bedrijf en hun klanten zal worden toegebracht. Meest relevant hier is het bekende artikel 138a over computervredebreuk. De onderzoekers hebben zich immers opzettelijk met een valse sleutel toegang verschaft tot het geautomatiseerde werk op de kaart.

De advocaat van de Radboud Universiteit brengt hier tegenin dat eventuele schade door onveiligheid in de chip te wijten is aan nalatigheid van de maker en niet de opzet van de ontdekkers van het lek. De onderzoekers handelen ook niet uit financieel gewin, maar in het maatschappelijk belang van goede beveiliging. Hij doet daarom een beroep op de ‘Vrijheid van meningsuiting’, artikel 10, lid 2 van het Europese Verdrag voor de Rechten van de Mens. Bovendien hebben de onderzoekers het lek volgens de verdediging op verantwoorde wijze onthuld volgens het principe van responsible disclosure, door eerst de bevindingen te delen met de partijen die iets kunnen doen aan het lek.

Op die dag valt dus voor het eerst het woord ‘responsible disclosure’ in een Nederlandse rechtbank. De rechter neemt het woord over in zijn uitspraak, want hij gaat volledig mee in de redenering van de advocaat van de Radboud Universiteit. Jacobs en consorten worden vrijgesproken en NXP moet de proceskosten betalen. Hiermee zijn niet alleen de Radboudonderzoekers, maar alle helpende hackers in Nederland enorm geholpen. Want, zoals dat werkt in het Nederlandse rechtssysteem, hebben we hiermee belangrijke jurisprudentie. Iedereen die hackt vanuit maatschappelijke motieven en de bevindingen verantwoord onthuld, maar toch in het beklaagdenbankje moet verschijnen, kan verwijzen naar deze zaak. Hoever je mag gaan met hacken en wanneer de onthulling nog verantwoord is, zal blijken uit twee andere zaken die hierop volgen en waarin de hackers wel worden veroordeeld.

Op 19 april 2012 logt politicus en journalist Henk Krol in op het Cyberlab van ‘Diagnostiek voor U’. Hij heeft van een bekende een code van vijf cijfers gekregen en dat is alles wat hij nodig heeft om vervolgens duizenden dossiers door te bladeren. Hij ziet uitslagen van bloed- en urinetests die aantonen of mensen ziek zijn, drugs gebruiken of seksueel overdraagbare aandoeningen hebben. Eerst zoekt hij op zijn eigen naam en vervolgens op namen van een paar bekenden. Niets. Als bewijs voor zijn vondst downloadt hij tien dossiers van enkele willekeurige mensen, print ze uit en streept hun namen door. Dan belt hij Diagnostiek voor U.

De receptioniste aan de lijn vraagt hem de volgende dag terug te bellen, omdat degene die over dit soort zaken gaat momenteel druk is. Daar neemt Henk geen genoegen mee, dus belt hij met Omroep Brabant. Die stuurt meteen een journalist en cameraman. Henk logt nogmaals in, nu onder het oog van de camera en betoogt dat het schandalig is dat dergelijke gevoelige gegevens zo slecht beveiligd zijn. Diagnostiek voor U is daar uiteraard niet blij mee, haalt de site offline en start een rechtszaak. De inzet: een schadevergoeding van 85.329 euro voor Diagnostiek voor U en 1.000 euro voor elke bekeken patiënt.

De zaak komt voor de rechter op 1 februari 2013. Henks advocaat verdedigt hem door te stellen dat zijn cliënt handelde vanuit maatschappelijk belang en net als de Radboudonderzoekers gewoon wil

aantonen dat een belangrijk systeem niet goed beveiligd is. Eerst volgt er een hele discussie over of het lek te wijten is aan degene die slordig is omgegaan met zijn inlogcodes, of dat vijf cijfers geen passende beveiliging is voor dergelijk gevoelig materiaal – een discussie die nog lang zal voortwoeden in de media. Daarna stelt de rechter dat er wel degelijk grenzen zijn aan hoever je mag gaan met hacken en onthullen. Hij hanteert daarbij twee bekende juridische principes: proportionaliteit en subsidiariteit.

Proportionaliteit betekent: staat de inzet van het middel in verhouding tot het te bereiken doel? In dit geval is dat dus hacken en lekken om aan te tonen dat gevoelige gegevens onvoldoende beveiligd zijn opgeslagen. Henk schendt in wezen de privacy van enkele patiënten een beetje, om grootschaliger privacyschending van alle patiënten te voorkomen. De rechter oordeelt dat één keer inloggen en enkele gegevens downloaden als bewijs nog wel proportioneel is, maar nogmaals inloggen en gegevens downloaden, nota bene met meekijkende journalisten, is dat niet.

Subsidiariteit betekent: je doel bereiken met het minst ingrijpende middel. Dat Henk zelf wil vaststellen dat het hier gaat om gevoelige patiëntgegevens, inlogt en enkele dossiers downloadt, daar wil de rechter nog wel in meegaan. Het is ook netjes van Henk dat hij de namen van de patiënten op de prints onherkenbaar heeft gemaakt en meteen het ziekenhuis heeft gebeld om zijn bevindingen te melden. Dat hij echter de gevonden kwetsbaarheid direct in de media heeft gebracht, nog voor Diagnostiek voor U maatregelen kon nemen, is volgens de rechter een te zwaar middel om het maatschappelijk doel te bereiken. Hiermee brengt de melder immers juist de patiëntgegevens in gevaar.

Henk Krol wordt uiteindelijk veroordeeld voor computervredebreuk en moet de proceskosten betalen. De boete wordt echter teruggebracht tot 750 euro. Het ziekenhuis heeft immers zelf ook aandeel in de onveiligheid van dit gevoelige systeem.

De derde zaak loopt dan al drie maanden, maar hierbij komt de rechter pas twee jaar later tot een eindoordeel omdat deze een stuk ingewikkelder is: het Groene Hart Ziekenhuis versus Jordy J., alias Bonnie van het Nederlandse Genootschap van Hackende Huisvrouwen. In die periode heb ik alle betrokkenen uitgebreid kunnen spreken en worden de drie criteria

maatschappelijk belang, subsidiariteit en proportionaliteit nog verder verfijnd voor reponsible disclosure.

Jordy scant eind september 2012 het netwerk van het Groene Hart Ziekenhuis. Hij is security onderzoeker, komt zelf weleens in het ziekenhuis en wil weten of de patiëntgegevens veilig worden beheerd. Hij treft een back-upserver, met een kwetsbaarheid die dan al een halfjaar algemeen bekend is voor dit type server. Hij stuurt een programma naar de server waardoor hij er direct mee kan communiceren. De kwetsbaarheid bestaat eruit dat als hij te veel code naar de server stuurt, die niet wordt geblokkeerd, maar ergens in de database wordt opgeslagen. Vervolgens crasht de server, start opnieuw op, voert de ingevoerde code uit en kan Jordy erin. Deze hacktechniek staat bekend als een ‘bufferoverflow’. Hij ziet nu ook het wachtwoord: ‘groen2000’. Hiermee kan hij enkele bestanden downloaden: het zijn patiëntgegevens.

Hij meldt zijn bevindingen aan journalist Brenno de Winter, die in die periode wel vaker lekken bekendmaakt. Brenno belt in de ochtend van zondag 1 oktober het ziekenhuis en krijgt het Hoofd Communicatie aan de lijn. Zij ziet direct de ernst van de zaak in en zegt die dag nog maatregelen te nemen en naar buiten te treden. Om andere journalisten voor te zijn, zegt Brenno toe dat zijn stuk om 15.00 uur op nu.nl verschijnt. Het ziekenhuis activeert onmiddellijk het Crisis Management Team (CMT).

Het CMT komt die middag samen en vraagt bij de afdeling IT de logfiles op. Daaruit blijkt dat er 7,5 GB aan patiëntengegevens is gelekt. Het team besluit het hele ziekenhuis af te sluiten van het internet en zeer precies en feitelijk naar buiten te brengen wat er is gebeurd. Ze sturen een melding naar de Autoriteit Persoonsgegevens. De patiënten van wie de data is gelekt, worden individueel geïnformeerd. Dit is, naar mijn mening, precies wat een CMT in zo’n situatie moet doen. Rest echter een belangrijke vraag: waar is al die data gebleven?

Het ziekenhuis wil in eerste instantie geen aangifte doen, maar doet dat op advies van de politie, justitie en het NCSC alsnog. Dan kan sporenonderzoek wellicht uitwijzen waar de data is gebleven. Brenno zal immers zijn bron niet vrijgeven, dat is zijn journalistieke code en hij heeft de hacker in zijn stuk verscholen achter het pseudoniem ‘Bonnie van het Genootschap van Hackende Huisvrouwen’. Bonnie is echter slordig

geweest in het wissen van haar sporen. In eerste instantie gebruikte ze nog een VPN-verbinding, maar toen die haperde, heeft ze de server via het gewone internet benaderd en daarmee haar IP-adres bekendgemaakt. Team High Tech Crime van de Nederlandse politie ontdekt zo dat Bonnie door het leven gaat als Jordy, pakt hem op en neemt al zijn computers in beslag voor onderzoek. Daarna volgt een lange rechtszaak.

Bij het ziekenhuis loopt inmiddels de schade flink op: eerst 300.000 euro voor securitybedrijven en juridische bijstand en vervolgens vijf miljoen euro om alle verouderde systemen te vervangen. Het ziekenhuis wil die drie ton in eerste instantie verhalen op de verdachte, maar daar gaat de rechter niet in mee. Verder aandringen heeft volgens de aanklager ook geen zin omdat er bij deze jonge hacker duidelijk niets te halen valt. De zaak lijkt vooral te draaien om genoegdoening voor het ziekenhuis en voor het OM om meer helderheid te krijgen over wat wel en niet mag bij hacken en melden. Wie bekend is met de zaak, weet dat er meer stond op Jordy's computer dan waar de politie naar zocht. Die andere zaak laat ik hier terzijde, maar het verklaart waarom de veroordeling meer tijd in beslag nam dan verwacht.

Op 3 december 2014 zitten we dus met z'n allen bij de rechtbank in Den Haag. Bij de behandeling van de feiten wordt gesproken over hack 1 en hack 2. De eerste betreft de hack die Jordy heeft bekend en waarvan de bestanden op zijn computer zijn aangetroffen: een spreadsheet met namen, adressen, woonplaatsen en telefoonnummers van 500.000 patiënten en twee afbeeldingen van röntgenscans. De tweede hack vond enkele dagen later plaats en daarbij was dus die grote hoeveelheid patiëntgegevens buitgemaakt.

De rechter vraagt hoe Jordy precies te werk is gegaan. Als hij vertelt over de software die hij heeft geïnstalleerd om met de server te communiceren, ontstaat er een interessante discussie tussen hem en de rechter over of dit malware is of niet. Verder blijkt dat hij niet een keer, maar meerdere keren heeft ingelogd op de server en daarbij niet alleen op zijn eigen naam heeft gezocht, maar ook op die van een bekende Nederlander. Hiermee schendt hij volgens de rechter de principes van proportionaliteit en subsidiariteit. Jordy ontkent dat hij de tweede hack heeft gepleegd en er blijkt geen hard bewijs voor te zijn. De Officier van Justitie

probeert dat wel aannemelijk te maken en eist een jaar gevangenisstraf wegens computervredebreuk. Uiteindelijk legt de rechter in haar uitspraak van 17 december Jordy 120 uur taakstraf op.

Deze drie zaken hebben het juridische schemergebied van responsible disclosure behoorlijk goed verlicht. Een beetje computervredebreuk mag, zolang je dat maar duidelijk doet om de digitale wereld voor anderen veiliger te maken. Om die onveiligheid aan te tonen, zal je op de een of andere manier het geautomatiseerd systeem moeten benaderen, bijvoorbeeld met een scan en, als je bewijs nodig hebt, ook enigszins moeten betreden. Je kunt zelfs zover gaan dat je enkele persoonsgegevens downloadt, liefst van jezelf. Toch lijkt het volgens het subsidiariteitsbeginsel beter als je gewoon wat screenshots maakt van de mappen met namen van documenten of, zoals Victor, alleen de titels van tabellen, zonder echt persoonsgegevens te downloaden. Dat is genoeg. Je hoeft als helpende hacker dan niet bang te zijn dat je direct vervolgd wordt. Verder kun je je bevindingen het best bij de organisatie zelf melden. Wordt er niet naar je geluisterd, dan kun je alsnog een journalist of het NCSC inschakelen. Maar zover komt het vandaag de dag meestal niet meer in Nederland, omdat we inmiddels goed beleid hebben voor responsible disclosure.

4. Overheid open voor hackers

Rondom deze drie rechtszaken speelde zich een uitgebreid maatschappelijk en politiek debat af. Voor mijn boek *Helpende hackers* heb ik honderden nieuwsberichten en Kamerstukken doorgenomen, die ik je hier zal besparen. Wat opvalt is dat de meeste Kamerleden net zoals de meeste mensen die voor het eerst worden geconfronteerd met een hack, niet begrijpen waarom iemand zou hacken om te helpen. Een veelgehoorde eerste reactie is: “Hacken is toch gewoon digitaal inbreken? Waarom zou je dat anders doen?”

Door de vele datalekken die op dat moment in de media verschenen en de toegenomen aandacht voor beveiliging, namen steeds meer Kamerleden het in het parlement op voor de helpende hackers. Ook het NCSC kreeg steeds vaker meldingen van hackers die via het net opgerichte centrum hun meldingen kwijt wilden. De toenmalige minister van Veiligheid en Justitie, Ivo Opstelten, werd meerdere malen gevraagd om een oplossing. Zijn standpunt was dat organisaties in eerste instantie zelf verantwoordelijk zijn voor hun beveiliging, niet de overheid. Als er gehackt wordt, dan volstaat het huidige juridisch kader. Het NCSC kwam daarom in januari 2013 met een typisch Nederlandse polderoplossing: een ‘Leidraad om te komen tot een praktijk voor responsible disclosure’.

Volgens deze leidraad begint alles 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 op meldingen 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 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 is gevonden 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 wel de voorkeur.

De organisatie en melder beslissen volgens de leidraad gezamenlijk wat een redelijke termijn is voor de onthulling en hoe ze dat doen. Voor kwetsbaarheden in software vindt het NCSC 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 melders staat vooral wat zij niet moeten 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 kunt, maak een screenshot van wat je ziet, log meteen uit en meld het alleen bij de eigenaar.

Het NCSC is in 2013 net een jaar oud en de opvolger van het GovCERT, het Governmental Computer Emergency Responce Team, oftewel de techneuten die de IT-systemen van de overheid moeten beschermen. Het jaarlijkse GovCERT symposium wordt opgeschaald naar een internationaal event: de One Conference. De eerste editie is op 28 januari 2013 en het lijkt de ambtenaren een mooie gelegenheid de ‘Leidraad Responsible Disclosure’ onder de aandacht te brengen. Ze zijn echter vergeten de hackers zelf uit te nodigen. Het maximum aantal inschrijvingen is al bereikt als er klachten komen uit hackerskringen. Snel wordt er een grotere locatie geregeld, maar het is al te laat. Hackers hebben een schaduwconferentie georganiseerd onder de naam Alt-S. Prominent op het programma: Henk Krol over zijn hack van Diagnostiek voor U.

Deze samenloop van omstandigheden is tekenend voor de moeizame relatie tussen hackers en de overheid in die tijd. De meeste hackers die ik

dan spreek, vinden de leidraad slapjes. Die geeft namelijk geen enkele garantie dat je als melder niet alsnog in een rechtszaak belandt met degenen bij wie je de meldingen doet. En ook als je er wel uitkomt met degene bij wie je meldt, kun je alsnog vervolgd worden door een overijverige Officier van Justitie van het Openbaar Ministerie. Het OM komt daarom zelf ook met een handreiking om duidelijk te maken wanneer hacken mag. Hun College van procureurs-generaal, oftewel de leiding van het OM, stuurt hierover op 18 maart een brief aan alle parkethoofden, met als onderwerp: ‘responsible disclosure (hoe te handelen bij ‘ethisch’ hackers)’. Hierin worden de juridische begrippen ‘maatschappelijk belang’, ‘proportionaliteit’ en ‘subsidiariteit’ nog verder uitgewerkt. De zaak-Krol speelt precies tussen het uitkomen van de leidraad van het NCSC en deze brief, en is dan ook volgens enkele NCSC-medewerkers een testcase voor hun leidraad.

Het jaar erna worden de hackers wel uitgenodigd op de One Conference. De ambtenaren willen graag de relatie met hackers verbeteren en vragen mij om advies. Op dat moment heb ik in Den Haag een praatprogramma, Tek Tok Late Night, waar ik aan een talkshowtafel moeilijke zaken in IT leuk maak. Mijn voorstel: zet onze Tek-Toktafel op een centrale plek op de congreslocatie, waar ik iedereen die daar iets wil vertellen interview, ook de hackers. We nemen het op en zetten het zo snel mogelijk op YouTube, zonder eindredactie van NCSC zelf. Tot mijn verbazing gaan ze akkoord met dit plan.

Een van de meest bijzondere gasten aan tafel is hacker Rickey Gevers (geen familie van Victor) die ter plekke onthult dat hij degene is die in het verleden de Universiteit Groningen heeft gehackt. Hij bekent dit nota bene tegenover de Security Officer van die universiteit, die vervolgens uitermate mild oordeelt over de hack. De schade die de universiteit destijds had opgelopen, was begroot op 100.000,- euro, maar dat is volgens de Security Officer vooral achterstallig onderhoud. Hij heeft zelfs bewondering voor hoe Rickey te werk is gegaan. Ook de agenten die hem in het verleden hadden opgepakt voor het hacken van andere universiteiten vonden het knap hackwerk. Sterker nog: via hen leerde ik Rickey kennen. Inmiddels is hij een bekende securityonderzoeker en adviseur. Zo open kan de wereld van cybersecurity zijn.

Tijdens de One Conference van 2014 heb ik veel helpende hackers leren kennen die uiteindelijk in mijn boek zijn verschenen. Ook Victor Gevers, die na afloop van mijn studioavontuur een melding kwam doen over mijn website. Typisch Victor.

Twee jaar later gaan Victor en ik, op uitnodiging van het NCSC, met een hele delegatie naar Boedapest voor het Global Forum on Cyber Expertise. Het is 23 maart 2016. Nederland is voorzitter van de EU, doet het secretariaat voor het GFCE en is dus ruim vertegenwoordigd. Naast ons en andere Europeanen zijn er ook enkele Amerikanen en Aziaten. In totaal ongeveer honderd deelnemers, met name CERT's en CISO's van overheden en grote bedrijven.

De stemming is optimistisch. Responsible disclosure is immers een positieve boodschap: er zijn mensen die gratis helpen de beveiliging te verbeteren. Hans de Vries, directeur NCSC vertelt trots over onze leidraad, hoe die tot stand kwam met vele stakeholders en nu succesvol wordt toegepast. Steeds meer bedrijven en het grootste deel van de Nederlandse overheid heeft nu RD-beleid en een meldpunt. Kwetsbaarheden in systemen aantonen mag, zolang je maar niet te ver gaat, wat hij illustreert met de zaak Diagnostiek voor U versus Henk Krol.

Ik mag deze dag aan elkaar praten en krijg zelf ook wat tijd om een presentatie te geven over de Engelstalige versie van mijn boek *Helpful Hackers. How the Dutch do Responsible Disclosure*. Ik laat zien hoe Nederlandse hackers met hun meldingen gratis en voor niets hebben geholpen banken, telecombedrijven, uitgevers, onlinewinkels en gemalen veiliger te maken. Net als het boek beëindig ik de presentatie met het bijzondere verhaal over Victor Gevers, bekend als 0xDUDE, en hoe hij gedurende een jaar elke dag 15 uur besteedt aan responsible disclosure. Na mij volgt een reeks netjes-geklede vertegenwoordigers met diplomatiek gewogen woorden die er vooral op neerkomen dat we moeten samenwerken om het internet veiliger te maken. In de pauze staan ze allemaal druk handen te schudden en kaartjes uit te wisselen. Victor niet, want hij staat dan al op het podium om zijn slides nog op het laatste moment te updaten. Hij heeft uiteraard geen pak en das aan, maar gewoon een zwarte spijkerbroek en een zwart hackers T-shirt.

Als alle vertegenwoordigers weer netjes zitten, geeft Victor een korte introductie over responsible disclosure en duikt hij meteen in wat hij ter plekke heeft gevonden. Zoals het betaalsysteem van het hotel waar iedereen die nacht heeft overnacht. Nee, hij heeft het niet gehackt, hij kon er gewoon in en heeft ook zeker niet gekeken wat iedereen de avond ervoor heeft uitgevreten – al zie ik toch wat delegatieleden inmiddels enigszins zenuwachtig om zich heen kijken. Een andere database die hij in de buurt vond is in het Hongaars, dus laat hij een screenshot zien en vraagt aan hij het publiek: “Anyone knows what this is?” Na wat rumoer in de zaal blijkt het hier te gaan om een groot farmaceutisch bedrijf dat naast het hotel zit. Hier zou je dus kunnen zien wie wanneer welke medicatie heeft aangeschaft. Die ochtend was het me bij het ontbijt in het hotel al opgevallen dat, terwijl iedereen vooral aan het kennismaken was met elkaar, Victor alleen maar met zijn laptop bezig was. Dit was dus wat hij aan het doen was. De lekken zijn die ochtend nog gemeld en gedicht.

De zaal kijkt aandachtig toe hoe Victor de ene na de andere open bron tevoorschijn tovert, vele duizenden per land. De top tien van die ochtend wordt aangevoerd door de VS met 14.406 internetadressen waar je zo een zoekopdracht op hun database kunt loslaten. Iemand van het Roemeense CERT steekt zijn vinger op en vraagt voorzichtig: “So, you do brute forcing to enter?” Victor: “No, these are just open” en hij klikt door naar de volgende slide: “Also, in Europe alone, there are still 227,279 devices vulnerable for Heartbleed and 5,893 for Shellshock. If we, as CERT’s, take a month or so, we can clean all this up.” De bezoekers zijn er stil van. Niemand durft meer iets te vragen, maar na afloop van zijn presentatie, tijdens de lunchpauze des te meer. Diverse CERT’s willen graag weten welke bronnen in hun land openstaan. Sommigen willen zelfs training krijgen van Victor en samen de kwetsbaarheden oplossen.

Terug in Nederland volgt twee maanden later een nog groter feest. Als voorzitter van de EU heeft Nederland cybersecurity hoog op de agenda staan en organiseert onze overheid een ‘EU high-level meeting on cybersecurity’ over ‘Enabling Partnerships for a Digitally Secure Future for the EU’. Die partnerships worden breed opgevat, want onder de genodigden zijn aardig wat hackers. Ze hebben er een mooie locatie voor gevonden: de

marinekazerne in de Amsterdamse binnenstad. Op het programma staat ook een panel met melders en ontvangers van kwetsbaarheden en ik word gevraagd het te leiden. Ze noemen het een ‘coordinated vulnerability disclosure focus session’.

Pardon? Het NCSC wil graag af van het woord ‘responsible disclosure’, want de betekenis blijkt steeds meer te wringen. Het legt namelijk de verantwoordelijkheid vooral bij de hacker, die de onthulling doet, terwijl toch juist de ontvanger zijn verantwoordelijkheid moet nemen om het te fixen. Bovendien, wat is eigenlijk verantwoordelijk en wat niet? Dat begrijp ik volkomen, maar waarom coordinated vulnerability disclosure? Los van dat dit een lastige tongbreker is, gaat ‘CVD’, de afkorting van dit woord nodeloze verwarring opleveren met een andere belangrijke securityterm, namelijk CVE, de ‘common vulnerabilities and exposures’, oftewel de lijst van bekende kwetsbaarheden waar veel hackers op scannen…

Maar goed, aan de andere kant klopt de betekenis wel. Het gaat om het onthullen van kwetsbaarheden en de kunst zit hem in het coördineren ervan, zodat degene die het kunnen verhelpen het eerder weten dan degenen die het willen misbruiken. Informeel krijg ik te horen dat een hoge ambtenaar daar veel waarde aan hecht. Bovendien loopt er al een aanvraag om dit als ISO-standaard aan te nemen. Dus doe maar CVD.

De sessie verloopt in een positieve stemming. Uberhacker Karsten Nohl van de Duitse Chaos Computer Club vertelt over een reeks kwetsbaarheden die hij heeft gevonden en alle ellende die hij over zich heen kreeg toen hij die op een verantwoorde wijze wilde onthullen. Dat is nu wel anders volgens hem, dankzij CVD. Ik bemerk zelfs wat nostalgie bij hem, naar de activistische dagen waarin hacken een soort anarchistisch protest was en het Chaos Computer Congress het podium was waar onthullingen werden gedaan. Na Karsten krijgen we drie CISO’s van grote bedrijven, die elk vertellen dat ze heel blij zijn met het vrijwilligerswerk van hackers en iedereen aanraden ook CVD-beleid te gaan voeren.

Op de laatste dag van dit congres over ‘partnerships for a digitally secure future’ komen de drie CISO’s, samen met vele anderen van andere grote Nederlandse bedrijven, op het podium om het ‘Coordinated Vulnerability Disclosure Manifesto’ te tekenen. We zien typisch Nederlandse bedrijven als NS, Eneco, Stedin, Gasunie, Schuberg Philis en

TNO. En grote Nederlandse multinationals als Tennet, Philips, Rabobank, ING, ABN AMRO, SNS-bank, KPN en Vodafone. Zelfs NXP, die van de rechtszaak tegen de Radboud Universiteit, staat erbij. Iedereen staat vrolijk te lachen en lijkt hiermee te zeggen: hackers welkom.

Het jaar erna, op de One Conference 2017, heb ik een keer geen optreden en kan ik rondlopen om te kijken wat er te doen is. Bij binnenkomst bij het World Forum word ik bijna omvergereden door twee heren met een kar vol computers. Het zijn Kas Clark van het NCSC en Karl Lovink van de Belastingdienst. “Dit is voor de OneCTF. Doe je ook mee?”, roept Karl. CTF staat voor Capture The Flag en is een hackerscompetitie. Er zijn vele vormen. Soms moet je elkaar hacken, maar meestal krijg je allemaal hetzelfde systeem om binnen te dringen. De vlag bestaat uit een stukje code. Ze hebben verschillende moeilijkheidsgraden met bijbehorende punten. Wie hem het eerste pakt, krijgt de meeste punten.

Ik schrijf weliswaar over hackers, begrijp enigszins wat ze doen, maar bak er zelf niks van. Ik bedank Karl daarom vriendelijk voor het aanbod, maar bedenk me dat ik er misschien wel een interessant stukje over kan schrijven. Dat mag volgens hem, zolang ik maar geen foto’s maak waarop hackers te herkennen zijn. Zijn collega’s blijken de challenges en software te hebben ontwikkeld. Ik vraag hen hoe de teams worden gevormd. “We hebben twintig teams van elk vier deelnemers. Ze weten vooraf niet met wie ze gaan samenwerken. Wij delen ze in, zodat we een mooie mix van skill levels hebben en iedereen van elkaar kan leren.”

We arriveren in een donkere achterafzaal. De kar vol computers blijkt slechts een deel te zijn van het digitale pandemonium dat hier terplekke wordt opgebouwd. Ik zie rijen laptops, verbonden met netwerkkabels die voorin de zaal samenkomen in een soort regieruimte van schermen, stapels apparatuur en mannen in zwarte shirts. Achter de regietafel staan medewerkers van het Security Operations Center van de Belastingdienst. Zij blijken de hardware te hebben geleverd, inclusief twintig laptops voor deelnemers die er geen bij zich hebben. Karl licht toe: “Het zijn buiten gebruik gestelde laptops, maar uiteraard wel met Kali Linux erop. Ze kunnen standaardtechnieken gebruiken als strings, Wireshark en grep, geen speciale tooling of zo.”

Elk van de mannen heeft op de rug een code van 32 tekens – net als de vlaggen die gevangen moeten worden. Vlak voor de grote tafel zie ik een klein mysterieus kastje, met een printplaatje erop en eronder een oude monitor met ruis. Is het een target of gewoon nerdy aankleding? Hoe dan ook, voor deze ambtenaren is dit evenement een mooie gelegenheid om te laten zien dat zij security niet alleen serieus nemen, maar ook in zijn voor nerdy fun. En wie weet, wil een van de deelnemers hierna wel bij hen komen werken.

De zaal stroomt vol. Ik tel 72 deelnemers: 64 mannen en 8 vrouwen. Ik zie ook bekenden voorbijkomen: van andere cybersecurity congressen, BNH'ers (Bekende Nederlandse Hackers van tv) en uit mijn boek *Helpende hackers*. Aangekomen bij hun tafels, stellen de deelnemers zich aan elkaar voor. Eerste opdracht: bedenk een naam voor je team, die begint met de letter van je tafel. Tafel A noemt zich 'ateam'. De hackerscode schrijft voor dat je hackers niet bij naam noemt, zonder uitdrukkelijk toestemming gekregen te hebben, maar een van de deelnemer is zo bijzonder dat ik een uitzondering maak: oud-politicus Ad Melkert. De klok start. Op het grote scherm verschijnen de 'Game rulez and hints':

- *If you solve a challenge, you earn points. Difficult challenges are worth more points.*
- *Piece of advice: if you're not familiar with CTF challenges, start with the easy ones.*
- *The flag is in the format OneCTF[example-flag], once you find this flag you have solved that challenge.*
- *Team with the most points wins. In case of a tie, the first team to score the most points wins.*
- *Hints may be released during the game. If so, they will be announced.*
- *No denial of service or performance-hogging attacks.*
- *Do not attack other teams.*
- *Do not change anything in the CTF infrastructure.*
- *No brute force attacks necessary: you won't have to crack any passwords or brute force any directories.*
- *No mapping on the game servers, all the relevant ports are provided to you.*

- *The RECON challenges involve external/public websites. Do NOT attack these sites!*
- *Violations are punished.*

Dan volgt de opdracht: “We have received some intelligence reports regarding a hacktivist group called the Cyber Resistance Liberation Front. They want to destroy the internet by hacking IoT-devices. You are a team of experts assembled from across the world to prevent them. The attack will happen in 2 hours and you have to stop them!” De teams krijgen een wachtwoord en een URL. Onderaan de slide staat: “Yes, we know it is a self-signed certificate. We ran out of budget :(”

We kunnen beginnen. De klok start: slechts twee uur te gaan. Iedereen duikt in zijn of haar laptop. Ik zie sommigen googelen op ‘Admin’ en ‘Log in’. Anderen typen van alles achter URL’s, op zoek naar verborgen directory’s. Uit de speakers klinkt een happyhardcoreversie van ‘Knocking on Heavens Door’. Sommigen spreken me aan: “Hee, Chris, heb je nog een verlengsnoer voor me?” Of: “Is dit de directory?” Dan realiseer ik me dat ik ook een zwart T-shirt aan heb en het lijkt of ik van de organisatie ben. Ik neem daarom plaats onder het grote scherm aan de andere kant van de zaal tussen team ‘Sharp’ en ‘Teem Teeeeet’ en kijk wat in het rond. Eerlijk gezegd heb ik geen flauw idee wat ik hier kan verwachten.

Gelukkig word ik snel vergezeld door Pieter Jansen, een ervaren CTF’er die vandaag niet meespeelt en even een praatje komt maken. “Ziet er goed uit. Enkele van de grote jongens doen ook mee. Er zijn zelfs een paar Eindbazen.” Dit is de naam van het roemruchte team dat veel internationale CTF’s won, zoals we volgens hem kunnen zien op CTFtime.org. Pieter was een van hen, dus ik vraag: “We doen het goed, hè? De jaarlijkse Cyberlympics worden steevast gewonnen door Nederland, toch?” Pieter: “Ja, Hack.ERS al vijf jaar eerste, gevolgd door veelal andere Nederlandse teams.”

Volgens hem is dat historisch zo gegroeid. Pieter: “In de jaren ’80 waren we al bezig met telefoonhacking. Vervolgens waren we het eerste land buiten de VS met internet. Het Amsterdamse internetcafé Freeworld was toen de plek van waaruit we de hele wereld hackten. Toen de Cyberlympics begonnen, waren wij er klaar voor. Maar ja, veel van die gasten van toen

zijn nu vader geworden en dan zie je ze wat minder bij de internationale events. Nu is Polen heel erg in opkomst."

Op het grote scherm begint het scorebord te ratelen. Team Quantum Crypto neemt de leiding, nauw gevolgd door Teem Teeeeet. Het ateam met Ad Melkert staat verrassend derde. Ik zie de oude partijleider wat onwennig naar zijn scherm staren en druk aantekeningen maken in een schriftje. Naast hem zit iemand onafgebroken in zijn oor te fluisteren. Hun derde plaats wordt echter overgenomen door team Noname, waarvan ik er enkelen herken als winnaars van het hack event Game of Toons. Zij hadden 'The Most Dangerous Hack'. Bij Teem Teeeeet zitten er ook twee. Hun team had toen de prijs voor 'The Weirdest Hack' gewonnen. Een van hen kijkt argwanend naar de overkant, waar de leden van team Quantum Crypto opvallend stil naar hun scherm zitten te staren. Hij zegt: "Die gasten houden iets achter, ik voel het."

Dat klopt. Een van de Quantumjongens gaat ineens rechtop zitten en smoort verkrampt zijn gejuich: "Yes!". Het is een van de Eindbazen. Op het scorebord schiet zijn team plots met 400 punten omhoog. Hij heeft de challenge 'Ancient Protocols' opgelost. Ik loop naar de regietafel om te informeren wat er is gebeurd. Karl wijst me op het mysterieuze doosje vooraan. Een van de begeleiders fluistert samenzwerend: "Ze hadden deze challenge ook kunnen oplossen als ze de aarddraad hadden aangesloten. Maar ja, wie komt nou op dat idee."

De verleiding is groot deze onthulling te delen, want als ik terug wandel tussen de laptops door hoor ik een bekende directeur van een cybersecurity bedrijf wanhopig uitslaan: "Ik heb een enorme database gedownload en kan er niks mee!" Een van de BNH'ers zit met hangende schouders. Zijn team staat helemaal onderaan. Maar, ze krijgen hulp. Iemand van het NCSC gaat langs de laagst scorende teams met adviezen. "Het moet wel leuk blijven", verzekert hij me. Het scorebord meldt: "Hints just been added." Een vrouw van de politie zwaait vrolijk vanachter haar laptop naar me en roept: "Dit is echt heel leuk, ook al snap ik er niks van". Gelukkig, ik ben niet de enige…

Teem Teeeeet stoomt ondertussen met het nodige kabaal door naar een score van 1.286 punten. Nu staan zij op nummer 1. Met nog maar een kwartier te gaan! De spanning neemt toe en de dj blaast nog wat vette

hiphop uit de speakers. Ook team Quantum Crypto haalt de 1.286 punten. Als we nog maar vijf minuten te gaan hebben, start een aftellende klok en klinkt het onheilspellende nummer ‘Tubular Bells’ van Mike Oldfield. De score blijft gelijk. Krijgen we een gelijkspel?

NCSC-directeur Hans de Vries is inmiddels gearriveerd en staat klaar met de prijzen: voor elk teamlid een NetAid Kit en uiteraard een T-shirt. Ik vraag hem waarom NCSC dit organiseert. “Dit is een manier om van elkaar te leren. De ervaren hackers zetten de beginnelingen aan het werk om eenvoudige challenges van vijftig punten op te lossen, terwijl ze zelf beziggaan met een challenge van een paar honderd.” Maar wat nu als het gelijkspel blijft? Dan wint het team dat als eerste die score heeft gehaald. Hans informeert welk team dat is.

Teem Teeeeet dus. Een van de leden vertelt me: “Leek ons zo gaaf om Hans heel hard ‘tiet’ te laten roepen, vandaar die naam.” Nu moeten ze met hem op de foto, wat ze zichtbaar minder leuk vinden. De BNH’ers zouden daar minder moeite mee hebben gehad, maar lijken nu vooral het slagveld zo snel mogelijk te willen verlaten. Een van de tv-sterren, die zesde werd, vertelt teleurgesteld: “Ik was eerst vooral bezig mijn teamleden aan het werk te zetten. Op een gegeven moment ben ik maar voor mezelf begonnen, maar ja, toen was het alweer bijna voorbij.”

Terwijl de zaal leegloopt, geeft de eigenaar van het doosje ‘Ancient Protocols’ nog een korte uitleg. Iets met voltageniveaus die je online kon manipuleren om een code te injecteren. Hij raakt een van de contactpunten op het printplaatje aan met de aarddraad. Op de oude monitor verschijnt: “ONECTF [01101001]”. Zo kan het dus ook. Je moet er maar net op komen.

Crypto draait simpelweg op geheimen, toch is informatiebeveiliging juist een heel open wereld. Op bijeenkomsten als deze zie je jonge hackers, ervaren ambtenaren, de top van bedrijven en justitie vriendschappelijk met elkaar omgaan. Waarom? Omdat de kennis in cybersecurity zo snel verandert, kun je je niet veroorloven je af te sluiten. Het is geven en nemen. En: het is leuk.

Weer een jaar later, 2018, is het tijd voor een update van de richtlijn. ‘Coordinated Vulnerability Disclosure’ is inmiddels opgenomen in de ISO-

standaarden als ISO 29147 en ISO 30111, dus dat wordt ook de titel van de nieuwe richtlijn die verschijnt op 2 oktober 2018. De feitelijke inhoud verschilt niet heel veel van de versie uit 2013, maar de manier waarop dat wordt gebracht des te meer. Geen to-do-lijstje, maar een uitgebreide beschrijving van wat hackers verwachten van je als ze je een melding sturen. Alles draait om samenwerking. Dus: krijg je een melding, doe geen aangifte en leg uit wat je doet met hun melding, want de hacker heeft immers geen zicht op je interne processen. Houd de hackers op de hoogte van de vorderingen en als alles gefikst is, zorg je voor een leuk presentje. Het NCSC biedt zich in deze leidraad ook aan als intermediair, voor als je er niet uitkomt. En als de gevonden kwetsbaarheid bij veel organisaties voorkomt, kan het centrum de melding ook doorzetten naar de rest van de security community.

Die community is ook duidelijk vertegenwoordigd in de nieuwe leidraad. Niet alleen in woord, maar vooral in beeld. De lopende tekst wordt afgewisseld met paginagrote portretten van bekende hackers: Rickey Gevers, Melanie Rieback, Mischa van Geelen, Edwin van Andel en Victor Gevers. Op de voor- en laatste pagina prijkt het portret van de nog jonge hacker Zawadi Done. Onder de portretten staat alleen hun naam, niet wat of wie ze zijn. Zelfs het woord ‘hacker’ komt niet voor in het stuk. Alleen op de laatste pagina, daar staat ‘Fotografie Tobias Groenland | hackershandshake.com.’

Dat zit zo. Vier jaar eerder had Tobias mij benaderd of ik wat hackers kende die wel voor de camera willen poseren. Hij had al eerder fotografische projecten gedaan waarin hij ingewikkelde technische onderwerpen op artistieke wijze in beeld bracht. Met deze nieuwe reeks wilde hij de hacker letterlijk een gezicht geven. Niet gewoon een gezellig portret of clichébeeld van iemand met hoody en laptop, nee, een foto van dichtbij, full in the face, op het moment dat ze in gedachten hun favoriete hacktechniek toepassen. Alleen hoe vind je hackers? Zo kwam hij bij mij. Ik adviseerde hem hackers niet te gaan mailen of bellen voor een afspraak, maar naar een event te gaan waar hackers rondlopen. Richt terplekke je studio in, dan probeer ik ze wel naar binnen te lokken.

Dat hebben we vier jaar lang gedaan, met als resultaat een reeks prachtige portretten. Het bleek best mee te vallen hoe bereid de hackers

waren om voor Tobias en zijn camera te poseren, terwijl hij zeker niet de makkelijkste is. Zo'n fotoshoot duurde meestal een uur, met allerlei houdingen, soorten licht, attributen en gedoe, maar de meeste hackers leken het wel leuk te vinden. Pas toen we klaar waren, kwam de onvermijdelijke vraag: wat gaan we hier eigenlijk mee doen? Een boek, een tentoonstelling, een site… allemaal leuk, maar wie wil daar nou voor betalen? Het NCSC natuurlijk! Als ze zo graag hackers in het zonnetje willen zetten, dan is een tentoonstelling een mooie manier.

In aanloop naar de One Conference 2018 greep ik daarom elke gelegenheid aan om bij NCSC'ers te peilen of ze wat voelden voor een fototentoonstelling op hun congres. Ze reageerden als typisch ambtenaren: leuk idee, maar ik ga daar niet over. Mijn ervaring met ambtenaren is dat je het beste iets voor elkaar krijgt als je zowel van onder naar boven, als van boven naar beneden werkt. Dan is er meestal wel iemand in het midden die de verantwoordelijkheid wil nemen en de rest meetrekt. Hoe dan ook, toen Tobias en ik een voorstel indienden bij het projectbureau dat het congres organiseerde, kregen we al binnen een week een akkoord. Al zijn materiaalkosten werden vergoed en ik mocht de begeleidende teksten schrijven. Leuk!

Op 1 oktober 2018, de dag voor de One Conference, betreden Tobias, ik, en twee helpers het prestigieuze World Forum in Den Haag. We hebben een toplocatie toegewezen gekregen: een prachtige grote witte marmeren zaal, midden in het congrescentrum, waar morgen duizenden bezoekers langkomen. Zelf zijn we momenteel niet zo chique. We lijken eerder een aannemersbedrijf, want als eerste komt uit ons busje een lading van 500 kilo steigerbuis om de portretten aan te bevestigen. Terwijl we met de lading zwarte staven langs de beveiligingspoortjes lopen die morgen pas geactiveerd worden, zeg ik tegen Tobias dat we zelf ook maar even een CVD moeten indienen. Want hoe kun je het beste een flinke hoeveelheid explosieven midden in een van de zwaarst beveiligde congressen van Nederland krijgen? Nou, zo dus.

Tobias kan er wel om lachen, maar is vooral bezorgd over de zestien portretten die niet beschadigd mogen worden. Na flink wat passen en meten hebben we eindelijk de stalen constructies staan. Dan trekt Tobias zijn witte

handschoenen aan om de grote foto's te onthullen. Als een goochelaar trekt hij stuk voor stuk de beschermende folie eraf en komt ons hackersleger tot leven. De finishing touch zijn de naambordjes met profielteksten van de zestien geselecteerde hackers: Nick Brands, Elger Jonker, Manon de Vries, Rickey Gevers, Mischa van Geelen, Melanie Rieback, Arnd Marijnissen, Stef van Dop, Zawadi Done, Tabitha Vogelaar, Jeroen van der Ham, Edwin van Andel, Wesley Neelen, Rik van Duijn, Oscar Koeroo en Victor Gevers.

De dag erna verschijnen we beiden netjes in pak. Patricia Zorko komt de tentoonstelling onthullen en knipt symbolisch een zwart-geel afzetlint met daarop 'cyber' door. Daarna reikt ze de eerste exemplaren van de kersverse 'Leidraad Coordinated Vulnerability Disclosure' uit. Niet aan een andere hoogwaardigheidsbekleder, maar aan de geportretteerde hackers waarvan de meesten live aanwezig zijn. Het is een prachtig schouwspel. Als de geportretteerden langs hun eigen afbeelding lopen, zie je bezoekers verwonderd kijken en wijzen op de foto's in de leidraad: dit zijn dus die hackers waar we het over hebben…

De foto's van Tobias komen later nog terug, maar voor nu is de belangrijkste conclusie dat responsible disclosure, pardon, coordinated vulnerability disclosure werkt in Nederland. Inmiddels hebben de meeste grote organisaties wel een pagina op de site waar hackers terechtkunnen met hun meldingen. Of ze hebben zelfs een heel programma lopen om hackers actief hun veiligheid te laten testen. Hacks verschijnen minder vaak in de media en worden nu discreet afgehandeld, met ludieke beloningen. Zo geeft de Nederlandsche Bank melders een namaakgoudstaaf, de Belastingdienst een plastic bokaal, de Rijksdienst Wegverkeer een nummerbord met HA-CK-ER en het NCSC uiteraard een T-shirt. Ik kreeg er ook een met de tekst: "I wrote a book on responsible disclosure and all I got was this lousy T-shirt". Dat boek is nog steeds te koop en, als je een beetje slim zoekt op internet, gratis te downloaden.

5. Waardevolle kennis vrij verkrijgbaar

Eerder maakte je kennis met Victor Gevers en Remco Verhoef, die geheel belangeloos het internet scannen op kwetsbaarheden en hopen dat er naar aanleiding van hun meldingen zoveel mogelijk wordt gefixt. Ze maken gebruik van online tools en bronnen die voor iedereen vrij verkrijgbaar zijn en stellen ook hun eigen vondsten gratis ter beschikking. Hackers delen kwetsbaarheden, zodat we daar samen sterker van worden. OSINT noemen we dat: Open Source Intelligence.

Elger Jonker is ook zo'n hacker. Hij heeft een andere benadering gekozen om gevonden kwetsbaarheden wereldkundig te maken: geen rauwe data in waarschuwende teksten, maar een mooie landkaart met kleurcodes. Elger is een hacker die naast zijn serieuze baan als pentester en securitytrainer de grote problemen in security op een leuke manier weet te brengen. Hij is vaak te zien op hackerevents met grappige demo's en ludieke acties. Zo heeft hij meegeholpen met het opzetten van hackerspaces als Awesome Space en Hack42, was hij betrokken bij de grote hackercampings HAR2009 en OHM2013 en was hij een van de leidende figuren achter de opvolger SHA2017.

De eerste keer dat ik Elger ontmoette, was tijdens een congres in 2016, met de titel 'In het hoofd van de hacker'. Ik leidde een paneldiscussie met bekenden uit de hackerscene: Victor Gevers, Rickey Gevers, Ronald Prins en dus Elger Jonker. Op die dag lanceerde hij zijn nieuwe initiatief: Faalkaart.nl. Elger: "Ik was de minst bekende hacker en wilde laten zien wat ik kon. Dus heb ik drie dagen van tevoren allemaal URL's gescand en met ranzige PHP-code aan elkaar gelijmd." Op het congres waren de reacties positief, ook van gemeenteambtenaren. En dat terwijl zij live op zijn Faalkaart konden zien hoe goed of slecht hun gemeentewebsite scoorde op online veiligheid. Op dat moment was duidelijk te zien dat de gemeente

Amsterdam rood kleurde en de lijst aanvoerde met slechtst beveiligde domeinen. Valkenswaard.nl was toen het meest veilig en kleurde groen. Vrij snel nadat de Faalkaart live ging, verbeterden de scores bij enkele gemeenten. Er werd blijkbaar geluisterd naar het ongevraagde securityadvies.

De scanner achter Faalkaart zoekt niet, zoals die van Victor en Remco, naar bepaalde kwetsbaarheden, maar checkt of een reeks internetstandaarden die veilig geacht worden wel of niet zijn ingesteld. Elger heeft namelijk in het verleden voor zijn werk dergelijke scanners ontwikkeld en maakte er zelf een die zoekt naar onveilige FTP, HTTP security headers en ontbrekende HTTP-versleuteling, oftewel sites met alleen http, zonder de ‘s’ van ‘Secure’. Hij past ook bestaande scanners toe, die iedereen kan gebruiken. Zoals de SSL Labs scanner die test op het inmiddels verouderde cryptografische protocol Secure Sockets Layer. Ga je naar ssllabs.com dan kun je daar een domeinnaam intypen en zien of je up-to-date bent.

Een andere scanner die hij gebruikt, kwam in die tijd net online, in de vorm van internet.nl, een testtool van het Platform Internetstandaarden. In dat platform werken verschillende partijen samen die het internet draaiende houden en beslissen aan welke standaarden je website, e-mail en internetverbinding in Nederland moeten voldoen. Dit is ook typisch hoe internet is georganiseerd: een netwerk van netwerken, maar vooral ook een netwerk van mensen. Van zowel publieke als private organisaties, die met elkaar afspreken hoe alles met elkaar communiceert. Die afspraken zijn neergelegd in standaarden die wereldwijd gelden. De Nederlandse overheid heeft vervolgens besloten dat deze lijst van veilige standaarden moet worden toegepast op al haar websites. Zo niet, dan moet je daar als overheidsinstelling wel een goede reden voor hebben. De lijst wordt daarom ook wel de Pas-toe-of-leg-uit-lijst genoemd.

Ook op internet.nl kun je je domeinnaam invullen en krijg je na een paar seconden te zien hoe je scoort: of je site bereikbaar is via een modern internetadres (IPv6), of je domeinnaam op echtheid wordt gecheckt (DNSSEC), of je verbinding voldoende beveiligd is (HTTPS) en of allerlei aanbevolen veilige opties voor applicaties zijn ingeschakeld. De beveiliging van je mailserver (STARTTLS en DANE) en je mailinstellingen worden

gecontroleerd, bijvoorbeeld op standaarden die de echtheid van de afzender controleren (SPF, DMARC en DKIM).

Ook als deze abstracte afkortingen je niet zoveel zeggen, zie je wel meteen dat je goed bezig bent als je 100% scoort. Zo niet, dan kun je een mailtje sturen aan je provider met: “Hee, kun je DNSSEC aanzetten en mijn SPF goed instellen?” Geloof me, het werkt. Heb ik zelf ook gedaan.

Je kunt bij dergelijke testtools ook het domein van iemand anders invullen om te kijken of die wel veilig genoeg is. Dat is dus wat Elger doet, maar dan met meerdere scanners en voor meerdere URL’s tegelijk. En dat is vooral ook de meerwaarde van Faalkaart. Hij scant namelijk niet alleen op het hoofddomein, bijvoorbeeld groningen.nl, maar onderzoekt ook welke subdomeinen eronder hangen, dus cultuur.groningen.nl. Die subdomeinen zijn ooit eens aangemaakt, bijvoorbeeld voor een tijdelijk project, vervolgens niet meer onderhouden en daardoor vaak kwetsbaar.

Alleen al het in kaart brengen van dergelijke subdomeinen is waardevolle dreigingsinformatie waar, volgens Elger, een levendige handel in bestaat – zowel voor bedrijven die ingehuurd worden om de site te beveiligen als criminelen die ze willen misbruiken. Faalkaart doet dat dus gratis voor het goede doel.

Wat tot slot bijzonder is bij Faalkaart, is dat de score van elke gemeente automatisch wordt omgezet in coördinaten op OpenStreetMap. Dit is net als Google Maps een online landkaart, maar dan ontwikkeld door een community en dus open source. Je kunt met deze kaart doen wat je wilt, zoals in dit geval op de kaart van Nederland elke gemeente een kleur geven op basis van hun score van de vele scanners.

Het resultaat is een mooi geografisch overzicht van alle geteste gemeenten. Dat zijn er op dat moment 355. Klik je op de gemeente, dan verschijnt er een rapport over wat er allemaal mis is met de beveiliging. Faalkaart presenteert ook een ranglijst van best en slechtst beveiligde gemeenten. Volgens Elger gebruiken sommige ambtenaren de kaart en ranglijst om aan hun collega’s te laten zien dat er achterstallig onderhoud is weg te werken. Ze zien precies wat er gedaan moet worden om punten te scoren en hoger in de ranking te komen, een soort securitygamification. De vier grote steden zouden elkaar zelfs uitgedaagd hebben om als eerste de eerste plek te bemachtigen van meest veilige gemeente. Maar er zijn ook

ambtenaren die niet begrijpen waarom hun gemeente zo slecht scoort. Als ze Elger en zijn kameraden dan mailen om uitleg, krijgen ze de Pas-toe-of-leg-uit-lijst en een lijst met URL's waar de problemen zijn aangetroffen. Vaak blijkt het probleem dan inderdaad te zitten in verouderde subdomeinen.

Na dit initiële succes willen Elger en zijn team dit hobbyproject omzetten in echt werk. Dat vindt zijn werkgever echter op dat moment niet zo'n goed idee, want het bedrijf heeft ook gemeenten als klant. Ze zouden dan als slager hun eigen vlees keuren. Elger richt daarom met twee andere hackers een stichting op en ze dienen een voorstel in bij het SIDN-fonds om het platform verder uit te bouwen. In het voorstel schetsen ze hun toekomstvisie: Faalkaart wordt een universele en internationale geografische mappingtool. Daar hoort dan ook een internationale naam bij. Ze noemen zich: The Internet Cleanup Foundation, met als URL internetcleanup.foundation. Het voorstel wordt eind 2017 gehonoreerd en ze kunnen aan de slag.

Op dat moment zijn er al veel zoekmachines, waarmee je het internet kunt scannen op security. Met Shodan kun je kijken welke computers aan het internet hangen, waar die staan en of ze verouderde softwareversies draaien. Met Nmap kun je hele netwerken in kaart brengen en er met Censys zoekopdrachten naartoe sturen. Ook interessant is HaveIbeenPowned, een onlinedatabase waarin je kunt opzoeken of je inloggegevens ergens zijn gelekt. De initiatiefnemer hierachter, Troy Hunt, verzamelt namelijk gelekte databases met inlognamen en wachtwoorden en bewaart daarvan – als het goed is – alleen de mailadressen. Type je op zijn site je e-mailadres in, dan krijg je netjes een lijst met waar en wanneer jouw gegevens gelekt zijn, gevolgd door het advies daar je wachtwoord te wijzigen als je dat nog niet hebt gedaan.

Een ander mooi voorbeeld van dreigingsinformatie zijn de wereldkaarten met actuele online dreigingen, de threat maps. Die laten letterlijk zien welke IP-adressen, van waar in de wereld worden aangevallen. Het lijkt wel een animatie van een cyberoorlog. Securitybedrijven, zoals FireEye, Kaspersky, Check Point en Fortiguard, laten de firewalls die ze bij hun klanten hebben seintjes teruggeven als er

verdacht verkeer is. Dat anonimiseren en aggregeren ze en plotten ze op die kaart. Het zijn hints dat er ergens grote aanvallen kunnen plaatsvinden, maar data over wat er feitelijk gebeurt, onthullen ze niet. Dat is immers gevoelige informatie over hun klanten. Omdat het niet open source is, tellen deze kaarten niet mee als OSINT. Maar de aanvallen zijn wel echt en bijna realtime, dus het is ook wel een beetje managementporno.

Het summum van OSINT is wel de CVE-lijst met 'Common Vulnerabilities and Exposures'. Als er in veelgebruikte software een kwetsbaarheid wordt ontdekt, kun je dat bij hen melden. Een groepje experts kijkt er dan naar en als het wat is, wordt het gepubliceerd, compleet met de naam en versie van de software waarin de kwetsbaarheid is gevonden. Wil je weten of iets kwetsbaar is, dan zoek je met de CVE-lijst naar die softwareversie. Belangrijk daarbij is dat elke kwetsbaarheid een uniek nummer heeft, zodat zowel de mensen als de databases weten wanneer ze over hetzelfde praten. Er zijn verschillende CVE-werkgroepen, een bestuur met vertegenwoordigers van verschillende IT-bedrijven en een wereldwijd netwerk van CVE Numbering Authorities – allemaal vrijwilligers die openlijk kwetsbaarheden delen, om samen sterker te worden.

Ook in het ontwikkelen van veilige software zien we veel vrijwilligers die hun kennis vrij delen, zoals OWASP, het Open Web Application Security Project. Ze zijn vooral bekend van hun top 10 van 'Most Critical Web Application Security Risks'. Het is overigens geen rangorde en ook niet zoals CVE een lijst met specifieke kwetsbaarheden in bepaalde software, maar eerder een checklist van soorten risico's die het meeste voorkomen. Hier de top 10 anno 2020:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization

9. Using Components with Known Vulnerabilities
10. Insufficient Logging & Monitoring.

Deze lijst zal de leek niet zoveel zeggen, maar helpt wel veel softwareontwikkelaars om tijdens het programmeren veiligheidsrisico's voortijdig te herkennen en tegen te gaan. Hackers keren dat om: zij scannen op de top tien om kwetsbaarheden te vinden. Maar OWASP is veel meer dan alleen een lijst. Het is een wereldwijde vrijwilligersorganisatie van meer dan 10.000 actieve leden. De ene helft heeft een security achtergrond, de andere helft is ontwikkelaar. Ze zijn georganiseerd in chapters. Zo is er een Nederlandse chapter, maar je zou er ook zelf een kunnen oprichten als je wilt. Iedereen kan een plan indienen, zelfs niet-leden. Als je genoeg mensen meekrijgt, heb je een leuk project.

Binnen de rijke en open wereld van OSINT is Faalkaart uniek, omdat het niet zozeer naar specifieke lekken zoekt, maar hele domeinreeksen langs checklijsten haalt en de resultaten op een geografische kaart zet. Ook dit project wordt gedraaid door vrijwilligers. Dat is zowel de kracht als zwakte, zoals bij veel OSINT-projecten: iedereen is bij aanvang enthousiast over het nieuwe idee en bereid om dingen op te zetten, maar de verdere uitwerking en het onderhoud verlopen stroef. Om Victor en Elger een handje te helpen met nieuwe vrijwilligers, organiseerde ik op 10 april 2018 een speciale Hack Talk over OSINT.

We beginnen de dag met een workshop. Tien jonge hackers hebben zich aangemeld. Victor laat zien hoe hij scant en wat hij vindt, gevolgd door intakegesprekken met potentiële vrijwilligers. Elger geeft een demo van Faalkaart en zet de hackers meteen aan het werk. Vooral de jacht op subdomeinen is interessant voor hem, want elke hacker heeft daar weer een eigen aanpak voor. Om er een leuke uitdaging van te maken, heeft Elger er een competitie van gemaakt: hoe meer internetadressen je toevoegt en scant, hoe meer punten. De winnaars krijgen een SHA-badge: een printplaatje met computertje en scherm, dat tijdens het beruchte hackerskamp diende als naamplaatje. Die middag worden er in totaal 600 URL's toegevoegd aan de kaart, met name van subdomeinen die onder de gemeentesites hangen.

Maar, hackers blijven hackers, dus wordt er in al het enthousiasme niet alleen achterstallig onderhoud weggewerkt. Nieuwe toepassingen bedenken is natuurlijk leuker, maar zorgen ook weer voor meer werk. Sommigen verbreden de scope van de scan en voegen domeinen toe van andere dan alleen de lokale overheden. OSINT-man Nick Brand maakt zelfs een crosslink tussen de gemeentelijke domeinen en gelekte emailadressen. Dat kan hij, omdat hij bij Spycloud werkt en daar een database met gelekte inloggegevens heeft die nog groter is dan HaveIbeenPowned. Alle grote steden blijken erbij te zitten en Amsterdam is weer nummer 1 met meer dan 8.000 gelekte, gemeentelijke e-mailadressen, o.a. via LinkedIn. Anders dan Troy Hunt zou Nick zelfs de wachtwoorden erbij kunnen geven, maar daar bereiken we toch wel de ethische en juridische grenzen van OSINT.

Nu ik twaalf hackers bij elkaar heb, is dit een mooie gelegenheid voor Tobias Groenland om wat portretten te schieten. De grote zaal wordt ‘s avonds pas gebruikt en is de perfecte locatie om zijn studio in te richten. Hij komt vooral voor Victor, die hij al lange tijd voor zijn camera heeft geprobeerd te krijgen. Dit is zijn kans. Victor zelf wil vooral de jonge onderzoekers aan het werk zetten, om ook zijn scan- en meldwerk voort te zetten, maar begrijpt dat dit een mooie gelegenheid is om een belofte van lang geleden in te lossen. Als ik zie dat de assistente van Tobias op een ladder klimt om een opgerolde internetkabel, bij wijze van rozenkrans, boven Victors hoofd te hangen, vraag ik me af of dit wel zo’n goed idee is. Gelukkig wordt het geen Messiasportret. De grote bos zwarte krullen, verwarde baard en het T-shirt met ‘Responsible Disclosure Kills the Zero-day Industry’ zeggen genoeg.

Ook Elger gaat voor de camera. Hij zet voor de gelegenheid een grote gele muts op met daarop ‘CYBER’. Niet dat hij zo’n fan is van cyber. Integendeel, Elger laat geen gelegenheid onbenut om te laten merken dat hij het een betekenisloos woord vindt. Met bril, dikke baard en een T-shirt van de Amersfoortse hackerspace Bitlair ziet hij er flink hackerig uit. Dat geldt ook voor Edwin van Andel. Hij is de baas van Zerocopter, een platform waar je je door hackers wereldwijd kunt laten pentesten voor bug bounties. Op zijn T-shirt prijkt de bekende grote ‘0’ van zijn bedrijf. Alsof zijn grote grijze baard en glimmende doodshoofdringen het beeld nog niet compleet maken, krijgt Edwin een gekleurd kapje met propeller op zijn hoofd.

Tobias denkt dat hij er dan wel is, maar onderschat het effect op de andere hackers die op dat moment Elgers Faalkaart aan het vullen zijn. Ze zijn nieuwsgierig naar wat er allemaal in de grote zaal gebeurt en willen ook wel voor de camera. Tobias kan meteen door met OSINT-man Nick Brand. Maar aangezien dit de vierde man met baard is, stel ik hem voor wat nieuwkomers van de hackerscene erop te zetten. We hebben die dag namelijk ook een groep jongeren van de Rotterdamse Cyberwerkplaats op bezoek. Twee ervan gaan voor de camera. Tabitha Vogelaar, die nog maar net begonnen is met hacken en normaal niet zo graag in de picture staat, laat zich de shoot welgevallen en kijkt vrolijk en zelfverzekerd in de lens. Zawadi Done poseert met een witte cowboyhoed, als hommage aan het begrip ‘white hat hacker’ en zwart shirt met: ‘I hacked the Dutch government and all I got was this lousy T-shirt’.

Die avond zitten we met meer dan honderd mensen in de grote zaal van club Worm te Rotterdam. Victor geeft een overzicht van wat hij het afgelopen kwartaal aan cyberellende heeft gevonden op internet. Eerst laat hij zien met wat voor scanners hij werkt: Shodan, ZMap, Nmap en Censys. Hiermee stuurt hij pakketjes en zoekopdrachten naar databases, zonder in die data te kijken. Zoals gezegd downloadt hij dan alleen de tabelstructuur en niet de data die erin staat. Of hij kijkt alleen welke softwareversie er draait. Is die verouderd, dan ziet hij welke kwetsbaarheden daar nog inzitten. Het lastigste is om de eigenaar van zo’n database te achterhalen en te overtuigen dat die iets moet doen. Soms benadert hij de hostingprovider van die eigenaar of, als het massale lekken zijn, de landelijke CERT’s. Zo heeft hij alleen al in dit eerste kwartaal 33 miljoen internetadressen gescand. Daarvan blijken er 151.000 kwetsbaarheden te bevatten. 140.000 zijn gemeld, waarvan er 90.000 zijn gefixt of offline gehaald. Het melden doet hij geautomatiseerd, met een standaardmail, anders is het niet meer te doen.

Victors stichting GDI, the Global Defense of the Internet, heeft net als die van Elger een financiële bijdrage gekregen van het SIDN-Fonds. Zo kunnen ze serverruimte huren en softwarelicenties betalen om al hun scans uit te voeren. Er zijn ook steeds meer vrijwilligers die willen scannen en melden. Die werken met templates om de rapporten te structureren en

kunnen bij de stichting een soort opleiding in responsible disclosure krijgen. Met de subsidie hebben ze ook een zogenoemde OSINT-compiler gebouwd, oftewel een dashboard voor open data, waar je in een oogopslag kunt zien welke kwetsbaarheden er zijn, zoals Memcached, EternalBlue en Heartbleed. Je kunt ook zien welke ISP's (Internet Service Provider) lek of gehackt zijn.

Deze manier van werken wordt wel steeds meer bemoeilijkt, omdat grote organisaties genoeg krijgen van al die scanners en hen blokkeren in hun firewalls. Omgekeerd krijgt Victor zelf veel internetverkeer te verwerken, met name abuse mail, oftewel automatische meldingen die denken dat hij degene is die misbruik maakt van het internet. Hij ontvangt daardoor meer dan 100.000 mails per dag, die hij uiteraard niet allemaal kan beantwoorden. In zijn mailbox staan op er dat moment nog meer dan 23 miljard aangemerkt als 'ongelezen'…

Ook wetgeving wordt steeds lastiger voor Victor en consorten. Volgens de Algemene Verordening Gegevensverwerking is een IP-adres ook een persoonsgegeven. Victor zou de eigenaren van de domeinen dus eigenlijk eerst moeten vragen of hij hun persoonsgegevens mag verwerken en uitleggen hoe GDI dat doet. Maar ja, doe dat maar eens voor de hele wereld. Hier in Nederland komt hij er nog wel mee weg, want hier begrijpen de meeste organisaties inmiddels wel waar hij mee bezig is, maar in andere landen blijft het toch nog lastig uitleggen.

De cijfers van GDI laten zien dat er nog heel veel oude troep online staat. Zo staan er bijvoorbeeld nog 7.500 Telnet-connecties online. Dit protocol is allang afgeschaft, omdat er geen versleuteling wordt gebruikt. Computers die erachter staan, zijn dus makkelijker te herkennen en te hacken en worden bijvoorbeeld misbruikt als bitcoin miners. Bijvoorbeeld omdat het een apparaat is waarvan het standaardwachtwoord in de gebruikershandleiding staat. Victor leest voor: "The default password is 'root'. You should change this, for example to '123'" Hij ziet vervolgens dat de ene helft van de apparaten 'root' heeft als wachtwoord en de andere helft '123'. Hij wordt er moedeloos van, maar de zaal vindt het wel grappig.

Ook deze hacktechniek is te automatiseren, zoals BrickerBot doet. Victor laat zien hoe deze tool computers die aangesloten zijn op het internet test op de gebruikersnaam en het wachtwoord uit de handleiding.

BrickerBot stuurt echter geen melding, zoals Victor doet, maar logt in en uploadt malware. Vele miljoenen apparaten zijn op deze manier besmet en onbruikbaar gemaakt. Ook de zogenoemde VNC (Virtual Network Computing) systemen worden systematisch gehackt. Op de website worldofvnc.net ziet hij dan screenshots van bijvoorbeeld kassasystemen, waar je je eigen malware kunt installeren. Victor ziet veel kleine Nederlandse ondernemers thuis hun administratie bijwerken met deze kwetsbare systemen. Maar er zitten ook betaalsystemen van banken en luchthavens bij.

Het meeste werk heeft Victor gehad aan het databasesysteem MongoDB, zoals beschreven in het tweede hoofdstuk. Gebruikers die de standaardinstellingen niet aanpassen, stellen hun database dus open voor iedereen. Het heeft hem drie jaar gekost om het bedrijf Mongo zover te krijgen die instellingen aan te passen, maar veel gebruikers blijven oude versies gebruiken zodat het misbruik blijft toenemen. Victor heeft voorbeelden van ziekenhuizen waarbij hun hele administratie of bestanden van langlopende onderzoeken zijn gegijzeld. Een ziekenhuis had losgeld betaald, maar zette de database vervolgens weer online met dezelfde kwetsbaarheid… Omdat het melden van de open Mongodatabases dweilen met de kraan open blijkt, heeft hij in zijn online overzicht voorbeelden van ransomenotes en bijpassende Bitcoinadressen erbij gezet. Als getroffenen dan gaan zoeken naar dat adres, komen ze uit bij GDI en kunnen Victor en zijn vrijwilligers hen helpen de databases juist in te stellen.

Daarna komt Elger aan de Hack-Talktafel. Hij begint met een demo van zijn Faalkaart, duikt in zijn laptop en roept: “Pray for the demo gods.” Met al die nieuwe gegevens die er die middag zijn toegevoegd, wordt namelijk het uiterste gevraagd van zijn database en hij weet niet of alles nog wel naar behoren werkt. Tot zijn eigen verbazing blijkt dat toch het geval: alle gemeenten staan er inmiddels in, met in totaal 4.700 URL’s. Je kunt per gemeente opvragen wat er nog gefixt moet worden. Elger kan terug in de tijd bladeren, tot wel vier weken. We zien dan dat niet alleen het aantal kwetsbare domeinen afneemt in de tijd, maar ook het totaalaantal, omdat verouderde domeinen offline worden gehaald. Iemand uit het publiek roept: “Kun je ook vooruit bladeren?” Elger gaat mee in de grap en zegt: “Jazeker,

je zult zien dat ze steeds meer gaan fixen.” Faalkaart geeft gemeenten immers een security to-do-lijst op maat.

Die avond onthult Elger dat team Rick and Morty het best heeft gescoord, met bijna 1.000 punten. De ranking is een stuk willekeuriger dan die op Faalkaart zelf, maar het team heeft in ieder geval 37 sites gevonden met TLS-problemen. Rick en Morty krijgen hiervoor elk de elektronische SHA-badge en mogen namens ons programma de hele avond gratis drinken. Elger vervolgt met zijn toekomstvisie op Faalkaart en wil uitbreiden naar Duitsland en België.

Volgens Elger pakken de Nederlandse gemeenten het ongevraagde veiligheidsadvies van Faalkaart goed op. Maar wat vinden die gemeenten er zelf van? Ik spreek hierover tijdens de Hack Talk erna met Daan Goumans van de IBD, de Informatie Beveiligingsdienst van de Vereniging Nederlandse Gemeenten. Daan is op dat moment degene die bij IBD de telefoon aanneemt als een gemeente in digitale nood verkeert. Wat vindt hij van een ongevraagd initiatief als Faalkaart? Is het niet teveel een digitale schandpaal?

Daan: “We zien weleens paniek als een gemeente slecht scoort. Toch moedigen we dit soort initiatieven juist aan, omdat we zo samen veiliger kunnen worden. We hebben veel contact met de CISO’s van gemeenten en die zijn blij met Faalkaart. Die kunnen ermee naar hun bestuurders. Rood op de kaart betekent meer budget voor beveiliging. Het is eigenlijk een soort benchmark.” Over het probleem met de onveilige subdomeinen is hij echter enigszins relativerend: “Je moet bij zo’n scan ook niet de context vergeten. Is het een kwetsbaarheid op, bijvoorbeeld, kinderboerderij.rotterdam.nl die op een aparte server staat? Dan is dat minder erg dan wanneer het op een site is waar je een zorgtoeslag aanvraagt. Risico is kans maal impact.”

Tijdens onze OSINT-avond hebben we ook twee gasten die OSINT een warm hart toedragen: pentester Rickey Gevers over hoe het bedrijfsleven gebruikmaakt van OSINT en Mieke van Heesewijk van het SIDN-fonds over hoe derde partijen de vrijwillige onderzoekers kunnen steunen. Rickey kennen we van zijn onthullingen over universiteiten en hij is ook opgenomen in de portrettenreeks Hackers Handshake van fotograaf Tobias.

Ik ontmoette hem in 2013 voor het eerst bij Team High Tech Crime van de Nederlandse politie. Hij had een rapport onder zijn arm met ‘Top Secret’ erop, met daarin informatie over het toen beruchte Pobelka-botnet – waardevolle OSINT dus. Bijzonder, zo’n informant en infiltrant, maar des te meer omdat hij door datzelfde team ooit is opgepakt voor het hacken van universiteiten. Nu is hij zelf forensisch onderzoeker en heeft hij bij verschillende securitybedrijven gewerkt, waaronder Multrix, Digital Investigation en Hacker Company. Op het moment van het interview werkt hij bij Red Sox.

Ik vraag Rickey hoe cybersecurity bedrijven omgaan met OSINT. Eigenlijk doen mensen als Victor en Elger gratis wat die bedrijven voor veel geld aanbieden. Of maken die bedrijven er vooral ook zelf goed gebruik van? Rickey: “De basis van OSINT-platformen ligt vaak bij één persoon. Neem bijvoorbeeld Zeus Tracker. Die houdt bij waar Command & Control Servers voor Zeus worden gehost, zodat je die kunt blokkeren. Ook Cuckoo Sandbox voor malwareanalyse is door één persoon gestart. Deze projecten leveren een significante bijdrage aan de internetveiligheid, maar zijn wel heel specifiek. Victor kijkt globaal en pakt af en toe verschillende onderwerpen op, zoals Memcashed. Elger is weer gefocust op Nederland. Commerciële partijen duiken veel dieper in de dreigingen. Dan heb je al snel 150 man die toegewijd bezig zijn. Maar als wij iets doen, is dat alleen voor een specifiek bedrijf. Wat Victor en Elger doen is voor iedereen en daardoor beter schaalbaar.”

Dragen bedrijven ook bij aan OSINT-platformen? Rickey: “Nauwelijks, want dat kost geld. Wij doen dat wel en hebben bij Cuckoo Sandbox contact gelegd en er ook dingen aan toegevoegd. Maar dan is het niet zo fijn als je ziet dat anderen het ook gebruiken en niet bijdragen. Het bedrijfsleven is meestal niet zo nobel. Er wordt vaak gezegd dat er veel verdiend wordt in cybersecurity, maar er wordt ook veel uitgegeven, ze hebben een snelle verbrandingsmotor.”

Stel, een bedrijf komt in OSINT bovendrijven als kwetsbaar, is dat dan schadelijk voor de securitybedrijven die aan hen hun diensten verlenen? Rickey: “Ja, dat gebeurt soms. De berichten daarover in de media kloppen meestal wel. Je ziet dat overheden meestal eerder bereid zijn het te erkennen als ze platgaan door een virus dan bedrijven.”

Mieke van Heesewijk is programmamanager van het SIDN-Fonds en kent OSINT zowel als aanbieder als supporter. Ze werkte bij Internet Provider XS4ALL, het ministerie van Binnenlandse Zaken en Waag Society, was directeur van stichting Netwerk Democratie en heeft klokkenluidersplatform Publeaks opgericht. Ze weet dus uit eigen ervaring hoe het is om met groepen vrijwilligers goede dingen voor het internet te doen en heeft nu de mooie taak dergelijke initiatieven te ondersteunen. Het SIDN-Fonds is opgericht en vernoemd naar de Stichting Internet Domeinregistratie Nederland, de mensen achter .nl, maar het fonds is wel een onafhankelijke stichting en steunt projecten die goed zijn voor een veilig en open internet.

Het fonds steunt ook GDI en Faalkaart. Mieke: “Dit zijn ook wel toppertjes en typisch het soort projecten dat we steunen. Doelstellingen van het fonds zijn: een sterk internet, empowerment van de gebruikers en ‘tech for good’. Projecten die wij ondersteunen, moeten hun kennis delen, liefst open source en dienen het algemeen belang.” Wat moeten hackers doen om geld te krijgen? Mieke: “We hebben twee calls per jaar: 10.000 euro voor pioniers, tot 75.000 voor het opschalen van prototypen. Je dient een formulier in met de omschrijving van je project en dat gaat naar de Raad van Advies. Daar zitten twintig zeer uiteenlopende mensen in. De grote projecten worden uitgenodigd voor een pitch. Naast financiering, ondersteunen we projecten met bijeenkomsten en vouchers om experts in te huren.”

Waarom doet de overheid zelf niet zoiets als Faalkaart? Het werkt toch? Mieke: “Ik heb zelf ooit bij Binnenlandse Zaken gewerkt en vroeg me af of Petities.nl niet een taak is voor de Vereniging Nederlandse Gemeenten. Ik ben zes keer langs geweest, maar niks. Hetzelfde met Publeaks. Ik was directeur bij Netwerk Democratie en vond dat er een plek moest zijn waar mensen misstanden moeten kunnen lekken. Dat hebben we toen zelf opgezet met open source software van Global Leaks. Bij Publeaks trainen we nu ook journalisten en geven we ze een goed beveiligde laptop. Mediapartijen dragen 1.000 euro per jaar bij om het draaiende te houden. En het werkt: wat je bij Publeaks lekt, komt terecht bij de grote kranten en andere media, zoals 1Vandaag. Zoals laatst die rel rondom het HagaZiekenhuis in Den Haag, waar tientallen medewerkers stiekem het

medisch dossier hadden bekeken van Samantha de Jong, beter bekend als Barbie."

Past OSINT, volgens Mieke en Rickey, in de Nederlandse cultuur? Duitsland en Frankrijk zijn veel hiërarchischer en in de VS en het Verenigd Koninkrijk heb je meer een vijandige claimcultuur. Hier zie je bij hackersbijeenkomsten gewoon mensen van de Belastingdienst of veiligheidsdiensten een biertje drinken met anarchistische hackers. Klopt dat beeld? Rickey: "Die bijeenkomsten heb je ook in andere landen, maar die in Nederland zijn inderdaad wel uniek." Mieke: "Jazeker. Zie bijvoorbeeld hoe verschillende internetproviders samenwerken om DDoS-aanvallen tegen te gaan in de Nationale Wasstraat. Of hoe hostingpartijen doen aan Open Source Abuse Management via AbuseIO."

Toevallig zit de projectleider van AbuseIO, Wido Potters, in de zaal en hij wil best een toelichting geven. Wido: "Wij doen zelf niet aan opsporing of detectie van kwetsbaarheden of problemen op systemen. Er zijn allerlei openbare bronnen die dat melden. Wij aggregeren en melden dat bij hostingpartijen. Bijvoorbeeld: open mail relay, fishing sites, open Wordpress-contentmanagementsystemen… Vaak gaat het niet om criminelen, maar onbewust onbekwame gebruikers. We zorgen ervoor dat hostingproviders die meldingen geautomatiseerd kunnen doorzetten. Het gaat om soms wel 10.000 meldingen per netwerk en dat kun je niet met de hand doen." Ook dit project wordt gesteund door het SIDN Fonds. AbuseIO is uiteraard ook open source en te vinden op Github.

Heel mooi, al die vrijwilligersinitiatieven, maar waar gaat het meestal mis? Mieke: "Het probleem is langetermijnplanning en financiering. Het zijn vaak kleine clubs die hard werken. Vaak zijn ze technisch georiënteerd en schort het aan marketingactiviteiten. Daar kunnen ze meer in begeleid worden. Dat doen wij, maar bijvoorbeeld ook Stichting NLnet. Het zou mooi zijn als meer internetbedrijven hun verantwoordelijkheid nemen en bijdragen. Zij verdienen immers hun geld met een open en veilig internet." Rickey: "Mee eens. Ook de overheid mag wel wat meer doen, want Nederland wordt hier veiliger door. We moeten dit soort projecten ook zien als kleine startups, die kunnen opschalen. Maar ja, dan heb ik misschien over vijf jaar geen baan meer…"

Die avond zijn we nog lang doorgegaan met het delen van kwetsbaarheden, geheimen en nieuwe ideeën om samen het internet veiliger te maken. Ook de hackers zelf stelden zich kwetsbaar op. Niet alleen door voor open publiek hun projecten te delen, maar ook door voor Tobias zijn camera te gaan staan zodat de mensen die zij helpen, ook een beeld bij hen hebben.

Twee jaar later, augustus 2020, kijk ik hoe het ervoor staat met Elgers Faalkaart. Als ik de URL intyp, zie ik dat ik word doorgestuurd naar een ander adres: basisbeveiliging.nl. Dat klinkt al een stuk vriendelijker dan Faalkaart. Afzender: Internet Cleanup Foundation, 'Cleaning the Internet, a thousand sites at a time'. De kaart is wel hetzelfde, met kleurcodes voor de best en slechtst beveiligde gemeenten. De ranglijst wordt nu aangevoerd door Appingedam, met maar liefst 85 'high risks'. Als je door het rapport bladert, zie je dat de score vooral te danken is aan het gebruik van onbetrouwbare certificaten. Alleen wat kleinere gemeenten als De Fryske Marren, Edam-Volendam en Tholen blijken wel 100% aan alle veilige standaarden te voldoen en scoren op alle risico's een '0'. Bovenaan de site staat: "Voor actuele resultaten zijn financiële bijdragen nodig."

Als ik Elger spreek, hoor ik terug waar Mieke van het SIDN-Fonds al voor waarschuwde: continuïteit blijkt lastig. Ze zijn nu met z'n vijven, maar het blijft vrijwilligerswerk naast hun betaalde banen, elk ongeveer vier uur per week. Omdat de kaart wel werd gewaardeerd door de meeste gemeenten, leek het Elger logisch dat een partij, zoals de Vereniging van Nederlandse Gemeenten, het project zou willen steunen, maar helaas. Hij heeft in 2019 op de One Conference gestaan met een demo, om eventueel andere overheden te trekken. Provincies en Rijksoverheid kunnen immers ook gescand worden. Wederom vonden de partijen het wel interessant, maar wilden ze er niets voor doen. De enige overheid die serieuze interesse toonde was die van Oezbekistan, maar dat leek Elger zelf niet zo'n goed idee gezien de mensenrechtensituatie aldaar.

Dan maar doen waar hackers het beste in zijn: naar de tekentafel om iets nieuws te ontwikkelen. Met als gevolg de Web Security Map. Het is een open source variant van hun kaart, waarmee iedereen zelf scans kan uitvoeren en de resultaten op OpenStreetMap kan zetten. Of je nu

gemeenten wilt scannen, of bijvoorbeeld alle goede doelen of geheime diensten in de wereld, alles kan op de kaart. De opzet blijft redelijk hetzelfde, maar de aanpak is wel anders. Elger: “De techniek was alleen toegankelijk voor nerds en autisten, daar liep het op vast.” Ze hebben daarom nu online tutorials voor Web Security Map. De filmpjes laten stapsgewijs zien hoe je de software downloadt, installeert en eigen maakt, met hier en daar een leuk hackergrapje. Als meer partijen de Web Security Map gaan gebruiken, kunnen Elger en consorten er als experts wellicht nog betaalde opdrachten aan overhouden.

Dat zou, wat mij betreft, mooi zijn, want de uren die Elger besteedt aan het online zetten van gevonden kwetsbaarheden vallen in het niet vergeleken met zijn offline werk als organisator van hackerevents. Daar zien we dat nerds niet alleen achter de computer zitten, maar ook meesters zijn in het omtoveren van saaie congreshallen en lege kampeerterreinen tot de beste feestlocaties met hoogwaardige programmering. En is daar, nog meer dan online, de meest waardevolle kennis gratis en vrij beschikbaar.

6. Nerds vieren de beste feestjes

Op 3 augustus 2017 zijn 3.650 hackers bijeen op het scoutingterrein van Zeewolde. Elger staat te stralen voor Omroep Flevoland als hij uitlegt wat hier aan de hand is: “Hier gaan we vijf dagen lang alles hacken wat we maar kunnen”. De journaliste vraagt met gespeelde bezorgdheid: “Maar dat is toch hartstikke illegaal?” Elger: “Nee, dat is helemaal niet illegaal. Wij doen juist heel toffe dingen. We hebben honderd gigabyte internet, zo snel krijg je nergens. We hebben alles zelf aangelegd. We hebben heel veel stroom, heel veel wifi, ons eigen telefoonnetwerk…” Ze vraagt: “Maar wat heb je daar nou aan?” Elger: “Dat is leuk, is gewoon cool, wij vinden het gewoon hartstikke mooi om nieuwe dingen uit te vinden.”

Die dag arriveer ik ook op het kamp. Op treinstation Nijkerk rijden shuttlebusjes met vrijwilligers af en aan. Opgepropt tussen een paar Duitsers, Italianen en vele rugzakken rijden we zwijgend het bos in. Daar worden we gedropt. Via een modderig kronkelpaadje kom ik aan bij een kleurrijke tent, waar alternatief uitgedoste dames en heren onze tickets scannen en ons een polsbandje omdoen. We krijgen een zakje elektronica: lampjes, een motortje, oordopjes, batterij en een printplaat met componenten en een klein schermpje. Dit is de SHA-badge. Je moet hem zelf in elkaar zetten en aan de praat krijgen. Dan kun je je naam op de display zetten. Je kunt er ook spelletjes op spelen, feestverlichting van maken, nieuwsberichten op tonen, van alles. Kom je er niet uit, dan ga je naar de wiki met uitleg of vraag je het aan iemand van het Badge Team.

Op het terrein heerst een enorme chaos. Tenten staan kriskras verspreid, overal infoborden die elkaar tegenspreken, zelfgemaakte voertuigen botsen bijna tegen elkaar op, mobiele toiletten zijn omgetoverd tot serverruimtes en verbonden met draden door het gras. Ik kijk mijn ogen uit naar allerlei vrolijk uitgedoste types die langsparaderen. De organisatie had me een

‘village’ toegewezen, maar aangezien er honderden villages blijken te zijn en de plattegrond nog niet up-to-date is, zoek ik maar een rustig plekje net achter een dijk.

Als ik de volgende ochtend ontwaak, is ook dat stuk helemaal volgebouwd. Ik blijk te zijn beland tussen de tenten van KPN, het NCSC en de Belastingdienst en ik zie overal bekenden die meteen een praatje maken over security en welke projecten ze deze week gaan doen. De een komt vooral om Capture the Flags te spelen, de ander voor een bijzondere spreker, maar de meesten zijn hier vooral om elkaar eens offline te zien. Ik meld me bij een balie met een bordje ‘Heaven’ aan als Angel, want zo heten de vrijwilligers hier. Ik ga helpen de bar op te bouwen. Dit is slechts een opwarmertje, want morgen begint het echte werk: ik ga hier een eigen radioprogramma maken.

Er is namelijk een tent met een grote FM-zendmast en ik heb zendtijd aangevraagd voor elke avond van 22.00-23.00 uur. Niet dat ik veel luisteraars verwacht, maar het is wel een goed excuus om ongegeneerd hackers uit te horen, onder andere voor dit boek. In de studio tref ik ene Psychic. Ik vraag hoe hij in het echt heet en wat voor werk hij normaal doet, maar krijg geen antwoord. Hij is vooral bezig draden te trekken en laat trots zien wat voor apparatuur hij heeft meegenomen. Ik vertel dat ik elke avond een samenvatting ga geven van wat er op het kamp gebeurt en vraag of hij nog wensen heeft voor bepaalde items. Nee, hij zorgt ervoor dat technisch alles werkt en wat ik door die microfoon wil roepen moet ik vooral zelf weten. SHA is eigenlijk de ultieme camping voor mensen die normaal niet van kamperen houden.

Elger (zijn nickname hier is Stitch) is tijdens SHA2017 samen met Attilla de Groot en Julius ter Pelkwijk eindverantwoordelijk voor het kernteam. Ze zijn twee jaar bezig geweest met de voorbereidingen. Om hen heen ontstond langzaam maar zeker een intelligente zwerm van meer dan 1.000 Angels. Hoe werkt dat zelforganiserend vermogen op een hackerskamp? Elger: “Dit is een traditie die teruggaat tot het eerste evenement in 1989, in Paradiso. Sindsdien hebben we er elke vier jaar één, met deels dezelfde mensen. De sfeer is intens chaotisch. Zo hebben we, bijvoorbeeld, op het allerlaatste moment de plekken van allerlei tenten omgegooid, maar dat

kan, want het zijn wel allemaal kundige mensen die er echt voor gaan. Er is geen hiërarchie, alleen thema's en teams met teamleads."

In totaal zijn er dertig teams. Zo is er een Network Operations Center voor de internetverbinding (100 Gbit/s uplink!), een Power Team voor energie (1,2 MW!), een Productiehuis voor de content, een Bar Team, een veiligheidsteam, een team voor parkeren, noem maar op. Er is ook een Cohesion Team dat mensen helpt die niet zo lekker in hun vel zitten en dat geleid wordt door Elgers vriendin Janneke. Alles wordt gedreven door vrijwilligers. Dat zijn niet alleen Nederlanders, maar ook Belgen, Britten, Italianen en vooral veel Duitsers van de Chaos Computer Club. Hun Chaos Vermittlung is vaak aanwezig op hackerevents om met DECT-systemen en veldtelefoons van de vorige eeuw, gratis, te kunnen bellen.

De elektronische badge die ik omheb, is gemaakt door het Badge Team. Elger: "Het Badge Team is hiervoor wel door een productiehel gegaan. Het was bizar veel werk. Ze hadden nog niet eerder zoiets gemaakt en moesten communiceren met leveranciers over de hele wereld. Dan gaat er in de productie één dingetje mis, maar dat is wel meteen keer 4.000 badges, terwijl ze in een week af moesten zijn."

De media blijken vooral geïnteresseerd te zijn in wat er aan spullen wordt gemaakt en gesloopt. NOS meldt: "Hackers kraken brandweerauto op hackerfestival" en laten een burgemeester van de naburige gemeente vertellen dat hij er blij mee is, want nu kunnen ze het veiligheidslek dichten. De krant Trouw schrijft over een groepje hackers dat ter plekke een ijskast heeft gemaakt van ventilatoren. NRC Handelsblad weidt uit over de elektronische badge. Tweakers geeft een hele opsomming van de hardware van het kamp: van de elektriciteitsvoorziening, supersnelle internetverbindingen en telefoonlijnen, tot en met de Tesla's, zelfgemaakte voertuigen en natuurlijk weer de badge. Waag Society heeft een mooie blog met '10 redenen waarom SHA2017 het leukste kamp van het jaar was': badge, voertuigen, community, muziek, eten, netwerk, feestjes, rook- en lichtshows, het terrein en nog wat fun stuff.

Maar een hackerskamp is niet alleen om samen te knutselen aan projecten, het is ook de plek waar je veel interessante lezingen en workshops kunt bijwonen. Meer dan 300 in totaal. Ze worden opgenomen en online gezet, waardoor de meeste hackers zeggen: "Die ga ik later

allemaal nog weleens bekijken", maar volgens mij doen maar weinigen dat omdat het er gewoonweg te veel zijn. Omdat ik met Hack Talk Radio elke avond verslag deed, heb ik er zoveel mogelijk bijgewoond. Ze staan als het goed is nog online, dus daarom hier een korte samenvatting van de lezingen die ik heb gezien. Zo niet, dan geeft deze opsomming toch een leuk beeld van wat je zoal aantreft op een hackersfestival. Daarom niet alleen de toppers, maar ook de flops en wat tips. Tot slot de flips, oftewel de lezingen waarvan je denkt "What the fuck zit ik nu te kijken"…

Een van de toplezingen was de presentatie van Bill Binny over 'How The NSA Tracks You'. Hij kan het weten, want hij werkte 34 jaar bij het Amerikaanse National Security Agency, dat hij nu 'The New Stasi Agency' noemt. Ondanks, of misschien juist dankzij, zijn rolstoel komt de oude baas zeer strijdlustig over en jast hij er een hele reeks programma's doorheen die maar één doel hebben: zoveel mogelijk data verzamelen over iedereen. Hij heeft destijds als Technical Director van de NSA de meeste van deze programma's zelf opgezet en zag van dichtbij hoe de datahonger volledig uit de hand liep. "But data is not intelligence", waarschuwt hij. De programma's hebben ervoor gezorgd dat zo'n beetje iedereen wel een fout profiel heeft bij de NSA. Gevolg: 1,2 miljoen mensen op de 'drone list' om met een gericht bombardement vermoord te worden, zonder een eerlijk proces. Binny heeft inmiddels veertig privacy-rechtszaken aangespannen tegen Trump om de programma's weer te stoppen, vooralsnog zonder succes.

Dat je af en toe ook best mag lachen om Amerikaans oorlogsgeweld laat Vincent Ossewaarde zien in zijn presentatie 'Hacking on a boat. Fun with onboard maritime systems'. Vaartuigen zitten vol met sensoren en zenden continu signalen uit, meestal gebaseerd op oude standaarden die makkelijk te hacken zijn. Zoals het AIS, Automatic Identification System, dat laat zien waar je bent, wat voor boot je hebt en hoe hard je vaart. Je moet hier eigenlijk een licentie voor hebben en een gecertificeerde zender, maar met een SDR, Software Defined Radio, kun je het signaal prima nabootsen. Ossewaarde ging hiermee met zijn zeilbootje over het Flevomeer en deed zich voor als het grootste Amerikaanse vliegdekschip met een snelheid van 100 knopen. De havenmeester van het Flevomeer zal zich rot geschrokken

zijn, maar had wellicht ook wel gezien dat dit een hackersgrap is. Op de AIS-kaart volgt de boot namelijk geen gewone route, maar vormt hij de letters ‘SHA’. Zo cool.

Even vermakelijk is de bijdrage van Walter Belgers, pentester en president van Toool, The Open Organisation of Lockpickers. In ‘Physical penetration testing’ laat hij zien hoe je met eenvoudige middelen als ijzerdraad, elastiek en touw deuren openkrijgt. Cilindersloten zijn een grotere uitdaging en vereisen professioneel gereedschap dat hij ook demonstreert. Uiteraard niet om ons te leren inbreken, maar om samen sloten veiliger te maken. Er zijn behoorlijk wat bezoekers op zijn praatje afgekomen, die bij elk geopend slot in juichen uitbarsten.

Belgers vertelt me tijdens Hack Talk Radio die avond waarom lockpicking onder hackers zo populair is: ontwerp- en implementatiefouten zorgen voor kwetsbaarheden, die je kunt opsporen en melden om te voorkomen dat kwaadwillenden er misbruik van maken. Het eindeloos proberen van mogelijkheden geeft een soort meditatieve focus en het oplossen van de puzzel een enorme kick. Maar er zijn ook verschillen: de cybersecurity wereld staat veel meer open voor het melden van kwetsbaarheden dan de slotenwereld. Die is, typisch, veel meer gesloten. Daar kunnen ze best wat van ons leren.

De spreker voor wie nog het hardst geklapt wordt, is Bart Roos met zijn ‘Trip to India’. Als ik op het applaus kom afgerend, heeft hij zijn presentatie net afgerond, maar ik kan hem gelukkig strikken om het tijdens Hack Talk Radio nog eens dunnetjes over te doen. Bart vertelt dat hij twee jaar geleden werd gebeld door iemand uit India die zich voordeed als een medewerker van Microsoft, om wat problemen met zijn computer op te lossen. Bart speelde het spel mee, niet op zijn gewone computer, maar op een virtuele machine. Dat is een programma dat een hele computer nadoet, die je ook weer kunt wissen om opnieuw te beginnen, hackbaar, maar wel vervangbaar. De helpdeskmedewerker installeerde daarop op afstand het programma Teamviewer. Bart zag hoe hij vervolgens van alles aanwijst dat voor storingen zou zorgen. Die konden verholpen worden, als Bart daarvoor betaalde. Niet dus. Later verneemt Bart dat honderden Nederlanders op deze manier zijn opgelicht en neemt hij contact op met AVRO Tros Opgelicht. Ze besluiten samen de criminelen te ontmaskeren.

Het programma laat eerst zien hoe de criminelen te werk gaan. Het roept kijkers op om niet meteen op te hangen als zij zo iemand aan de lijn krijgen, maar een nummer te geven waarop zij teruggebeld kunnen worden. Als de nietsvermoedende oplichter vervolgens terugbelt, zitten Bart en zijn collega's klaar met een geprepareerde computer. Ze hebben zelfs een nepsite ontwikkeld van een bank om transacties te plegen en zo meer sporen te vinden. Bart heeft de communicatie met de helpdeskmedewerker via Teamviewer opgenomen en het is hilarisch om te zien hoeveel moeite die doet en in gebrekkig Engels de grootst onmogelijke onzin vertelt om Bart te laten betalen.

Wat de oplichter niet weet, is dat hij op dat moment zelf gehackt wordt door Bart, die Teamviewer op zijn computer installeert. Eenmaal aan zijn kant, ziet Bart een callcenter van zestig medewerkers die dan al in totaal vijf miljoen telefoontjes hebben gepleegd. Door verder speurwerk komt de Nederlandse politie achter de locatie en is de bende in samenwerking met de Indiase politie opgerold. Geweldige hackerdetective. Absolute aanrader.

Dan de geflopte sprekers van SHA, want die zijn er uiteraard ook. De eerste spreker op het programma was meteen al een gedenkwaardig drama van nota bene cryptoheld Phil Zimmermann. De vader van PGP (Pretty Good Privacy) software had eind jaren negentig langslepende rechtszaken met de Amerikaanse overheid. Door versleuteling beschikbaar te stellen, zou hij volgens de wet aan internationale wapenhandel doen, terwijl PGP juist helpt mensen te beschermen. Afgelopen jaren ging Zimmermann aan de slag met Silent Circle, om iedereen van versleutelde communicatie te voorzien, maar dat bedrijf kwam niet echt van de grond. Nu woont hij in Nederland, tot het klimaat in de VS weer beter is.

Is dit een inleiding? Nee, dit is eigenlijk zijn hele verhaal, zonder slides of iets wat we nog niet wisten. "I will be happy to take some questions", besluit hij, met nog veertig minuten te gaan. Na wat ongemakkelijk geschuifel in de zaal loopt er eindelijk iemand naar de microfoon en vraagt: "Are you related to Bob Dylan?" (Deze popster heet in het echt ook Zimmermann.) Een volgende vraagt: "Do you have an invisibility cloak?". Op beide vragen weet Phil niet echt te reageren en waarschijnlijk begrijpt hij dat dit eigenlijk een beleefde manier is om te zeggen: "Dude, you are

here at an awesome hacker congres, so we expected a bit more than that!" Vrijwel direct na dit gênante optreden verdwijnt de voormalige cryptogrootheid met het pontje naar het vasteland.

Zo zijn er nog wat sprekers die onvoorbereid een eind in de ruimte stonden te kletsen. Zoals het Italiaanse driemanschap COD met hun 'Zanshin Tech: the digital martial art'. Op zichzelf een fascinerende gedachte om principes uit vechtsporten toe te passen op digitale zelfverdediging. En hard nodig, want volgens Claudio plegen honderden jongeren zelfmoord vanwege cyber bullying. Hij zou als judoka principes hebben die kunnen helpen. Iets met Ying en Yang, maar veel verder komt hij niet. Zijn twee compagnons staan vooral glazig in de zaal te staren en ook hier gaan we na twintig minuten al over op Q&A met een leeglopende zaal.

Ook gênant is de bijdrage van Sijmen Ruwhof: 'How hackers could have hacked all Dutch elections since 2009.' Op zich al een pretentieuze titel, waar dan ook aardig wat publiek op afkomt. Ruwhof zou in de afgelopen acht jaar maar liefst dertig kwetsbaarheden hebben gevonden in het stemsysteem: geklooi met onbeveiligde USB-sticks, gebruik van verouderde versleuteling, geen wachtwoordenbeleid, onbeveiligde mail, etc. Controle achteraf is niet mogelijk, want de papieren stembiljetten worden zomaar vernietigd. Hij heeft het allemaal voorbij zien komen op YouTube en alles steeds gemeld bij de overheid, maar niemand wilde naar hem luisteren… Wat we volgens Ruwhof zouden moeten doen, is al deze kwetsbaarheden oplossen en de stembiljetten bewaren om na de eerste telling een audit te doen of alles wel klopt. Elke gemeente moet die resultaten publiceren.

De zaal lijkt in eerste instantie wel onder de indruk van zijn vlammende betoog voor eerlijke democratie. Totdat iemand de microfoon grijpt en rustig uitlegt dat wat Sijmen voorstelt allang gebeurt. Het is Jeroen van der Ham van het NCSC, die we later in dit boek nog tegenkomen. Hij vertelt dat hij vrijwilliger is bij een stembureau en raadt Sijmen aan zich ook aan te melden. Jeroen: "Kun je nog eens wat van leren." Die kwetsbaarheden die Sijmen op YouTube zag, zijn namelijk allemaal opgelost, zo ook de papieren hertelling en rapportage per gemeente. Jeroen blijkt niet de enige

te zijn en de een na de andere stembureauvrijwilliger staat op om Sijmens verhaal onderuit te halen.

Wat ook niet uit de verf komt, zijn de twee Tesla's, die al in de media werden aangekondigd als interessante target. Als ik niks op het programma vind, loop ik maar even naar het Italiaanse kamp waar de twee zwarte bolides staan te blinken in de zon. Ik zie veel mensen eromheen lopen, uit de koplamp hangt een draadje met printplaat, maar eigenlijk gebeurt er niks. Ik vraag de eigenaar of er al kwetsbaarheden zijn gevonden. Nee, daar hebben ze eigenlijk geen tijd voor gehad, want ze zijn vooral pasta aan het eten en aan het feesten. Ik probeer er toch nog wat van te maken en opper dat, terwijl alle anderen hun auto ver buiten het terrein op een betaalde plek moeten parkeren, hij hier als enige gratis naast zijn tent kan staan. Dan heb je dus eigenlijk het parkeersysteem gehackt, of niet? Ja, dat is eigenlijk wel het geval, moet hij lachend bekennen.

De grootste flop was wellicht een van mezelf. Ik had namelijk toegezegd een sessie te leiden om 10.00 uur in de ochtend. Ik word die dag echter pas om 11.15 uur wakker, met een telefoon vol gemiste oproepen. Tsja, dat krijg je als je elke avond van 22.00-23.00 uur een radioprogramma draait, niet uitgepraat raakt met hackers en vervolgens nog om 3.00 uur staat te barbecueën met bekende Nederlandse hackers… Oeps. Ik waggel vervolgens naar de tent en tref daar een man of tien die naar een niet te lezen scherm zit te kijken. Nee, mijn hulp is niet meer nodig. Sorry.

Flops zijn onvermijdelijk als je als organisatie openstaat voor de wat minder voor de hand liggende sprekers. Dat kan verkeerd gaan, maar soms juist heel goed uitpakken. Hier de flips, oftewel de sprekers waarvan je eerst denkt 'wtf is dit nou?' en die vervolgens juist erg cool blijken te zijn. Wie Matt Westcott heeft gezien, begrijpt wat ik hiermee bedoel. Op het programma: 'Zero to chiptune in one hour'. Hij vraagt het publiek om een bekend deuntje te noemen. Iemand roept: "The Archers". Matt gaat aan de slag en tweakt een uur lang hexadecimale codes op zijn ZX Spectrum, een pc van begin jaren tachtig. Dan denk je: saai. Maar nee, het is een prachtig display van uber nerdiness en bij elke aangepaste versie van het deuntje juicht het publiek harder. Mocht je hiervan de video niet willen zien, dan is het eindresultaat te beluisteren op Soundcloud.

Het ‘wtf-gehalte’ bereikt een hoogtepunt bij de lezing ‘Dickpics for privacy’ van Anus en Ranzbak. Deze van Twitter bekende internettrollen hebben op SHA ook een praatprogramma, DeFeest, elke avond voorafgaand aan het mijne, dus ik heb mogen genieten van hun ultramelige improvisaties. De titel van hun lezing doet het ergste vermoeden. Ze hadden de lezing eigenlijk ingestuurd als grap, maar tot hun stomme verbazing werd het voorstel gehonoreerd. Nu moeten ze wel.

Wat krijgen we te zien? Penissen verkleed als bekendheden. Vooral die van Trump is treffend. Kunst met penissen. Pogingen van mannen om hun penis zo te fotoshoppen dat die door de dickfilters komen. Maar ook voorstellen om penissen als biometrisch identificatiemiddel te gebruiken, bijvoorbeeld bij betalingen. En als iedereen zijn dickpic op zijn smartphone heeft, dan letten we wel wat beter op met wie we zomaar data delen. Wel jammer dat deze innovaties alleen opgaan voor een helft van de bevolking. Maar het moet gezegd worden: deze heren wisten toch op zeer vermakelijke wijze een uur vol te lullen.

Flippen is op SHA ook een serieuze aangelegenheid. Bits flippen welteverstaan, oftewel met spanningsschommelingen, magnetisme, warmte of andere invloeden van buitenaf enen en nullen omzetten. Ramiro Pareja en Nils Wiersma zijn hier meester in en laten zien hoe ze besturingssystemen in auto’s kunnen beïnvloeden met pieken en dalen in de stroomtoevoer. Ze kunnen ook de score van een gokautomaat flink opschroeven met slechts de vonk van een Piëzo-elektrische aansteker. Simpel maar doeltreffend.

Een stuk geavanceerdere flip is de ‘Flip Feng Shui’ van Victor van der Veen en Kaveh Razavi. Wat zij doen, vergt een hoofdstuk op zich, maar kort gezegd komt het erop neer dat ze bits die dicht bij elkaar liggen op de chip, elkaar kunnen laten flippen. ‘Rowhammering’ heet dat. Deze kwetsbaarheid is alleen op te lossen door de schakelingen op chips verder van elkaar te zetten, maar, zoals we weten, worden ze juist steeds dichter op elkaar gezet om in de pas te blijven lopen met Moore’s Law… Niet te fixen dus. Ook hierbij denk je: WTF!

Tot slot de sprekers die niet de zaal plat kregen, flopten of flipten, maar elk op hun eigen manier bijzonder zijn. Zo betreedt Loek Gijben voor zijn

lezing ‘The human body as an electric input-output system’ het podium met allerlei sensoren op zijn lijf en hoofd. Best lef, want we zien live hoe zijn hersengolven pieken en zijn huid geleidt op momenten dat hij nerveus wordt. Wat kun je hier nog meer mee? Een leugendetector maken, een voertuig besturen of deep brain stimulationtherapie? Of wat te denken van schrijver Arnon Grunberg, die zijn lezers wil laten raden wat hij schrijft op basis van de meetbare activiteit in zijn hersenen? Nee, dat is allemaal flauwekul volgens Loek, want die signalen zeggen niet zoveel. En al die pieken op zijn eigen livescan? Dat is vooral interferentie van de omgeving… Wellicht teleurstellend, maar zeker nuttig om ook wat mythes te ontkrachten. Dat was ook zijn opzet.

In de categorie ontnuchterende praatjes valt ook Erica Portnoy met: ‘My safe in your house. Keeping secrets on remote machines’. Ze opent met de bekende zin: “There is no cloud, it’s just someone else’s computer”. OK, dus moet je je bestanden daar versleuteld opslaan. Echter, kun je ze dan nog wel doorzoeken? Je zou een index kunnen maken van trefwoorden die je versleutelt met een zogenoemde ‘one-way hash function’. Die hashwaarde kun je dan op afstand uitlezen en weer ontsleutelen. Ze geeft een demo. We zoeken op een trefwoord, dat wordt versleuteld tot het hexadecimale getal ‘A5876’, dat ergens staat in 220 files. Daar kan een aanvaller echter frequentieanalyse op loslaten en alsnog raden waar je naar zoekt, of op zijn minst zien waar blijkbaar interessante informatie staat. En zo heeft ze nog wat andere ingewikkelde technieken in petto, met als slotconclusie: nee, kan niet. Ook al versleutel je je bestanden in de cloud, je zoekgedrag geeft al van alles prijs.

Even onverminderd strijdbaar is Christopher Clay, met ‘Lets stop EU-copyright’. Hij begint met een opsomming van aankomende EU-regulering die best heel strikt is: blogs mogen niet onbetaald doorlinken naar nieuwssites, worden hierop automatisch gescand en zo nodig geblokkeerd. De grote Google en Facebook ontspringen de dans, omdat ze te machtig zijn. Zullen de Members of European Parliament (MEP) instemmen met de wetten? Waarschijnlijk wel, want ze weten maar half wat de gevolgen zijn en laten zich beïnvloeden door de machtige lobby. Daarom moeten wij als burgers onze MEP’s hierop aanspreken. Hoe? Volgens Clay kun je ze het beste gewoon bellen. Dat doet hij zelf ook weleens en het blijkt dat je dan

werkelijk de MEP aan de lijn krijgt. Er is nu zelfs een tool voor: de MEP-roulette van Bits of Freedom, waar je dus random een MEP krijgt met nummer.

Hoop voor de toekomst krijgen we vooral van onze jongste spreker: Jurre Groenendijk. Deze 15-jarige hacker is in het nationale nieuws gekomen omdat hij zijn school had gehackt. Met toestemming en resultaat. Ja, hij zou zijn cijfers kunnen aanpassen, maar doet dat niet en hij wil ook niet uitleggen hoe dat zou kunnen. Dat is zijn erecode. Wat hij wel wil laten zien, is hoe hij de schoolkluisjes kan hacken, door met een Arduino, vermomd als lunchbox, ID-kaarten van anderen af te luisteren. Daar zou hij behoorlijk foute grappen mee uit kunnen halen, maar in plaats daarvan heeft hij netjes een rapport opgesteld voor de school om het te fixen en kreeg hiervoor veel dank en bioscoopbonnen. Zo kan het dus ook. De bijdrage van Jurre was vooral een les in responsible disclosure aan de oudere hackers die wel geneigd zijn kwetsbaarheden onverantwoord te onthullen.

Dit overzicht is uiteraard subjectief en selectief, want met driehonderd lezingen mis je meer dan je ziet. Maar goed, als ik terugkijk op SHA en me afvraag welke sprekers uiteindelijk de meeste indruk hebben gemaakt, kom ik uit bij de mensen van de organisatie zelf, die naast hun zware taak als teamlid, ondanks chronisch slaaptekort, ook nog lezingen geven. Brenno de Winter houdt naast zijn verantwoordelijke taak als havenmeester een presentatie over de Titanic als metafoor voor het falen van security. Jeroen van der Ham heeft de academische track onder zijn hoede, moet vechten tegen vooroordelen van hackers tegenover het NCSC en houdt een presentatie over ethiek en een over responsible disclosure. Oscar Koeroo is dag en nacht in de weer met het Productiehuis om alle video's goed te krijgen en geeft en passant een presentatie over cryptografie.

Het mooiste moment is als in de namiddag van 8 augustus onze coreorga's Attilla en Elger, samen met de andere Team Leads en Angels, afsluiten. Elk team geeft een review. Team Bar over hoeveel er gedronken is. Team Content over al het videomateriaal dat terug is te zien. Team NOC van het Network Operations Center over hoeveel dataverkeer er is geweest en hoe het lokaal opgezette netwerk ondanks de zware belasting goed bleef presteren. Dit team had maar één vervelende bug: iemand heeft op een van

de netwerkkabels die in het gras lag gepoept, wat geïllustreerd wordt met een foto.

Het NOC laat zien dat de SHA-badge een succes is. Hij werd zoveel gebruikt dat volgens hun netwerkmonitor de wififrequentie 2,4 GHz meer gebruikt werd dan de gebruikelijke 5 GHz voor telefoons en laptops. Op nummer 1 van de lijst meest gebruikte besturingssystemen staat niet Android of iOS, maar het Micro Python waar de processor van de badge op draait. Geen hackerskamp heeft ooit zo'n awesome badge gehad, waarmee SHA2017 een nieuwe standaard heeft gezet.

Na al deze technische hoeraverhalen moeten ze er dan uiteindelijk toch een einde aan breien. Daar is blijkbaar niet erg over nagedacht, want Elger en Attilla zoeken naar woorden om iedereen die zich heeft ingezet te bedanken. Het blijken er te veel te zijn. Kom dan maar allemaal op het podium, zodat we samen afscheid kunnen nemen. Het podium stroomt vol met hackers, meer dan honderd. De een staat verlegen aan de kant, de ander in het midden te juichen. Ik zie Brenno zelfs tranen wegpinken. Het is een collectieve ontlading van een groep mensen die gewoonlijk geen groepsmensen zijn, maar nu, op dit feest wel.

De hossende massa op het podium komt enigszins tot stilstand en enkele mensen lijken al te vertrekken als Elger ons nog herinnert aan een belofte die we allemaal hebben gedaan. Bij het vorige kamp, OHM2013, verliet iedereen plots het terrein en bleven zij achter met de troep. Typisch hackers: goed in dingen opzetten, maar slecht in afronden. Dat moet nu anders. Te beginnen met deze zaal: "Pak allemaal je eigen stoel en zet die op de stapel. Kijk daarna waar je nog kunt helpen, zodat we dit prachtige kamp ook samen afbreken. The teardown starts here and now!"

De tent is in no-time leeg, dus loop ik nog een keer langs de Angel Desk of er nog taken openstaan. Omdat ik me redelijk verwend voel als radiopresentator zeg ik tegen de vrouw aan de balie: "Doe mij maar een of ander klusje dat niemand anders wil doen". Ze lijkt mijn vraag heel gewoon te vinden en zegt: "Loop maar met hem mee", terwijl ze wijst naar een jongen van nog geen twintig. Hij en ik springen op een golfkarretje met een grote opgeblazen eenhoorn erop. Nog een jonge knul komt erbij met een grote rol vuilniszakken. We gaan de vuilnisbakken legen.

Overal op het terrein treffen we rolcontainers die overstromen van de plastic verpakkingen voor etenswaren en frisdranken, omringd door grote zwermen wespen. Ik voel me een hele held als ik er een stuk of tien weet te legen, zonder geprikt te worden en het afval naar de centrale afvalverwerking rijdt. Als ik de knullen vraag hoe lang ze al bezig zijn, antwoorden ze rustig: “De hele dag. Eigenlijk elke dag sinds het begin.” Ik reageer stomverbaasd: “He, jullie zijn jonge hackers, komen hier op een groot hackerevent waar van alles te beleven is en het enige wat jullie doen is vuilnis ophalen?!”

Zelf lijken de jonge hackers dit helemaal niet zo vreemd te vinden: “Hoezo, iemand moet het toch doen?”

Daarom vieren nerds de beste feestjes. Zoals we ook zullen zien bij onze Oosterburen, die het allemaal nog net wat groter en grondiger aanpakken.

7. Grondig georganiseerde chaos

Mijn eerste ervaring met het zelforganiserende vermogen van de hackerscene waren de zogenoemde whiskyleaks. Het was in de tijd dat er veel vertrouwelijke overheidsgegevens werden gelekt via Wikileaks. Begin 2011 besluit een groep wat oudere hackers die graag een goede whisky drinken, een avondje te organiseren waarop iedereen geheimen kan delen. De omgangscode is volgens de Chatham House Rule, oftewel je kunt achteraf doorvertellen wat je hebt gehoord, maar niet van wie. Anders dan het Britse Chatham House, waar deze regel naar is vernoemd, is hier geen centrale organisatie. Het begon op Twitter en zo werkt het nog steeds.

De meeste hackers zitten op Twitter. Dat zou je misschien niet zo snel verwachten omdat iedereen alles kan meelezen, maar dat vinden de meesten juist leuk. Sommigen twitteren onder pseudoniem, omdat ze hun meningen niet vanuit hun professionele werk willen geven, bang zijn vervolgd te worden voor iets wat ze beter niet hadden kunnen doen, ze het leuk vinden om te trollen of gewoon omdat een nickname er nu eenmaal bij hoort. Toch zie je de meesten gewoon met hun echte naam erbij. Dat maakt het makkelijker om elkaar te volgen.

Om de zoveel tijd tweet iemand: “Tijd voor weer een #whiskyleaks” en als er genoeg animo is, dan start iemand een online lijstje waarop je kunt invullen waar en wanneer je aanwezig kunt zijn. Met de meeste stemmen gelden, rolt er dan een dag en locatie uit en komen er tussen de twintig en vijftig hackers samen. Dat kan in een kroeg zijn, bij iemand thuis of op kantoor, maar ook weleens in een oude bunker. Tijdens grote hackercongressen is er ook vaak een whiskyleaks. Overigens drinken jonge hackers meestal niet en lusten ze al helemaal geen whisky. Die hebben daarom hun eigen variant: #fristileaks. Via die leaks heb ik veel van de

hackers beter leren kennen en aardig wat verhalen verzameld voor mijn vorige boek.

Op een van deze leaks, in september 2016, waarop al druk wordt gesproken over de voorbereidingen van SHA2017, ontmoet ik een Duitse hacker van ongeveer mijn leeftijd. Hij moet ook naar Rotterdam en we reizen samen terug met de trein. Zijn nickname is Mc.Fly en hij vertelt me dat, als ik naar SHA wil, ik vooral eerst ook naar het congres van de Duitse Chaos Computer Club moet komen. Dat is elk jaar tussen kerst en oudjaar. Er komen vele duizenden hackers op af van over de hele wereld, er zijn goeie presentaties en workshops en ook daar is een whiskyleaks.

OK, stuur me maar een linkje. Nee, zo werkt dat niet. Je krijgt van iemand die zich al heeft ingeschreven een voucher in de vorm van een lange code. Die vul je in op de site, je betaalt het kaartje en krijgt dan zelf ook een code waarmee iemand anders zich kan inschrijven. Dat moet wel binnen 24 uur, anders vervalt de code en is de voucherketting verbroken. Waarom al dat geheimzinnige gedoe? Hackerevents zouden toch gewoon open moeten zijn voor iedereen? Hij vertelt dat de laatste keer dat er nog open inschrijving was, alle kaarten binnen 14 seconden waren uitverkocht.

Dit lijkt me een congres waar ik bij moet zijn. Ik heb sowieso een hekel aan kerst, dus dit is een mooi excuus om er tussenuit te knijpen. En zo denken er meer over, want dat jaar trekt de 33e editie van het Chaos Communication Congress maar liefst 12.000 bezoekers.

26 december 2016 arriveer ik in Hamburg. Ik heb gelukkig nog een hotel kunnen vinden op loopafstand van het congres, want ik vermoed dat de komende dagen niet echt volgens de gebruikelijke ov-tijden zullen verlopen. Het congres begint morgen pas, maar je kunt wel alvast je polsbandje ophalen. Dat scheelt tijd. Als ik daar aankom, zie ik een groot oud grijs, typisch Duits, congresgebouw. Ervoor staat een kleurrijke raket, die rechtstreeks uit een cartoon lijkt te komen. Een zwerm van zwartgeklede mannen met rugzakken stroomt naar binnen, onder de letters 33c3. Het thema dit jaar: ‘Works for me’.

Bij binnenkomst wordt mijn ticket gescand en krijg ik een polsbandje om. Om me heen zie ik, naast de gebruikelijke nerds, ook veel punkers, anarchisten, transgenders, hippies en ander artistiek uitgedost volk. Wat ook

opvalt is dat er gezinnetjes rondlopen. Volgens Wikipedia beschrijft de Chaos Computer Club (CCC) zichzelf als ‘a galactic community of life forms, independent of age, sex, race or societal orientation, which strives across borders for freedom of information’. Dit is duidelijk geen cybersecurity congres, maar meer de fysieke verschijningsvorm van het zelforganiserende vermogen van de Duitse hackers, kunstenaars, activisten en andere vrijdenkers. Ik heb een lijstje gemaakt van sprekers die ik wil zien, maar ben vooral benieuwd naar hoe ze hier chaos organiseren.

Ik stel mijn vraag aan een groepje vrijwilligers achter een bureautje met een bordje ‘Press’. Na wat bellen komt een man met baard en gothic shirt aangelopen. Hij heeft een oude Nokia in zijn handen en stelt zich voor: Falk Garbsch. In het dagelijks leven is hij softwareontwikkelaar bij een bedrijf voor mobiele technologie. Nu dus even niet, want hier is hij een van de vier woordvoerders namens de CCC. En ja, hij heeft ook enkele responsible disclosures op zijn naam.

Hij vertelt dat de vereniging inmiddels vijfduizend leden telt. Voorafgaand aan het congres sluiten ook andere, meer lokale verenigingen aan. Vooral hackerspaces en ook zij delen mee in de besluitvorming. Een klein kernteam doet de zakelijke dingen, zoals het gebouw en de financiën, en begint in de zomer al met de planning. De rest bestaat uit vrijwilligers die zo’n beetje vanaf de herfst alles onderling organiseren. Tijdens het congres melden zich nog meer vrijwilligers aan. Net als bij SHA, heten ze hier Angels, verdeeld over verschillende teams, met vergelijkbare namen. Falk noemt ze op.

Het NOC Team is wellicht het belangrijkste, want als een echt Network Operations Center houden deze vrijwilligers het zwaarbelaste netwerk in de lucht. Capaciteit: 180 Gbit/s, meer dan een gemiddelde Duitse universiteit en meer dan SHA. Hun planning start begin december, een week voor het evenement wordt het netwerk aangelegd en de dag na het evenement weer afgebroken. Het POC, Phone Operating Center, beheert het DECT-systeem: Digital Enhanced Cordless Telecommunications, dat vroeger gebruikt werd voor draadloze telefoons thuis of op kantoor. Het is dan wel verouderd, maar hier superhandig want het is stabiel en interfereert niet met de andere frequenties, zoals de wifi. Elke vrijwilliger kan een oude telefoon

meenemen, die hier instellen op DECT en elkaar bellen met slechts vier cijfers. Vandaar de oude Nokia van Falk.

Het LOG Team is wellicht het grootste, al zie je deze vrijwilligers nauwelijks. Zij zijn het Logistics Operations Center en zorgen achter de schermen ervoor dat alle spullen op hun plek komen. Niet alleen binnen het gebouw, maar ook alle objecten die van de Berlijnse thuisbasis van de CCC naar hier moeten. Team LOC doet de Lights and Electricity Operations, BOC de Bar Operations (150.000 flessen Club Mate in vijf dagen…) en VOC de video's en live-vertalingen.

Het inhoudelijke programma wordt vastgesteld door het Content Team. Sprekers hebben in totaal vijfhonderd voorstellen ingediend waar nog geen kwart van gehonoreerd kan worden. Om partijdigheid te voorkomen, moeten al deze voorstellen door meerdere teamleden bekeken worden. Best veel werk. Het Content Team heeft overigens om begrijpelijke redenen de analogie met Operating Center niet overgenomen. Dat brengt ons bij het laatste team: het Awareness Team. Zij waken over gender, ethnicity en Lesbian Gay Transgender Bi-issues. Of beter gezegd, zij benadrukken dat het niet uitmaakt wat je geaardheid is, welke kleur je hebt, man of vrouw bent, of ergens tussenin. Ze hebben er bijvoorbeeld voor gezorgd dat alle toiletten uniseks zijn.

Dit klinkt erg georganiseerd, maar omdat het zo'n grote groep vrijwilligers is, loopt het volgens Falk toch elk jaar weer anders. Hoe chaos zichzelf organiseert, is nog het beste te zien bij de zogenoemde Assemblies. Dat is een enorme hal met meer dan honderd grote tafels waar iedereen aan een project kan werken. Falk vertelt dat de plekken meestal worden aangevraagd door hackerspaces, maar er zijn ook makers die elkaar alleen op het congres zien, meestal rondom een bepaald project. In wezen kan iedere groep een tafel reserveren, als zij zich maar uiterlijk de dag voor het congres melden, anders gaat de tafel naar een andere groep.

Waarom is dit congres tussen kerst en oud & nieuw? Volgens Falk is dat vooral om mensen te trekken die echt gedreven zijn door de inhoud. Bezoekers die dit congres zien als 'business opportunity' blijven weg. Het is ook om aan het einde van het jaar terug te blikken, samen met mensen met wie je normaal veel online contact hebt en met wie je nu eens face to face, off the record, actuele kennis deelt uit de hackerscene. Ik vraag hem

voorzichtig: “Kerstvakantie breng je normaal door met je familie. Zijn jullie ook een soort familie?” Hij lacht: “Ja, dat klopt eigenlijk wel.”

Ik meld me aan als Angel, maar al snel blijkt dat ‘Heaven’ al genoeg vrijwilligers heeft geregistreerd: vijfduizend in totaal. Wel kan ik naar de angelmeetings om te kijken hoe dat eraan toegaat. In een achterafzaaltje zie ik ongeveer honderd goedbedoelende bezoekers in afwachting van instructies van vier teamleiders: twee typische computernerds, een vrouw met lang zwart haar en een man met een tijgermuts. De nerds informeren of het boekingssysteem met klusjes werkt. Ja, al zijn er niet genoeg klusjes voor iedereen. Ze hadden ook niet verwacht dat er zoveel Angels zouden zijn.

De vrouw blijkt van het Awareness Team te zijn en benadrukt dat iedereen vooral aardig moet zijn voor elkaar. Niet dat er incidenten zijn geweest, het gaat vooral om bewustwording. De tijgermuts blijkt de toegang tot het Angelsysteem te beheren en meldt dat, gezien de hoge opkomst, de beloningen in dinervouchers worden gehalveerd. Een van de Angels vraagt: “Geldt dat ook voor de nachtdiensten?” Ja. Ook dat blijkt geen probleem. De bezoekers willen blijkbaar graag wat doen voor het congres. Wel belooft hij dat ze tussen 2.00 en 6.00 uur extra Club Mate krijgen om wakker te blijven. Hij sluit af met de oproep vooral ook na het congres te blijven om te helpen met opruimen, want dat is echt erg cool. En oh ja, of er nog iemand goed is in SQL, want het boekingssysteem is weer vastgelopen…

Op 27 december 2016 gaat het 33e Chaos Communication Congress officieel van start. In een enorme zaal met naar schatting achtduizend mensen nemen een vrouw en een man in zwart CCC-shirt om en om het woord. Ze leggen de spelregels uit voor de komende dagen, die er vooral op neerkomen dat iedereen aardig moet zijn voor elkaar. Niet dat dat nodig is. Sterker nog, ze besluiten met tips om een ‘post-congress depression’ te voorkomen. Ze weten uit ervaring dat na zo’n week met gelijkgestemden de confrontatie met de harde buitenwereld zwaar valt. Probeer daarom de geest van het congres vast te houden en ook aardig te zijn tegen mensen buiten het congres. Ze besluiten met het thema: ‘works for me’. Achter hen staat de TARDIS, de telefooncel waarmee Doctor Who door tijd en ruimte reist.

Na een eerste dag van veel lezingen en bijzondere ontmoetingen, ontdek ik een achterafzaal, waar een houseparty gaande is. Er wordt stevig gedronken, hier en daar geblowd en flink gedanst. Een ventilator blaast nepgeld het publiek in en overal wordt druk gepraat. Als ik pas om 6.00 uur aftaai, zie ik dat er nog steeds makers aan de assemblytafels bezig zijn hun apparaten aan de praat te krijgen. Wat een gedrevenheid!

De volgende dag zwerf ik enigszins brak door de gangen. Al komt dit allemaal heel gemoedelijk over, ik heb me voorgenomen geen risico's te nemen te midden van al die hackers. Ik heb een gloednieuwe laptop bij me die ik na de congresdagen zal schoonvegen. Mijn telefoon staat op vliegtuigmodus. Lichtelijk paranoïde durf ik niet eens via een VPN op de wifi. Mijn mail en Twitter checken heb ik steeds in het hotel gedaan. Maar ja, ik wil heel graag weten of er nog programmawijzigingen zijn.

In de wandelgangen kom ik iemand van het NCSC tegen. Ik loop met hem mee een zaal in waar de lezing nog moet beginnen en vraag hem of ik de wifi '33c3' kan vertrouwen. Hij checkt voor mij met zijn telefoon de certificaten. Die kloppen volgens hem, maar hij verzekert me dat je nooit helemaal zeker kunt zijn. Ik bedank hem, zet de wifi op mijn telefoon aan en zie een inlogscherm. Als ik hem vraag welke gebruikersnaam ik kan gebruiken en wat het wachtwoord is, moet hij enorm lachen: "Je kunt van alles invullen". Ach natuurlijk, zo creëert iedereen een eigen unieke sleutel! Maximale entropie. Ik meld me aan als 'eidjejfaxfdeffkxnk' met wachtwoord 'xskjfnndsjfdcak' en besluit elke keer een andere willekeurige toetsencombinatie in te typen. Works for me.

Terwijl ik wat lieve berichtjes van mijn vriendin binnenkrijg, realiseer ik me dat ik ben aanbeland bij een sessie over wifi-hacking. Dus log ik snel weer uit. Mathy Verhoef vertelt tegenover een volle zaal over WPA2-attacks en reconstrueert minutieus de handshake die je telefoon of laptop uitwisselt met de router. Daar waar entropie wordt verondersteld, blijkt volgens hem het aantal te raden sleutels klein genoeg om die met zijn laptop in vier minuten te kraken. Hm, entropie. Ik gok dat ik als 'eidjejfaxfdeffkxnk' me niet al te veel zorgen hoef te maken, log in met weer een andere willekeurige reeks tekens en app tijdens zijn demo mijn vriendin terug dat alles hier goed gaat.

Op weg naar de volgende lezing tref ik in een hoekje achteraf op wat oude kussens een hacker van de Nederlandse veiligheidsdiensten. Hij zit daar met een schoongeveegde laptop en klaagt dat het dit jaar wel erg moeilijk was voor hem om een kaartje te bemachtigen. En dat er dit jaar niet echt schokkende onthullingen op het programma staan. “Vroeger was CCC de plek waar je je onthullingen deed. Nu weten hackers steeds makkelijker de media te vinden. Kwetsbaarheden krijgen nu ook meteen een mooie naam en logo. Mensen staan er meer voor open. Op zich wel een goede zaak, want zo worden ze eerder gefixt.”

Hij blijkt zelf nog wat kwetsbaarheden te hebben gevonden en laat ze zien: een waarmee hij in een betaalsysteem van een vereniging kan inbreken en een andere waarmee hij iemands locatie kan achterhalen. Ik vraag hem of die kwetsbaarheden wellicht ook interessant zijn voor zijn werkgever. Nee, verzekert hij me, die worden gemeld bij de eigenaar van het systeem. Te midden van deze georganiseerde chaos tegen de gevestigde orde handelt hij volledig in de geest van de CCC.

Naast dat ik wil weten hoe chaos wordt georganiseerd, ben ik hier ook om onthullingen te registreren. Volgens de Hollandse staatshacker zijn die er nu dus niet meer zoveel als vroeger, maar als ik het programma goed doorloop, vind ik er toch nog een paar. Er blijken aardig wat hackers los te gaan op het veel gehypte Internet of Things. Zo laat Netanel Rubin zien dat veel slimme meters zwakke encryptie hebben. Hij kan ze vanaf straat hacken en zou er zelfs iemands huis mee kunnen opblazen. Dat laatste lijkt me wellicht wat vergezocht, maar hij trekt daarmee wel de aandacht van de internationale pers.

Matt Knight, een zendradiofanaat, demonstreert hoe hij afgevangen LoRa-signalen weet te ontcijferen. Dat zijn de Long Range radiosignalen voor allerhande sensortechnologieën. Dat is voor ons best alarmerend, omdat KPN net landelijke dekking aan het uitrollen is voor LoRaWAN en het Nederlandse The Things Network op dat moment de wereld verovert met deze technologie. De lange afstand is mogelijk vanwege de lage frequentie, maar daardoor kun je ook maar weinig data heen en weer sturen. Dat kun je dus afvangen, maar de vraag is hoe interessant die data dan is.

Boeiend is de presentatie van ene ‘Ray’: ‘Lockpicking the IoT’. Dat doet hij letterlijk, want hij heeft namelijk de Noke, een fysiek slot met Bluetooth, gekraakt. Eerlijk gezegd dringt deze technische presentatie in eerste instantie niet helemaal tot me door, omdat het inmiddels al 22.00 uur is. Totdat de volledige zaal van vierduizend man ineens in geklap en gejuich uitbarst bij een slide met een code. Erboven staat: “So here is the 0-day.” Daarna volgt een lowtechversie van zijn hack: gewoon met een magneetje over het slot rollen tot het opengaat. That works for me…

Softwarehacks zijn er natuurlijk ook volop. Zoals die van drie jongens van nog geen twintig jaar, die om en om in een monotone computerstem stap voor stap uitleggen hoe ze de Nintendo Wii kunnen laten doen wat ze willen. Met ‘arbitrary code execution’, oftewel een computer willekeurige commando’s geven terwijl die net wat aan het uitvoeren is, laten ze het ding net zo lang opstarten en verstoren tot ze de sleutels krijgen. Een van hen weet zelfs de code uit te voeren via een geluidsbestand en doopt zijn techniek ‘soundhax’. Al met al hebben ze acht bugs gevonden. Die zijn niet alleen gefixt, maar Nintendo heeft sindsdien ook een bug-bountyprogramma opgezet. Works for them.

Karsten Nohl, die ik een halfjaar geleden in Amsterdam mocht interviewen tijdens de EU-meeting over coordinated vulnerability disclosure, laat op het grote podium zien hoe slecht het Passenger Name Record van vliegmaatschappijen beveiligd is. De zes tekens die elke reiziger voor zijn reis krijgt toegekend, zijn verre van willekeurig en makkelijk te raden. Met een willekeurige code kun je meestal al in het systeem om te kijken waar iemand naartoe gaat, zijn bestemming aanpassen of Airmiles afsnoepen. Specifieke personen kun je targetten met de code van hun bagagelabel. Er zijn steeds meer mensen die een selfie posten met hun ticket, uiteraard voorzien van die code. Dit verhaal wordt opgepakt in de media buiten het congres.

Naast de vele nieuwe hacks valt op dat er op dit congres veel politiek gekleurde presentaties zijn, vooral tegen Amerika. Op dat moment heeft Trump tot ieders verbazing net het Witte Huis overgenomen en zien we zijn rare hoofd vaak terugkomen op het scherm. Ongeloof overheerst. Is er wellicht geknoeid met de Amerikaanse stemmachines? Matt Bernhard en

Alex Halderman laten in hun bijdrage zien dat dat zeer waarschijnlijk is, maar moeilijk te bewijzen.

Eerst laten ze zien hoeveel verschillende vormen van elektronisch stemmen er afgelopen november tijdens de Amerikaanse presidentsverkiezingen zijn gebruikt: papieren stembiljetten die optisch worden ingelezen, verschillende elektronische stemkastjes en stemmen via internet. De meeste van deze stemmethodes zijn makkelijk te hacken: man-in-the-middle attacks via slecht beveiligde verbindingen, updates die vanaf een slecht beveiligde leverancier worden uitgevoerd of zelfs stemkastjes waarvan je de geheugenkaart kunt verwisselen. Ze hebben zelfs van een van de stemmachines een pacman-spelletje gemaakt…

Maar eigenlijk wisten de bezoekers dat al. Spannend is vooral hun zoektocht naar het aantonen van eventuele stemfraude. Je krijgt niet zomaar de stembiljetten of papieren back-up. Daar moet eerst een van de kandidaten protest voor aantekenen. Hillary Clinton durfde daar haar vingers niet aan te branden, maar er bleek nog een derde kandidaat te zijn: Gill Stein van de Green Party. Die kreeg weliswaar nog niet één procent van de stemmen, maar wilde wel protest aantekenen en een crowdfundingactie starten. Daarmee haalde ze negen miljoen dollar binnen en het project kon worden uitgevoerd.

Het onderzoeksteam richtte zich op de staten Wisconsin, Michigan en Pennsylvania, want die zouden het verschil hebben gemaakt. Echter, na veel juridisch getouwtrek, tegenwerkingen en speuren naar verloren stembiljetten, heeft geen van deze staten een hertelling kunnen doen. Kortom, de hack was technisch mogelijk, maar is nu niet meer aan te tonen. Dat is hoe het Amerikaanse stemproces werkt en de enige die dat kan aanpassen om dergelijke toestanden in de toekomst te voorkomen, is de huidige president…

Naast deze kritische onderzoekers staat er ook een echte Amerikaanse soldaat op het programma: Cian Westmoreland met ‘The Global Assassination Grid’. De jonge Amerikaanse netwerkspecialist is ooit bij het leger gegaan omdat hij mensen over de hele wereld wilde bevrijden, maar zag zich gaandeweg onderdeel worden van een gewetenloze moordmachine. Westmoreland verzorgde namelijk jarenlang de communicatie tussen drones, air command en intelligence centers.

Een van die centers staat in Duitsland, op de militaire luchthaven Ramstein. Daarom is hij aanwezig tijdens het Chaos Communication Congress, om ons te wijzen op onze medeplichtigheid. Hij had echter geen zaal met achtduizend mensen verwacht en prevelt: “Wow, I didn’t know the room was so big.” Om het ijs te breken, probeert hij voorzichtig “Anyone knows Snowden?” Ja natuurlijk, die stond een paar jaar geleden op ditzelfde podium en belt straks nog even in…

Net als Snowden is Westmoreland een techneut met een maatschappelijke missie. En hij is een klokkenluider. Na een korte intro van de techniek achter het communicatienetwerk beschrijft hij de besluitvorming voorafgaande aan de aanval: “With drones, killing is a shared decision: a Signal Analyst or Geospacial Analyst only looks at the data. There are translators in between, while a Mission Intelligence Coordinator integrates the whole, after which a pilot makes the final kill decision, while sensor operators guide the missile.”

Door deze taakverdeling neemt elk een deelbeslissing en voelt geen van de betrokkenen zich verantwoordelijk. Het probleem is volgens hem dat er geen overzicht en nauwelijks toezicht is. Missies worden geleid door de CIA, Joint Special Operations Command (JSOC) of een bedrijf dat het uitvoert. Hoe de lijst met targets tot stand komt en welke algoritmen eraan te pas komen, is geheim. En het gaat regelmatig fout, want volgens hem zijn er vele onschuldige burgers op deze manier vermoord. Met medewerking van landen, zoals Duitsland, die niet eens officieel in oorlog zijn met het land waar de aanvallen plaatsvinden…

We zijn op dit congres collectief verontwaardigd over de komst van de nieuwe president, maar volgens Westmoreland is Obama ook geen lieverdje. Die heeft namelijk het droneprogramma flink uitgebreid. Onder het mom van ‘clean kill’ zijn er, volgens Obama, bij alle missies tezamen zo’n 161 onschuldige slachtoffers gevallen. NGO’s ter plaatse schatten het aantal slachtoffers echter op vele duizenden. De jonge soldaat is zichtbaar ontdaan over de vele onschuldige slachtoffers en roept: “If you have a problem with someone, you should tell him in the face. At least you can talk, perhaps de-escalate. With drones you are telling them: fuck you, you need to die.” Hij is daarom gestopt met zijn werk bij de Amerikaanse defensie en zet zich nu in als vrijwilliger om nabestaanden van

droneslachtoffers te helpen. Intussen wordt hij continu lastiggevallen door de Amerikaanse veiligheidsdiensten.

Hackers en veiligheidsdiensten blijven toch altijd een haatliefdeverhouding houden. De beste codemakers en -brekers werken graag bij de diensten, omdat ze daar een maatschappelijke bijdrage kunnen leveren en kunnen beschikken over de beste middelen en mensen. Tegelijkertijd weten ze dat hun werkgever diezelfde middelen maar al te vaak zal inzetten om onschuldige burgers overmatig in de gaten te houden of beveiligingen in systemen bewust te verzwakken. Wat te doen? Join them or beat them?

Hier op CCC zien we vooral activistische sprekers die kritisch zijn op de veiligheidsdiensten. Zoals Kurt Opsahl van de Electronic Frontier Foundation. Hij begint zijn bijdrage ‘The fight for encryption’ met een interessante constatering: “We moved from a debate on privacy vs security to security vs security.” En inderdaad: als het gaat om veiligheid verliest privacy het altijd. Maar wat nu als de veiligheidsmaatregelen van de overheid juist diezelfde burgers in gevaar brengen?

Dat is vooral te zien in de discussie over achterdeurtjes. Zodra overheden sleutels afdwingen bij bedrijven, kunnen die altijd in verkeerde handen vallen. Elke achterdeur kan uiteindelijk ook door criminelen worden gebruikt. Aan politici is dat volgens Opsahl moeilijk uit te leggen. Tim Cook van Apple deed nog een dappere poging, door de FBI uit te leggen dat zij hun klanten willen beschermen door geen achterdeur in te bouwen. Illustratief is Trumps reactie hierop: “Who the hell do you think you are?” De positie van de beoogde CIA-chief Mike Pompeo is ook weinig hoopgevend. Die zou van mening zijn dat “The use of encryption may be a red flag in itself.”

Volgens Opsahl moeten we ons niet veilig wanen omdat we in Europa zitten. Ook hier willen overheden achterdeurtjes. Als enige positieve uitzondering noemt hij Nederland, waar het parlement zich juist duidelijk heeft uitgesproken tegen het verzwakken van encryptie om veiligheidsdoelen. Tegelijkertijd wordt wel gesteld dat kwetsbaarheden benut mogen worden door de veiligheidsdiensten en nu ook de politie, mits ze die later wel bekendmaken, maar dat terzijde. Opsahl ziet de toekomst

van Europa somber in. De opkomende rechtspopulistische leiders zullen het Amerikaanse voorbeeld volgen en encryptie zien als een rode vlag.

We kunnen deze tendens volgens Opsahl maar op één manier keren: “If everybody uses encryption, it becomes less of a red flag.” Een van de initiatieven die daar werk van maken is Let’s Encrypt, een platform waar een groot aantal bedrijven en onderzoeksinstellingen samenwerken om open en vrij certificaten te delen. Zij hebben nu 21 miljoen sites voorzien van certificaten. Ook hoopgevend is dat internetters momenteel twee derde van hun tijd besteden op HTTPS-sites.

Maar de CCC zou geen echte hackersconferentie zijn, als de strijd tegen de grote machten niet ook met ludieke en artistieke middelen wordt gevoerd. Bij Digital Courage kan iedereen een ‘Lichtbildausweis’ laten maken, oftewel een ID-kaart waarvoor je zelf gegevens aanlevert. Ik heb er ook een laten maken, van ene Hans Acker, oftewel H.Acker. Journalist Brenno de Winter is met zijn Lichtbildausweis het Nederlandse Parlementsgebouw binnengekomen, om aan te tonen dat de veiligheidsmensen daar toch wel wat te goedgelovig zijn.

Bij kunstenaar Adam Harvey kun je ‘Hyperface’-prints krijgen. Dat zijn patronen op kleding die door beveiligingscamera’s gezien worden als heel veel gezichten, waardoor ze overvoerd raken. Er is ook een Social Engineering Poetry Slam, voor methodes om elkaar geheimen te ontfutselen. En een flashmob van dertig gemaskerde bezoekers verstoort continu de orde door in de meeste creatieve formaties door de menigte te bewegen. Gewoon, om te laten zien dat het kan.

Hackers zijn volgens hun eigen definitie geen brekers, maar vooral onderzoekers die nieuwe mogelijkheden verkennen van technologie. Dat is te zien op het CCC. Het hele congrescentrum is volgestampt met kabels, laptops, printers, kunstwerken en objecten waarvan je maar moet raden wat het is. Als het congres bijna op zijn einde is, loop ik nog een keer door de Assembly Hall om een inventarisatie te maken. Aan een van de tafels tref ik iemand met een 3D-printer die alles maakt wat anderen hem opdragen. Op de tafel ernaast staat een oude matrixprinter bonnetjes uit te spugen. Elke tweet met de hashtag #33C3 wordt hier uitgeprint. De berg papier is volgens de maker een analoge vorm van dataretentie. Lock picking blijkt

nog steeds populair. Vooral onder de jongere deelnemers, die aan drie grote tafels vol ijzerwaren allerlei soorten sloten openmaken zonder sleutel.

De tafel van de Duitse hackerspace Binary Kitchen staat vol met oude kasten met draden en pluggen. Ze blijken een telefooncentrale te hebben ingericht voor oude veldtelefoons, maar dan wel, net als het internet, gebaseerd op het Domain Name System. De operator vertelt trots dat hij een analoog signaal, via de centrale, naar een gsm-mast heeft gekregen, die een Nokia-mobieltje belt die weer met een andere veldtelefoon in contact staat. “Trace that!”, roept hij enthousiast uit, terwijl hij hard aan de hendel draait en er aan de andere kant van de zaal een belletje klinkt.

Spielerei? Nee. Mocht het internet ooit platgaan, dan kunnen deze jongens ervoor zorgen dat we nog kunnen bellen. En muziek luisteren, want even verderop streamt een dj muziek vanachter een grote kast met dezelfde draden met pluggen. Net als de medewerkers in de oude telefooncentrales, zit hij druk verschillende draden in en uit te pluggen. Elke draad is een kanaal waar andere muziek te beluisteren is, het hele congres lang. Als ik hem vraag hoeveel luisteraars hij inmiddels heeft en wat ze van zijn muziek vinden, laat hij me op subtiele wijze weten dat dat een stomme vraag is: “Don’t know”. Waarom doet hij dit dan? Gewoon, omdat het kan!

De ultieme vintage communicatie op 33c3 is nog wel de Seidenstrasse: een systeem van vacuümbuizen waar capsules met boodschappen door worden gezogen. Net als vroeger bij de kledingwinkels van C&A. Deze groep makers komt hier elk jaar samen om het systeem te verfijnen. In een week tijd trekken ze een kilometer aan gele buizen door het pand. Een jongen met lang haar en laborantenjas laat me trots zien hoe ze al 3D-printend bij de juiste vorm capsule zijn uitgekomen. Die wordt door de buis geleid met een ledsignaal. Hij stuurt vanuit de centrale diverse routers aan om de capsule bij het juiste eindpunt te krijgen. Enthousiast vertelt hij dat de grootste uitdaging is de interferentie van de dimlichten uit het ledsignaal te filteren. Als ik hem vraag hoeveel boodschappen al bij de juiste ontvanger terecht zijn gekomen, reageert hij achteloos dat hen dat nog niet gelukt is. Wel klinkt er telkens applaus als er een van de capsules hoorbaar door de laaghangende buizen raast. Bij 33c3 gaat het blijkbaar vooral om het plezier van samen knutselen.

En overal staan eenhoorns… Want waarom zouden er geen eenhoorns staan?

Op de laatste avond komen de Nederlandse hackers die ik ken van de whiskyleaks samen in een uithoek van de Assembly Hall. Ook de Duitse hacker Mc.Fly, van wie ik mijn voucher heb gekregen. Ik dank hem alsnog hartelijk en vraag of we nog whisky gaan drinken. Nee, ze gaan biervaten kopen. Een Amsterdamse hackerspace heeft namelijk een hele biertapinstallatie meegenomen dat ludiek The Lawfull Interception Tap wordt genoemd. Volgens Mc.Fly kan ik meedoen door een unieke token te kopen voor tien euro en hij laat me een geprint Chinees aandoend stuk plastic zien. Nee, dank je. Ik had me voorbereid op een whiskyleaks, dus ik heb een fles Jack Daniels gehaald. Die moet ook nog op. Wat er verder is gebeurd die avond weet ik niet meer, maar het was een onvergetelijke CCC.

Terug in Nederland vraagt Mc.Fly me of hij in Rotterdam ook eens een Cryptoparty kan organiseren. Dat is een bijeenkomst waar hackers uitleggen hoe je je digitale spullen versleutelt. Dat lijkt me leuk en ik stel mijn praatprogramma Hack Talk hiervoor beschikbaar. Hij regelt dat Marie Gutbub, die al honderden cryptoparties heeft georganiseerd, uit Berlijn hier naartoe komt en ik regel via de Hogeschool Rotterdam tien studenten cybersecurity.

Op 12 december 2017 leren we de bezoekers hoe ze een TOR-browser gebruiken, mail versleutelen en een wachtwoordenkluis aanmaken. Dat alles onder het genot van veel discussies over privacy en security. De groep technische mannen laat zich prima leiden door de enige vrouw van het gezelschap en we hebben weer een goed feest, gratis en vrij voor iedereen en georganiseerd door de beste nerds.

Twee weken later ben ik weer op het Chaos Communication Congress, editie 34C3. Wederom dankzij Mc.Fly en zijn vouchercodes. Zo ook de edities van 2018 en 2019. Wat er daar gebeurt, lees je in de volgende hoofdstukken.

8. Autisme heeft ook voordelen

Hackers zien dingen anders dan anderen. Mensen met autisme ook. En wat blijkt, juist datgene waardoor ze op school of in sociale contacten problemen hadden, blijkt in de wereld van informatietechnologie een talent te zijn. Moeite met mensen? Nee, vooral dol op apparaten. Snel overprikkeld? Nee, oog voor details. Dwangmatige handelingen? Nee, goed in gestructureerd werken. Toch zitten er vele tienduizenden mensen met autisme werkloos thuis op de computer. Steeds meer organisaties ontdekken dit en nemen ze in dienst als programmeur, softwaretester en natuurlijk als helpende hacker.

Autisme en IT, voor de één een vanzelfsprekende combinatie, voor sommigen een verassende verklaring, maar ook voor velen nog een taboe. Techneuten hebben meestal niet zoveel op met psychologie: te persoonlijk, ongrijpbaar en te soft. Maar er zijn er steeds meer die de diagnose autisme juist wel handig vinden. Het is een verklaring voor eventueel ongepast gedrag, erkenning dat je niet de enige bent en een praktische handleiding hoe hiermee om te gaan. Of nog mooier: autisme als een talent.

29 december 2018, 17.00 uur, de Autismus Meetup tijdens het 35e Chaos Communication Congress in Leipzig. Het programma is niet bekend, alleen het tijdstip en een locatie, die zo ver als mogelijk is verwijderd van de gebruikelijke chaos. Gelukkig ben ik op tijd en kan ik rustig wachten in een rij stilzwijgende mensen met koptelefoons op. Voorafgaand had ik nog een oproep gedaan in het chatkanaal van ons groepje Hollandse hackers of er iemand meewilde, maar dat leverde alleen maar flauwe grappen op. “Mag je ze voeren?”, “Ja, met ongesorteerde Skittles” en “Geef ze dan alleen witte”. Flauw. Deze reactie vond ik nog wel leuk: “Maar ik heb al autisme!”

In de workshopruimte tref ik een bord met gekleurde prikkertjes, allemaal door elkaar. Ik maak er een foto van en stuur een berichtje aan de groep: “Laat de gekleurde Skittles maar thuis” en orden de prikkers netjes op kleur. Niemand reageert. We zijn met ongeveer twintig deelnemers en twee workshopleiders van het CCC AutiTeam. De ene met lang haar zit naar de grond starend volledig in zichzelf gekeerd. De tweede kijkt juist met opengesperde ogen en vrolijke glimlach de zaal rond en heet iedereen welkom, zonder zich voor te stellen. Ik noem ze daarom voor het gemak hier Bert en Ernie.

Voor we echt gaan beginnen, snijdt Ernie eerst een punt van orde aan: vinden de mensen met autisme het goed als er ook neurotypische mensen aanwezig zijn? Neurotypisch is de wetenschappelijke term voor mensen die geen autisme of enige andere psychische kwalificatie hebben. Een deelnemer roept: “Wanneer heb je nu wel of geen autisme? Ik wacht al jaren op een diagnose!” Hij krijgt direct bijval van andere deelnemers. “Ja, diagnose is moeilijk”, besluit Ernie, “dus laten we het erop houden dat je autisme hebt als je dat zelf vindt. Aldus: wie vindt zichzelf neurotypisch?” Drie jonge vrouwen steken hun hand op. De rest vindt het geen probleem dat ze er zijn, zolang ze maar geen foto’s maken.

Bert, die er tot dan toe vooral in zichzelf gekeerd bij zat, komt plots in beweging en richt zich tot Ernie: “Maar eh, waar wil je het eigenlijk over hebben in deze workshop?” Daar had Ernie eigenlijk niet over nagedacht. Hij vond het al heel wat dat we hier zo met z’n allen samen zijn en dat het goed is om ervaringen te delen. Hij geeft daarom nog wat praktische tips. Ze hebben hier op CCC stilteruimtes en coaches waar je terechtkunt als het je allemaal teveel wordt. Je kunt ook een speciale badge krijgen met de tekst: “Hallo. Met mij gaat het goed. Ik heb momenteel problemen met communiceren. Ik heb gewoon rust nodig. Raak me alsjeblieft niet aan.”

Een lange stilte volgt… Ernie begint daarom maar te vertellen over zijn eigen ervaringen met autisme. In het dagelijks leven had hij veel moeite met omgaan met andere mensen, en juist daarom heeft hij hier op CCC veel organisatorische taken op zich genomen. Hier kan dat, omdat iedereen meer begrip toont voor mensen die anders zijn. Die ervaring heeft hem ook geholpen met mensen om te gaan buiten CCC. Vervolgens legt hij uit hoe

hij, als hij in een hotel logeert, het niet kan laten de temperatuurknop van de douche te herijken en besluit met: “Iemand anders ervaringen?”

Als dan weer een lange stilte volgt, waag ik het erop in mijn beste Duits: “Ik wil een stelling poneren: autisme heeft ook voordelen. Hebben jullie daar wellicht voorbeelden van?” Iedereen kijkt op en de zaal komt ineens helemaal los. De een roept dat hij in een krant in een oogopslag de spelfouten ziet. De ander zegt kampioen te zijn in puzzelen. En een derde blijkt succesvol kunstenares te zijn. Ernie heeft zichtbaar moeite met de spontane uitbarsting van bekentenissen en maant de zaal tot orde.

Ik vervolg met de vraag of autisme ook handig is in cybersecurity. Bijvoorbeeld dat je sneller kleine foutjes in softwarecode ziet of makkelijker complexe systemen kunt doorgronden. Ik merk aan de reacties dat dit een stomme vraag is. Iemand achter mij mompelt: “Natuurlijk. Waarom zitten er anders zoveel mensen met autisme in dit vak?” Na de sessie probeer ik nog wat deelnemers aan te spreken, maar al snel gaan de koptelefoons op en vervolgt iedereen zijn eigen schema met technische presentaties op het CCC.

Het jaar daarop heb ik me al voordat het congres begint aangemeld als Angel voor het AutiTeam. Als ik in de trein er naartoe een Nederlands stel tegenkom dat ik ken van andere cybersecurity evenementen, knoop ik een praatje aan. De man vertelt dat hij vooral geïnteresseerd is in de technical talks over netwerkbeveiliging en duikt vervolgens in zijn laptop. De vrouw vertelt dat CCC voor haar altijd een soort thuiskomen is. Niet lang geleden kreeg ze, na een zware burn-out, de diagnose autisme en dat maakte veel duidelijk voor haar.

Enthousiast vertel ik dat ik me heb aangemeld als Angel bij het AutiTeam. Ik wil graag de stiltekamer bewaken. Ze vertelt dat ze zich het jaar ervoor ook had aangemeld, maar geen taak kreeg. Toen is ze naar Heaven gegaan. Dat is de balie waar Angels terechtkunnen voor hun naamkaartje en vragen. Ze werd doorgestuurd naar de teamlead AutiTeam en trof een man met paardenstaart die in elkaar gedoken zat met een koptelefoon op. Na wat handgebaren kreeg ze eindelijk contact met hem en vroeg of er misschien een soort online-introcursus is voor het AutiTeam. De man stond op en begon ineens te schreeuwen: “Shit, dat was het wat ik was vergeten!” Ze probeerde hem te kalmeren, maar tevergeefs. Later trof ze

nog iemand anders van het AutiTeam die wel aanspreekbaar was, maar eigenlijk alles vooral zelf wilde doen. Ik vermoed dat dit Bert en Ernie waren.

Ondanks het verhaal van de vrouw ga ik wel naar Heaven en de stiltekamer, maar ook ik krijg niets uit de takenlijst toegezonden en vind het eigenlijk wel best zo. Iedereen lijkt zich te vermaken op het CCC. Daar hebben ze, denk ik, geen AutiTeam voor nodig.

De meeste neurotypische mensen zullen bij autisme denken aan die jongen van de lagere school die met een helm op de hele dag heen en weer zat te wippen en rare geluiden maakte. Of aan die jongen die juist helemaal niet opviel omdat hij zich niet mengde in de groep, totdat hij flipte en de hele boel bijeen schreeuwde. Of aan dat meisje dat alleen met dieren omging. Of aan de film ‘Rain Man’, waarin Dustin Hoffman zeer indringend het karakter van een onhandelbare man vertolkt die bij tijd en wijle iets uitzonderlijk knaps doet.

Of je beeld van autisme is juist gekleurd door enkel grootheden uit het verleden. Naar verluid hadden ook Leonardo Da Vinci, Pythagoras, Van Gogh, Mozart en Andy Warhol het. In hun tijd bestond de diagnose autisme nog niet, maar psychologen claimen wel uit hun biografieën te kunnen afleiden dat ze ergens in het autistisch spectrum zitten: dwangmatige gewoontes, snel overprikkeld, in zichzelf gekeerd, moeilijk in de omgang – maar wel geniaal.

Kijken we in de IT, dan wordt van de grote namen, zoals Mark Zuckerberg, Bill Gates en Elon Musk, gezegd dat ze ook enige vorm van autisme hebben. Het mooiste voorbeeld vind ik nog wel Alan Turing, de Britse wiskundige die in de Tweede Wereldoorlog Enigma, de codeermachine van de Duitsers kraakte. Zijn Turingmachine en de Bombes die hij ontwikkelde om alle versleutelingscombinaties uit te proberen, draaiden weliswaar op zware relais, maar schakelingen op basis van enen en nullen vormen de blauwdruk voor de computer zoals we die vandaag de dag kennen. Dat hij typisch autistische trekjes zou hebben gehad, is ook mooi te zien in de verfilming van zijn leven, *The Imitation Game*, met een glansrol voor de excentrieke Benedict Cumberbatch.

Maar, wat is autisme nu eigenlijk? Wat zeggen de experts? Die hebben het vandaag de dag over een ‘autisme spectrum stoornis’, volgens de DSM-5, oftewel het Diagnostic and Statistical Manual of Mental Disorders, versie 5. Daarin staan deze criteria. Ten eerste “tekorten in de sociale communicatie en interactie, zoals blijkt uit: tekorten in sociaal-emotionele wederkerigheid, tekorten in het voor sociale omgang gebruikelijke non-verbale communicatieve gedrag en tekorten in aangaan, onderhouden en begrijpen van relaties.”

Ten tweede “beperkte zich herhalende gedragspatronen, beperkte interesses en activiteiten, zoals blijkt uit: stereotype of repetitieve motorische bewegingen, gebruik van voorwerpen of spraak, hardnekkig vasthouden aan hetzelfde, star gehecht aan routines of geritualiseerde gedragspatronen, zeer beperkte, gefixeerde interesses die abnormaal intens of gefocust zijn en over- of onderreageren op zintuiglijke prikkels of ongewone belangstelling voor zintuiglijke aspecten van de omgeving.” Daar word je niet vrolijk van, want het gaat alleen over tekorten en beperkingen. Aan de andere kant is dat ook wel weer begrijpelijk voor een diagnostisch handboek, want als iets geen probleem is, hoef je het niet vast te stellen voor een behandeling.

Wat verder interessant is aan de DSM-5 is dat het stelt dat autistisch gedrag te herkennen is vanaf de vroege kindertijd en niet pas later ontstaat. Dan zou er sprake zijn van een andere oorzaak. De oorzaak is dus aangeboren en zit in de manier waarop deze mensen van nature informatie verwerken, met de hierboven beschreven criteria als gevolg van een problematische persoonlijke ontwikkeling te midden van mensen die geen autisme hebben. Omgekeerd kan het zo zijn dat iemand op jonge leeftijd problemen had met het anders verwerken van informatie, maar er door de juiste omgeving uiteindelijk redelijk goed mee heeft leren omgaan. Tot die categorie behoor ikzelf, denk ik.

De eerste keer dat ik in aanraking kwam met de DSM, destijds nog versie 4, was toen ik in 2015 met mijn dochter bij de psycholoog zat voor een persoonlijkheidstest. Ze had al een diagnose voor dyslexie, maar bleek ook een nogal afwijkend IQ-profiel te hebben waardoor ze niet mee kon komen op school: bijzonder laag op performatief, bijzonder hoog op systeem-

analytisch en hoogbegaafd op verbaalcognitief niveau. Of in mijn woorden: ze heeft moeite met makkelijke dingen, terwijl de moeilijke dingen voor haar juist makkelijk zijn. Bijvoorbeeld: een lijst met korte woorden in hoog tempo foutloos oplezen lukte haar niet, maar een lijst met honderden dinosaurussoorten rolde er zo uit, inclusief tekstcorrecties. Buitenspelen met leeftijdsgenootjes deed ze nauwelijks. Ze zat liever alleen thuis te knutselen. Dan maakte ze prachtig gedetailleerde fantasiewezens, maskers en kostuums, waarvan ze er ook nog aardig wat heeft verkocht. Praten met volwassenen ging haar makkelijker af dan met leeftijdsgenoten.

De diagnose van de psycholoog: het syndroom van Asperger. Dat is een vorm van autisme, met de typische informatieverwerking die leidt tot overprikkeling, moeite met sociale contacten en dwanghandelingen. Anders dan bij klassiek autisme, is er bij Asperger geen achterstand in communicatieve vaardigheden, maar juist sprake van formeel zeer correct taalgebruik. Als ik haar bijvoorbeeld naar de kinderopvang bracht, had ze altijd dinosaurussen bij zich. Een keer vroeg een begeleidster: “Oh, meisje, heb je een paardje meegenomen?” Mijn dochter antwoordde: “Nee, dit is een Parasaurolofus. Een planteneter, dus niet gevaarlijk.” Voordat de juf er goed en wel op kon reageren, zat ze alweer op haar vaste plek om de hele dag dino’s te ordenen.

Tijdens die tests en het bespreken van de uitkomsten van onze dochter dacht ik telkens: Dit gaat ook over mij. (Misschien is het typisch voor mensen met autisme dat ze bij alles denken dat het over henzelf gaat…) Ik had op die leeftijd ook veel problemen op school. Dan werd mijn moeder naar school geroepen omdat ik weer doorgeslagen was door alle drukte of juist omdat ik alleen maar zat te dromen. In de pauze zat ik met verbazing te kijken naar die zwerm rondrennende kinderen, van waaruit om onverklaarbare redenen allerlei kreten en objecten mijn kant op vlogen. De leraren zeiden dat ik ook een leesprobleem had. Nou, dan lees ik toch niet. Probleem opgelost. Bij hoofdrekenen was ik juist de beste. Stuur me maar naar de technische school, dan kan ik apparaten maken.

Wel een probleem was dat ik om de een of andere reden alles in getallenreeksen van drie moest doen. Oftewel: zes stappen om van hier tot de deur te komen. Dilemma: zes stappen is links en rechts evenveel (symmetrie), maar negen stappen is drie keer drie (kwadraat). Dodelijk

vermoeiend, maar wel lekker, zo'n ritmisch wereldje. Later maakt ik er een vier van, om het symmetrieprobleem op te lossen, maar dat maakte de kwadratische reeksen weer erg lang… Ik leek er maar niet vanaf te komen. Tot ik plaatsnam achter een drumstel. Na een korte uitleg speelde ik meteen al vier- en driekwartsmaten. Eindelijk een wereld waarin alles wel klopt. Daar kon ik mijn getallen kwijt en in de gewone wereld kon ik doorlopen zonder te tellen.

Een ander veelvoorkomend probleem bij mensen met autisme is dat die niets kunnen met 'zomaar een praatje maken'. Vooral als een onbekende uit het niets begint over iets wat niet ter zake doet, slaat de paniek toe. Het heeft me lange tijd gekost om te begrijpen dat zo'n gesprekje niet gaat over de inhoud, maar puur om de vorm en vooral een vanzelfsprekende, menselijke neiging is. Ik kan er nog steeds weinig mee en denk dat ik daarom presentator ben geworden en graag interviews doe: je spreekt iemand op een vooraf gepland moment, over een duidelijk afgebakend en ter zake doend onderwerp. Je bereidt je voor op wie het is en waar het over gaat, met een duidelijk begin en eind aan het gesprek. Heerlijk!

Naarmate ik steeds meer overeenkomsten zag tussen mijn dochters diagnose en mijn eigen gedrag, vroeg ik haar psychologe of ik die test zou kunnen doen om te kijken of ik ook Asperger heb. Dat had volgens haar geen zin, omdat, volgens haar, bij deze vorm van autisme mensen allerlei copingmechanismen ontwikkelen, waardoor de effecten op de lange termijn nauwelijks nog meetbaar zijn. Soms is er terugval, maar meestal redden ze zich prima. OK, hoopgevend, maar ook een beetje teleurstellend.

De diagnose hielp onze dochter namelijk enorm om aan haar omgeving uit te leggen waarom ze anders reageerde dan de andere leerlingen. En ons als ouders ook. Door een goede balans te vinden in dagelijkse prikkels – niet te veel alledaagse ruis en juist meer intellectuele uitdagingen – hadden we eigenlijk een heel makkelijk kind. Uiteindelijk ging ze nauwelijks nog naar school, slaagde ze met de beste cijfers en is ze nu voltijd schrijfster.

Mede dankzij haar en mijn eigen zoektocht op het spectrum herken ik eerder mensen om me heen die ook een vorm van autisme hebben. Niet alleen in hun gebreken, maar juist in hun talenten. Met name in de IT. Ik vraag me af hoe zij ermee omgaan. En ervaren zij naast de nadelen ook

voordelen van dat ze de wereld anders beleven? Zoals wel vaker bij lastige vragen, beantwoord ik die met mijn praatprogramma.

9 april 2019, Hack Talk 12. Thema: ‘Autisme heeft ook voordelen’. De week ervoor was net de Autismeweek geweest, met op 2 april de Internationale Autismedag. Dan zijn er allemaal bijeenkomsten op verschillende plekken, waar je leuke dingen kunt doen en nieuwe mensen kunt ontmoeten. Dat lijkt me persoonlijk een perfect rampscenario voor mensen met autisme. Daarom doe ik mijn programma pas de week erna, een speciale prikkelarme editie. De dj draait Ambient in plaats van Break Core beats, de VJ en lichttechnicus zijn gedimd en club Worm heeft een stilteruimte ingericht voor wie even wil bijkomen van alle indrukken.

Aan tafel Peter van Hofweegen en Frans de Bie van ITvitae. Toen ze het instituut in 2013 oprichtten, was hun motivatie zowel persoonlijk als maatschappelijk. Peter: “De Nederlandse Vereniging voor Autisme had toen net onderzoek gedaan waaruit bleek dat er 20.000 mensen met autisme thuiszitten, terwijl ze hbo-niveau hebben. Zelf had ik toen een zoon van zestien die niet zijn bed uitkwam, omdat hij niet meer mee wilde doen. Frans en ik waren collega’s en hadden de juiste ervaring: ik in detachering en hij als IT-ondernemer.” Frans: “Volgens mij hebben de beste IT’ers een vorm van autisme. De meesten redden het zelf wel, sommigen niet. Dat DSM-handboek spreekt over een stoornis, wij spreken over een profiel.”

Als je googelt op ‘opleiding, ICT en autisme’ krijg je ITvitae als eerste hit. Bovenaan de site staat: “ICT academy én baanbemiddeling voor jongeren met autisme en/of hoogbegaafden, ongeacht vooropleiding.” Zo komen de meeste studenten bij hen. Nieuwkomers ondergaan een uitgebreid selectieproces van meerdere gesprekken over hun achtergrond en motivatie en doen verschillende tests in technische vaardigheden. Frans: “We zijn een fabriek in zelfvertrouwen. We krijgen hier mensen die anders zijn, buiten de groep vallen, gepest zijn of faalden op examens omdat ze dat als te veel druk ervoeren. Ze weten vaak onvoldoende wat ze al kunnen. Wij moeten daarom nieuwsgierig zijn en veel doorvragen. Laatst had ik een jongen met een leeg cv die er ongemotiveerd bij zat. Later bleek dat hij twaalf programmeertalen kende. Dat had hij niet vermeld omdat hij dacht dat dat normaal was.”

De opleidingen bij ITvitae zijn Software Test Engineer, Cyber Security Specialist, Software Developer en Data Scientist. Deze profielen zijn gebaseerd op de vraag uit de arbeidsmarkt en passend bij de doelgroep. Ook de leeromgeving past bij de doelgroep: een mooi en rustig klooster in een park in Amersfoort. Van de studenten stroomt 91% na 12-18 maanden door naar een reguliere baan. De werkgevers waar ze uiteindelijk terechtkomen, zijn ook zeker niet de minsten: Rabobank, ABN AMRO, Achmea, Belastingdienst, Sogetti, Deloitte, Ernst &Young, Northwave Security en Team High Tech Crime van de Nederlandse politie. Zeer succesvol dus en dat zonder overheidssubsidie. Het eerste stuk van de opleiding is voor ITvitae namelijk een investering die via een detachering van een jaar wordt terugverdiend. Daarna worden de studenten overgenomen door de werkgever.

Zelf heb ik er al meerdere keren gastlessen verzorgd en dat is altijd een bijzondere ervaring. Dan krijg ik vooraf een instructie over de groep, bijvoorbeeld over een leerling die altijd om een vaste tijd zijn boterham wil of een andere die wel veel vragen stelt, wat de rest van de groep dan weer stoort. Maar eigenlijk gaat het altijd om een heel makkelijke groep: de deelnemers luisteren aandachtig en stellen goede vragen.

Behalve dan die ene keer, want toen was iedereen bezig met wat anders: de jaarlijkse AIVD-kerstpuzzel. Deze reeks cryptografische opgaven werd tot voor kort gebruikt om de analytische vermogens van de werknemers bij de dienst te testen, maar staat sinds 2011 ook online. Ik weet niet of de dienst dit, net als Alan Turing tijdens de Tweede Wereldoorlog, doet om nieuwe medewerkers te werven, maar de puzzel is wel een begrip in cybersecurity land. De studenten bij ITvitae kijken er elk jaar naar uit en gaan er meteen mee aan de slag. Ze doen de puzzel niet individueel, maar samen als team, want ze weten dat elk goed is in iets anders. Dan roept er één: “Ik heb de code van opgave 18, maar weet niet wat het betekent”. Een ander bedenkt dat het een reeks frequenties is, maar herkent het muziekje niet. Weer een ander zegt dan: “Dat is het deuntje van de Efteling. We hebben dus een locatie.” Team ITvitae eindigde dat jaar op plek 34 van de 1.100 inzendingen. De AIVD kwam toen langs om met ze te praten over de uitkomsten. Of daar een Turing-achtige stage of baan uit voortkwam, is uiteraard staatsgeheim.

Nog iemand die talent herkent in autisme is Sjoerd van der Maaden, oprichter van Specialisterren. Ook hij is deze avond aan tafel bij Hack Talk om te vertellen over zijn ‘testfactory’, waar verschillende teams voor klanten de ‘online customer journey’ doorlopen. Als je bijvoorbeeld nieuwe klant wordt bij een bank, dan ga je door een clickmenu waar je van alles in moet vullen. Dan kan het zijn dat je vastraakt omdat jouw categorie er niet bij zit, iets niet logisch is of de software om een andere reden raar reageert. De testers van Specialisterren doorlopen die paden, handmatig en met testtools, en rapporteren de uitkomsten op het online klantendashboard.

Het idee voor Specialisterren ontstond toen Sjoerd in 2008 terugkwam van een sabbatical. Hij was een jaar gaan zeilen met zijn vrouw en drie zonen. Zijn jongste zoon, Max, heeft een vorm van autisme en was toen nog leerplichtig. Zijn vrouw gaf hem daarom les, tijdens het zeilen. Al snel bleek dat Max de lesstof veel sneller oppakte dankzij de rustige omgeving, minder tijdsdruk en heldere leerdoelen. Sjoerds vrouw schreef hier een artikel over in Balans Magazine. Eenmaal terug, kreeg Sjoerd veel vragen uit zijn werkkring over dit artikel. Blijkbaar werd dat tijdschrift daar veel gelezen. Tijdens zijn loopbaan als manager in de IT was het hem opgevallen dat autisme veel voorkomt in de sector. Nu zag hij een businessmodel. Als hij voor deze doelgroep de juiste omgeving creëert, zouden deze mensen dan, net als Max, beter presteren?

Door zijn uitgebreide netwerk in de IT had hij de financiering en ondersteuning snel rond. Inmiddels werken er zo’n vijftig mensen bij Specialisterren, waarvan het merendeel een vorm van autisme heeft. Sjoerd: “Het zijn toegewijde collega’s, die gestructureerd werken. Ze hebben vaak een goed geheugen en herinneren zich bijvoorbeeld een fout in een formulier die ze zeven maanden terug hadden gezien. Zodra een test geautomatiseerd kan worden, schrijven ze er een script voor dat 24/7 doortest.”

De teammanagers, die ook het klantcontact verzorgen, zijn over het algemeen neurotypisch, maar hebben wel geleerd zich aan te passen. Sjoerd: “Ze kunnen dus niet zeggen dat de testers moeten doortrekken op cola en pizza’s om deadlines te halen. Ze gaan ook niet iemand aankijken en vragen hoe het staat met de planning. Ze staan ernaast en samen kijken ze naar hun planning.”

Sjoerd drijft zijn onderneming met winst en zonder subsidie: “Als ik mijn budget vergelijk met een gewoon bedrijf, dan zijn wij 10% meer overhead kwijt, onder andere aan testmanagers. Maar dat betaalt zich terug in continuïteit en hoogwaardige dienstverlening. Je ziet in de IT veel bedrijven die hip zijn met innoveren, lekker disruptief. Maar goed onderhoud is net zo nodig. Laat ons maar lekker gestructureerd testen. Daar is misschien nog wel meer behoefte aan.”

Die avond hebben we ook gasten met autisme aan tafel. Elk vertelt over de zware jonge jaren, het gevoel nergens thuis te horen en niet begrepen te worden. En over het gevoel van thuiskomen in de IT, een wereld waarin de dingen veel meer lijken te kloppen. We hebben ook hun collega’s aan tafel, die vertellen over hoe eerlijk, gestructureerd en toegewijd mensen met autisme te werk gaan, zo lang er maar passende begeleiding is. En hun verbazing, dat mensen met autisme dus wel sociaal kunnen zijn. Ook uit het publiek komen veel persoonlijke ervaringen. Veel van hen vertellen me dat ze het heerlijk vinden om samen hun eigen autistische zelf te kunnen zijn. Uiteindelijk ben ik de enige die deze avond nog gebruikmaakt van de stilteruimte.

9. Vrouwen welkom

Nu je al aardig wat hackers voorbij hebt zien komen, zal het je niet ontgaan zijn: hackers zijn vrijwel altijd mannen. Ik vind dat raar, want als iedereen informatietechnologie gebruikt, waarom zou slechts één helft van de bevolking over de beveiliging gaan? Ik vind het jammer als ik op cybersecurity congressen weer een geheel mannelijke line-up aantref. En als er dan eens een vrouw tussen zit, kunnen de meeste mensen het niet laten daar iets over te zeggen. Gelukkig vindt het grootste deel van de sector ook dat we beter af zouden zijn met meer vrouwelijke collega's en zijn er veel initiatieven om meer vrouwen in de IT te krijgen. Wat vooral goed werkt, is niet alleen aandacht te hebben voor het tekort, maar vooral te kijken naar de vrouwen die wel in de IT werkzaam zijn.

Eerst even terug in de geschiedenis. De eerste echte programmeur was een vrouw: Augustus Ada Byron, beter bekend als Ada Lovelance. Zij schreef eind 18e eeuw een programma voor de 'analytical machine' van de Britse wiskundige en filosoof Charles Babbage. Haar programma zette de mechanische handelingen van het apparaat om in taal. Ada voorspelde dat dergelijke machines ooit weleens gebruikt zouden gaan worden voor het maken van afbeeldingen, het componeren van muziek of zelfs het bedrijven van wetenschap. Babbage kon zich er weinig bij voorstellen en zei dat het niet meer is dan gewoon een rekenmachine. Ada was haar tijd dus ver vooruit. Later, in de tijd van de ponskaartsystemen, werden deze voorlopers van de computer ook voornamelijk bediend door vrouwen.

Dat beeld is vandaag de dag anders. Volgens Eurostat is in Nederland, anno 2019, slechts 16% van de IT'ers vrouw, net iets onder het Europees gemiddelde. Kijken we naar het aantal vrouwen in IT-opleidingen, dan staat Nederland helemaal onderaan met 8%. Opvallend is dat juist in landen die

we niet echt kennen als zeer geëmancipeerd, de deelname van vrouwen aan IT-opleidingen het hoogst is: Roemenië, Bulgarije, Estland en Letland. Zelfs Italië en Griekenland scoren substantieel beter dan Nederland. Is Nederland toch niet zo geëmancipeerd als we denken?

Hoe zit het met de genderbalance onder hackers? Exacte cijfers zijn er helaas niet. Want hoe definieer je een hacker? Zelf definieer ik hackers als mensen die technologie maken, breken en bespreken. Maar met zo'n definitie kunnen statistici niet zoveel. Wat je wel kunt doen, is bij grote hackerevents, tijdens een drukbezochte presentatie, de koppen tellen. Dan kom je uit op ongeveer 1 vrouw op 10 mannen. (En nog aardig wat mensen die daar ergens tussenin zitten, maar dat is weer een ander verhaal.) En werk je zelf in de IT-security, dan behoeft het wellicht geen onderbouwing: je weet gewoon dat er weinig vrouwen zijn. De consensus is dat dat er best wat meer mogen zijn. Omdat we meer mensen nodig hebben, je met een diverser team beter problemen oplost, maar ook omdat het gewoon gezelliger is.

Om te laten zien dat het anders kan, hebben we bij Hack Talk 12 maart 2019 een speciale vrouwenavond: Hacksters. Het is ook bedoeld als spoedcursus voor mannen: hoe om te gaan met vrouwen in de IT. Omdat ik ook maar gewoon een man ben, doen we een kettinginterview: telkens een eraf en een erbij, zodat ze ook elkaar kunnen interviewen. We starten met de maaksters: een agile testcoach en een security engineer. Dan de breeksters: een pentester en malwareanaliste. Daarna de vrouwen met macht, die alles bijeen moeten brengen, de Chief Information Security Officers, oftewel CISO's. We eindigen met de uitreiking van het Roze Slot: de prijs voor het cybersecurity bedrijf met de meeste vrouwen in dienst.

We beginnen met onze eigen Ada Lovelace. Janneke van den Brand is namelijk van origine softwaretester en nu Agile Testcoach bij Bartosz ICT. Hoe is ze in de IT terechtgekomen? Janneke: "Ik wilde al de IT in voordat ik ging studeren, maar koos toch voor de Universiteit voor Humanistiek, de Master in Kritische Organisatie & Interventiestudies, Levensbeschouwing & Onderzoek. Eigenlijk vond ik alles wel interessant, maar de technische kant bleef trekken. Ik deed toen een traineeship in softwaretesten, haalde wat certificaten en werd Scrummaster. Je bent dan meewerkend

voorman/vrouw, om problemen voor je team weg te werken. Je draait in tweewekelijkse cycli, van ontwikkelen naar testen en implementeren van software en houdt je team bij elkaar. Hoe, dat hangt af van je team. Soms moeten alle ontwikkelaars zelf testen en soms heb je verschillende rollen: ontwikkelaar, tester, analist of product owner die de inhoud bepaalt. Het technische en sociale loopt dan erg door elkaar."

Ziet ze in zo'n rol als testcoach meer vrouwen dan elders in de IT? Janneke: "Coaching wordt misschien iets vaker ingevuld door vrouwen, maar de meeste testcoaches zijn toch man. Kijk je naar een team, dat meestal uit acht personen bestaat, zijn dan maximaal twee van hen vrouw. Ik heb me harder moeten bewijzen als vrouw, ook bij klanten. Al heb ik de meeste technische ervaring, ze stellen eerst de vragen aan de mannen. Vervolgens komen ze dan toch uit bij mij en ben ik ineens 'one of the guys'. Technisch, dus je bent een man. Of als een vrouwelijke collega zegt: 'Ik ben wel goed in programmeren, maar niet met computers', dan zeggen ze: 'Oh, dan ben je dus toch een meisje'. Ik noem dat 'death by a thousand papercuts': veel kleine dingetjes die optellen. Dat is demotiverend."

Kortom, beoordeel iemand op de bijdrage aan het team en niet of die persoon een hij of een zij is. Daar draagt Janneke ook aan bij tijdens hackerevents. Zo was ze bij hackerskamp SHA2017 Team Lead van het Cohesion Team. Wat houdt dat in? Janneke: "Het team heette eerst Code of Conduct, maar dat klinkt dan zo streng. Cohesion is een positievere insteek. Het gaat er vooral om dat mensen hard werken op zo'n kamp en weinig slapen. Dan krijgen ze weleens ruzie. We zorgen dan voor een safe space, of sturen ze gewoon naar een hotel om bij te slapen."

Even wat getallen over het event: 3.750 mensen gaan een week lang door, op een kamp, met veel drank, terwijl één op de acht vrouw is. Hoe vaak gaat dat fout? Janneke: "We hadden in totaal tien gevallen, waarvan één die ons wel een dag werk kostte. Maar het was toch vooral dat af en toe iemand een schouder nodig heeft of een gesprekje omdat ze aan het eind van hun Latijn zijn." OK, dus enkele gevallen die je altijd wel hebt als er mensen bijeenkomen, maar geen vrouwen die lastig worden gevallen. Vergelijk dat eens met een gewoon festival. Dan is de hackerswereld toch wel vrouwvriendelijk, al zeg ik het zelf.

Onze volgende maakster is Antoinette Hodes. Zij wordt betrokken bij het ontwerp van systemen voor de security. Ze heeft ruime ervaring als security engineer, o.a. bij SecureLink en Motiv. Daarvoor heeft ze gewerkt als IT-support, o.a. bij KPN, Centric en Alcatel. Ze begon ooit in de IT als System Administrator bij een gemeente. Nu is ze security expert bij het internationale cybersecurity bedrijf Check Point Software Technologies.

Hoe ziet het dagelijks werk van een security engineer eruit? Antoinette: “Je lost security vraagstukken op met je klant. Je kijkt naar proof of concepts, checkt baselines en zet boxen in het netwerk om mee te kijken: intrusion detection, zero-dayprotectie, shadow IT die naar de cloud gaat, dat soort dingen. De klant wil weten of hij kwetsbaar is, maar we kijken ook of die kwetsbaarheden uit te buiten zijn en of alles, bijvoorbeeld, achter een goede firewall staat. De IT-afdeling van de klant is niet altijd blij als ik in hun koninkrijk kom en die box in hun netwerk zet. Je gaat mogelijk aantonen dat er iets niet goed zit.”

Haar werkgever Check Point kennen we van hun threat map, een kaart van de wereld met live cyberaanvallen. Maar wat zien we daar eigenlijk? Antoinette: “Het is niet live, maar met een vertraging van een paar uur. We detecteren 86 miljard transacties per dag. Een veelvoud van wat Google heeft aan zoekopdrachten. Niet alleen de box, maar ook security in mobieltjes, cloud-omgevingen, eigenlijk alles waar kritieke data staat.”

Hoe is ze in de IT terechtgekomen? Op haar LinkedIn-profiel zie je namelijk geen opleiding, maar wel een hele lijst met certificaten en inmiddels twintig jaar ervaring in IT. Antoinette: “Klopt. Ik heb mbo gedaan, maar ben daarna meteen de IT in gegaan. Ik heb altijd wel zin om wat nieuws te leren, grenzen te verleggen. Als je iets doet wat je hobby is, werk je niet. Blue Coat, Infoblox, Cisco, Palo Alto – dat zijn allerlei vendor certificeringen die ik gaandeweg heb opgepikt. Check Point Certified Security Expert is, denk ik, nog wel de belangrijkste. Met CISSP (Certified Information Systems Security Professional) en CISM (Certified Information Security Manager) ben ik nog bezig. Ik kan inmiddels ook wel aardig met Kali Lunix overweg en heb ook zelf trainingen ontwikkeld, bijvoorbeeld over SMB (Server Message Block) en SCADA/ICS (Supervisory Control and Data Acquisition / Industrial Control Systems). OT (Operationele

Technologie) heeft namelijk een andere aanpak dan IT: het staat vaak open, kan lastig gepatched worden, want het moet wel continu draaien."

Hoe is het om als vrouw in deze mannenwereld te werken? Antoinette: "In Nederland is nog wel veel te doen. Kom ik bij een klant binnen en denkt die IT-administrator dat ik de accountmanager ben en mijn mannelijke collega de techneut is. Dan zet ik die doos in zijn netwerk en dan vindt hij dat niet prettig. Maar, omdat Check Point een Israëlisch bedrijf is, hebben wij juist veel technische vrouwen. Die komen uit het leger, Unit 8200, het onderdeel van Defensie dat communicatie en decryptie doet. Mijn held Maya Horowitz komt daar vandaan. Mijn CEO ook." Zo kan het dus ook. Ik stel voor om dan in Nederland maar weer de dienstplicht in te voeren, maar dat vinden Janneke en Antoinette allebei niet zo'n goed idee.

Na maakster Janneke, halen we er een breekster bij. Sanne Maasakkers is namelijk pentester bij Fox-IT en hackt in opdracht van klanten in hun IT-systemen. Na haar opleiding computerwetenschappen aan de Universiteit Utrecht was ze zelfstandig webdeveloper en associate engineer bij Everett Identity & Access Management Solutions. In 2016 begon ze bij Fox-IT als trainee op de afdeling Crypto, waar ze ook haar CISSP haalde en nu Certified Ethical Hacker is.

Waarom security? Sanne: "Ik maakte webapplicaties, als eigen bedrijfje. Dat deed ik tijdens een andere studie, niet IT. Steeds meer mensen vroegen of ik websites wilde maken. Die moet je ergens online zetten en als je dat niet goed doet, kan er van alles misgaan. Dus ging ik zelf testen met PHP-code en SQL-injections. Op een banenmarkt sprak ik iemand van Everett Identity & Access Management Solutions. Die zei: 'Kom bij ons werken, dan krijg je een leaseauto.' Dat vond ik wel wat, maar vooral omdat ik daar zowel webdevelopment als security kon doen. Ik moest dan bepaalde pakketten implementeren, zodat alleen de juiste mensen binnen kunnen komen. Toen dit bedrijf werd overgenomen, sprak ik tijdens een BBQ iemand die bij Fox-IT had gewerkt en zo kwam ik daar terecht."

Naast haar opleiding en werk heeft Sanne lesgegeven in IT. Onder andere via DigiVita, een programma van VHTO, het landelijk expertisebureau meisjes/vrouwen en bèta/techniek. Sanne: "Ze zetten vrouwelijke rolmodellen in op de basis- en middelbare scholen om te laten

zien dat meisjes ook technische beroepen kunnen hebben. Scholen melden zich aan voor gastles en zij zoeken iemand die bij de vraag past. Ze hadden mij benaderd omdat ik een IT-opleiding deed. Ik heb veel lesgegeven in web- en appdevelopment, en geef ook Capture the Flag. Dat doe ik zelf ook weleens. En de AIVD-kerstpuzzel natuurlijk. Ik vind het leuk om cryptopuzzels op te lossen. Samen met collega's is best gezellig."

Ook Sanne heeft een aantal van de bekende securitycertificaten. Maar wat houden die eigenlijk in? Sanne: "CISSP is een soort vereiste, brede certificering. Die gaat over onderwerpen als encryptie, Identity & Access Management, Secure Software Development, Risk Management en Business Continuity. Veel mensen vinden CISSP saai, maar ik vind het wel goed om van alle vlakken wat te weten. OSCP (Offensive Security Certified Professional) is wel wat anders. Je krijgt een paar URL's, moet daar binnen 24 uur kwetsbaarheden zien te vinden, terwijl er een webcam op je staat." OSCP is dus een hackexamen met liveopname. Die zou je kunnen hacken en op een scherm kunnen zetten. Dan zie je meteen hoeveel man en vrouw zijn, een soort levende enquête.

Vindt Sanne pentesten nog meer een mannending dan de rest van de IT? "Nou nee. Daar heb ik zelf niet zo'n last van. In mijn team is het best gezellig en zijn er aardig wat vrouwen, ongeveer een kwart." Antoinette vraagt aan haar: "Doe je ook aan insluiping, social engineering?" Sanne: "Ja, dat is tof, want als vrouw verwachten ze het niet van je. We proberen dan Post-Its met wachtwoorden van monitors te halen en belangrijke documenten uit de prullenbak naast de printer te pakken, of we zetten een Raspberry Pi in het netwerk. Ik ben een keer mee geweest met een collega die mijn vader speelde. En zei toen, als jong meisje: 'Ik moet even naar de wc'. Ze liepen niet mee en ik kon overal komen. Als ze me zouden pakken, had ik gewoon gezegd: 'Oh sorry, ik wist niet dat ik hier niet mocht zijn.' Zo doen echte criminelen het ook."

Antoinette geeft het stokje over aan de volgende breekster: Saskia Hoogma-Ton, malwareanalist bij Tesorion. De afdeling waar zij werkt, is het overgenomen bedrijf Quarantainenet en doet netwerkbeveiliging. Met haar collega's beschermt ze ruim 3.500.000 eindgebruikers. Wat doet een malwareanaliste? Saskia: "Je analyseert het netwerkverkeer, neemt malware

samples en zet die in een sandbox. Dat is een afgesloten computer die je daarna weggooit. Komen er veel samples van één host, dan kun je die URL blacklisten. Je gaat samples uit elkaar halen om te kijken of ze op elkaar lijken. Hoe groot is de familie, hoe ver zitten ze qua tijd uit elkaar? Zitten er domain generating algorithms in, die dan elke dag andere URL's opvragen?"

Kijkt Saskia op codeniveau of gaat dat automatisch? "Je doet dat als team, elk met een eigen rol. De een doet veel met tooling en sandboxing, een ander is reverse engineer en haalt de code uit elkaar. Collega's komen met leuke nieuwe ideeën en dan kijk ik of die werkbaar zijn. Dat verschilt per project, het is geen standaardwerk. Je kijkt wel hoe je dingen aggregeert. Als we bijvoorbeeld van klanten niet-bestaande host names krijgen, kunnen we kijken of er overeenkomsten zijn. Daar heb ik een algoritme voor bedacht, dat nu in productie is."

Saskia is van oorsprong geen IT'er, maar wiskundige. Hoe is ze hier terechtgekomen? Saskia: "Eigenlijk per ongeluk. Ik was eerst projectmanagementondersteuner en tester. Toen zag ik deze vacature voorbijkomen. Ik dacht eerst: daar reageer ik niet op. Maar toen zei een recruiter: 'Moet je wel doen, ik denk dat er wel een match is.' Op gesprek bij Quarantainenet zeiden ze: 'Je mist kennis, die kunnen we je leren, maar je kunt wel goed nadenken.' Ik kreeg een lijstje met host names en ze vroegen: 'Welke moeten er op de blacklist komen, denk je?' en 'Wat voor technieken zou je kunnen bedenken?' Ik kreeg informatie mee en kon op een tweede gesprek komen. Ik denk dat ze me vooral wilden hebben omdat ik vanuit wiskundige vaardigheden patronen kan herkennen."

Sanne vraagt aan Saskia: "Wat is het allertofste wat je hebt gezien? Als je erover mag praten dan." Saskia: "Een clusteralgoritme met scoremodel. Dat heb ik samen met een collega helemaal zelf bedacht. Er zit veel wiskunde achter en dan ben ik trots dat het dan ook werkt. Veel domain generation algorithms kenden we al, maar we zien nu ook veel nieuwe."

Is volgens Saskia de wiskunde misschien een goede ingang voor vrouwen in cybersecurity? Of nog beter: puzzelen. In de Tweede Wereldoorlog werden cryptografen geworven met kruiswoordpuzzels en daar zaten ook veel vrouwen bij… Saskia: "Misschien, maar ik heb nooit het gevoel gehad dat ik tegengehouden werd als vrouw. Of ben ik net een

man omdat ik het niet doorheb?" Eigenlijk laten juist deze twee breeksters zich nog het minste tegenhouden door het feit dat ze vrouw zijn in een mannensector, maar dat is misschien weer eigen aan pentesters. Hun vak is immers ergens binnenkomen.

Toch kan er volgens Sanne nog veel verbeterd worden. "Het zou wel helpen als vrouwen zien hoe we ons werk doen. Ze denken bij hackers al snel dat je een zwarte hoody aan hebt, drie dagen niet gedoucht hebt en alleen op een zolderkamer zit. Hacken is juist een leuk en sociaal beroep."

Wat vinden ze van het woord penetratietesten, is dat niet te mannelijk? Zou het niet beter ovulatietest moeten heten? Het gaat er immers niet alleen om of je ergens kunt binnenkomen, er moet ook iets waardevols uitkomen, toch? Sanne is de grappen over penetratietesten inmiddels wel zat, en of ovulatietest nou zo'n goed alternatief is? Nee.

Na de makende en brekende techneuten komen de vrouwen die het voor het zeggen hebben in cybersecurity: de Chief Information Security Officers, oftewel CISO's. De 'C' in de functietitel betekent net als de Chief Financial Officer en Chief Operations Officer, dat je in de bestuurskamer jouw deel binnen het bedrijf vertegenwoordigt op het hoogste niveau.

We beginnen met Cynthia Schouten van Cybersprint die niet alleen CISO is, maar ook nog van een cybersecurity bedrijf, een soort CISO in het kwadraat. Hiervoor heeft ze 15 jaar bij KPN Consulting gezeten als Senior Business and Information Security Consultant. Cybersprint is een snel groeiend Haags bedrijf dat in kaart brengt waar en hoe de klanten kwetsbaar zijn op internet. Naast automatische scans doen ze ook pentests en organiseren ze jaarlijks Hâck The Hague, waar de gemeente jaarlijks een dag lang door vele hackers op de proef wordt gesteld.

Hoe ziet haar dagelijks werk als CISO eruit? Cynthia: "Heel gevarieerd. Cybersprint is een scale-up. We zijn in twee jaar gegroeid van 11 naar 43 werknemers. In het begin deed ik ook sales en consultancy erbij, maar nu kan ik me volledig richten op mijn rol als CISO. Bijvoorbeeld met de implementatie van de ISO 27001-standaard voor informatiebeveiliging. Ja, als ik dat zeg, zie ik mensen al snel verveeld kijken, maar zo'n normenkader helpt wel. Als groeiend securitybedrijf ben je bezig met

maatregelen, maar het opschrijven daarvan in beleid, blijft bij een hoop IT'ers achter en het is mijn taak dat op orde te brengen."

De eerste keer dat ik Cynthia ontmoette, was tijdens het hackerskamp SHA2017. Pieter Janssen, directeur van Cybersprint, had haar daar uitgenodigd voor haar sollicitatiegesprek. Hoe ging dat? "Ik moest zitzakken meenemen omdat Cybersprint de Capture the Flag sponsorde. Het was een relaxte sfeer en goede setting voor een sollicitatiegesprek. Ik heb ook doorgevraagd bij iedereen die in die CTF-tent zat. Daarvoor had ik niet zo contact met de hackercommunity. Pieter wel. Die heeft bij de Eindbazen gezeten (een zeer succesvol CTF-team) en die vinden het gewoon leuk om zo'n challenge in elkaar te zetten."

Net vers van KPN Consultancy was dat zeker wel een cultuurovergang? Cynthia: "Jazeker. Zo'n consultancy is soms net een grote overheidsorganisatie, maar ik was zelden intern. Ik was vooral bezig bij klanten met verandermanagementopdrachten. Als Rotterdammer was het Havenbedrijf mijn favoriete klant. Die houding van 'Niet lullen maar patchen', zeg maar."

Hoe is zij in de IT beland? "Ik ben ooit begonnen bij een IT-helpdesk: mensen helpen ISDN te installeren. Daarna naar IT-beheer en daar tot de conclusie gekomen dat je het proces pas kunt verbeteren als je de organisatie goed op orde hebt. Ik heb daarom mijn ISACA en CISM gehaald. Misschien ben ik ook wel in de IT beland, omdat mijn beide ouders technisch zijn. We hadden thuis de Commodore 64, het leukste computertje ooit. Daarmee heb ik leren programmeren. Dan ging ik via de radio van die programmaatjes opnemen en installeren. Ik heb nog wel een jaar IT gedaan op de Hogeschool Rotterdam. Van de vierhonderd leerlingen waren er zeven vrouw. Dat was geen warme ontvangst. Die baan bij de helpdesk beviel me beter en daarom heb ik alles vooral geleerd door het gewoon te doen."

Is dat nu nog zo, dat je meer hebt aan IT leren tijdens je werk dan op een IT-opleiding? Cynthia: "Ik ken meisjes die het op de IT-opleiding wel naar hun zin hebben. Ik merk dat er nu ook meer ondersteuning is vanuit het bedrijfsleven en de overheid. Het verschilt per bedrijfscultuur. Soms is het wel fijn om 'one of the guys' te zijn. Dan krijg je meer voor elkaar. Maar als je een manager hebt die iets tegen vrouwen heeft, dan is het heel lastig.

Dat probeer ik dan maar te negeren en te bewijzen dat ik het wel kan. Je zult als vrouw wel vaker iets meer je best moeten doen.” Heeft vrouw-zijn volgens haar ook voordelen in de IT? Cynthia: “Nee.”

We vragen Jessica Conquet erbij. Ze heeft meer dan twintig jaar ervaring in IT-security en is de Global IT Security Officer bij ABN-AMRO Clearing Bank. Zij heeft met plezier een studie informatica afgerond en begon daarna samen met iemand anders Unison, een consultancy om UNIX-systemen in de lucht te houden. Dat deed ze veertien jaar. Daarna heeft ze twaalf jaar net als Cynthia bij KPN gewerkt, als security- en riskmanager. Jessica was ook drie jaar security- en riskmanager bij Deloitte, gevolgd door een detacheringsavontuur in Zuid-America met PayU. Sinds 2018 zit ze bij ABN AMRO.

Haar functie was eerst CISO, maar is nu GITSO: Global IT Security Officer. Hoe dat zo? Jessica: “Je bekijkt de dingen niet alleen vanuit IT-security, je doet aan riskmanagement. En dat ‘Gobal’ betekent veel reizen. Het team dat onder security valt, zit in verschillende landen. Clearing Bank zit dichtbij waar de handel zit, de grote beurzen: New York, Parijs, Hong Kong, Tokio, Sidney en Singapore. Je hebt te maken met verschillende culturen, met verschillende systemen die op een andere manier in het verleden zijn opgezet, terwijl een incident al snel iedereen raakt. Je moet elkaar vertrouwen en leren samenwerken.

“Het Global team heeft onder andere pentesters, governance, NIST, ISO 27001-implementatie en techneuten die specifieke technologieën doen. Als GITSO moet je de vertaalslag maken naar de board, uitleggen waarom zij bepaalde maatregelen moeten nemen. Techniek interesseert hen niet, wel de impact op de business. Dat moet soms echt in jip- en janneketaal. Zo van: ‘We hebben hard gewerkt aan een Mercedes. Die staat buiten te ronken. Nu hebben we een ander team nodig om hem van A naar B te rijden en iemand die er in de winter andere banden onder zet.’ Zoiets…”

Jessica is ook voorzitter van PvIB, het Platform voor InformatieBeveiliging, een beroepsvereniging van 1.500 securityexperts. Hoeveel procent van de leden is vrouw? Haar inschatting is 5% en dat is wel representatief voor de sector. Is dat lage percentage een probleem? Jessica: “Ik houd er niet van om het als probleem te zien. Je moet doen wat

je leuk vindt. Als vrouwen er tegenop zien in IT te gaan, vind ik het belangrijk hen te helpen."

Is het niet een maatschappelijk probleem dat we iets missen als er zo weinig vrouwen in de IT werken en dat het dus ook voor ons mannen een probleem is? Jessica: "Mannen hebben wel een hoog gehalte van pik op tafel leggen en als ze echt wat verder gaan dan willen ze hem ook wel helemaal uitrollen om te kijken wie de langste heeft. Vrouwen hebben daar meestal wat minder zin in en door die omgeving kiezen ze liever voor een rol waar het wat leuker is met anderen."

Dus, meer vrouwen betekent minder competitie? Jessica: "Nee, vrouwen kunnen ook wel echt bitches zijn. Maar, als er veel mannen aan de top zijn, gaan ze niet ineens vrouwen erbij vragen. Als die mannen elkaar allemaal goed begrijpen, werkt het allemaal wat makkelijker en als er dan een vrouw bijkomt, moeten ze ineens moeite doen. Maar als het eenmaal mengt, snap je elkaar beter en gaat het ook beter."

Zouden we meer vrouwen aan de top kunnen krijgen met vrouwenquota? Minister Ollongren van Binnenlandse Zaken zei eens dat 30% in de boardroom vrouw moet zijn en er zijn maar weinig bedrijven die dat halen. Moet je dat afdwingen met een wet, of alleen de getallen laten zien en hopen dat het verandert? Jessica: "Nee, het moet geen doel op zich zijn om meer vrouwen te krijgen. Je moet leren hoe je het beste een bedrijf kunt besturen en dat is door een gezonde combinatie te hebben. Als je twee CISO-afdelingen tegenover elkaar zet, de ene wordt bestuurd door een vrouw, de andere door een man, dan zie je de verschillen. Percentages afdwingen vind ik gek. Het is belangrijk om jonge vrouwen die het vakgebied in willen, te motiveren, maar blijf vooral ook jezelf."

Jonge vrouwen motiveren om in de IT te gaan, is ook wat Cynthia en Jessica zelf veel doen. Ze zitten in een netwerk van vrouwelijke mentoren voor jonge vrouwelijke professionals. Cynthia doet ook met Cybersprint cybersecurity programma's op scholen en Jessica heeft in haar tijd bij Deloitte het Girls Hack Lab opgezet. Jessica: "Er was al een hacklab en daar kwamen alleen jongetjes op af. Toen heb ik met een collega een girls lab opgericht en actief meiden gevraagd. Het werd wel een beetje een kippenhok, gillen enzo, terwijl jongens toch wat stoerder zijn, maar het was wel superleuk."

Cynthia vraagt aan Jessica wat ze het allerleukste vindt aan haar baan. Jessica: “Alle mensen met wie ik werk, houden van hun baan. Er zit niemand bij die denkt: ‘Ik kan zo weer naar huis’. Als ik de mensen nu zou bellen over een incident, klimmen ze allemaal in een conference call, ook al is het nu vroeg in de ochtend in Sydney en middag in Chicago. Deze mensen zijn bloedfanatiek en willen van elkaar leren. Dat vind ik echt leuk.” Cynthia: “Ja, dat herken ik. Dat zorgt ervoor dat we veel bereiken.”

Cynthia maakt plaats voor Petra Oldengarm, directeur van brancheorganisatie Cyber Veilig Nederland. Ook zij heeft ooit bij KPN gewerkt, als research innovation manager. Verder is Petra teamhoofd geweest bij het ministerie van Binnenlandse Zaken, senior-manager windmolenonderzoek en IT-manager bij Energieonderzoek Centrum Nederland en director cybersecurity en lid van het managementteam bij Hoffmann Bedrijfsrecherche. Een indrukwekkende loopbaan, waarin ze vaak technisch onderzoek combineerde met managementtaken.

Petra heeft net als Jessica informatica gestudeerd. Petra: “Ik kwam bij die opleiding terecht dankzij een campagne, de ‘Thea studeert techniek-dagen’. Ik ging eerst kijken bij elektrotechniek, maar dat vond ik niks. Daarna ging ik met vriendinnen naar technische informatica. Dat sprak me erg aan, want ik was goed in wiskunde. Technische informatica gaat ook over logisch nadenken, maar dan meer toegepast. Ik hou van puzzelen en cryptoachtige dingen. Maar ja, daar zat ik dan tussen vijftig jongens en nog één ander meisje. Die kwam van de Antillen en had haar vader beloofd informatica te gaan studeren. Een week later zat ze op de kunstacademie. Dat was wel even slikken, want hoe handhaaf je je als enig meisje tussen vijftig jongens?”

Hoe verklaart ze het lage percentage vrouwen in het IT-onderwijs? In de internationale statistieken bungelt Nederland onderaan, terwijl de lijst wordt aangevoerd door landen als Bulgarije en Roemenië, die niet echt bekend staan om emancipatie. Petra: “IT zorgt voor baanzekerheid. Maar IT-banen zijn ook typisch 40-uurs banen en in Nederland willen veel vrouwen liever een deeltijdbaan. Ik zie veel passie en energie bij de vrouwen op deze avond en dat zie ik ook bij mijn mannelijke collega’s. Ik zou willen dat we dat wat

breder uitdragen. Ik geloof ook in diversiteit binnen teams en enthousiasme werkt aanstekelijk."

Deze avond is ook een spoedcursus voor mannen om te leren hoe ze moeten omgaan met vrouwen in IT. Aldus, wat moeten wij mannen vooral niet doen? Petra: "Ik ging eens naar een conferentie in het buitenland met een vrouwelijke technische collega en een mannelijke leidinggevende die zei: 'I brought two women, to be beautiful.' Die introductie kost je, als vrouw, een hele dag om je positie te heroveren en pas als je een presentatie geeft, zie je ze denken: 'Oh, ze is geen tolk maar een techneut'. Nog een voorbeeld. Ik werd een keer geïntroduceerd in het managementteam door mijn leidinggevende. Hij zei: 'Hiermee heb ik aangetoond dat er in deze organisatie geen glazen plafond is.' Ik merkte toen bij wijze van grap op dat er best nog wat vrouwen bij zouden kunnen, ook in de directie. Eenmaal buiten zei hij: 'Als je nog een keer zo'n opmerking maakt, dan heb je hier een buitengewoon overzichtelijke carrière'."

Ik leg Petra en Jessica een dilemma voor: Stel dat jullie zouden moeten kiezen tussen een team met alleen maar mannen of een team met alleen maar vrouwen. Waar zouden jullie het liefst werken? Beiden kiezen dan toch voor het mannenteam. Jessica: "Ik vind het best OK dat mannen wat eigenwijzer zijn en niet direct geloven wat er staat. Dat kritisch zijn, mogen vrouwen ook wel vaker doen." Petra: "Ik heb ook weleens gewerkt met allemaal vrouwen. Dan heeft die weer gedoe met die en dan praat je met die en dan heb jij weer gedoe met die andere… Dat heb je niet zo snel met mannen. Heb je ruzie en praat je het uit, dan is het daarna ook goed. Mannen hebben niet zo'n olifantengeheugen, al heb je wat dat betreft ook wel vrouwelijke mannen."

Hoe dan ook, een gezonde gendermix is het beste. We hebben deze avond daarom ook de uitreiking van het Roze Slot voor het cybersecurity bedrijf met de meeste vrouwen. Ik praat met Petra over hoe we tot de winnaar zijn gekomen. We hebben namelijk samen deelnemers geworven met een oproep op Twitter en LinkedIn en via de ledenlijst van Cyber Veilig Nederland. De oogst: vier inzendingen… Petra: "Dat laat wel zien dat veel bedrijven al denken nooit de norm te halen. Het gemiddelde is 8% en de inzenders zitten daar ver boven. De anderen zitten er dus ver onder."

Echter, welke vrouwen tel je wel en welke vrouwen tel je niet mee? Iemand had namelijk op Twitter gevraagd of secretaresses ook meetellen. Nee, alleen de specialisten, niet het ondersteunend personeel. Vervolgens: welke specialisten? Ook psychologen en onderwijskundigen die aan security awareness doen? En de complience officers en andere juristen? Die kunnen nog wel meetellen, mits ze in gemengde teams werken met techneuten en niet alleen maar 'zachte skills' hebben. Tot slot moet een bedrijf wel enige omvang hebben, want anders kan een zelfstandige hackster al snel de 100% claimen…

En de winnaar is … Deloitte. Daar is 25% van de cybersecurity afdeling vrouw. De prijs wordt symbolisch in ontvangst genomen door een vrouw en een man. Anne Ardon is consultant Cyber Risk Advisory in het Strategy Team. Als ik haar het slot wil geven, zegt ze dat het eigenlijk naar haar mannelijke collega moet: Jelle Niemantsverdriet. Hij is directeur Cyber Risk Services en verantwoordelijk voor de werving en selectie. Het is volgens haar vooral aan hem te danken dat hun club zo'n goeie genderbalance heeft.

Jelle vindt dat zelf te veel eer: "Ik ben er wel officieel verantwoordelijk voor, maar het komt vooral door onze cultuur van openheid en verbinden die leidt tot meer diversiteit, ook in manvrouwverdeling. Het is een soort zeepbel: ik kan hem in een bepaalde richting blazen, maar als ik te dichtbij kom, blaas ik hem kapot." Mooie metafoor, maar wie neemt nu die prijs in ontvangst? We geven Anne de sleutel en Jelle krijgt het slot, met een ketting om zijn nek. Zo krijgt hij de prijs, maar houdt Anne de controle erover.

Het was tof dat Cyber Veilig Nederland ons heeft geholpen met de werving en selectie voor het Roze Slot. Eigenlijk had ik ook nog een Loden Lul willen uitreiken, de prijs voor het cybersecurity bedrijf met de minste vrouwen. Maar dat vond Petra niet zo'n goed idee: "Naming en shaming werkt niet, positief zijn wel." Toch hoopt ze dat ook een prijs als het Roze Slot binnenkort niet meer hoeft, omdat er dan wel genoeg vrouwen in cybersecurity werken.

Laat ik besluiten met een gedachtenexperiment. Stel *the cybershit hits the fan* en Nederland wordt digitaal zwaar aangevallen. Hoe verloopt dan de escalatie? De eerste signalen dat er wat mis is, zullen waarschijnlijk

binnenkomen bij het Nationaal Cyber Security Centrum en, als het een nationale ramp lijkt te worden, opgeschaald worden naar de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Daar worden uiteraard de ministers van Binnenlandse Zaken en Defensie bij betrokken, die vervolgens het Dutch Cyber Command inschakelen. Een goede Nederlandse poldertraditie is publiek-private samenwerking, zeker in het digitale domein. Daarover adviseert onder andere de Cyber Security Raad. Via de Information Sharing and Analysis Center komen netwerkbeheerders, banken en telecombedrijven erbij. Cybersecurity bedrijven worden betrokken via de brancheorganisatie Cyber Veilig Nederland en de overige IT-bedrijven via Nederland ICT. Individuele cybersecurity experts kunnen ze bereiken via Platform voor Informatiebeveiliging.

Welnu, wie zitten daar dan in anno 2019? Wie zijn daar de leiders en verbindingsofficieren ten tijde van cyberoorlog? Allemaal vrouwen!

Patricia Zorko is directeur cybersecurity bij het ministerie van Justitie en Veiligheid en daarmee de baas van het NCSC en de ISAC's. De NCTV is weliswaar een man, maar hij zit daar nog maar net en weet weinig van cyber, dus wie is de plaatsvervangend NCTV? Jawel, ook Patricia. Zij informeert de betrokken ministers: Kajsa Ollongren van Binnenlandse Zaken en Ank Bijleveld van Defensie. Generaal Elanor Boekhold-O'Sullivan mobiliseert en leidt de Dutch Cyber Command. Elly van den Heuvel neemt vanuit de Cyber Security Raad contact op met de CISO's van bedrijven die gaan over onze kritieke infrastructuur: Jaya Baloo bij KPN en Louisella ten Pierik bij netbeheerder Stedin. Bij Cyber Veilig Nederland zal directeur Petra Oldengarm de Nederlandse cybersecurity bedrijven betrekken en Jessica Conquet mobiliseert de cybersecurity experts via PvIB, overigens naast haar taak als CISO bij ABN AMRO Clearing Bank.

Dit zijn dus het escalatieschema en de communicatiestructuur van Nederland ten tijde van cyberoorlog. Dan hebben we natuurlijk Mark Rutte nog. Zou hij dan wellicht als enige heer in het gezelschap even thee willen zetten terwijl ze aan het werk zijn? Zal hem goed bevallen, want Mark heeft een zwak voor slimme vrouwen.

We hebben vrouwen dus hard nodig in de wereld van cyberellende. Niet alleen bij een grote crisis, maar vooral ook op de verbindende posities om escalatie te voorkomen. Want als je niet alleen naar de technische functies

kijkt in cybersecurity, zie je genoeg vrouwen: managers, communicatie-experts, onderzoekers, ambtenaren en juristen. Onder andere bij de politie en het Openbaar Ministerie, zoals we zullen zien in het volgende hoofdstuk.

10. Politie helpt cybercriminelen

Een beetje computervredebreuk moet kunnen, als je het maar doet voor het goede doel. Doe je het voor financieel gewin, wraak of gewoon voor de lol, dan kan daar een flinke straf op staan: maximaal vier jaar gevangenis. Toch komt het meestal niet zover. Justitie begrijpt steeds meer dat cybercriminelen geen gewone criminelen zijn. Vaak zijn het jongeren die nog nooit eerder iets hebben misdaan, het internet willen ontdekken en gewoon wat uitproberen zonder al te veel na te denken over de consequenties. Terwijl de schade toch behoorlijk kan zijn. Zaak is ze niet direct te bedreigen of te straffen, maar tijdig aan de goede kant te krijgen door ze op hun verantwoordelijkheid te wijzen. Of zoals Spider-Man zei: “With great power comes great responsibility”.

Vanuit de hackerscene kunnen hackerspaces behoorlijk deescalerend werken. Daar ontmoeten jonge hackers de ervaren hackers en wordt er weleens een hartig gesprek gevoerd over de ethische grenzen van hun kunnen. Zelfregulering gebeurt ook online op chatfora. Soms lopen hackers elkaar daar juist op te jutten, om met bewijs te komen dat ze ergens hebben ingebroken, maar het gebeurt net zo vaak dat ze elkaar terechtwijzen. Nu de nieuwe generatie hackers aan de slag gaat, hebben die van mijn generatie zich verenigd als de GGOH, Guild of Grumpy Old Hackers. Zij zijn nog uit de tijd dat alles kon en mocht online, weten als geen ander wat nu niet meer kan en begeleiden jonge hackers on- en offline.

Ook bij politie en justitie is doorgedrongen dat jonge cybercriminelen anders zijn dan gewone criminelen. Voor die jongeren is er nu een programma: Hack_Right. Daarin kunnen cyberdaders van 12 tot 23 jaar invulling geven aan een alternatieve taakstraf. Zelf heb ik bij drie veroordeelden hun taakstraf van twintig uur mogen helpen uitvoeren. Tijdens de intake kreeg ik te horen wat de jonge veroordeelden hadden

gedaan en probeerde ik hun hacking skills in te schatten. Vervolgens moesten ze mijn boek *Helpende hackers* lezen. En alsof dat nog niet genoeg straf was, moesten ze ook in mijn praatprogramma live voor het publiek opbiechten wat ze hadden gedaan. Gevolgd door het oordeel van de Guild of Grumpy Old Hackers.

12 februari 2019 is het zover: Hack Talk 10 over 'Cyberboefjes'. Voor het programma zijn uitgenodigd: criminologen, politie, Openbaar Ministerie, reclassering, de GGOH en de drie veroordeelden. Vanwege het thema haakt naast onze gebruikelijke sponsoren Stedin, gemeente Rotterdam en dcypher ook veiliginternetten.nl aan. We hebben hierdoor wat extra geld voor pizza voor iedereen en kunnen een extra zaal huren om de fototentoonstelling Hackers Handshake naar Rotterdam te halen. Zo hebben het publiek en de boefjes letterlijk een beeld van wie de hackers zijn die aan de goede kant van de wet staan.

We beginnen met een introductie van de Guild of Grumpy Old Hackers: Edwin van Andel, CEO van Zerocopter, Hans van de Looy, onafhankelijk IT-securityexpert met 36 jaar ervaring bij verschillende bedrijven, Mattijs van Ommeren, securityconsultant bij het Finse bedrijf Nixu, en helpende hacker Victor Gevers. Samen zijn ze goed voor meer dan honderd jaar hackervaring. Ze zitten het hele programma naast het podium om gevraagd en ongevraagd commentaar te geven op alles. Hans heeft voor de gelegenheid zijn T-shirt aan met Statler en Waldorf, de oude mannetjes van The Muppet Show.

Eerst komen twee criminologen aan het woord over de vraag: wat is cybercrime en hoe erg is het als je daarvoor veroordeeld wordt? Wytske van der Wagen is assistent-professor aan de Erasmus Universiteit. In het verleden heeft ze gewerkt bij het Wetenschappelijk Onderzoeks- en Documentatie Centrum van het ministerie van Justitie en Veiligheid en stagegelopen bij de politie en bij de Nederlandse ambassade in Moskou. Ervaring in Rusland is best handig als je hackers wil onderzoeken. Elina van 't Zand-Kurtovic is ook assistent-professor, maar dan aan de Universiteit Leiden. Ze heeft zeven jaar zaken afgehandeld over Verklaringen Omtrent Gedrag bij Van Oosten Advocaten. Ze heeft ook bij

het Openbaar Ministerie gewerkt en doet veel vrijwilligerswerk voor gedetineerden.

Is cybercriminaliteit vooral computervredebreuk of gaat het gepaard met andere delicten? Volgens Wytske kun je grofweg onderscheid maken tussen computervredebreuk als het inbreken in systemen als doel op zich, bijvoorbeeld om lekken aan te tonen, en computervredebreuk als middel voor een ander doel dat vaak gepaard gaat met overtredingen, zoals fraude, het verkopen van gegevens, sextortion (afpersing door te dreigen pikante beelden vrij te geven) of problemen in de relationele sfeer.

Stel dat je gepakt wordt en een strafblad krijgt, wat zijn daar dan de gevolgen van? Elina heeft hier haar proefschrift over geschreven: *'Invisible bars: the impact of having a criminal record on young adults' position in the labour market'* (2017). Volgens Elina hangt het effect van een strafblad voornamelijk af van het soort baan dat je wilt. Bij de overheid vragen ze vaker om een antecedentenscreening en Verklaring Omtrent Gedrag. Dan kun je het dus wel vergeten als je een strafblad hebt. Ze kijken overigens tot vier jaar terug bij volwassenen en tot twee jaar als je jonger bent dan 23 jaar, dus die strafaantekening verjaart best wel snel. En er zijn ook veel banen waar helemaal geen screening wordt gevraagd.

Wat Elina opvalt, is dat het aantal VOG-aanvragen de laatste jaren explosief is toegenomen: inmiddels meer dan een miljoen per jaar. Dat zal volgens haar wel iets te maken hebben met de toename in securitymaatregelen, vanuit een gevoel controle te willen hebben. Wat ook meespeelt, is dat zo'n aanvraag vrij weinig kost. We vragen de zaal wie er een VOG heeft aangevraagd. Ongeveer een derde steekt de hand op. En wie heeft hem niet gekregen? Enkelen steken hun hand op, waarvan een van de cyberboefjes en iemand van de politie. Een interessante vraag voor deze avond is uiteraard of een veroordeling voor computervredebreuk niet juist een goed cv is in de hackerswereld. Dat zou kunnen, maar daar is volgens Elina nog geen onderzoek naar gedaan.

Dat cybercrime toch wel echt iets anders is dan gewone misdaad betoogt Wytske in haar proefschrift: *'From Cybercrime to Cyborgcrime'* (2018). De huidige criminologie gaat volgens haar nog te veel uit van een antropocentrisch perspectief waarbij de verklaring voor criminaliteit vooral

gezocht wordt in bepaalde psychische en sociale omstandigheden die ervoor zorgen dat mensen overgaan tot daden die door anderen gezien worden als misdaad. Kijk je echter naar cyberdaders dan moet je ook kijken naar de rol van technologie en hoe daders interacteren met de technologie.

Informatietechnologie speelt dus zelf een grote rol in wat wel en niet kan. Cyberdaders willen graag verkennen wat die techniek allemaal kan en of het ze lukt om de technische grenzen en die van hun eigen kunnen steeds te verleggen. Hierbij kan dan de grens tussen goed en kwaad, ethisch en onethisch vervagen. Cyborg is een mens die een relatie aangaat met een technologie die zelf ook handelt binnen het netwerk. Of simpel gezegd: je gaat niet 100.000 x belletje drukken, maar je kunt wel met een druk op de knop een DDoS plegen, zodat er 100.000 x op de bel wordt gedrukt. Digitale schakelingen maken dat mogelijk, de mechanische niet.

Pleit de rol van technologie als mededader je dan vrij van schuld? Nee. Wel wordt het volgens hen lastiger om de intentie achter de daad te achterhalen. Was het verspreiden van een virus opzet en kon je de gevolgen overzien? Of als je computer besmet is en deelneemt aan een botnet, ben je dan dader of slachtoffer? Ook bij de vervolging van daders worden tools ingezet die op hun beurt een rol spelen in het bepalen of iets een crimineel feit is of niet. Kortom, ook daarin is nog genoeg onderzoek te doen.

Wytske en Elina zijn net gestart met een nieuw onderzoek om een typologie te ontwikkelen voor daders van computervredebreuk op basis van onder andere hun achtergronden, motieven en de tools die ze gebruiken. De vraag is dan of deze specifieke groep cyberdaders een ander soort interventies en sancties vereisen dan de gebruikelijke criminelen. De criminologen hebben al veel experts gesproken en zoeken nu contact met de betrokkenen zelf. Onder de aanwezigen bij Hack Talk zullen er vast een paar rondlopen die zelf dader zijn geweest, op z’n minst andere daders kennen of getuige zijn geweest. Wytske en Elina zetten hun onderzoek dus ook deze avond voort. Opdrachtgever is het ministerie van Justitie en Veiligheid. De uitkomsten kunnen effect hebben op hoe ze daar in Den Haag aankijken tegen cyberboefjes.

Over naar Hack_Right. Floor Jansen van Team High Tech Crime van de Nederlandse politie had het programma eerder gelanceerd bij Hack Talk 4

over ‘Next Gen Hackers’. We zijn nu precies een jaar verder. Vandaag is ze hier met Ymkje Lugten, themaspecialist cybercrime van het Openbaar Ministerie. Samen met Bureau Halt, reclassering en coaches vanuit cybersecurity bedrijven hebben ze inmiddels elf jongeren succesvol begeleid.

Floor: “Dat zijn nog geen schokkende aantallen, maar het worden er steeds meer en uit heel Nederland. We zijn een soort uitzendbureau om vraag en aanbod aan elkaar te knopen.” Ymkje: “Het gaat vooral om jongeren die nieuwsgierig zijn naar IT en gaandeweg strafbare dingen doen. Als ze eerlijk zijn over wat ze hebben gedaan, kunnen ze hun skills ook op een goede manier inzetten bij bedrijven.”

De maximale leeftijd om mee te doen is 23 jaar. De jongste deelnemer is op dit moment 15. Floor: “Deze jongen was al op zijn 11e begonnen met cybercrime. We dachten eerst dat het zijn oudere broer moest zijn. Tussen de leeftijd 15 tot 21 jaar worden de meeste delicten gepleegd. Jongeren zijn nog impulsief, zoeken naar identiteit, willen laten zien wat ze kunnen, zichzelf overtuigen hoe ver ze kunnen komen en gaan dan een grens over. Maar ze zijn op die leeftijd ook nog veranderbaar. Voor iemand van 50 jaar werkt ons programma waarschijnlijk niet.” Iedereen kijkt naar de GGOH, waarop Floor zegt: “Dat is een toch al verloren generatie”. De heren moeten lachen. Behalve Victor, want die zit aandachtig in zijn laptop te werken, omdat hij weer ergens een lek heeft gevonden.

Hoe voorkom je dat cyberboefjes Hack_Right gebruiken als een makkelijke manier om onder een strafblad uit te komen? Volgens Ymkje moet je niet onderschatten wat een aanhouding met je doet. “Er staat ineens een heel politieteam in je kamer en ze nemen al je apparatuur in beslag. Dat is geen pretje en heeft veel impact. Je krijgt ook geen stage cadeau van ons. We kijken goed naar wat je moet leren, ook over de slachtoffers die je maakt.” Floor: “We willen positieve alternatieven aanbieden. Hackerspaces kennen ze vaak nog niet en in hun omgeving vinden ze ook geen gehoor. Dat horen we ook van de coaches, met wie we nu onze eerste evaluatie hebben gedaan. Die merken dat de ouders en docenten van de jongeren hen niet snappen. De coaches kunnen wel uitleggen waar de grenzen liggen van wat wel en niet kan.”

De GGOH beamen dit. Mattijs: “Ik vind Hack_Right een heel mooi initiatief.” Hans zit ook in een van de werkgroepen van coaches. Victor vult aan dat veel jongeren via Twitter Direct Messaging contact zoeken met hem. “Dan is bijvoorbeeld hun hack net op het nieuws geweest en zijn ze bang om gepakt te worden. Dan hebben ze behoefte aan een veilig kanaal.” Zo doen de GGOH dus ook aan online coaching. Zawadi Done, die eerder bij Hack Talk aan tafel was en wiens portret te zien is in de fototentoonstelling Hackers Handshake, is momenteel de jongste Hack_Right-coach. Hij heeft video’s online geplaatst waarin hij daders van cybercrime interviewt.

Preventie is belangrijk. De politie heeft een campagne gelanceerd met de titel ‘Je bent slechts één klik verwijderd van cybercrime’. Op Instagram postte vlogster Marije Zuurveld een bericht waarin ze schrijft: “Heb dus een maniertje gevonden om stiekem op d’r insta in te loggen! (Linkje in mn bio)”. Als je daarop klikt, word je doorgelinkt naar een video waarin ze uitlegt dat het overnemen van iemands account strafbaar is. Vergelijkbare berichten verschenen op social media over manieren om gamegeld te stelen in Fortnite of een DDoS-aanval te kopen. Je wordt dan doorgestuurd naar Vraaghetdepolitie.nl, waar uitleg volgt over wat wel en niet mag, compleet met chatfunctie.

Iemand uit het publiek vraagt: “Je kunt die jongeren wel vertellen dat het niet mag, maar is de pakkans niet zo laag dat jongeren denken dat het toch wel kan?” Een politieagent springt op: “Inmiddels heeft elk team een cybercrime specialist en we zijn nu ook actiever op het dark web, dus de pakkans wordt steeds groter.” Volgens Floor speelt de pakkans bij de jongeren die zij ziet niet zo’n grote rol. Het gaat er meer om dat ze niet weten wat wel en niet mag. Waar het volgens haar vaak misgaat, is dat jongeren minder geduld hebben. Zo had een jongen lekken in het schoolsysteem gevonden en gemeld, maar de schoolleiding deed er niets aan. Toen heeft hij er zijn profielwerkstuk van gemaakt, de lekken gepubliceerd en deed de school aangifte.

Daarmee komen we aan bij coordinated vulnerability disclosure. Is dat een manier om jongeren aan de goede kant te krijgen? Volgens Ymkje wel. Ze heeft hier een boek over geschreven: *Ethisch hacken. Hoe kan de positie van de ethische hacker het beste juridisch beschermd worden?* Dat was in

2014, toen er nog veel onzekerheid was onder hackers over of ze wel of niet vervolgd konden worden bij het melden van lekken. Inmiddels heeft het Openbaar Ministerie hier richtlijnen voor. Ymkje: “Ethisch hacken mag, zolang je niet te ver gaat. Je kunt bijvoorbeeld kwetsbaarheden aantonen bij een ziekenhuis door eenmalig een dossier te bekijken. Maar ga niet alles downloaden of zoeken op namen van bekende Nederlanders.”

Tot slot: hoe kunnen wij als hackercommunity Hack_Right helpen? Floor: “Help ons met stageplaatsen en coaching. Reclassering en HALT zijn enthousiast en er zijn al aardig wat bedrijven die willen meehelpen, maar we kunnen wel wat meer stageplaatsen gebruiken. We zoeken vooral meer coaches. Die hoeven niet altijd Grumpy en Old te zijn. Jonge begeleiders zijn ook welkom.”

Na onderzoek, type daders, arrestatie en veroordeling, nu de man die vanuit reclassering de cyberboefjes begeleidt: Ton Starrenburg. De manier waarop hij bij Hack Talk is terechtgekomen, is bijzonder. Bij de aflevering Next Gen Hackers het jaar ervoor speelden we de rechtszaak Groene Hart Ziekenhuis na. Het ging over iemand die een ziekenhuis had gehackt en daarbij te ver was gegaan. Drie bezoekers werden met een dobbelsteen willekeurig aangewezen om samen het publieksoordeel te vellen. Hun oordeel was 80 uur taakstraf, precies hetzelfde als bij de echte rechtszaak. Wat bleek, de bezoekers waren helemaal niet zo willekeurig. Een ervan was al betrokken bij Hack_Right, de tweede was van reclassering en de derde een net-veroordeelde cyberboef. Huh, een of andere Mindf*cktruc? Nee, gewoon toeval.

De vrouw van reclassering bleek de partner van Ton te zijn en zij stuurde hem naar mij omdat hij net drie cyberboefjes onder zijn hoede had gekregen. We spraken met elkaar af in het Rotterdamse café Rotown en kwamen zo op het snode plan de jonge veroordeelden mijn boek te laten lezen en op het podium hun misdaden te laten bekennen. Dat is een stuk zinvoller dan sponsjes inpakken, wat de taakstraf van de Groene-Harthacker was. Dat vonden de cyberboefjes wel wat en zo is het dus gekomen dat Ton en zij bij Hack Talk zijn.

Ton is ooit begonnen bij de douane in de haven van Rotterdam, werd toen maatschappelijk werker in de drugshulpverlening en kwam zo bij

reclassering terecht. Ongeveer de helft van zijn tijd besteedt hij aan cybercriminelen. Reclassering is overigens geen onderdeel van politie of de overheid, maar een onafhankelijke stichting die werkt in opdracht van justitie. Ze schrijven adviezen, begeleiden veroordeelden terug de samenleving in en voeren Hack_Right uit. Elk cyberboefje krijgt twee jaar reclasseringstoezicht.

In hoeverre verschillen, volgens Ton, cyberdaders van gewone criminelen? Ton: “Ze zijn heel verschillend, maar er wordt ook wel te snel een psychologisch sausje overheen gegooid. Zo van: je bent autist of je hebt ADHD en daar doen we dan wat mee. Zo werkt dat niet. Het gaat volgens mij vooral om hun sociale netwerk en hoe offline en online gedrag elkaar beïnvloeden. Wat ik wil weten is: wanneer je met de computer bent begonnen, wie daarbij een rol speelde, hoe je te werk bent gegaan en hoe je die keuze hebt gemaakt waarbij je de verkeerde kant op bent gegaan. We kijken ook anders naar de slachtoffers. Dat kunnen er online veel meer zijn dan offline. We proberen, voor zover mogelijk, de daders in contact te brengen met slachtoffers, zodat ze de gevolgen kunnen zien.”

Daarna vertellen de drie cyberboefjes bij Hack Talk om de beurt wat ze hebben gedaan. De Guild of Grumpy Old Hackers verhoort hen en geeft een oordeel: is het cyberboefje een echte hacker en heeft hij op een gepaste manier geboet voor wat hij verkeerd heeft gedaan?

We beginnen met Owen, die zijn school heeft gehackt. Hij was ooit begonnen met Kali Linux, de standaard hacker toolkit, maar dacht dat het makkelijker is om gewoon te googelen op ‘How to hack a website?’ Zo leerde hij hoe hij een SQL-injectie kan doen: commando’s invullen bij een tekstvakje op de site, om zo direct de database aan te sturen. Dat probeerde hij bij de website van zijn school. Het eerste wat hij zag, was wat technische documentatie over de site, die bleek te zijn gebouwd door eerstejaars hbo-studenten in 2011. Niet erg up-to-date dus. Het leek hem in eerste instantie niet erg interessant.

Twee weken later probeerde Owen een andere SQL-injectie en verkreeg zo de hashcode (versleutelde waarde) van het wachtwoord van de ICT-beheerder. Door de gebrekkige versleuteling kon hij die waarde terugbrengen tot het oorspronkelijke wachtwoord. Dat bleek de naam van

een stad te zijn. Niet zo'n sterk wachtwoord dus en het bleek te werken op alle sites van de school. Nu kon hij overal in. Owen: "Ik ging cijfers aanpassen, roosters wijzigen en lessen laten uitvallen. Ik ging er ook over opscheppen tegen medeleerlingen: 'Hee, zal ik je cijfer aanpassen?' Het boeide me niet zo, vroeg of laat zouden ze er toch wel achter komen. Ik ging in die tijd ook niet zo veel meer naar school."

De school deed aangifte. Vroeg in de ochtend verscheen bij Owen een arrestatieteam voor de deur. Dat had hij niet verwacht. "Ik was pas om 5.00 uur naar bed gegaan en toen mijn moeder om 7.00 uur riep dat we bezoek hadden, wilde ik verder slapen. Kwamen er ineens drie mannen tegelijk binnen. Een vroeg: 'Ben je van plan om weg te rennen?' Ik zei: 'Als ik de mogelijkheid had, deed ik het graag, maar dat zal niet lukken.' Ik werd meegenomen en moest van 8.00 tot 16.00 uur wachten in een cel. Daarna werd ik verhoord, over wat ik had gedaan en wie erbij betrokken waren. Ik wist niet precies waarvan ik werd verdacht, maar het ging in ieder geval om computervredebreuk."

Ton kan beamen dat het verhaal van Owen klopt en voegt eraan toe: "Mijn voorstel vanuit reclassering was om eerst zijn dag-nachtritme terug te brengen."

De GGOH start het verhoor:

Mattijs: "Als je niet had opgeschept, was je ermee weggekomen. Wilde je juist gepakt worden?"

Owen: "Nou, het boeide me gewoon niet zo."

Victor: "Ik snap wel dat je een speelplek zoekt, maar toch jammer dat je je school hebt gekozen. Er zijn genoeg andere speelplaatsen, zoals een Capture the Flag."

Hans: "Weet je waar je over de grens bent gegaan?"

Owen: "Ja, dat ik in de database was gekomen en dat niet heb gemeld."

Hans: "Stond de school daar wel voor open?"

Owen: "Ik denk het niet. Die ICT-mensen wisten al weinig. Als ik al het wachtwoord had en overal kon gebruiken…"

Edwin: "Zou je het weer doen?"

Owen: "Niet opnieuw. Ik zou het de volgende keer wel melden, maar voor deze keer was het wel leuk."

Heeft Owen volgens de GGOH genoeg straf gekregen zo? “Ja”, roepen ze in koor, “Hij moest jouw boek lezen!” Dat blijkt hij nog niet te hebben gedaan. Ik pleit daarom voor een strafverdubbeling: hij moet ook Wytskes proefschrift lezen. Heeft Owen tot slot nog een tip voor andere jonge hackers? “Ja, als je een lek vindt, meld dat gewoon.”

Na de pauze gaan we verder met een jongen van 19 jaar die wel wil bekennen, maar liefst niet onder zijn eigen naam. We noemen hem ‘A’. Als hij opkomt, heeft hij zijn capuchon dichtgetrokken en zegt: “De muziek staat wel erg hard!” Ik vermeld dat de muziek onderdeel is van zijn taakstraf en vraag of hij mijn boek *Helpende hackers* heeft gelezen. A: “Ja. Ik reis elke dag met de trein naar mijn werk en dan lees ik een stukje”. Mooi. Je hebt een site gehackt die populair is onder jongeren. Hoe ben je te werk gegaan? A: “Met blind XSS. Kon shell uploaden.”

XSS staat voor cross-site scripting en een shell is een gebruikersinterface waar je commando’s kunt invoeren. A legt uit: “Als een site niet goed beveiligd is, kun je HTML-code of Javascript invoeren. Blind XSS betekent dat als ik dat aan de voorkant van de pagina invoer het aan de achterkant bij de medewerker wordt uitgevoerd. Ik kon de achtergrondfoto van de pagina aanpassen of een bestandje uploaden. Ik heb toen een shell geüpload en daarna de database gedownload. Ik zag gebruikersnamen, wachtwoorden, emailadressen, het favoriete dier van de gebruikers en andere profielgegevens.”

Victor reageert verbaasd: “Hoe heb je die credentials uit de database gehaald? Waren die niet gehashed?” A: “Ja, met MD5.” De heren van de GGOH moeten er hard om lachen. MD5 is vandaag de dag geen goede versleuteling meer.

Waarom deed hij dit? A: “Het begon 10 jaar geleden. Ik wilde credits op een site, maar geen geld uitgeven. Op die site waren wat mensen die vervelend deden tegen mij, waardoor ik dit terug deed. Daarna ging ik steeds meer hacken, ook buiten die site.” Ton neemt het voor hem op: “Wat ik hier vooral interessant aan vind is de invloed van anderen. Het elkaar opjutten.”

Hoe verliep de arrestatie? A: “Ze kwamen op een maandag om 8.00 uur binnen. De politie wist dat ik thuis was. Dat hadden ze op school gevraagd.

Het waren er twee: een politieagent en een rechercheur. Ik lag nog op bed en mocht me niet omkleden zonder hen erbij. Ze pakten mijn computer, laptop, USB en PlayStation. Daarna moest ik een jaar wachten tot ik op verhoor moest komen. Ze hadden niet één, maar acht zaken tegen me. Allemaal online dingen die te maken hadden met hacken, vooral Habbo, Minecraft of personen die ik had gehackt. Slechts drie van de acht zijn bewezen."

Intussen heeft A geleerd dat hij zijn vaardigheden ook ten goede kan gebruiken en doet hij aan coordinated vulnerability disclosure. Hij vond en meldde kwetsbaarheden op sites van Bol, SIDN en IBD (de Informatiebeveiligingsdienst voor Nederlandse gemeenten). Dat zijn toch zeker niet de minsten. Hij had zelfs een melding voor Zerocopter, waarvan Edwin de baas is. A: "Ik had me als hacker aangemeld bij Zerocopter, maar was nog niet geaccepteerd. Toen vond ik twee kleine foutjes op hun site en kreeg ik een T-shirt, stickers en nog wat kleine dingetjes." Bij een ander bedrijf vond hij wat zwaardere kwetsbaarheden, meldde die en kon meteen op sollicitatiegesprek komen. Daar werkt hij nu.

A heeft nu een project op Github, het platform voor opensourceprojecten. Hij heeft daar een tool staan waarmee je een Blind XSS geautomatiseerd kunt uitvoeren. Ik heb er een hacker naartoe gestuurd met de vraag: "Is dit een exploitkit voor dummies? Het zou toch niet zo best zijn als iedereen hiermee kan hacken zonder de consequenties te overzien." Het antwoord was: "Nee, het is eerder een tool voor ervaren hackers. Het maakt XSS vinden niet makkelijker, maar helpt wanneer je het resultaat van je invoer niet zelf kunt zien, zoals bij Blind XSS. Je moet weten hoe XSS werkt, wil je er überhaupt gebruik van kunnen maken." De GGOH is het daarmee eens.

Het eindoordeel over A is eenduidig: hier hebben we een echte hacker in wording. Volgens Edwin moet hij nog één ding doen om zijn taakstraf te volbrengen: een flesje Club Mate opdrinken. Dat doet A meteen. Heeft hij zelf nog tips voor jonge hackers? "Nee". Hij is zichtbaar blij dat hij ervan af is. Het hele traject heeft hem vier jaar gekost.

Ons derde en laatste cyberboefje noemen we 'B'. Hij is 20 jaar, heeft netjes zijn middelbare school afgemaakt en studeert. Hij is veroordeeld voor

computervredebreuk en Marktplaatsfraude. B: “Het begon op een gameforum. Daar zat ik sinds 2015. Ik zag mensen erover praten dat je online spullen kan bestellen, bijvoorbeeld via Bol.com en dan doen alsof die niet waren aangekomen en je geld terugvragen. Als je je gegevens aan iemand op die site gaf, konden ze het voor je doen en deelde je de winst. Ik vond iemand en ging met hem Skypen. Hij vertelde hoe makkelijk het was en dat je niet gepakt kon worden. Ik probeerde het op een dag en werd inderdaad niet gepakt. Toen nog een keer… Ik deed het gedeeltelijk voor het geld want ik had een studielening, maar veel van de spullen die ik kreeg gaf ik aan mijn vrienden. Maar dat maakt voor de wet niet uit. Ik dacht: het zijn grote bedrijven, die missen die 300 euro niet echt. Zo rationaliseer je wat je hebt gedaan.”

Toen werd hij opgepakt. Hoe ging dat in zijn werk? “Om 6.00 uur werd er op de deur gebonsd. Ik woonde met meerdere mensen samen, dus ik dacht dat het niet voor mij was. Toen stonden er ineens zes mannen in mijn kamer. Ze wezen naar me en zeiden: ‘Jou moeten we hebben! Wie zijn er nog meer binnen?’ Ze waren niet hardhandig, maar wel duidelijk. Ze vroegen toestemming om spullen mee te nemen. Op diezelfde dag was de politie ook bij mijn broer in Groningen. Dat ging wel anders, want daar werd de deur geforceerd. Toen ze binnenkwamen, pakte mijn broer zijn mobiel om de politie te bellen. Ze dachten dat hij een pistool pakte en riepen: ‘Stilliggen’. Op dat moment flitste zijn leven even aan hem voorbij. Hij doet computerwetenschappen, ik doe biochemie, dus ze dachten eerst dat ze hem moesten hebben.”

Wat vinden de GGOH van het verhaal van B? De heren zijn eensgezind en duidelijk: “Je bent geen hacker. Dit is gewoon ordinaire winkeldiefstal.” Maar B is ook veroordeeld voor computervredebreuk. Op het forum kocht hij namelijk inloggegevens voor Spotify- en Netflix-accounts. Dat is volgens artikel 138a het ‘aannemen van valse hoedanigheid of identiteit’. Nee, de heren zijn onverbiddelijk: “Dat maakt je nog geen hacker”. OK, B, laat dat je straf zijn: volgens de GGOH ben je geen hacker.

B heeft inmiddels zijn taakstraf goed vervuld. B: “Omdat ik zelf op school nooit les heb gehad over wat online wel en niet kan, heb ik nu zelf een les ontwikkeld en ik geef die op verschillende middelbare scholen. In die lessen doe ik een enquête over wat ze wel of niet weten van cybercrime.

Dan blijkt dat ouders en omgeving daar toch echt wel wat meer mee moeten doen.”

Na de vraag wat cybercrime is en wie de boefjes zijn, nu de stageplaatsen. De kracht van Hack_Right is immers om hackers een beter perspectief te gunnen. We praten daarover met Barry van Kampen, directeur van cybersecurity bedrijf S-Unit en voorzitter van hackerspace Random Data. Hij is ook actief bij het jaarlijkse hackerevent Hack in the Box en doet het programma Hack in the Class, waarmee hij gastlessen verzorgt op scholen. In de tussentijd heeft hij een cyberboefje onder zijn hoede gehad. Zo ook Ad Buckens. Hij is directeur cybersecurity bij IT-bedrijf CGI en gaat daar over de penetratietesten, Red Teaming en het crisismanagement. De heren blijken elkaar te kennen van zowel Hack_Right als Hack in the Class.

Hun cyberboefjes zijn er niet bij deze avond. Barry kent die van hem al jaren en wil hem liever anoniem houden. Dit boefje is een bijzonder geval, want hij blijkt al sinds zijn 11e betrokken te zijn bij cybercrime. Uiteindelijk werd hij gepakt omdat hij een website had waar hij DDoS-aanvallen verkocht. Barry: “Het doel was om hem uit zijn isolement te halen en te laten merken wat normaal is en wat niet. Dat kan in de omgeving van onze hackerspace. We hebben in de intake ook een soort ‘good cop-bad cop’ gespeeld om uit te zoeken met wie we te maken hadden en hoe we van zoiets toch iets positiefs konden maken. Vanuit Hack in the Class gaven we hem opdracht om een wachtwoordchecker te bouwen. In totaal heb ik in het afgelopen halfjaar 100 uur aan hem besteed. We hebben nog steeds WhatsApp-contact. Je ziet hem echt groeien.” Barry is wat dat betreft een echte vaderfiguur in de hackerscene. Via projecten als deze heeft hij al meer dan 1.000 uur besteed aan de begeleiding van jonge hackers.

Het boefje van Ad heet Erik en is ook een geval apart. Erik was op het journaal te zien, om te bekennen dat het niet goed was dat hij zijn school had gehackt. Maar wat betekent het voor Ad om zo iemand in zijn bedrijf op te nemen als stagiair? Ad: “Wij zijn een groot bedrijf, dus dat geeft intern best wat gedoe. De intake van de hacker is dan heel belangrijk: wat zijn de achtergronden, hoe kun je hem helpen? Maar ook: heeft hij niet een van onze klanten onderuitgehaald?” Erik ging bij CGI aan de slag met de ‘Leidraad Coordinated Vulnerability Disclosure’ van het NCSC. Ad: “Erik

heeft geholpen de tekst te verjongen. Wij vonden de tekst wel sterk, maar hij keek ernaar en zei: ‘Wat jullie in 180 woorden zeggen, kan ik in 100.’ Hij had een soort flowchart gemaakt. Dat was voor ons wel een openbaring.”

We praten met deze coaches, de GGOH en het publiek over de oorzaken van cybercrime op jonge leeftijd. Conclusie is dat zowel het onderwijs als de ouders te weinig weten van cybersecurity om dergelijk hackgedrag te herkennen en bij te sturen. In hun online ontdekkingstocht ontbreekt het jongeren aan context en begeleiding. We kunnen dat ook niet verwachten van hun omgeving dus legt dat de verantwoordelijkheid bij ons als securitysector om het talent van jonge hackers ten goede te keren.

Na deze avond volgt een rondreizend circus van Hack_Right langs verschillende congressen, om de overheid te laten zien dat de aanpak van cybercriminaliteit anders kan en bedrijven te trekken die coaching en stageplaatsen kunnen bieden. Op 29 oktober 2019 maken we de balans op met een gezamenlijk event. In een mooi oud kasteel in Woerden zijn alle betrokken partijen aanwezig om bedrijven te laten zien wat ze kunnen verwachten. Doen ze mee, dan mogen ze hun bedrijfslogo en handtekening op een groot wit bord zetten. De foto ervan staat nog steeds op politie.nl en we zien daar veel bekende security bedrijven: Zerocopter, Fox-IT, KPN Security, Deloitte, Secura, Radically Open Security, Guardian360, Northwave, Qbit, Access42, CGI en S-unit. Maar ook banken: ING, ABN-AMRO, de Volksbank, Rabobank en de Nederlandse Betaalvereniging. De gemeente Rotterdam staat er ook bij. En ons nieuwe hackersclubje, het Dutch Institute for Vulnerability Disclosure, oftewel DIVD, maar daarover meer in het laatste hoofdstuk.

11. Den Haag veiliger na flinke hack

Alles is uiteindelijk wel op de een of andere manier te hacken. Dan kun je er dus maar beter zeker van zijn dat degene die dat doet aan jouw kant staat. Steeds meer organisaties huren daarom pentesters in, die je IT-omgeving onder handen nemen zoals kwaadwillenden dat zouden doen. Je geeft ze dan een lijstje van je systemen, een bepaald tijdsbestek waarbinnen ze van alles mogen proberen en je krijgt na enkele weken een keurig rapport met bevindingen en advies. Een andere methode is je eigen IT-afdeling in tweeën te splitsen in een red team (aanvallers) en een blue team (verdedigers). Beide methodes blijken effectief, maar zijn ook beperkt, omdat elke hacker een eigen methodiek heeft. Als je veel verschillende hackers wilt inzetten, kan dat het beste met een hack event.

Kies een dag waarop iedereen die dat wil jouw systemen kan beproeven op kwetsbaarheden. Spreek met de deelnemers duidelijke spelregels af. De kunst is dat je enerzijds de hackers een spannende target geeft en voldoende ruimte om hun eigen technieken toe te passen. Anderzijds mag je oproep niet resulteren in datalekken, het platleggen van systemen of reputatieschade. Ook hier komen de leidraden van responsible disclosure en coordinated vulnerability disclosure van pas: wie iets vindt, meldt dat bij de organisatie. Als organisatie laat je weten wat ermee wordt gedaan en geef je de betreffende hacker de credits. Je moet dan wel je hele backoffice in stelling brengen om de meldingen te ontvangen en wat externe experts erbij halen om de bevindingen te beoordelen.

Vervolgens maak je er een echt evenement van: een leuke locatie met goede werkplekken voor de hackers, een paar bekende gezichten om het event te openen en te sluiten, leuke prijzen en veel Club Mate, de typische cafeïnedrank voor hackers. Je zorgt dan niet alleen voor een goede opkomst, maar laat ook aan de buitenwereld zien dat je hackers serieus

neemt. Voor de hackers zelf is zo'n evenement leuk: ze ontmoeten andere hackers om bij te praten, van elkaar te leren en elkaars krachten te meten.

Zelf heb ik twee keer zo'n evenement georganiseerd. De eerste was in opdracht van Eneco, die hun slimme thermostaat de Toon weleens op de pijnbank wilden leggen. We noemden het evenement 'Game of Toons', hadden een geweldige dag, maar het bleek achteraf onduidelijk wat er precies met de uitkomsten is gebeurd. Het tweede evenement deed ik met The Things Network en hun LoRaWAN applicaties. We noemden het 'Lord of the Things', hadden een geweldige dag, maar ook hier was het onduidelijk wat er nu eigenlijk was gevonden en wat ermee werd gedaan.

Het moeilijkste van hack events is dus het opvolgen van de bevindingen van hackers. Soms komen twee hackers met dezelfde bevinding. Wie wint dan? Degene die het eerst was of degene die de beste proof of concept heeft geleverd? Of een hacker vindt een serieuze kwetsbaarheid, maar die blijkt dan in een onbelangrijk systeem te zitten of in dat van iemand anders. Of erger nog: de kwetsbaarheid is alleen te fixen als je daar heel veel tijd en geld in steekt, terwijl dat niet opweegt tegen de grootte van het risico dat je loopt als je dat niet doet. Dan kun je dus besluiten de bevinding niet op te volgen. Maar accepteert die hacker dat dan wel?

Toch blijken de meeste helpende hackers wel begripvol te zijn. Ze snappen dat zij de systemen slechts oppervlakkig kunnen bekijken en het er aan de kant van de eigenaar anders uitziet. Bovendien vinden de meeste hackers het vooral gewoon leuk om mee te doen. Dat leerde ik toen ik werd gevraagd om mee te doen aan een hack event voor de gemeente Den Haag, waar niet een systeem, maar de hele gemeentelijke online omgeving werd getest, drie jaar op rij. De aanleiding hiervoor was een raadsvergadering in het Haagse gemeentehuis.

Den Haag, 20 juni 2017. Het Haagse gemeenteraadslid Daniel Scheper van D66 stelt vragen aan het college van burgemeester en wethouders over het ethisch hacken van gemeentesystemen. De maand ervoor had hij namelijk een oproep op zijn partijwebsite gezet: 'Hack de gemeente'. D66 wil zo testen waar de zwakke plekken van de beveiligingssystemen van de gemeente zitten. De partij denkt daarmee criminele hackers een stap voor te zijn. Scheper: "We willen op deze manier voorkomen dat er

privacygevoelige informatie van, bijvoorbeeld, inwoners op straat komt". De oproep wordt direct overgenomen door de lokale media en een relletje is geboren. De partij had een dergelijke oproep eerst moeten overleggen met de gemeente.

Scheper krijgt die dag uitgebreid antwoord van het college. De gemeente neemt namelijk "structureel verschillende maatregelen om de informatieveiligheid van de gemeentelijke systemen te borgen en kwetsbaarheden te detecteren". Wat volgt is een lijst met preventie, detectie en respons, uitgevoerd door grote namen van overheidsorganisaties en securitybedrijven. De gemeente blijkt ook al enkele responsible-disclosuremeldingen te hebben afgehandeld, zowel van losse individuele hackers als van een groepje via bugbountyplatform HackerOne. Het college vindt de oproep van D66 "ongelukkig", maar als ze een hack event willen, kunnen ze dat krijgen. Eind september is de Haagse Cyber Security Week en dat is een mooie gelegenheid om te laten zien dat de gemeente Den Haag de veiligheid van haar systemen serieus neemt en openstaat voor hackers.

Het gezicht van Hack Den Haag 2017 wordt PvdA-wethouder Rabin Baldewsingh. Hij is naast politicus ook schrijver, dichter en filmmaker. Niet echt een man met een hart voor technische zaken, maar als wethouder heeft hij naast zaken als Volksgezondheid, Duurzaamheid, Organisatie, Personeelsbeleid, Monumentenzorg, Archeologie, Communicatie en Media toevallig ook ICT in zijn portefeuille. Hij heeft vernomen van de CIO van de gemeente, Marijn Fraanje, dat een hack event erg leerzaam kan zijn en een mooie gelegenheid is om het Haagse responsible-disclosurebeleid wereldkundig te maken. Wethouder Baldewsingh is enthousiast en wil het avontuur wel aan.

Het nieuwe Haagse securitybedrijf Cybersprint wordt gevraagd om te helpen met de organisatie van het hack event. Cybersprint heeft een Digital Risk Protectionplatform dat websites continu scant op kwetsbaarheden, een soort geautomatiseerde helpende hacker. Dat gebeurt bij verschillende gemeenten, bedrijven, financiële instellingen en organisaties met een kritieke digitale infrastructuur. Directeur Pieter Jansen heeft in het verleden als zelfstandige voor de gemeente gewerkt en toen hij Cybersprint oprichtte, was Den Haag de eerste klant.

Ook nu nog scant Cybersprint de websites van de gemeente op kwetsbaarheden. Een hack event lijkt Pieter dan ook een goede test om te kijken hoe volledig de scans zijn en waar ze die eventueel kunnen verbeteren. Bovendien kent hij de hackergemeenschap vrij goed. Hij heeft meegespeeld met het roemruchte team Eindbazen, dat regelmatig internationale CTF's won. Daarnaast won hij met een gelegenheidsteam de OneCTF in 2018, waarin hij samen met Thijs Bosschert, Rik van Duijn en Wesley Neelen de eerste plaats pakte.

De maand erna word ik benaderd door Pieter Jansen, die ik nog ken van de OneCTF het jaar ervoor, met een mail: "Kun je mij bellen wanneer het uitkomt? Cybersprint mag met de gemeente Den Haag een CTF/Hackme-event organiseren eind september en het lijkt mij leuk als jij als middagvoorzitter optreedt." In het gesprek vertrouwt hij me toe dat iedereen het best spannend vindt dat de gemeente zich publiekelijk openstelt voor hackers. De burgers zouden bijvoorbeeld bang kunnen worden dat hiermee hun persoonsgegevens op straat komen te liggen of niet begrijpen dat hackers geld krijgen voor iets wat niet mag.

De gemeente wil het event dan ook niet meteen al te groots aankondigen en noemt het discreet "Mystery Bug Bounty The Hague". Pas kort voor het event wordt wereldkundig gemaakt dat het om de gemeente Den Haag gaat. Als spelregels nemen we de richtlijn voor responsible disclosure: meld kwetsbaarheden bij de eigenaar, onthul pas als die gefixt is, maak niets stuk, etc. De winnaars krijgen "€€ reward". We doen geen ranglijst, want dan krijg je weer veel discussie over hoe zwaar de gevonden kwetsbaarheden zijn, maar drie categorieën: 'Most Impactful Hack', 'Most Sophisticated Hack' en 'Most Surprising Hack'. Lekker vaag dus. Om het toch wat spannender te maken, zet Cybersprint in de oproep: "The famous Dutch ethical hacker Victor Gevers has signed up. Can you beat him?"

Op 29 september is het zover. In het grote hoge witte gemeentehuis, dat lokaal het 'IJspaleis' wordt genoemd, wemelt het om 8.30 uur van de zwarte T-shirts. In totaal veertig hackers zijn op de oproep afgekomen. De meeste deelnemers hebben uit de locatie wel kunnen afleiden dat hun target vandaag denhaag.nl is en zijn alvast gaan kijken op de site. Ze krijgen van 9.00 tot 12.00 uur de tijd om zoveel mogelijk kwetsbaarheden te vinden.

Wat we verstaan onder ‘impactful’, ‘sophisticated’ en ‘surprising’ laten we over aan de verbeelding. Dat geeft ons de gelegenheid om de bevindingen naar eigen inzicht te beoordelen. De prijzenpot was eerst 2.000 euro, maar de wethouder is het gelukt om er op het laatste moment 5.000 euro van te maken. Daar ben ik blij mee. Niet alleen omdat er dan ook echt iets op het spel staat, maar ook omdat ik vreesde dat een cheque met € 666,- erop tot protesten zou leiden onder de christelijke fracties. Met € 1.666,- blijft ons dat bespaard.

De beeldvorming is belangrijk bij zo’n hack event. Hier worden namelijk niet alleen technische kwetsbaarheden verholpen. Dit is ook een pr-stunt om te laten zien dat de gemeente het belangrijk vindt om de persoonsgegevens van Haagse burgers goed te beveiligen. De hackers worden daarom midden in de grote witte hal aan zwarte tafels gezet en kunnen daar met hun eigen laptop aansluiten op het netwerk. Aan weerszijde staan tafels met snacks, koffie, frisdrank en uiteraard een stapel kratten met het verkwikkende Club Mate. Ik pak een fles en loop wat rond.

Hier en daar zie ik IT’ers en secretarieel personeel van de gemeente. Sommigen lopen zenuwachtig heen en weer om instructies te delen en van alles te controleren, terwijl anderen juist verstard met grote ogen rondkijken naar wat er op hen afkomt. Cybersprint is aanwezig met een heel team. Pieter is netjes in pak en staat te stralen te midden van alle hectiek. Ik herken zijn collega Ingeborg van der Geest als informeel leider van de cybersprinters. Ze loopt druk heen en weer met telefoon en papieren in de hand terwijl haar collega’s links en rechts T-shirts en een papiertje met de spelregels uitdelen aan de hackers. “Pers kan naar mij” roept ze in het voorbijgaan.

Intussen gaat de dienstverlening aan de burger gewoon door. De baliemedewerkers zitten al klaar als ze straks om 9.00 uur opengaan. Dit lijkt me een mooie gelegenheid om even te informeren wat zij vinden van ons hack event, dus roep ik enthousiast: “Hallo allemaal. Zijn jullie er klaar voor?”

“Eh, wat gaat er dan gebeuren?” roept een van de baliemedewerkers verbaasd.

“Een hack event. Deze jongens gaan jullie systemen hacken.”

“Oh, mogen we dan naar huis?” roept een andere en hij krijgt de lachers op zijn hand.

“Zijn jullie dan niet geïnformeerd?”

“Nee, fijn dat u dat alsnog even doet”, zegt een baliemedewerkster formeel. Dan wijst ze op mijn halflege fles Club Mate. “Maar eh, waarom zit u zo vroeg in de ochtend al aan het bier?” Nu liggen de ambtenaren helemaal dubbel over hun balies. “Dit is Club Mate, een soort thee met veel cafeïne.” Ze lijkt me niet te geloven en ik druip maar af.

Terug in de mierenhoop van zwarte shirts komt een man in pak rustig en met een stralende glimlach op me af. Het is D66-raadslid Daniel Scheper en hij vertelt trots dat hij het mooi vindt om te zien wat zijn oproep van destijds teweeg heeft gebracht. Als hij weer wegloopt, word ik aangeschoten door een gehaaste man die me een stevige hand geeft. Hij blijkt een perswoordvoerder te zijn van wethouder Baldewsingh. Als ik vertel over Schepers heldendaad, reageert hij geërgerd: “Dat raadslid kan wel denken dat hij dat allemaal bedacht heeft, maar het is wel Rabin die hier de verantwoordelijkheid neemt dat dit allemaal kan.” Een van de ambtenaren fluistert me toe: “Zo gaat dat hier altijd. Als iets een succes is, is het van hun. Gaat het mis, dan is het van een ander”.

Ik voel politiek gedoe aankomen bij de uitreiking dus loop ik naar Ingeborg om te informeren wie straks bij de prijsuitreiking wat gaat doen. De wethouder gaat niet de prijzen uitreiken, maar wel een toespraak houden, want het is nog onzeker hoe laat hij er kan zijn. We moeten daarom wat improviseren met de toespraken van andere ambtenaren om de aandacht van de hackers vast te houden. Dat gaat wel lukken, want de prijsuitreiking wordt gedaan door privacy activiste en lijsttrekker van de Piratenpartij Ancilla van de Leest. Ze is ook hoofd van de jury, waar naast Pieter CTF-kampioen Thijs Bosschert in zit. Net als Pieter was hij een van de Eindbazen, en heeft met het team Jobless Hackers en het Hack.ERS menige edities van de Cyberlympics en andere CTF’s gewonnen.

Om 9.00 uur grijp ik de microfoon en roep door de grote galmende hal dat de hackers kunnen beginnen. Dan zie ik Thijs samen met Michiel Prins, een van de oprichters van HackerOne, achter een scherm op de hoek van de lange zwarte tafel met hackers. Hier komen dus de meldingen binnen. Op het dashboard is te zien dat iedereen inmiddels een account heeft

aangemaakt en dat de teller van meldingen nog op nul staat. De hackers hebben nu drie uur om mee te dingen naar de vele euro's en eeuwige roem.

Het event verloopt rustig. Eigenlijk te rustig. Als dagvoorzitter heb ik weinig te doen, behalve dan een beetje heen en weer lopen om te kijken of iedereen het naar zijn zin heeft. Links en rechts informeer ik of er al wat gevonden is. Op de schermen van de hackers zie ik naast de bekende zwarte Kali Linux-schermen dat sommigen gewoon met Google zoeken op denhaag.nl. Na een uur hebben we nog maar één melding: een XSS, oftewel cross-site scripting. Je zou dus, door wat code achter het internetadres te zetten eventueel een sessie van een andere bezoeker van de website kunnen overnemen. Dat kan ernstig zijn, ware het niet dat op deze site geen gevoelige gegevens worden verwerkt. XSS is ook in de jaarlijkse statistieken van het NCSC de meest voorkomende kwetsbaarheid die gevonden wordt op websites. Ik loop wanhopig naar Victor, of hij niet iets heeft gevonden. "Nee joh, alles staat dicht", zegt hij terwijl hij ondertussen nog wat mailtjes afhandelt van lekken die hij eerder elders heeft gemeld.

Met nog maar een halfuur te gaan, zie ik hackers die wat anders doen op hun laptop of bij de snacks en drankjes een praatje maken met elkaar. We hebben nog maar vier meldingen binnen, of eigenlijk drie, want een is echt te licht om vermeld te worden. Ik probeer de boel nog wat op te jutten door telkens om te roepen hoeveel tijd ze nog hebben, voor hun claim op eeuwige roem, maar er zit weinig energie meer in het hackersgilde. Om er toch nog een leuk einde aan te breien, zet ik een paar seconden voor 12.00 uur The Final Countdown van Europe op de speakers.

De prijsuitreiking verloopt rommelig. PvdA-wethouder Baldewsingh is ruim op tijd, dus we moeten de andere speeches skippen. Ancilla kwam pas halverwege het event binnen, moest daarna nog haar make-up doen en had weinig tijd om met juryleden Thijs en Pieter te overleggen. Als ik haar mijn microfoon geef, leest ze van een briefje voor dat de prijs voor de Most Sophisticated hack gaat naar team Loony Toons. Het zijn Rik van Duijn en Wesley Neelen van Dearbytes, die ook bij Game of Toons in de prijzen waren gevallen. Ze horen ook bij de hackers die al ver voor het einde bij de snacktafel stonden te kletsen en kijken enigszins verbaasd wanneer ze de bokaal en check in ontvangst nemen. Ancilla licht toe: "Een cross-site

scripting, dat is erg technisch.” Ook de andere twee winnaars nemen hun prijzen enigszins vertwijfeld in ontvangst. De wethouder is er niet minder enthousiast onder. In een vlammende toespraak bedankt hij de deelnemers uitvoerig en prijst hij de gemeente Den Haag, die hiermee laat zien dat zij de beveiliging serieus neemt en openstaat voor hackers.

De verwachte kritiek van media of burgers blijft uit. Niemand heeft de zorgen geuit dat de gemeente zich openlijk laat hacken of dat persoonsgegevens van burgers in gevaar zijn geweest. De aanwezige journalisten zijn vooral geïnteresseerd in het feit dat het event er is, en niet hoe goed of slecht denhaag.nl beveiligd is. Dat er die ochtend eigenlijk nauwelijks iets is gevonden, weten we uiteindelijk goed verborgen te houden. Achteraf bezien, was de editie 2017 vooral een goeie vingeroefening voor het echte werk.

Voor de editie 2018 wil de gemeente meer hackers, betere hackers en een flinke uitbreiding van wat gehackt mag worden. Den Haag heeft inmiddels een nieuwe CISO: Jeroen Schipper, een IT’er die hiervoor zestien jaar bij Defensie heeft gewerkt. Toen hij hoorde over het aanstaande hack event nam hij het initiatief om naast de IT-omgeving van de gemeente, ook hun leveranciers te betrekken. Dat bleek nog best lastig. Jeroen: “Er staat wel ‘gemeente Den Haag’ onder die applicaties, maar je kunt niet zomaar die leveranciers noemen. Dan krijg je een soort naming en shaming.” Enkele leveranciers reageerden dan ook sceptisch of direct afwijzend op het aanbod van Jeroen. Waarop hij zei: “Oh, ben je bang dat ze wat vinden? Wanneer loopt jullie contract ook alweer af?” Maar er waren ook leveranciers die juist wel benieuwd waren of hackers nog iets kunnen vinden in hun applicaties. Zij zagen het als een gratis pentest.

Probleempje: tussentijds zijn er gemeenteraadsverkiezingen geweest en het is niet waarschijnlijk dat de wethouder die het vorig jaar voor ons opnam, terugkomt. Van zijn PvdA is namelijk niet veel meer over. Groep De Mos, onder leiding van de ex-PVV’er Richard de Mos is in een klap de grootste partij in de gemeenteraad. Ze sluiten een coalitie met VVD, D66 en Groen Links. Wie van hen over ICT zal gaan, blijft nog onduidelijk. Pas in september krijgen we goedkeuring voor een volgende editie. Te laat om het nog tijdens de Cyber Security Week te organiseren. Gelukkig draagt ook dit

college de cybersecurity een warm hart toe. Ik krijg namelijk een verzoek van de evenementenafdeling of we tijdens de Cyber Security Week de tentoonstelling Hackers Handshake in het gemeentehuis kunnen neerzetten.

Tijdens de opening op 8 oktober kondig ik naast fotograaf Tobias Groenland ook NCSC-directeur Hans de Vries aan en de nieuwe wethouder Saskia Bruines. Geen hack event dus in het IJspaleis, maar wel grote afbeeldingen van hackers waarvan enkelen ook hebben meegedaan aan de Mystery Bug Bounty The Hague: Victor Gevers, Rik van Duijn en Wesley Neelen. Ze zijn ook live aanwezig, tezamen met de andere hackers uit de tentoonstelling. Dit is de perfecte gelegenheid om de nieuwe editie aan te kondigen, maar dat is de wethouder om de een of andere reden vergeten en ik vind het ongepast om dat dan maar voor haar te doen. Zij blijkt uiteindelijk ook niet de wethouder die de verantwoordelijkheid zal nemen voor het hack event, dat wordt een wethouder van Groep de Mos: Rachid Guernaoui.

Op 22 november 2018 is het dan zover. Dit keer geen mysterieuze bug bounty, maar gewoon Hâck Den Haag. (Die “â” is bedoeld om het uit te spreken in plat Haags, maar dat zal menigeen zijn ontgaan.) De hackers krijgen vandaag meer tijd: zes uur maar liefst, dus is er extra eten en Club Mate ingeslagen. De prijzenpot was in eerste instantie weer 5.000 euro, maar is ook dit keer door de wethouder op het laatste moment verdubbeld naar 10.000 euro. We hebben dezelfde categorieën, maar ook daarbinnen een eerste, tweede en derde prijs, met bokaal en een cheque van respectievelijk 2.000, 1.000 en 500 euro. (Ik had, als nerd, ervoor gepleit om de bedragen binair te laten lijken, door er 512, 1.024 en 2.048 euro van te maken, maar dat zou volgens Communicatie niet echt begrepen worden door het publiek.) Elke deelnemer krijgt een medaille, goodiebag en een onvergetelijke ervaring.

Cybersprint is massaal aanwezig, onder de informele leiding van Ingeborg die druk heen en weer loopt met badges, stapels papieren en dozen vol met zwarte T-shirts. Het team is nu herkenbaarder omdat ze allemaal een Cybersprint-hoodie aan hebben. De triage vindt dit keer plaats op het Zerocopter-platform, dat wordt beheerd door Chantal Stekelenburg. De directeur van Zerocopter, Edwin van Andel, is een van de juryleden, samen

met Pieter van Cybersprint, CISO Jeroen, John Sinteur, een senior-pentester van Radically Open Security en Remko Sikkema, Adviseur informatiebeveiliging van de Informatiebeveiligingsdienst voor gemeenten (IBD). Een behoorlijk zware vertegenwoordiging dus.

Wethouder Rachid Guernaoui is al bij aanvang aanwezig. Hij zal de prijzen uitreiken en heeft er zichtbaar zin in. Ik heb lang geoefend om zijn naam goed uit te spreken en test of ik het goed doe: “Zeg ik Kuwernahoewie?”, vraag ik beleefd. “Ja hoor, maar zeg maar gewoon Kwerni. Dat doen ze hier allemaal.” Hij kijkt om zich heen en lijkt trots op het leger aan ambtenaren dat vandaag op de been is.

Het gehele CIO-office is aanwezig, onder leiding van Marijn Fraanje. Vooral de nieuwe CISO Jeroen Schipper is druk bezig iedereen in het gelid te krijgen. Bij de afdeling IT stuurt Team Lead IT-Security Peter van Eijk acht man aan die klaarzitten in een kamer waar veel kabels naartoe lopen en die vol staat met grote schermen. Het is een soort dependance van de control room op de Leyweg van waaruit gemeenteambtenaren continu hun kritieke processen monitoren. Hier en daar lopen Information Security Officers van BEC, het Bedrijfsvoering Expertise Centrum. Zij zijn het dagelijks contact met leveranciers, waarvan er vandaag drie meedoen, met best wel spannende systemen.

Een leverancier levert het begrotingssysteem van de gemeente. Aan de URL zie ik dat het de echte omgeving is en geen testomgeving. Een tweede leverancier levert de web interface voor de gemalen die het water door de stad pompen en een derde levert het zogenoemde Pollers, een systeem dat gebruikt wordt voor de verkeersregulatie in de stad, onder andere met paaltjes die uit of in de grond gaan bij bepaalde nummerborden. Deze applicaties staan uiteraard wel in een testomgeving, anders zou een overenthousiaste hacker de stad onder water kunnen zetten of het hele verkeer ontregelen. De hackers krijgen er een gebruikersaccount bij, van waaruit ze kunnen proberen hogere rechten te krijgen.

We hadden in totaal zeventig aanmeldingen van hackers, terwijl we plek hebben voor 45. Dus moesten we een selectie maken. Dat was nog best een klus, want waar selecteer je dan op? Eén riep: “We kunnen nu de meer ervaren hackers uitnodigen”, terwijl de ander riep “Het gaat om diversiteit, dus juist een mengeling van meer en minder ervaren hackers, Nederlanders

en allochtonen en als het kan een meisje.” Daar kwamen we niet uit. We besloten daarom met het hele team elk voor zich punten te zetten achter de namen op een uitgeprinte spreadsheet. De vijfentwintig die afvielen, werden op een wachtlijst geplaatst. Dat was een goede oplossing, want van de gelukkige geselecteerden komen er die dag tien niet opdagen. Die plekken zijn opgevuld door hackers die op de wachtlijst stonden en er nu wel zijn. Ik herken enkele studenten van de Hogeschool Rotterdam. Die hadden zich inderdaad massaal aangemeld.

Ook bij deze editie zitten alle hackers aan lange zwarte tafels met hun eigen laptop, midden in de grote witte hal van het gemeentehuis. Nieuw is een groot scherm met een dashboard waarop het netwerkverkeer wordt weergegeven. Hiermee laat de control room van Peter iedereen zien wat er real time gebeurt. Het zal de argeloze, langslopende Hagenees allicht niet veel zeggen, maar het ziet er wel spannend uit. En we hebben ook de portretten van Hackers Handshake. Victor is er niet, maar zijn grote portret prijkt aan de kop van de tafel. Aan het andere einde van de tafel hangt het portret van jurylid Edwin van Andel. Het lijkt net alsof beide Grumpy Old Hackers toekijken of de jonge hackers zich wel gedragen. Enkele anderen van de fototentoonstelling doen mee als deelnemer: Zawadi, Mischa en Tabitha van de Cyberwerkplaats en natuurlijk serial winners Rik en Wesley.

Om 9.30 uur kunnen we aftrappen. Jeroen, Marijn en Pieter doen elk een korte intro, over de regels, de scope en de prijzen. Antoon, een van de leden uit de control room, somt kort op wat er vorig jaar was gevonden en wat ermee is gedaan. De drie findings zijn gefikst. Ik roep of er nog vragen zijn. Nee. De hackers lijken het allemaal wel te begrijpen en lopen rustig naar hun plekken om hun laptops aan te sluiten en aan de slag te gaan.

Dan is er toch nog een vraag, van Peter Geissler, alias Bl4sty. Ik ken hem als de helpende hacker die in 2013 KPN meldde dat hun 300.000 modems lek waren en van de OneCTF die hij vorig jaar won. Hij is ook een van de medeoprichters van Radically Open Security en al jaren CTF Overlord bij Hack in the Box. Peter kijkt bezorgd als hij me het A4’tje met de bekende spelregels en de targets toont en vraagt: “Kloppen die IP-adressen wel?” Ik kijk op het velletje en zie “Gemeente Den Haag, IP reeks

217.68.51.0/24.” Dat staat ook op de instructie die ikzelf heb gekregen, dus het zal wel kloppen, denk ik…

Het gaat meteen hard. Binnen tien minuten hebben we al twintig meldingen. Ik zie Mischa en Zawadi op en neer stuiteren en naar hun schermen wijzen. Als ik vraag wat er aan de hand is, roept Mischa: “Moet je kijken, gewoon een open filesharingsysteem! We hebben al twee zware findings.” Een journalist herkent het duo van de portrettententoonstelling en snelt toe voor een interview. Ook in de control room is er hectiek. Een van de IT’ers komt op me afgerend: “We hebben een foutje gemaakt in de switchconfiguratie. Het IP-adres moet niet /24 zijn, maar /20.” Ik stel hem gerust met “Ik zal het omroepen” en vraag: “Maar wat zit er dan achter /24?” “Oh, dat zijn de IP-adressen van de deelnemers”, zegt hij laconiek.

De vele kwetsbaarheden die gevonden zijn, zitten dus op de laptops van de hackers zelf! Dat was dus waar Bl4sty me voor waarschuwde. Als ik omroep dat we opnieuw moeten beginnen omdat ze vooral elkaar aan het hacken waren, dringt het pas tot iedereen door hoe grappig dit eigenlijk is en galmt er gelach door de grote hal. De baliemedewerkers kijken even op, maar gaan direct weer verder met het bedienen van de Haagse burgers.

Nog een ander foutje: van de Pollers hadden we alleen de URL moeten geven, niet het IP-adres. Dat nummer was goed bedoeld om te whitelisten, oftewel ervoor te zorgen dat verdacht verkeer niet geblokkeerd wordt. De leverancier blijkt echter nog andere applicaties achter het IP-adres te hebben hangen die niet binnen de scope van het hack event vallen. Oeps. Maar zowel de gemeente als de leverancier nemen het licht op: eventuele meldingen worden doorgegeven, maar vallen niet in de prijzen. Als ik check bij Chantal van Zerocopter hoe het loopt met de meldingen, zie ik dat ze staat te praten met een van de deelnemers. “Hee, dat mag niet, jury beïnvloeding” roep ik. Nee, de hacker had een zware kwetsbaarheid gevonden die buiten scope lag en wilde het toch even melden omdat de getroffene buiten het event om al bij het Zerocopter-platform is aangemeld. Nog meer dan de vorige editie, zet Den Haag een behoorlijke bijvangst door aan derden.

Bij deze editie heb ik het best druk als dagvoorzitter. Mijn stappenteller staat inmiddels op twaalf kilometer, want telkens als er iemand vanuit de organisatie met een aanwijzing komt, moet ik die eerst controleren voordat

ik deze door de microfoon omroep. Een ervan is wel hoogst charmant. De leverancier van de webinterface voor gemalen komt met een router aanlopen. Dit is dus het apparaat dat tussen de pompen en het internet staat. Of hij hem mag laten zien. Leveranciers mogen natuurlijk niet direct in contact treden met de deelnemers, om beïnvloeding te voorkomen, maar na overleg lijkt dit ons een mooie gelegenheid om de gemalen ook hun portie aanvallen te geven. Op de monitor zien we namelijk alleen verkeer naar denhaag.nl, het begrotingssysteem en vooral de Pollers. En inderdaad, als ik met het apparaat als een trofee in de lucht langs de tafels loop, neemt het aantal hits snel toe.

Pollers krijgt het zwaar te verduren. Ik spreek een hacker die beweert admin-rechten te kunnen krijgen over het verkeersregulatiesysteem, maar hij heeft zijn melding teruggekregen. De jury kon uit zijn proof of concept niet goed afleiden wat hij precies heeft gedaan. Nu heeft iemand zijn account geblokkeerd en kan hij er niet meer in. Het blijkt Rik van Duijn te zijn. Ook hij heeft admin-rechten verkregen en wel een goede proof of concept ingediend. Om zijn vondst kracht bij te zetten, heeft hij meteen alle accounts gereset. Dat is niet erg netjes, maar met adminrechten heb je wel gewonnen wat er te winnen valt bij deze target. Ik vraag hem waarom hij van deze testomgeving niet meteen een leuk computerspelletje heeft gemaakt door zogenaamd paaltjes in de stad op en neer te laten gaan. Een soort Snake of Pac Man. Hij reageert echter laconiek: “Oh, was het dat? Nee joh, soms als ik iets hack weet ik niet eens waar ik in zit.”

Deze actie van Rik was misschien op het randje, maar er zijn ook hackers die zich echt niet aan de spelregels houden. Daarin staat duidelijk dat brute-forcing en flood-basedaanvallen niet zijn toegestaan. Automatische tools, zoals Dirbuster, Nmap, Skipfish, mogen slechts een keer specifiek worden ingezet en niet om continu de hele omgeving te scannen. Dat genereert namelijk zoveel verkeer dat het netwerk plat kan gaan, alsof we een DDoS te verduren hebben. Maar blijkbaar hebben we hiermee enkele deelnemers juist op een idee gebracht.

Nadat meerdere vermaningen door het omroepsysteem niet over lijken te komen, dreig ik dat de identiteit van degene die het nog een keer doet, bekend zal worden gemaakt bij de AIVD. Er wordt wat schaapachtig gelachen hier en daar, maar het lijkt te werken. Tijdelijk dan. Als we nog

maar een half uur hebben te gaan, neemt het verkeer van scans en brute forcing plotseling weer flink toe. Blijkbaar een laatste wanhoopspoging van gefrustreerde hackers. We laten het maar gebeuren, want we hebben immers al meer dan genoeg meldingen binnen om de negen prijzen kwijt te kunnen.

Een van de deelnemers wordt zelf overladen door verkeer, menselijk verkeer welteverstaan. Tabitha, wiens portret ook in de hal staat, is het enige meisje in het hackersgilde en dat vinden de journalisten interessant. Zijzelf minder, maar door de continue verstoring is ze niet aan hacken toegekomen. Mischa wil wel voor de camera, maar ook hij valt uiteindelijk buiten de prijzen. Rik en Wesley hebben wel beet en staan triomfantelijk te wachten bij de snacks en drankjes op de uitslag. Om 15.30 uur zet ik The Final Countdown op.

Om 16.00 uur is de prijsuitreiking. Wederom hectiek, want de uitslag is bekend, maar moet in korte tijd worden overgedragen aan wethouder Guernaoui. Intussen komen er steeds meer ambtenaren bij die ook graag op het podium willen staan. Als ik ze weggejaagd heb, geef ik snel de microfoon aan de wethouder die na een enthousiaste speech overgaat tot de prijsuitreiking. Binnen elke prijscategorie zijn er drie prijzen. Bug hunter Wouter van Rooij weet twee derde prijzen in de wacht te slepen en krijgt twee keer 500,-. Rik en Wesley krijgen twee tweede prijzen, 1.000,- elk. De eerste prijs voor Most Surprising Hack gaat naar twee leerlingen van de Hogeschool Rotterdam, die dankbaar gebruik hebben kunnen maken van hun plek op de wachtlijst en met 2.000 euro naar huis gaan.

Grootste verrassing was dat de twee andere eerste prijzen werden gewonnen door één hacker: Peter Geissler, alias Bl4sty. Op de foto die ook in de media wordt geplaatst, kijkt hij wat ongemakkelijk in de lens terwijl de wethouder trots twee cheques van elk 2.000,- voor hem houdt. De rest staat er vrolijk op en het is een prachtig beeld: de wethouder die verantwoordelijk is voor ICT staat te midden van een hele groep hackers om te laten zien dat zijn gemeente hen serieus neemt.

Een maand later kijk ik met CISO Jeroen Schipper en Team Lead IT Security Peter van Eijk terug op het event om de balans op te maken. Jeroen heeft kort daarvoor nog met de wethouder gesproken en die was heel blij en tevreden. Niemand vond het een probleem dat er meer kwetsbaarheden zijn

gevonden dan het jaar daarvoor. Ze zien het eerder als: we hebben er meer opgelost. Niet alleen voor de gemeente Den Haag, maar ook voor andere gemeenten. Ze kunnen daarom ook niet ingaan op de specifieke kwetsbaarheden. Die zijn misschien bij Den Haag wel opgelost, maar niet bij de andere getroffenen.

Een kwetsbaarheid kunnen we niet onvermeld laten: de eerste prijs Most Impactful Hack van Bl4sty. Hij had namelijk een kwetsbaarheid gevonden in een printer waarmee je kon inloggen en de bestandsnamen van alle geprinte documenten kon inzien. De kwetsbaarheid was nog maar net bekendgemaakt als CVE 2018:18006, terwijl de Japanse leverancier nog geen patch beschikbaar had. Uit eigen onderzoek van de gemeente Den Haag bleek dat meerdere gemeenten dezelfde printers gebruikten. De Informatiebeveiligingsdienst voor gemeenten werd ingelicht en er werd een alert gestuurd naar alle Nederlandse gemeenten. Ook het NCSC werd ingelicht, die de melding doorstuurde naar het CERT van Japan. Binnen drie dagen kwam de leverancier met een patch.

Dit voorbeeld laat zien hoe lastig het is om bij hack events kwetsbaarheden wereldkundig te maken, oftewel coordinated vulnerability disclosure toe te passen, zoals te doen gebruikelijk. We hadden daar ook wat berichten over ontvangen via Twitter. Maar wat als die kwetsbaarheid bij andere gemeenten nog bestaat? Dan onthul je het wel op een verantwoordelijke manier voor je eigen systemen, maar niet voor die van anderen. Verder hangt het voor de ernst van een kwetsbaarheid nogal af van in welk systeem die zich bevindt. Soms wordt een kwetsbaarheid aanvaard als een aanvaardbaar risico, maar je wilt niet in de media lezen dat de gemeente ondanks het goede werk van hackers, lekken niet dicht.

Ook in de beoordeling van de meldingen waren veel onzekerheden. Een hacker had een pdf-document gevonden waar de naam van de auteur nog in stond. Dat kan in sommige gevallen een probleem zijn, maar dat hoeft niet altijd zo te zijn. Verder hangt veel af van hoe ze hun melding indienen, zoals de hacker die als eerste in Pollers zat, maar zijn melding weer terugkreeg. Peter: “We hadden de wijze van beoordeling beter moeten communiceren. We keken niet alleen naar de gevonden kwetsbaarheden, maar ook naar reproduceerbaarheid van het proof of concept en de geboden oplossingsrichting. Over die finding in Pollers zei het triageteam dat ze

ongeveer begrepen wat hij had gedaan, maar het niet konden reproduceren. De betreffende hacker was erg teleurgesteld toen hij zag dat de prijs naar Rik ging, die hem later had gevonden, maar wel een goeie proof of concept had." Jeroen: "Het triageteam zat boven, en krijgt niet mee wat beneden gebeurt."

Omgekeerd was het voor al die ambtenaren, projectmensen, bezoekers en journalisten beneden ook niet helemaal duidelijk wat er boven bij het triageteam en in de control room gebeurde. Het scherm dat er stond, liet vooral netwerkverkeer zien en trok veel aandacht. Daar hadden we meer vragen van publiek kunnen afvangen door bijvoorbeeld een uitleg neer te zetten. Wellicht kunnen we daar volgend jaar ook het aantal meldingen op zetten. Niettemin was het beeld met die 45 hackers aan lange tafels midden in het gemeentehuis erg sterk. Als pr-stunt is het zeker geslaagd, want we kregen volop aandacht. Er was lokale media aanwezig: Omroep West, de Haagse editie van het Algemeen Dagblad, TV Scheveningen en de krant Loosduinen. Trouw deed een interview met de wethouder en de NOS pikte het bericht van Omroep West op. Er was zelfs een weddenschap op Radio 1, dat er voor 12.00 uur persoonlijke data gelekt zou zijn. Dat is gelukkig niet gebeurd.

Al met al was de oogst van de dag: 90 meldingen, waarvan 62 uniek en 12 high impact, waarvan er op dat moment 10 zijn opgelost. De leveranciers blijken goed mee te werken en als een bug is gefikst, dan zien de hackers dat in hun Zerocopter-account. Dat is de belangrijkste winst van Hâck Den Haag. Maar wat heeft het gekost? Peter: "Alleen al de afdeling IT heeft in totaal 200 uur besteed aan het event en is nu nog bezig. Dat lijkt veel, maar het was het waard, want de potentiële risico's die zijn opgelost zijn moeilijk in tijdswinst uit te drukken."

Kortom, deze tweede editie was goed, maar het kan altijd beter. Belangrijkste lessen? Betrek alle afdelingen voor, tijdens en na het event: CIO, IT, Communicatie en bovenal een enthousiaste wethouder. Zorg ervoor dat zoveel mogelijk leveranciers meedoen. Geef de hackers duidelijke targets en regels over wat wel en niet kan en hoe hun meldingen worden beoordeeld. Bekijk per geval welke bevindingen openbaar mogen worden gemaakt en overleg dat met de hacker. Wees open naar de media en

het publiek met dashboards en woordvoerders die vertellen dat hackers altijd wel wat zullen vinden en we ze hiermee aan onze kant hebben. Maar bovenal: hoe goed je je ook voorbereidt, er gaat altijd wel iets mis. Zo niet, dan heb je gewoon te weinig risico genomen. Met die ambitie gingen we 2019 in. Het moest allemaal nog groter en beter.

Daar kunnen we kort over zijn: dat is gelukt. Op 30 september 2019 vonden 79 hackers in totaal 107 kwetsbaarheden in de systemen van Den Haag. Vele meldingen over systemen die buiten scope waren, zijn doorgezet. Het event werd goed opgepakt in de media. Alleen al de aankondiging werd in de eerste vijf dagen 1,34 miljoen keer bekeken. Hâck Den Haag werd een showcase in de vele evenementen die volgden tijdens de European Cyber Security Month.

We hadden voor de derde editie meer voorbereidingstijd en natuurlijk de ervaring van de twee voorgaande edities. Het NCSC nam ook deel aan de jurering, in de persoon van mister coordinated vulnerability disclosure, Jeroen van der Ham. Zijn baas, Hans de Vries, zou die dag ook komen, om direct na ons event de OneCTF af te trappen. Verder was de teamsamenstelling grotendeels hetzelfde: Cybersprint als medeorganisator van het event, Zerocopter voor de triage en een enorm ambtenarenapparaat vanuit alle betrokken afdelingen van de gemeente Den Haag, met als boegbeeld wethouder Guernaoui.

De werving van de deelnemers ging ook een stuk makkelijker. We hadden immers al een aardige reputatie opgebouwd. Om het internationale allure te geven, werd het nu “Hâck The Hague 2019” en er meldden zich inderdaad ook hackers uit het buitenland aan. (Die Haagse â hadden ze, wat mij betreft, daarom wel weg kunnen laten, maar dat terzijde). Naast de bekende drie vage prijscategorieën kwam er een bij: de studentencompetitie, met dezelfde geldprijzen van 500, 1.000 en 2.000 euro. De studenten kregen een eigen plek in de Raadszaal. De rest van de hackers zaten gewoon in de hal.

Die maandagochtend kom ik het gemeentehuis binnenlopen en ik voel meteen dat de sfeer anders is dan voorgaande edities. Er heerst rust. Ik tref als eerste Jeroen Schipper, de gemeentelijke CISO. Hij blijkt het hele weekend te hebben doorgewerkt met zijn collega’s om alles op tijd klaar te

hebben. “Huh, maar ambtenaren werken toch niet in het weekend”, plaag ik hem een beetje. Jeroen: “Nou, dit vinden we juist harstikke leuk, joh”. Ik realiseer me dan dat zo’n hack event nog een belangrijk neveneffect heeft op de gemeentelijke organisatie: het is voor collega’s met een hart voor security ook gewoon leuk om te doen en dat motiveert ze. Dat klopt volgens Jeroen. Ze hebben als gemeente behoorlijk wat talent rondlopen en hebben geen moeite om die mensen vast te houden. Dat is volgens mij bij andere gemeenten wel anders. Het is Jeroen dit keer gelukt om meer leveranciers te betrekken: twintig maar liefst en zeker niet de minsten. Enkele leveranciers zullen vandaag ook aanwezig zijn.

Ook het Cybersprint team zit er relaxed bij. Ingeborg loopt dit keer niet te slepen met hoodies en goodies, maar heeft nu een balie met drie medewerkers die dozen vol zwarte kleding uitpakken. “Kijk, iedereen krijgt een keycord met eigen kleur”, zegt ze trots terwijl ze een bos ophoudt: “De hackers hebben rood. De organisatoren, leveranciers en bezoekers blauw. De ambtenaren en cybersprinters groen. En de pers geel.” Het groen en geel staat natuurlijk voor Den Haag. Rood van de hackers verwijst naar het red team, de aanvallers. Blauw is van blue team, de verdedigers. De juryleden en ik krijgen een paars keycord. En een zwarte hoodie met voorop “Hâck The Hague 2019” en achterop “EFFûH HÂCKûH!”.

De jury is compleet. Ze hebben een eigen kamer waar elk uur juryberaad plaatsvindt. Het triageteam van Zerocopter heeft naast Chantal en Edwin ook nieuwe medewerker Ricardo ten Cate meegenomen, bekend van het Security Knowledge Framework dat hij samen met zijn broer onderhoudt voor de wereldwijde OWASP-community. Ze zitten samen met IT-security Team Lead Peter en zijn mannen klaar in de control room. De rest van zijn gemeentelijke IT’ers zit op de locatie Leyweg, van waaruit ze dagelijks hun werk doen, maar nu met de control room zijn verbonden via een livestream.

Om 10.25 uur roepen we om dat alle hackers naar de gemeentelijke raadzaal moeten komen. Dit is de zaal waar het college van burgemeester en wethouders dagelijks hun debatten voeren en waar op 20 juni 2017 het idee ontstond voor de eerste editie. Nu wemelt het hier van de hackers. Onder de tafels van de raadsleden liggen bundels met netwerkkabels. Daar

mogen straks de studenten gaan zitten. Die zitten nu samen met de professionele hackers op de tribune, die daardoor helemaal vol is.

Als dagvoorzitter heb ik het makkelijk: mooie zaal, goed geluid en een flink scherm achter ons. We starten met een videocompilatie van de voorgaande editie. CISO Jeroen legt daarna kort uit wat we gaan doen, hoeveel hackers meedoen en wat er te winnen valt. Team Lead Peter gaat kort in op de bevindingen van vorig jaar en wat de scope is van vandaag. Pieter sluit af met de spelregels en wijst naar Chantal en Ricardo voor de triage. Na een groepsfoto knippen we symbolisch een zwart-geel afzetlint door en kunnen de studenten plaatsnemen in de raadszaal. Ze hebben daarmee een kleine voorsprong op de professionele hackers die nog naar beneden moeten om in de grote hal, te midden van de Haagse burgers in te pluggen. Hâck The Hague 2019 is begonnen.

De dag erna zie ik veel van de mensen van Hâck The Hague op de One Conference. Zelf had ik me ruim van tevoren ingeschreven, net als de rest van ons team, want deze conferentie staat erom bekend snel volgeboekt te zijn. De winnende deelnemers, waarvan de meesten nog nooit op de One waren geweest, hebben van het NCSC naast hun prijs ook een kaartje voor deze dag gekregen. Sommigen waren zelfs die avond nog doorgegaan met de OneCTF die het NCSC in de hal van het IJspaleis had gehouden. Uiteraard onder het genot van de nodige Club Mate.

In de wandelgangen van het Worldforum kom ik ze tegen. De jonge hackers kijken wat verlegen om zich heen tussen al die pakken, terwijl veel van de gemeenteambtenaren staan te stralen van het succes van de dag ervoor. We delen onze ervaringen en vertellen trots tegen anderen dat alles helemaal volgens het boekje ging dit keer. Geen incidenten met verkeerde IP-adressen, hackers die elkaar hackten of boze organisaties die onbedoeld een target bleken te zijn, maar gewoon een goed hack event. Een van mijn persoonlijke anekdotes van de dag was een leverancier die naar me toe kwam om mede te delen dat de gevonden bug gefikst was. Hij vroeg: “Kunnen we de applicatie updaten, zodat ze meteen de nieuwe versie kunnen testen?” Dat hebben we gedaan.

Het gezicht van Hâck The Hague wordt op de One Conference de Haagse CIO Marijn Fraanje. Om 10.30 uur betreedt hij het hoofdpodium

om voor meer dan duizend mensen te spreken over ‘Cyber resilient cities’. Als hij een foto laat zien waarop wethouder Guernaoui samen met Richard de Mos gratis veilige wifi op de Haagse Markt aanbiedt, gaat er geroezemoes door de zaal. Die ochtend was er namelijk een inval van de nationale recherche. Groep De Mos is verdacht van fraude en corruptie. Hun hele administratie en dus ook die van Guernaoui is in beslag genomen. De wethouder is op non-actief gesteld. Ik probeer me voor te stellen hoe Hâck The Hague 2019 zou zijn verlopen als de recherche een dag eerder hun inval had gedaan. Of hebben de agenten wijselijk een dagje gewacht?

Hoe verliep het uiteindelijk met de afhandeling van de 107 gevonden kwetsbaarheden? Dat zien we terug in het Zerocopter-platform. De deelnemende hackers zien daarin hun melding geclassificeerd als ‘Low’, ‘Medium’ of ‘High’. Het zijn drie ‘code injections’, drie ‘open directories’, twee ‘cross-site scriptings’ en de rest gaat vooral over gevoelige informatie die niet zichtbaar zou moeten zijn. De melders kunnen op het platform ook de voortgang van de afhandeling volgen. Eerst staat hun melding op ‘Work in progress’, daarna op ‘Retest requested’ en uiteindelijk op ‘Resolved’. Enkele kwetsbaarheden blijken echter niet verholpen te kunnen worden, omdat ze niet in de systemen van de gemeente zitten, maar bij derden. Of ze blijken achteraf niet echt gevaarlijk. Dan wordt er een risico-inschatting gemaakt: hoe waarschijnlijk is het dat deze kwetsbaarheid misbruikt wordt en wat kan er dan misgaan? Als het uiteindelijk meer werk kost dan het oplevert, dan gaat de melding op ‘Won’t fix’.

Kijken we naar het tijdsverloop, dan zien we dat van de twaalf prijswinnende kwetsbaarheden er zeven binnen een maand zijn opgelost en nog eens twee in de maand erna. Een wordt op ‘Won’t fix’ gezet omdat de applicatieleverancier, om onbekende redenen, heeft besloten het te laten zoals het is. Twee meldingen staan een halfjaar na het evenement nog steeds open. Van de overige vijfennegentig meldingen, die niet in de prijzen vielen, zijn er dan nog vijftien in behandeling, terwijl er eenentwintig uiteindelijk niet gefikst worden. Lekken vinden blijkt toch makkelijker dan ze te fixen…

En de editie 2020 dan? Al in juni besluit de gemeente deze editie te cancelen vanwege COVID-19. Hackers hebben er over het algemeen geen

probleem mee om anderhalve meter van elkaar te zitten, dat vinden ze juist fijn. Maar bij een evenement dat draait om security, kun je nu eenmaal niet gezellig met honderden mensen door het IJspaleis lopen, zeker niet als je daar zo'n beetje iedereen bij elkaar hebt die verantwoordelijk is voor de digitale bewaking van de gemeentelijke systemen. De deelnemers vanuit huis laten hacken zou een optie zijn, maar dan mis je toch het evenementengevoel en het nieuwsmoment. Bovendien kan dat nu ook al, gewoon via de CVD-pagina van de gemeente Den Haag.

Om toch de aandacht vast te houden voor eventuele volgende edities, besluiten de gemeente en Cybersprint in augustus alsnog een webinar te besteden aan het event en een overzicht te publiceren van de afgelopen edities. Op dat moment leg ik net de laatste hand aan dit hoofdstuk. Ze mogen het alvast hebben voor op de site, want alles wat ik schrijf is onder Creative Commons. Verder willen ze graag wat interviews met de hackers. Ook die heb ik al. Zie het volgende hoofdstuk.

12. Bug Hunting: baan zonder baas

Een hack event is leuk en leerzaam, maar ook een tijdsopname. Beter is continu open te staan voor hackers van allerlei pluimage. Dat kan met een coordinated vulnerability-disclosurepagina op je site en wachten tot de vrijwilligers zich melden. Het is dan wel de vraag wat je krijgt. Beter is om hackers actiever uit te nodigen voor een bug-bountyprogramma en betalen voor hun bevindingen. Grote IT-bedrijven als Microsoft, Google en Apple doen dat al jaren, maar ook steeds meer kleine bedrijven en overheden loven bug bounties uit.

Ik vroeg me af wie die bug hunters zijn die net dat vinden wat anderen over het hoofd zien, hoe ze te werk gaan en wat dat nu eigenlijk oplevert, zo'n baan zonder baas. Maar hoe vind je ze? Ik vroeg Chantal Stekelenburg van Zerocopter of ze me in contact kon brengen met bug hunters. Mijn voorkeur ging dan vooral uit naar bug hunters die niet alleen voor hun platform werken, maar die ook voor de andere platformen werken om zo een vergelijking te kunnen maken. Ik kreeg vijf namen door en sprak met hen aan de Hack-Talktafel op 11 juni 2019.

De eerste is Wietse Boonstra. Toen ik hem belde voor een voorgesprek zat hij net met zijn dochtertje in het ziekenhuis. Ik vroeg hem of het wel uitkwam. Wietse: "Ja hoor, ik zat me hier toch te vervelen en heb daarom de site van het ziekenhuis gehackt. Ik kon sollicitatiebrieven inzien en via de webcam naar couveusekindjes kijken. Maar dat heb ik niet gedaan. Ik ken de systeembeheerder inmiddels goed en heb het meteen gemeld. Ik meld altijd alles netjes." Hij hackt dus niet alleen voor geld, maar ook als vrijwilliger, onder de regels van coordinated vulnerability disclosure. We praatten wat verder over zijn achtergrond. Hij heeft, net als ik, de lagere technische school elektrotechniek gedaan. We zijn het erover eens dat die

opleiding wel de beste manier is om alle plezier in techniek eruit te rammen. Wietse heeft meer geleerd van zijn vader, met wie hij radio's maakte, en vooral door alles zelf uit te proberen. "Als kind wilde ik alles binnenstebuiten keren. Slopen, om te kijken hoe het werkt en dan zelf iets beters bouwen."

Tijdens Hack Talk gaan we dieper in op hoe hij in IT-security terecht is gekomen. Hoe ging zijn eerste hack? Wietse: "Het begon met een single quootje in een URL achter een ID plaatsen, om te kijken of ik een foutmelding in SQL kreeg. Uit die foutmelding kun je al afleiden of je zelf commando's naar de MySQL-database kunt sturen, zonder dat te doen. Zo ben ik er eigenlijk ingerold, vanuit de webhosting kant, door zelf te testen." Waar ligt volgens hem de grens tussen wat je nog wel en niet kunt doen? "In dit geval ligt de grens bij die foutmelding. Je gaat geen tabellen bekijken of downloaden."

Sinds 2017 werkt hij als senior-securitytester bij Isatis Cyber Security. Daarvoor was hij security engineer bij I-Real en systeembeheerder bij TotaalNet. Zijn werk als pentester doet hij als zelfstandige onder de naam WBsec. Wietse: "Ik werkte bij een hostingbedrijf, waar de server om de haverklap werd gehackt. Ik vroeg me af hoe dat kon en ging op onderzoek uit. Daarna werkte ik bij een bedrijf dat SCADA-systemen heeft. Die moeten natuurlijk echt veilig zijn. Ze zeiden: 'Laten we Wietse maar op training sturen.' Dat beviel me erg. Je leert niet alleen breken, maar ook van je eigen fouten als systeembeheerder. Dingen waarvan ik toen vond dat het normaal is, daarvan denk ik nu: moet je niet doen. Inmiddels doe ik alleen de breekkant. Alles wat kapot kan, gaat kapot. Eerlijkheid duurt het langst: meld altijd, ook als ze geen responsible-disclosurebeleid hebben. Dat heb ik tot nu toe altijd goed gedaan."

De trainingen waar Wietse het over heeft zijn CAST 611 Advanced Penetration Testing, van EC-Council Certified Ethical Hacker en die van Offensive Security: OSCP (Offensive Security Certified Professional, zowel Prof als Advanced level) en de OSCE (Certified Expert). Wietse: "Die van Offensive Security zijn volgens mij wel het hoogst aangeschreven wat ik kon halen. Echt een uitdaging. Bij OSCP krijgt je drie URL's die je moet hacken en succes ermee. Daar heb je 24 uur de tijd voor. Vooral de tijdsdruk

is het grootste probleem. Ik ga nu ook de OSWE (Web Expert) doen. Dan moet je exploits schrijven. Echt next level."

Naast zijn werk als pentester en het doen van vrijwillige disclosures is Wietse ook bug hunter, onder de naam WBsec. Hoe ontdekte hij dat hij geld kon krijgen voor zijn meldingen? Wietse: "Twee jaar geleden deed ik een melding bij een bedrijf. Ze vroegen me of ik een rapport kon opstellen en ik kreeg daar 50 euro voor. Het bleek dat ze een bugbountyprogramma hadden lopen via Zerocopter. Ik mailde of ik mee mocht doen aan dat programma en zo ben ik erin gerold. Inmiddels heb ik meer dan honderd rapportages gedaan." Verdient dat nog een beetje? "Ja hoor, je hebt een lekkere 13e maand. Of een 14e, of 15e… Nou OK, ik heb er in totaal 13.000 euro mee verdiend."

Wat vindt hij de leukste hacks? Wietse: "Vooral webapplicaties. Je drukt op allerlei knopjes en kijkt wat er misgaat. Laatst nog eentje, die ineens allemaal sms'jes genereerde. Maar ik weet niet of ik daarover mag vertellen…" Hij kijkt naar Chantal van Zerocopter, die vanuit de zaal roept: "Je mag het wel vertellen, als je de naam maar niet noemt." Wietse: "OK. Ik was stiekem een beetje automatisch aan het testen. Daardoor werd meerdere malen een URL aangeroepen. Die stuurde een token via sms. Die persoon kreeg dus 500 sms'jes, midden in de nacht. Die heeft niet lekker geslapen."

Wat is zijn advies aan beginnende hackers? Wietse: "Je moet een natuurlijke aanleg hebben, vooral in nieuwsgierigheid. En doe het responsible. Wie goed doet, die goed ontmoet. Ga niet zomaar melden: 'Ik heb jullie gehackt en doe eens effe geld.' Je moet je netjes voorstellen: wie je bent, waarom je dit doet en precies aangeven wat je op welk IP-adres hebt gevonden."

Bij de 2019 editie van Hâck The Hague won Wietse de eerste prijs voor Most Sophisticated Hack. Wat hij vond, kan hij niet vertellen, maar het was blijkbaar iets heel bijzonders. Het leverde hem in ieder geval 2.000 euro op. Na de media-aandacht rondom dit event, kreeg hij ook een interessante onderzoeksopdracht voor de Dienst Justitiële Inrichtingen.

De tweede bug hunter in ons programma is Erik van Oosbree. Hij is pentester bij Sinserus en heeft de afgelopen vijf jaar aan bug hunting gedaan via Bugcrowd. Erik: "Bugcrowd kwam toen net op. Ik zat na twintig

meldingen in de top 100 van de ranking.” Zijn naam prijkt ook in vele Hall of Fames, onder ander van Gamma, Yahoo, Sony, Deutsche Telekom, Erasmus Universiteit, NCSC en de datingsite OkCupid. Wat is zijn drijfveer om aan bug hunting te doen? Erik: ”Het is een perfecte combi van vrijheid om te doen wat je wilt en er ook wat geld mee te verdienen. Toen ik ermee begon, wist ik natuurlijk nog niet wat ik allemaal kon. Het gaf me ook een playground om dingen te proberen en te kijken wat mogelijk is. Het is een tool om te groeien, door meer applicaties te zien en te testen. In die tijd waren ook de banken net begonnen met responsible disclosure. Daar heb ik veel van geleerd.”

Ik ken Erik nog van onze eigen hackcompetitie Lord of the Things in 2017. Hij nam toen deel met een team van de Hogeschool Leiden, richting forensische IT. Erik: “Dat was toen best uniek, want we hadden nog nooit als school meegedaan aan een hackwedstrijd. Zij waren ouderejaars en ik tweedejaars. Ik had op een oproep gereageerd en we hebben elkaar bij Hack Talk eigenlijk pas voor het eerst ontmoet.” Het team won de prijs van Most Techy Hack. Wat hadden ze gevonden? “We hadden een scenario waarbij we van de ene kwetsbaarheid naar de andere gingen. Het begon met een configuratiescherm dat publiekelijk toegankelijk was. We bezochten die pagina via ons eigen wifi-access point, dat we als naam een stukje Javascript hadden gegeven. Die code werd toen uitgevoerd op die pagina. Je kon niet iemands sessie overnemen, maar je kon je wel voordoen als iemand anders, bijvoorbeeld voor een fishing campagne.” Het valt me op dat ik vaak studenten van zijn opleiding zie winnen bij hack events. Wat is zijn verklaring? “Bij forensische IT leer je sporen analyseren, hoe hackers ergens binnenkomen. Dan leer je tegelijk ook hoe je dat zelf kunt doen.”

Ook bij Hâck Den Haag 2018 sleepte Erik een prijs in de wacht: 2e prijs Most Techy Hack. Dit keer op eigen titel. Erik: “Ja, die vondst was eigenlijk een beetje van het padje af. Ik had binnen een subdomein van de gemeente gezocht naar een specifieke applicatie waarvan ik wist dat die kwetsbaar was en kwam uit bij een reserveringssysteem van een sportlocatie. Toen ik die meldde, bleek de applicatie van een andere gemeente te zijn.” Niettemin kreeg Erik toch de prijs en heeft de gemeente Den Haag de melding netjes doorgegeven aan die andere gemeente en daar uiteraard niet over gepubliceerd.

Voordat hij naar de Hogeschool Leiden ging, had hij eerst vmbo Techniek gedaan en daarna mbo – Computer Networking and Security. Daar leerde hij Olivier Beg kennen, de hacker die al op jonge leeftijd veel bug bounties binnenhaalde en nu Head of Research is bij Zerocopter. Erik: “Olivier en ik waren klasgenoten en toen hij vertelde over hacken vond ik dat meteen interessant. Dat was 2012 en ik was dus 16 jaar toen ik ermee begon. Ik heb toen, geloof ik, alle banken wel gehad. Zo ben ik ook aan mijn stage gekomen. Via een responsible disclosure kon ik aan de slag bij het Security Operations Center van ABN AMRO. Ik vond toen ook een lek in onze online studieomgeving. Een docent zei: ‘Laat mij eens zien’. Ik heb het toen tijdens de les voorgedaan. Die docent heeft mijn melding niet doorgegeven, maar ik moest wel later op gesprek komen bij de opleidingsmanager. Die zei dat ze gezien hadden dat ik probeerde in te breken… Het was nog allemaal nieuw in die tijd.”

Wat vindt hij zo leuk aan hacken? “Je wilt weten hoe het werkt en laten zien dat iets niet klopt. Ik vind het leuk als ik naar een klant ga en toegang krijg tot een netwerk, waarvan ze dan zeggen: ‘Succes ermee’. Dan ga ik kijken. Wanneer ik, bijvoorbeeld, een open account vind, werk ik van daaruit verder. Eind van de week lever ik een rapport op, waarin ik laat zien dat ik de hoogste rechten heb verkregen vanuit het niets. De week erna kom ik op gesprek en zeggen ze: ‘We hebben dit systeem al zoveel jaren en jij krijgt binnen een dag de hoogste rechten!’. Ik ben puur met de beveiliging bezig, terwijl zij vooral hun organisatie draaiende moeten houden. Voor hen is security niet de hoogste prioriteit. Ze maken foutjes en slordigheden waar ze overheen kijken, want ze moeten snel releasen. Of ze hebben het uitbesteed aan een serviceorganisatie die hun eigen bedrijfsnaam als wachtwoord instelt. Lekker makkelijk. Nog een tip voor domeinbeheerders: zet alsjeblieft niet het wachtwoord in de gebruikersomschrijving. Dat komt nog te veel voor.”

De derde bug hunter is Jorik Berkepas. Hij heeft hbo Technische Informatica gedaan, is certified scrum master en werkt nu acht jaar als ontwikkelaar bij Embrace Social Business Software. Toen zijn werkgever een bug-bountyprogramma startte via Zerocopter, zag Jorik hoe hackers allerlei fouten ontdekten in hun programma’s. Hij dacht dat ook wel te

kunnen, schreef zich in bij de Kamer van Koophandel als zelfstandige en ging naast zijn baan bug hunten. Niet alleen bij Zerocopter maar ook via andere platforms. In twee jaar tijd heeft hij al behoorlijk veel meldingen op zijn naam staan: 200 via Zerocopter, 35 via het Belgische Intigriti en nog enkele meldingen via HackerOne en het Franse platform Yogosha. Ziet hij verschillen tussen de Nederlandse en Belgische bug-bountyprogramma's? Nederland is immers voorloper in responsible disclosure. Jorik: "Nee hoor. De Belgen doen het net zo goed, zo niet beter. Ze hebben er goed over nagedacht hoe je meldingen afhandelt en begrijpen ook dat je daar capaciteit voor moet reserveren."

Hij ziet namelijk in de praktijk dat meldingen niet altijd goed afgehandeld worden. Jorik: "Bug hunting is voor je vertrouwen in de mensheid niet bemoedigend, maar voor je motivatie wel. Je ziet gewoon heel veel kleine foutjes. Bijvoorbeeld XSS. Is makkelijk op te lossen, maar er glipt er altijd wel een tussendoor. Dan kun je de code in Javascript invoeren op de site, de gebruikerskant overnemen en de code uitvoeren als een andere gebruiker. Afhankelijk van hoe creatief je bent en hoeveel tijd je hebt, kun je daar best veel mee doen. Maar het zijn geen losse probleempjes, meer categorieën aan problemen. Bij alles in software hangt de ernst van de kwetsbaarheid af van waar het zit. Het is toch elke keer weer net iets anders en daar leer je weer van. Het is niet bam erop afvuren, je moet echt gericht op zoek gaan. Die bedrijven hebben meestal wel al pentesten laten uitvoeren over het geheel, maar lossen de problemen op bij twee plekken en vergeten de andere twintig. Er zijn ook organisaties die gewoon hopen dat je niks vindt en er helemaal niet op ingesteld zijn iets te fixen. Dan vind je een halfjaar later nog steeds die bug."

Wat is zijn favoriete hacktechniek? Jorik: "Je doet als eerste de veelvoorkomende kwetsbaarheden waar de hoogste bounties tegenover staan. Dus niet die van 50 euro, maar die van 1.000 euro. In veel sites zit een IDOR (Insecure Direct Object Reference). Als je bijvoorbeeld een nummertje wijzigt in de URL van jouw factuur, dan kom je in die van je buurman. Dan liggen er ineens best veel gevoelige gegevens op straat. Vaak ga ik in de Javascript-code die een site meestuurt neuzen of er interessante dingen in zitten. Ik heb het voordeel dat ik die code dagelijks lees en daarom vind ik sneller iets."

Is bug hunting goed te combineren met zijn baan als developer? Jorik: “Nou, mijn vriendin is er niet zo blij mee. Dan begin ik om acht uur ’s avonds en denk ik dat ik die bug bijna heb gevonden, maar wordt het toch weer twaalf uur. Maar het schuift best goed. Findings variëren meestal van 50 tot 1.000 euro. De hoogste die ik heb gehad was 2.500 euro, voor een halfuurtje werk. Dat is best lekker. Maar je zit ook weleens een hele dag aan een programma en dan vind je niets. Of dat je een bug meldt die net door iemand anders is gevonden. Ik kon een keer op de site van een vliegmaatschappij met wat trucjes de identiteitskaarten van passagiers achterhalen. Daar stond een dikke bounty op. Maar die was, vlak voor ik kwam, gemeld door iemand anders. Twee dagen werk voor niks.” Ook bij Hâck The Hague 2019 sleepte hij prijzen in de wacht: de derde prijs in de categorie Most Impactful Hack (500 euro) de tweede prijs Most Sophisticated Hack (1.000 euro).

De grootste beloning is wellicht nog dat Jorik veel leert van bug hunting voor zijn werk als ontwikkelaar. “Door de bug bounties is mijn algemene gevoel en niveau qua security in softwareontwikkeling flink gestegen. Hierdoor kan ik mogelijke beveiligingsproblemen in nieuwe delen van onze software vrijwel direct zien. Andersom werkt het ook. Door mijn ervaring als ontwikkelaar kan ik delen van een code lezen, vanuit daar problemen beredeneren, deze problemen eerder vinden en preventief optreden. Zo houd ik ook mijn collega’s scherp. Dus softwareontwikkelaars: ga dit ook doen.”

De vierde bug hunter is Daniel Bakker. Hij laat zien dat je ook binnen de wereld van de bug hunters kunt opklimmen. Na maar liefst 584 bugs te hebben gerapporteerd via HackerOne, is hij daar nu Security Analyst en beoordeelt hij de rapportages van andere hackers, oftewel de triage. Net als de andere bug hunters, heeft Daniel een achtergrond als softwareontwikkelaar. Als Lead Engineer bij Topic Embedded Products werkte hij 11 jaar voor grote namen als Océ en Philips. En net als de andere hunters werd hij in 2013 getriggered door de Nederlandse banken die aan responsible disclosure gingen doen en kwam hij via dit vrijwilligerswerk in aanraking met de bug-bountyprogramma’s. Hij staat in de Hall of Fame van AOL, Microsoft, Netflix en de OV-chipkaart.

Hoe hij bij HackerOne heeft gescoord als bug hunter is te zien op hun dashboard met ranking. Daarop prijken maar liefst 300.000 hackers van over de hele wereld, veelal onder pseudoniem. Deze ranglijst is een mooie introductie in hoe het werk van bug hunters wordt beoordeeld. Daniel heeft een ‘Signal’ van 5.41. Dat is een gemiddelde van de kwaliteit van zijn rapportages op een schaal van -5 tot 7. Hij zit op een ‘Percentiel’ van 91. Dat betekent dat hij op de 91ste plek staat als het gaat om de hoogte van zijn bounties. Daniels ‘Impact’ score is 18.75. Dat zegt iets over hoe zwaar de kwetsbaarheden zijn die hij vindt. Dit alles telt op tot een ‘Reputation’ van 14.220, waarmee hij in de overall ranking op de 16e plek staat. Best een zware jongen dus.

Echter, hoe kun je bug hunter zijn en tegelijkertijd rapporten van andere hunters beoordelen? Spelen daar conflicterende belangen? Daniel: “Jazeker. Als analist kan ik geen zero-days of bijzondere hacktechnieken die ik beoordeel zelf gebruiken. Alleen de dingen die ik al ken en wat je publiekelijk op het internet ziet. En ik kan natuurlijk niet meedoen aan de programma’s die ik zelf beoordeel. Maar het kan dus wel zo zijn dat collega’s hacken binnen elkaars programma’s.” Zakt hij daardoor in de ranking? “Ja. Ik kan minder hacken nu. Maar die 16e plek is ook maar gewoon een nummer. Je Signal is belangrijker. Dat zegt iets over de kwaliteit van je werk.”

Wat vindt hij zijn leukste hack tot nog toe? Daniel: “Dat was een grote onlinewinkel, waar ik de creditcardgegevens van andere klanten kon gebruiken om bestellingen te doen. Dat had te maken met de cashing van de site. Best moeilijk te reproduceren. Dus na heel veel heen en weer schrijven, zei de man van die webshop: ‘Ik heb net een order geplaatst, kom maar op met mijn creditcardnummer.’ Die had ik na vijf minuten en hij reageerde met het bekende F-woord.”

Heeft Daniel nog advies aan beginnende hackers? “Ja. Kijk eerst goed naar het bedrijf dat je hackt en schat in wat voor hen echt belangrijk is. Is dat bijvoorbeeld de gebruikersdata? Veel hackers kijken naar één techniek, bijvoorbeeld XSS of SQL. Combineer die technieken om echt impact te hebben. Dat moet je ook in je rapport beschrijven.”

Bij Hâck The Hague won hij in 2019 de tweede prijs in de categorie Most Surprising Hack. Bij HackerOne is hij inmiddels Triage Team Lead

geworden. Die promotie zal niet bevorderlijk zijn voor zijn overall score, want er zijn nog maar weinig hackprogramma's waar hij zonder voorkennis kan meehacken.

De vijfde en laatste bug hunter aan tafel is Wouter van Rooij, sinds 2017 Business Unit Leader Cyber Security Netherlands bij IT-dienstverlener Onepoint. Daarvoor zat hij vier jaar bij Sogeti, eerst als pentester, daarna als operations manager van het Security Center of Excellence. Ook hij heeft zijn OSCP. Als zelfstandige testte hij verschillende versies van iOS. Sinds een halfjaar doet hij ook bug bounties. Onder andere bij het Havenbedrijf Rotterdam. We praten daarom ook met hun Security Officer Rob de Charro. Maar eerst Wouter, want hij laat zien hoe bij hackers de neiging om van alles uit te testen al jong begint.

Wouters eerste hack deed hij toen hij 11 jaar was. "Mijn ouders vonden dat ik te veel op de computer zat, dus toen stelde mijn vader een wachtwoord in. Niet voor Windows, maar voor de BIOS, het opstartprogramma. Dat vond ik heel vervelend, dus ik zocht allerlei manieren om dat te omzeilen. Eerst ontdekte ik dat ik dat kon door de batterij er even uit te halen. Maar toen ontdekte mijn vader natuurlijk zelf ook dat er ineens geen wachtwoord meer nodig was. Uiteindelijk vond ik een programmaatje waarmee ik het BIOS-wachtwoord kon uitlezen. Daar kwam hij pas drie maanden later achter toen hij thuiskwam en mij achter de computer aantrof. Hij baalde, maar vond ook wel dat ik het knap had gedaan."

Zijn vader blijkt zelf ook hacker te zijn en was een van de oprichters van het securitybedrijf Madison Gurkha. Hij nam Wouter al op zijn 13e mee naar hackersevents, zoals HAL2001, Hackers At Large, de voorloper van SHA. Wouter: "Ik zag veel langharige mannen met baarden. Een soort LAN-party keer honderd. Er werden hele kasten naartoe gezeuld met oude computers. Nu zie je ook veel kinderen op die hackerkampen. Die kunnen met LEGO spelen enzo. Dat zag je toen nog niet."

In 2010 was Wouter de eerste die WhatsApp hackte. De chatapp was het jaar ervoor gelanceerd en beschikbaar op mobiele telefoons. Wouter installeerde de app op zijn iPhone4, maar kon hem niet op zijn iPad zetten. Na wat puzzelen lukte het hem alsnog en ontdekte hij een beveiligingslek.

“Als je WhatsApp installeert, moet je je telefoonnummer invullen. Daar sturen ze een sms naartoe met een code die je moet invullen. Zo weten ze dat je eigenaar bent van dat nummer. Ik kon die code al uitlezen in de property list file, dus voordat ze je die sturen. Dus heb ik het telefoonnummer van mijn moeder gebruikt. Ze kreeg die sms dus niet, maar ik kon wel als haar appen, terwijl ze toen gewoon een oude Nokia had. Ik appte mijn vader, die verbaasd reageerde met: ‘Wie is dit?’. Ik antwoorde: ‘Je zoon. Ik heb iets gevonden wat niet de bedoeling is.’”

Wouter meldde zijn vondst bij info@whatsapp.com en kreeg een reactie van de oprichter van WhatsApp. “Ik vroeg of ik er nog wat voor kreeg, want ik heb er toch tijd en moeite in gestoken. Bug bounties bestonden nog niet, dus we gingen nog wat onderhandelen over het bedrag. Prompt kreeg ik een brief van een advocaat, zo een die grote zaken had gedaan. Daar ga je als student natuurlijk niet op in. De kwetsbaarheid was twee weken erna gefixt.” Hij heeft veel geleerd van dit incident en ging zijn meldingen doen onder responsible disclosure en bug-bountyprogramma’s.

In zijn huidige rol als businessunit leader doet hij steeds minder techniek en moet hij vooral deals verkopen. Dan mist hij het hacken wel en zijn de bug-bountyprogramma’s een prettige uitlaatklep. Wouter: “Het gaat me niet zozeer om het financiële gewin, maar meer omdat ik daar los mag gaan. Ik zie het vooral als een competitie tegen mezelf.” Hij deed ook mee aan Hâck The Hague, waar hij in de 2018 editie twee keer een 3e prijs won. En via Zerocopter deed hij een melding bij het Havenbedrijf Rotterdam.

Om ook een beeld te krijgen van de ontvangers van meldingen is Rob de Charro erbij gevraagd. Hij is Information Security Officer bij het Havenbedrijf. Ik ken hem ook omdat ik voor hen de zogenoemde Port Cyber Cafés in de haven leid. Rob en Wouter kennen elkaar van hun tijd bij DICTU, de Dienst ICT Uitvoering. Rob deed daar eerst de helpdesk, daarna technisch beheer en vervolgens coördinatie. Nu bij het Havenbedrijf zit hij vooral op het Security Operations Center om de digitale omgeving te monitoren. Rob: “Ze hadden bij het Havenbedrijf al een sterke safety mindset. Daar komt nu security bij. Ik kan zelf best aardig wat kwetsbaarheden vinden, maar het echte pentesten laat ik liever aan de jongeren over. Het is een sfeer van samen die puzzels oplossen.”

Toch ziet Rob het pentesten slechts als een deel van de oplossing. Ze moeten als bedrijf ook openstaan voor bevindingen die buiten de scope van de tests vallen. Hiervoor zette hij een responsible-disclosureprogramma op en bracht dat onder bij Zerocopter. Ze krijgen dan weleens meldingen voor andere bedrijven die via hun site te benaderen zijn. “We zijn in principe alleen verantwoordelijk voor portofrotterdam.com en wat online producten die daaronder hangen, maar helpen die andere bedrijven door meldingen door te zetten. Het gaat ook om de naam van Rotterdam.”

Het responsible-disclosureprogramma draait continu en op gezette tijden openen ze ook een bug-bountyprogramma. Rob: “We krijgen twee of drie meldingen per maand. Bij triage valt er vaak al een af, bijvoorbeeld omdat de hack niet reproduceerbaar is. Die andere hacks geven we door aan de ontwikkelaar. Die kan via het platform contact opnemen met de melder. De hacker krijgt pas uitbetaald als wij echt wat kunnen met de melding.”

Het bug-bountyprogramma van het Havenbedrijf houdt ook de pentesters scherp. Rob: “Ik zeg weleens tegen pentesters: ‘Let wel, er komt een bug-bountyprogramma achteraan, dus ik zou wel erg teleurgesteld zijn als daar wat uitkomt.’ Dan jaag je elkaar aan om de producten goed vorm te geven. Het programma loopt nu anderhalf jaar en ik merk dat we de hackers steeds eerder inzetten. Zo kunnen we dingen nog makkelijk aanpassen. De plan-do-check-actcyclus wordt korter. Ik houd ook van ontwikkelaars die kunnen hacken en van hackers die kunnen ontwikkelen. Leuk om hier te zien hoe ze het als een spelletje ervaren en de wereld op een next level krijgen. Ga dus vooral kijken bij ons en als we niet snel genoeg reageren, meld dat ook.”

Maar, wat voor kwetsbaarheid heeft Wouter nou gevonden bij het Havenbedrijf? Dat kan hij nog niet vertellen, want het moet nog gefixt worden. Wel ziet hij het Havenbedrijf als een goed voorbeeld van hoe je een bug-bountyprogramma opzet. “Als je aan bug bounties wilt gaan doen, dan moet je eerst goed nadenken wat er op je afkomt. Het kan veel werk en tijd kosten en het moet wel wat opleveren. Begin dus net als zij met één site en bouw dat uit. Maak gebruik van kennis die er al is en omarm iedereen die wil helpen.”

Heeft hij tot slot nog een tip voor hackers? “Ja: focus op de niet-standaard dingen. Er zijn al grote groepen Indiërs die vanuit een financiële

drijfveer veel standaardkwetsbaarheden eruit halen. Kijk meer naar de flow in de applicaties: kun je stappen overslaan of stappen dubbel doen? Onlogische keuzes maken, daar zijn hackers goed in."

Dat is inderdaad wat al deze bug hunters gemeen hebben: ze kijken en doen gewoon net anders dan waar de makers van IT vanuit gaan. Opvallend is dat de meesten eerst zelf aan de maakkant zaten, om het daarna te slopen en frustratie met fouten in het ontwikkelproces omzetten in creatief testen. Ze zijn zeer competitief: ze willen slimmer zijn dan de makers en andere brekers voor zijn. En al vertonen deze hackers hun kunsten voor harde cash, dat lijkt niet hun primaire drijfveer te zijn. Net als de meeste andere hackers die we zijn tegengekomen, hacken ze vooral om de samenleving veiliger te maken. Hopelijk geldt dat ook voor de laatste categorie hackers die we in dit boek bespreken: de staatshackers.

13. Openheid over de geheime diensten

“Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz. Allen, die deze zullen zien of horen lezen, saluut! doen te weten: Alzo Wij in overweging genomen hebben, dat het wenselijk is nieuwe regels te stellen met betrekking tot de taken en bevoegdheden van de inlichtingen- en veiligheidsdiensten in het kader van de nationale veiligheid, de coördinatie van de taakuitvoering van deze diensten, de verwerking van gegevens door deze diensten, de nationale en internationale samenwerking van deze diensten, de uitoefening van het toezicht en de behandeling van klachten en de geheimhouding, alsmede in verband daarmee enkele wetten te wijzigen en de Wet op de inlichtingen- en veiligheidsdiensten 2002 te vervangen…”

Als je denkt “wat staat daar nou?”, dan heb je hem blijkbaar destijds niet gelezen: de Wiv, oftewel de nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Waarschijnlijk heb je er wel over gestemd, woensdag 21 maart 2018. Ik ook en ik heb lang getwijfeld of ik voor of tegen zou stemmen. Aangezien vooral het Nee-kamp in de media was gekomen en we nu aan de wet vastzitten, beschrijf ik in dit hoofdstuk mijn zoektocht langs vele meningen. Uiteraard heb ik er een Hack Talk over georganiseerd.

Zelf vond ik het best even schrikken. De eerste berichten over de nieuwe wet gaven aan dat de veiligheidsdiensten ongericht internetkabels kunnen gaan tappen, de data drie jaar bewaren en delen met het buitenland. Maar de wet biedt ook meer waarborgen tegen ongebreidelde inmenging van de diensten: een toetsingscommissie gaat de inzet van de middelen vooraf toetsen, een andere commissie evalueert dat achteraf en voor burgers komt er zelfs een mogelijkheid op beroep wanneer je je digitaal betast voelt. Dat

is uniek in de wereld. Bovendien, in een democratie is elke wet immers een compromis. Nooit zal iedereen 100% tevreden zijn.

Na akkoord van de Tweede Kamer, de Eerste Kamer en de Raad van State zou de wet 1 januari 2018 van kracht moeten zijn. Dat gebeurde niet. Vijf studenten hadden, gesteund door Amnesty, Bits of Freedom, de Piratenpartij en Arjan Lubach, 400.000 handtekeningen opgehaald voor een referendum over deze, vanaf dat moment genoemde, ‘sleepwet’.

Een van die studenten zag ik tijdens het Chaos Communication Congress in Leipzig. Op 30 december 2017 gaf Nina Boelsum een presentatie: ‘Fuck Dutch Mass surveillance, let’s have a referendum’. Deze titel geeft al duidelijk haar standpunt weer. Interessant vond ik vooral hoe de actievoerders aan zoveel handtekeningen kwamen. Ze kregen hulp van Amnesty, die een vliegtuigje huurde met ‘Ik word gevolgd, u ook. Stem tegen de sleepwet’. Bits of Freedom en de Piratenpartij hielpen ook mee in de pr. Samen haalden ze maar liefst 100.000 handtekeningen op, maar niet genoeg voor de benodigde 300.000. Met nog slechts een week te gaan, hadden ze de moed opgegeven.

Tot ze op zaterdagavond werden gebeld door Arjan Lubach. “Je kunt maar beter extra serverruimte regelen, want we gaan morgen een item doen over de sleepwet”. Die zondagavond vertelde hij dat de overheid voorzieningen treft om iedereen af te kunnen luisteren, maar daar in principe niets mee doet… Zo schoten ze ineens door naar 400.000 handtekeningen, genoeg voor een referendum. Markant detail: die moesten allemaal geprint worden en naar Heerlen worden gebracht. Onmogelijk voor de vijf studenten, maar daar heeft Amnesty ze bij geholpen.

Met een referendum komen er subsidies beschikbaar: maar liefst 2 miljoen euro, waarvan zes ton voor een campagne ‘voor’, zes ton voor een campagne ‘tegen’ en acht ton voor ‘neutraal’. Wie wat kreeg, is online te lezen bij de referendumcommissie. Slechts vier organisaties hebben elk 50.000 gekregen voor een campagne ‘voor’. Ik heb ze gegoogeld, maar vond niets over hun campagnes. In het kamp ‘tegen’ wel. We zien de studenten van het referendum onder Stichting De Kabel en Bits of Freedom, die elk ook 50k kregen. Zeer welbesteed, zou ik zeggen. Ook waren er veel politieke partijen die campagnegeld kregen, wat ik een beetje dubieus vind

in verkiezingstijd. Geenpeil, die zegt ‘neutraal’ te zijn, kreeg 50k voor ‘informatie op de website’. Op die site staat alleen een knop met ‘doneer’. In het ‘tegen’ kamp zie je veel kleine groepjes privacy-activisten die 50k krijgen voor ‘een website en een evenement’.

Dus ging ik, naar aanleiding van een blogpost, naar een ‘kritisch’ debat in Amsterdam. Het was een zolderkamer – “gratis, van een vriend”, zei een van de organisatoren – met acht bezoekers: vijf vertegenwoordigers van de stichtingen die elk 50k hadden gekregen, twee andere bezoekers die bij voorbaat tegenstemden en ik. Na drie uur wederzijdse bevestiging en geklaag over de staat, vroeg ik of dit nu dat event was waar zij die 50k voor kregen. Nee, ze gingen ook nog een kritisch essay online zetten en bierviltjes rondbrengen. Voor 50 euro per uur (exclusief btw). Privacy is big business.

Het ‘voor’-kamp had steun van gratis kijkcijferkanon Rob Bertholee. De AIVD-baas mocht bij College Tour en DWDD uiteenzetten waarom we vooral vóór de wet moeten zijn. En passant werd gelekt dat de AIVD de Russen had gehackt. Dit werd door de media opgepikt, compleet met beelden van Mark Rutte die trots zegt te zijn op zijn diensten. Het publiek raakte echter steeds meer in verwarring. Volgens I&O Research was er in september 2017 nog een meerderheid ‘voor’ en een minderheid ‘tegen’. Die meerderheid brokkelde gaandeweg af vanwege een groeiende groep die nog niet wist wat te stemmen. De stand op 6 februari 2017 was 42% voor, 28% tegen en 30% weet niet. Tot die 30% behoorde ik zelf toen ook en ik ging me inlezen.

Allereerst: hoe groot is het zogenoemde sleepnet? In de wet zelf gaat het over ‘onderzoeksopdracht gerichte interceptie’. Lekker vaag dus, want als je de onderzoeksopdracht maar breed genoeg definieert, kun je in wezen alles tappen. Als je verder leest, zie je dat dat niet het geval zal zijn. Elk onderzoek waarbij de dienst bijzondere bevoegdheden wil inzetten, moet eerst voorgelegd worden aan de minister van Binnenlandse Zaken en een Toetsingscommissie Inzet Bevoegdheden (TIB). Die kijken of er niet te veel wordt getapt en of hetzelfde doel niet met minder ingrijpende middelen bereikt kan worden. Tijdens en achteraf evalueert de Commissie Toezicht Inlichtingen- en Veiligheidsdiensten (CTIVD) wat de dienst doet. Mocht je

als burger toch onevenredig nadeel ondervinden van het werk van de dienst, kun je terecht bij deze zelfde CTIVD, die vervolgens een bindend oordeel uitspreekt. De minister brengt tot slot jaarlijks verslag uit.

De wet gaat niet alleen over tappen, maar vooral over de regels waar de diensten zich aan hebben te houden. Bijvoorbeeld: “De verwerking van persoonsgegevens wegens iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven vindt niet plaats.” Ze doen ook geen onderzoek naar strafbare feiten, maar naar personen die een bedreiging vormen voor de Nederlandse rechtsorde. Afluisteren van journalisten of advocaten moet naast deze hele procedure ook nog eens voorgelegd worden aan de rechtbank in Den Haag. Inbreken op andermans computer mocht al en wordt nu veel strikter omschreven. Het verzwakken van encryptie – iets wat de NSA stelselmatig doet – is zelfs verboden, want daarmee brengt de dienst zelf de veiligheid van digitale communicatie in gevaar. Dit vind ik winst.

In diezelfde wet lees ik echter ook dat de diensten hun gegevens kunnen delen met diensten van andere landen, zelfs als die gegevens niet geëvalueerd zijn. Ze moeten hier echter wel een “dringende en gewichtige reden” voor hebben en “de ondersteuning kan niet bestaan uit het bieden van gelegenheid tot het zelfstandig verzamelen van gegevens door de desbetreffende dienst in Nederland.” Die landen moeten wel voldoen aan de voorwaarden voor een democratische rechtsstaat. De VS lijkt me daarmee uitgesloten, maar ik kan me niet voorstellen dat dat ook gebeurt. Wat ik ook te ver vind gaan, is het hacken van derden om bij het onderzoeksdoel uit te komen en bevoegdheid om databases te vorderen bij bedrijven zonder toestemming van de minister. Aan de andere kant kan ik me wel noodscenario’s voorstellen waarbij het doel de middelen heiligt.

Kortom, de wet geeft de diensten een aantal verregaande bevoegdheden, maar tegelijk ook meer regels waar zij zich aan hebben te houden en de overheid middelen om hen te controleren. Ik wist nog steeds niet wat ik moest stemmen. Daarom besloot ik zelf een debat te organiseren met mensen van wie ik weet dat ze kennis van zaken hebben: drie voor en drie tegen de wet. Ik deed het overigens zonder campagnesubsidie.

Hack Talk, 13 maart 2018. Club Worm te Rotterdam is met 120 bezoekers lekker vol. Er is een divers publiek: jong, oud, hackers, academici, anarchisten, zakenlui en ambtenaren. Het eerdere betoog is mijn inleiding, inclusief de vreemd aandoende inleiding van Willem, waarna een ketting van zes sprekers volgt, voor en tegen, om en om. Hun opdracht: mij en het publiek overtuigen.

Mijn eerste gast is Ton Siedsma, jurist en Senior Policy Advisor bij Bits of Freedom (BoF). Vanaf het begin, vijf jaar geleden, is zijn organisatie betrokken geweest bij de totstandkoming van de wet. Tijdens de internetconsultatie hebben ze hun reactie geformuleerd. Met een online tool, met uitleg en reactieformulier, verzamelden ze nog eens 1.100 reacties. Ze hebben de vijf studenten geholpen met pr voor hun handtekeningenactie, onder andere door 20.000 brieven te versturen naar Nederlandse huishoudens, namens ‘Rijksveiligheidsdienst’, met een link naar een Kieswijzer met de titel: ‘Waar trekt u de grens?’. Op hun website eenbeterewet.nl is te lezen welke vijf punten volgens BoF beter kunnen. Bob Hoogeboom is mijn tweede gast. Hij is professor aan Nyenrode Business Universiteit, docent aan de Politieacademie en organiseert politiedebatten. Over de wet schreef hij een artikel in NRC: ‘Slepen of niet slepen, dat is niet de vraag.’

Ton trapt af. Hij vindt het goed dat er een AIVD en MIVD is, maar niet met deze wet. Met name vanwege het sleepnet, dat het mogelijk maakt grootschalig en stelselmatig burgers in de gaten te houden. De bevoegdheid om deze data drie jaar lang op te slaan is te veel, vooral als dat kan zonder die gegevens eerst te evalueren. Uitwisseling met Duitsland kan nog wel, maar hoe zit het met landen zoals Rusland? Zorgelijk vindt hij het hacken van derden om bij het doel uit te komen, het gebruik van informanten en toegang vorderen tot databases van bedrijven. Het toezicht hierop wordt beter, maar vindt hij nog niet goed genoeg. Tot slot zal de wet, op termijn, leiden tot zelfcensuur omdat mensen denken dat ze in de gaten gehouden worden – een ‘chilling effect’.

Bob reageert fel op Tons uiteenzetting en de beeldvorming in de media in het algemeen: “Het is een verkleutering, versimpeling – een ‘dumbing down’ – van een complex vraagstuk. Het doet geen recht aan de belangrijke functie die veiligheidsdiensten hebben en de verbeteringen die deze wet

biedt op de controle op de diensten.” Vooral de term ‘sleepnet’ vindt hij misleidende framing.

Ik vraag hoe breed de onderzoeksgerichte interceptie is. Ton geeft een voorbeeld dat hij van minister Plasterk zou hebben. “Ze nemen bijvoorbeeld alle wifi-hotspots in een middelgrote stad om alle WhatsApp-berichten tussen Nederland en Syrië af te tappen.” Een hele wijk aftappen zal niet zo snel gebeuren, omdat dat technisch lastig is. Bob vult aan: “Deze interceptie vindt pas plaats als er al heel veel is gedaan. De diensten hebben informanten gesproken, agenten uitgezet voor observatie, telefoontaps gezet, systemen gehackt, want dat mag ook al onder de huidige wet en pas in een bepaalde omstandigheid kan het misschien nuttig zijn om op grotere schaal te inventariseren wie met wie contact heeft gehad. Dat kan alleen met opdrachten en die worden vooraf getoetst door de minister en de TIB, en tijdens en achteraf door de CTIVD.”

Ton vindt de controle inderdaad al een verbetering. De minister moet oordelen, de TIB kan weigeren en de klachtenregeling voor burgers is bindend. De uitkomst van de evaluatie achteraf, door de CTIVD, zou bindend moeten zijn, vindt hij. Daar is Bob het wel mee eens. Maar goed, het kan altijd beter. Bob: “Zo’n wet blijft toch een uitkomst van een politiek spel.” Ton vindt dat we daarom tegen moeten stemmen, voor een betere wet. Bob vindt van niet: “Stem je tegen, dan behoud je de oude wet en ben je slechter af.”

Intussen wordt D66-kamerlid Kees Verhoeven, die straks als laatste aan tafel komt, wat ongeduldig en roept vanuit de zaal: “Dit is wel erg veel Ton voor ons geld!” – verwijzend naar de referendumsubsidie. OK, verder met het kettingdebat. Exit Ton, enter Mary-Jo de Leeuw. Zij is van cybersecurity bedrijf Revnext, een van de oprichtsters van de Rotterdamse Cyberwerkplaats en tegen de Wiv.

Mary-Jo heeft weinig vertrouwen in commissies die toetsen: “Wat opvalt is dat voor leden van dergelijke commissies onduidelijk is wat het profiel is, hoe je onderdeel wordt. Als je vriendjes naar voren schuift, zijn die commissies niks waard.” Ik vul aan: “Maar de Kamer stemt over de benoeming.” Mary-Jo: “Is dat al gebeurd?”. Ronald Prins, een van de leden

van de Toetsingscommissie Inzet Bevoegdheden, blijkt in de zaal te zitten en roept: “Ja”.

Ronalds benoeming had kritiek opgeleverd omdat beweerd werd dat hij bij de AIVD had gewerkt en dus niet onafhankelijk zou zijn. Ik heb het hem voorafgaand aan dit debat gevraagd en hij vertelde dat hij twintig jaar geleden, gedurende negen maanden heeft gewerkt bij wat toen de BVD heette. Toen was hij er klaar mee. In de media is hij vooral bekend als de voormalige directeur van Fox-IT, een IT-securitybedrijf dat veel voor de AIVD heeft gedaan. Oftewel: hij weet wat tappen in de praktijk betekent. De Tweede Kamer heeft daarom ingestemd met zijn benoeming. Door de verkoop van zijn bedrijf heeft hij bovendien een financieel onafhankelijke positie. Ik vraag hem zich te mengen in het debat, maar dat wil hij niet: het gaat immers over zijn nieuwe baan. Maar wel leuk dat hij erbij is.

Mary-Jo vervolgt: “De overheid zegt eerst ‘Je hebt toch niks te verbergen?’. Vervolgens organiseren ze de landelijke awareness campagne Alert Online en zegt de overheid dat je wel wat te verbergen hebt. En nu komen ze lekker met een sleepnetje. Ze spreken zich op dat vlak tegen.” Ze heeft ook weinig vertrouwen in de evaluatie van het functioneren van de dienst. “Hoe gaat er gerapporteerd worden? Het is wel duidelijk hoe dat gebeurt. De Cyber Security Raad zou ook geëvalueerd worden. We hebben een WOB-verzoek ingediend, maar kregen niets. Wat je leest in de berichtgevingen over diensten is dat ze zoveel aanslagen zouden hebben voorkomen. Maar dat wordt nooit aangetoond. Laat dat zien.” Bob: “De controlestructuren zijn op papier veelbelovend, maar ik deel je opmerking dat we daar kritisch naar moeten kijken. De CTIVD heeft over tal van zaken rapportages gemaakt waardoor we inzicht kregen in werk van de diensten. Meer kan ook niet altijd.”

Exit Bob, enter Pim Takkenberg, Directeur Cyber Security bij Northwave en in het verleden teamleider bij Team High Tech Crime van de politie en werkzaam geweest bij de AIVD, waar hij een team leidde dat onderzoek deed naar spionage. Wat vindt Pim van Mary-Jo’s argumenten tegen de wet, met name dat de controles en rapportages te onduidelijk zijn gedefinieerd? Pim: “In een democratie stem je op je vertegenwoordiger. We hebben een mooi bestel en polderen om compromissen te sluiten. De rapportage zal

zich in de praktijk moeten bewijzen." Mary-Jo: "Als je zegt dat de praktijk het nog moet bewijzen, dan laat je het dus op zijn beloop. We moeten strakker definiëren waaraan zo'n rapportage moet voldoen, wat het kader is en de frequentie."

Pim: "Ik heb vooral wel vertrouwen in de toetsing door die commissies. Toen ik bij de AIVD werkte, was de inzet op controle vele malen ingewikkelder dan bij de politie. Als je de minister wilt overtuigen, moet je echt wel van heel goede huize komen. Bij de politie was het: je zet een middel in en de rechter toetst achteraf. Bij de dienst is er toetsing vooraf: kan het doel niet met minder ingrijpende middelen bereikt worden en wordt het middel niet te veel ingezet? Dat wordt met deze wet nog vele malen strakker geregeld."

Over naar de stelling van Pim. Hij betoogt: "Als wij deze wet niet krijgen, gaat het economische verdienmodel van Nederland naar de kloten. Ik heb jaren gekeken naar digitale aanvallen op onze kritieke infrastructuur. Het bedrijfsleven is onvoldoende in staat zich hiertegen te weren. Er gaat met vrachten tegelijk aan intellectueel eigendom en geheimen naar het buitenland, waar andere bedrijven producten mee maken en overnames mee doen. Dan hebben we een dienst nodig die in staat is om op knooppunten te zoeken naar indicatoren voor deze aanvallen."

In de praktijk betekent dit dat de AIVD vooral verkeer tapt aan de grenzen en die data scant op aanvalsindicatoren die ze vooraf hebben gedefinieerd, bijvoorbeeld IP-adressen of configuratiebestanden. Veel grote Nederlandse bedrijven doen al aan dergelijke monitoring vanuit hun Security Operations Centers, maar volgens Pim is hun blik te beperkt: "Ze kijken alleen naar hun eigen omgeving, met commercieel beschikbare indicatoren. De AIVD kijkt landelijk en heeft meer informatie."

Mary-Jo: "Ik hoor niets nieuws. Die geheimen worden al op andere manieren gestolen en we hebben toch het Nationale Detectienetwerk van het NCSC?" Pim: "NCSC monitort beperkt en is geen AIVD. Het gaat om de kwaliteit van je indicatoren en waar je kunt kijken. Wat we nu hebben, is niet genoeg om de Nederlandse economie te beschermen." Mary-Jo: "Dat snap ik, maar ik blijf weerstand houden. Ik hoop van harte dat, als we hier over twee jaar weer staan, je me alsnog ongelijk kan geven."

Exit Mary-Jo, enter Brenno de Winter. In zijn tijd als journalist heeft hij vele datalekken aan de kaak gesteld. Momenteel is hij beveiligingsonderzoeker, schrijver, spreker en trainer. Wat vindt hij van Pim zijn betoog, dat zonder deze wet het economische verdienmodel van Nederland naar de klote gaat? Brenno: “Dat gaat eigenlijk alleen over de vitale infrastructuur en niet over een regulier bedrijf. Ik kom bij kleinere organisaties waar het stelen van data grote problemen geeft, maar in de meeste gevallen komt dat door verouderde software en configuratiefoutjes. Heel geavanceerde aanvallen zijn er niet zoveel. En wanneer wel, dan krijgen ze die informatie niet van de AIVD. Zomaar delen is voor hen geen optie.”

Brenno keert zelfs Pim zijn stelling om: “Door de Wiv gaat ons economisch verdienmodel naar de klote. Als je wilt monitoren, moet je dus alles wat binnenkomt op de kabel analyseren. Daardoor zal voor bedrijven Nederland minder interessant worden als vestigingsplaats voor hun data.” Volgens Pim laat de praktijk in het Verenigd Koninkrijk het tegendeel zien. “Britse diensten kunnen tijdig zien of er aanvallen zijn en hebben meer methodes om info te delen met bedrijven. Dat is voor veel bedrijven juist aantrekkelijk.”

Volgens Brenno moeten we sowieso tegenstemmen, want: “De wet gaat toch door. De AIVD en MIVD zijn nog nooit zo open geweest. Stem je voor, dan stopt dat proces. De checks en balances zijn namelijk nogal ingewikkeld geworden.” Pim geeft toe dat het toezicht wat rommelig is geworden. “Er zijn al veel rapportages. Ik heb dat intern meegemaakt: ongelofelijk veel gedetailleerde regels waar je makkelijk foutjes in maakt. Daar waar gewerkt wordt, gaat altijd wel iets mis. Het wordt interessant om te zien of die commissies body genoeg hebben om dit allemaal af te handelen.”

Wat vinden de heren ervan dat straks bij wet is geregeld dat de diensten encryptie niet mogen verzwakken? Daar zijn beiden blij mee. En de specifiekere eisen voor hacken? Idem. Inbreken op computers mocht al, maar is nu veel preciezer omschreven. Brenno maakt zich wel zorgen om de onvoorziene effecten bij het hacken van derden. “Er hangt veel gevoelige apparatuur aan het internet: een beveiligingscamera in een sauna of systeem in een ziekenhuis.” Pim: “Het is flauwekul dat diensten die gaan hacken. Ze

willen bij een target uitkomen. Als bijvoorbeeld een bedrijf wordt gehackt, dan willen ze zien waar de command and control server zit, of er meer bedrijven gehackt zijn en achterhalen wie erachter zit. Ga je die zelf als AIVD direct hacken, dan zien ze je. Dan kan het handig zijn om een systeem te hacken dat daar in de buurt zit, bijvoorbeeld bij de provider en niet een ziekenhuis."

"Maar met de Wiv krijgen we toch juist meer inzicht in wie ze hacken, of niet?" probeer ik. Volgens Brenno niet. Pim bevestigt dat de uiteindelijke rapportages inderdaad niet specifiek laten zien wie gehackt is, maar de diensten zullen wel vooraf kijken wie er achter het IP-adres zit voor ze die hacken. Wat dat betreft, vertrouwt hij op het inzicht van de TIB om dergelijke risico's goed in te schatten, met name de technisch expert die daarin zit. Iedereen in de zaal kijkt naar Ronald die zich wijselijk afzijdig houdt.

Exit Pim, enter Kees Verhoeven, Tweede Kamerlid voor D66 en woordvoerder ICT, privacy, Europa en terrorisme. Hij is een van de weinige Kamerleden die campagne voert om voor te stemmen en doet dat zonder subsidie van de referendumcommissie. Toen de Wiv nog niet was aangenomen, was hij tegen en heeft hij maar liefst twintig amendementen ingediend, waarvan er niet een is aangenomen. Hij was daarom een van de 36 tegenstemmers. Met 114 Kamerleden voor, werd de wet aangenomen.

Kees: "Dan is de wet dus een feit. Toen kwam de formatie en kon ik iets unieks doen, namelijk de wet amenderen in het regeerakkoord. Hierdoor hebben we de politieke afspraak dat wanneer er een sleepnet is, dus ongericht wordt getapt, we de wet, na evaluatie over twee jaar, gaan aanpassen als daar aanleiding toe is." Dankzij deze wijzigingen stemt Kees dus voor. Bovendien: "Stem je voor die wet, dan kunnen we die evalueren. Stem je tegen, dan wil je eigenlijk de oude wet behouden."

Wat vindt hij van Brenno's stellingen? Ik doe nog een schepje op het economische argument: "Datacenters zijn een enorme groeimarkt in Nederland, mede dankzij de AMS-IX en ons vestigingsklimaat. Schrikt de Wiv die markt niet af?" Kees: "Er zullen bedrijven zijn die zich daar zorgen om maken. Die zullen overigens niet naar Duitsland gaan, want dat is vreemd genoeg het slechtst verbonden land van Europa. In Frankrijk mogen

de diensten encryptie doorbreken, dus daar wil je ook niet naartoe. Veel bedrijven vinden juist dat de diensten helpen de infrastructuur intact te houden. Daarom profileert het Verenigd Koninkrijk zich als ‘a safe place to do business’. Ik zie de wet eigenlijk niet echt als plus- of minpunt voor bedrijvigheid.”

Kees kan zich behoorlijk opwinden over Brenno’s stelling dat je sowieso tegen moet stemmen, omdat zo de wet scherper gecontroleerd wordt. Kees: “Natuurlijk, is er nog veel mis. Het is een wet waar je met een vergrootglas veel tekortkomingen in kunt vinden, maar mensen moeten niet denken dat ze door een tegenstem wel een perfecte wet krijgen. Wat wel kan, is een praktijk met toetsingscommissies en Kamerleden, maar ook mensenrechtenorganisaties, die beter kunnen controleren hoe de wet wordt ingevoerd.”

Brenno: “Het is een fundamentele verandering, de schaal waarop straks data wordt verzameld. De tijd zal leren of het Europees Hof voor de Rechten van de Mens niet ingrijpt.” Kees: “Als het Hof ingrijpt, ben ik blij. Bertholee zegt dat zijn dienst niet massaal data gaat verzamelen. Als het misgaat, volgens de commissie, of de rechter, dan hebben we ten minste bewijslast. Nu heb ik alleen maar de doemscenario’s van mensen die zeggen wat mis kan gaan – nota bene met subsidies van de referendumcommissie. We hebben dus een land waarin de oppositie betaald wordt om campagne te voeren. Hoe mooi is dat? Nederland is ook een van de weinige landen die zeggen dat ze geen encryptie gaan verzwakken. En er is straks geen land waar de inlichtingdiensten zo gecontroleerd worden als hier.”

Wanneer is het nu een sleepnet en wanneer onderzoek? Kees: “De suggestie is dat je heel breed, heel lomp, heel veel data gaat binnenhalen. Dat is niet zo. Per keer dat ze intercepteren moeten de diensten precies omschrijven wat ze gaan doen, wanneer en of er geen ander middel is. Dat is niet ongericht, ook niet gericht, het zit er tussenin.”

Exit Brenno, enter Ton. Hij opende namelijk het debat en hiermee is de ketting rond. Ton: “Kees heeft ongelofelijk veel werk gestoken in het verbeteren van de wet. Jammer dat zijn amendementen niet zijn overgenomen. Nu hebben we een nieuwe politieke realiteit en zegt hij:

‘Stem voor, vertrouw mij, het komt goed.’ Dat kan ik niet. Als er een kabinetscrisis komt, zijn die afspraken van tafel.” Kees: “Heel formeel is dat een goed argument. Maar als je tegenstemt, krijg je geen betere wet. Dat is niet hoe een referendum werkt. Je krijgt de oude wet terug. Dat hebben we gezien bij het Oekraïnereferendum. De regering gaat inderdaad weg. Als er een regering komt die privacy slechtgezind is, kunnen ze ook de hele Wiv afschaffen.”

Stel het volk stemt 21 maart tegen, wat doet Kees dan? “De referendumwet was nog van kracht toen dit referendum is gestart, dus dan zal het kabinet de wet moeten heroverwegen. Dan komt er een stemming: ze kunnen de Wiv intrekken of in stand houden. Een tussenvorm vind ik niet waarschijnlijk, omdat veel Kamerleden hebben voorgestemd. Dat zullen ze pas doen als we ook feiten hebben en dat is over twee jaar.”

Stel, het volk stemt voor, houdt Bits of Freedom dan op over de privacy-bezwaren tegen de Wiv? Ton: “Nee. Het feit dat we dit debat hebben, is al winst. Het privacy-debat is daardoor volwassener geworden. Wat de verhouding ook is, miljoenen mensen zullen tegenstemmen. We gaan naar de Europese rechter, ook als de meerderheid voorstemt. Het gaat om het beschermen van een minderheid tegen de meerderheid.”

Ik heb veel voors en tegens gehoord die ik hier nu niet zal herhalen. De Wiv is voor mij geen sleepwet, want er wordt per opdracht gekeken wat de diensten mogen verzamelen en alleen als er geen andere manier is. Wat mij zorgen blijft baren, is dat de diensten ongeëvalueerde data mogen delen met het buitenland en de bevoegdheid krijgen om te hacken via derden. Dat ze die methodes ook gaan inzetten om de Nederlandse kritieke infrastructuur te monitoren en te beveiligen, vind ik een pluspunt. Door dit debat heb ik meer vertrouwen gekregen in de rol die de TIB en CTIVD gaan spelen in controle vooraf en achteraf. Ik ben heel benieuwd wat de klachtenprocedure gaat opleveren, zodat we eindelijk echte voorbeelden hebben en niet alleen maar doemscenario’s.

Dit zijn de rationele redenen waardoor ik al neigde voor te stemmen. In een democratie is elke wet immers een compromis en, vergeleken met de oude wet, hebben we met de nieuwe wet meer voor- dan nadelen.

Maar stemmen doe je ook op basis van emotie. Vertrouw je de overheid? Ik wellicht iets meer dan de gemiddelde Nederlander. In ieder geval meer dan veel van mijn vrienden, collega's en bezoekers van Hack Talk die waarschijnlijk tegen de Wiv gaan stemmen. Dat weegt ook mee. En als ik openlijk voorstem, zal ik nog een hoop shit krijgen van privacy-activisten en Twittertrollen. Toch wil ik niet bezwijken voor het chilling effect dat deze links conservatieve populisten uitoefenen op iedereen die voorstemt, door hen publiekelijk aan te vallen. Denkend aan de bijeenkomst op het zoldertje in Amsterdam, voel ik zelfs een zekere boosheid opkomen over hun zelfbevestigende debatten en flyers met kortweg 'Nee'. Ik wil feiten, nuance en wederzijds begrip. Daarom is mijn stem niet alleen vanwege rationele overwegingen, maar ook een proteststem. Daarom stemde ik voor.

Op 21 maart 2017 bracht 51,54% van de Nederlanders hun stem uit, waarmee de kiesdrempel van 30% ruim werd gehaald. Van de uitgebrachte stemmen was 46,53% voor invoering van de Wiv 2017, 49,44% tegen en stemde 4,03% blanco. Reken je die blanco's niet mee, dan was dus een kleine meerderheid tegen. De vraag is: waartegen? Het kabinet was niettemin verplicht om de wet te heroverwegen en kondigde op 6 april enkele aanpassingen aan. Geen drastische aanpassingen, maar vooral wat aanscherpingen om van het woord 'sleepwet' af te komen. Zo werd in de wet opgenomen dat de bijzondere bevoegdheden, waaronder ongerichte interceptie, zo gericht mogelijk moeten plaatsvinden. Delen van ongeëvalueerde data met buitenlandse diensten mag alleen als die landen goed 'gewogen' zijn. Voor het bewaren van kabeltaps moet jaarlijks opnieuw toestemming worden aangevraagd bij de minister. De maximale bewaartermijn blijft drie jaar. Als de diensten medische gegevens aantreffen die niet mogen worden ingezien, moeten deze direct vernietigd worden. En gegevens over journalisten mogen niet worden gedeeld met buitenlandse diensten, tenzij dat noodzakelijk is voor de nationale veiligheid.

Het moge duidelijk zijn: het 'tegen' kamp had meer verwacht. Dit referendum kent dus alleen maar verliezers.

Behalve Ronald Prins, want die kreeg de taak al die onderzoeken van de AIVD in te zien en te beoordelen. In de TIB kwamen naast hem twee juristen, dus het technische deel was geheel aan hem. Best een leuke job. Als ik hem twee jaar later vraag hoe het hem bevalt, moet hij lachen: “Regelmatig komen er voorstellen voorbij die door iedereen in de lijn al goedgekeurd zijn, maar ik vind ze dan te abstract en het is me is niet helder wat er technisch zal gaan gebeuren. Door door te vragen wordt dat duidelijker. Soms wordt dan ook besloten om het anders te doen.” Bij de eerste evaluatie van de wet bleek dat één op de twintig onderzoeksvoorstellen van de AIVD door de TIB werd afgewezen. Bits of Freedom en veel andere tegenstemmers zien dit percentage als bewijs dat de diensten zich niet aan de wet houden. Zelf vind ik het juist een redelijk percentage, want als alles goedgekeurd zou worden, lijkt het erop dat de TIB niks doet.

We zullen voorlopig nog wel doordebatteren over de Wiv en vooralsnog ben ik nog steeds voor de wet. Ik ben ook benieuwd naar de eerste zaken van burgers die zich onrechtmatig onderzocht voelen door de diensten. Die zijn er vooralsnog niet. Dat kan ook zijn omdat die burgers er niets van gemerkt hebben of omdat de diensten wel wat beters te doen hebben dan onschuldige burgers lastigvallen. Ik denk dat laatste, want de cyberoorlog is inmiddels begonnen.

14. Oorlog zonder gewonden

20 juli 2017. We zitten met een man of veertig in havencafé Courzand, op het container schiereiland Heyplaat voor ons eerste Port Cyber Café. Het Havenbedrijf Rotterdam heeft samen met de gemeente, Deltalinqs en de politie een cybersecurity-awarenessprogramma opgezet: Ferm. Dat is geen afkorting, maar gewoon een Rotterdams woord voor het op dat moment veelgebruikte ‘cyber resilience’, oftewel digitale weerbaarheid. Ik mag de gastsprekers introduceren en het gesprek leiden. Maar veel hoeven we niet te doen aan awareness. Op 27 juni 2017 is namelijk een groot deel van de Rotterdamse haven drie dagen platgegaan door een cyberaanval met de ransomware NotPetya.

Enkele maanden daarvoor heeft de wereld al kennisgemaakt met de ransomeware Wannacry, waarbij veel bedrijven platgingen. De ransomware die we nu te verduren krijgen, maakt net als Wannacry, gebruik van een exploit die we later hebben leren kennen als EternalBlue. Maar anders dan Wannacry krijg je bij deze aanval je bestanden niet terug als je betaalt, want het sloopt je computer op het diepste niveau. NotPetya is sabotagesoftware waardoor al snel het vermoeden rijst dat we hier niet te maken hebben met ordinaire cybercriminelen, maar eerder met een vijandige staat.

Waarom de Rotterdamse haven? Het Deense transportbedrijf Maersk heeft hier twee grote containerterminals, APM 1 en 2. Het is een internationaal bedrijf, dat in vrijwel alle havens in de wereld containers levert. Dat moet allemaal verrekend en gefactureerd worden en iedereen gebruikt daar weer andere software voor. Eén daarvan is de facturatiesoftware van het Oekraïense bedrijf M.E.doc dat in hun update NotPetya meestuurde. Maersk blijkt hun netwerken niet te hebben gesegmenteerd, dus al snel gaan alle systemen op zwart. Zelfs de poorten van containerterminal APM 1 en 2 kunnen niet meer open, met als gevolg

een lange rij wachtende containerschepen en vrachtwagens. Kosten van deze cyberellende in de Rotterdamse haven: 300 miljoen euro. De schade wereldwijd wordt door onderzoeker Andy Greenberg uiteindelijk geschat op meer dan tien miljard.

Een betere cybersecurity-awarenesscampagne konden we niet hebben. Op het programma hebben we die middag John Fokker van politie Team High Tech Crime met een toepasselijk nieuw project: Nomoreransom.org. Het is een platform van een hele lijst cybersecurity bedrijven en handhavers die ransomware te lijf te gaan. Als er weer nieuwe ransomware gedetecteerd wordt, werken ze samen om de software te ontleden, onderzoeken op kwetsbaarheden en eventueel zelf methodes te ontwikkelen voor ontsleuteling. Dat is al bij aardig wat varianten gelukt. Helaas nog niet bij NotPetya dus we moeten onze bezoekers teleurstellen.

Wat kunnen we volgens John zelf doen om ransomware tegen te gaan? Ten eerste: zorg voor back-ups. Als je besmet raakt, kun je die weer terugzetten. Ten tweede: stel segmentatie in, zodat besmettingen niet meteen over je hele systeem uitzaaien. Ten derde: updaten. Malware komt vaak binnen via bekende kwetsbaarheden in verouderde software, die in nieuwe versies verholpen zijn. Of op z'n Rotterdams: niet lullen maar patchen. Tot slot: betaal niet, want zolang er nog mensen blijven betalen, blijven cybercriminelen ons bestoken met ransomware en dat moet stoppen. Maar over wie er achter NotPetya zit zwijgt de agent wijselijk, want dat is op dat moment alleen maar gissen.

Drie maanden later heb ik de eerste aflevering van mijn praatprogramma Hack Talk en vraag ik John voor een update van Nomoreransom. Aan tafel vertelt de boomlange ex-marinier hoe het allemaal begon. Zijn team kreeg het jaar ervoor via anti-virusbedrijf Kaspersky de sleutels in handen van de ransomware Wildfire. Ook McAfee en Europol haakten aan en een samenwerkingsverband was geboren om decryptietools te ontwikkelen en die online beschikbaar te stellen. Nu, een jaar later, bestaat het project inmiddels uit meer dan honderd partners, een bonte verzameling van security bedrijven en overheidsinstellingen van over de hele wereld. Ze hebben decryptietools ontwikkeld voor vele tientallen ransomwares.

De site nomoreransom.org is inmiddels helemaal vormgegeven volgens Wild-Westthema's, compleet met 'cryptosheriff'. Daar kun je een besmet bestand uploaden en dan kijkt hij wat het is en of het ontsleuteld kan worden. Je kunt ook de decryptietools downloaden en zelf aan de slag gaan. Helaas nog niet voor NotPetya.

Die avond is ook Rik van Duijn te gast aan tafel en hij kan wat meer kan vertellen over de oorsprong van Wannacry en NotPetya. Hij is op dat moment ethisch hacker bij DearBytes en we kennen hem nog van Game of Toons, toen hij met zijn team LooneyToons de prijs won voor The Most Dangerous Hack. Twee weken daarvoor viel hij ook in de prijzen bij de Haagse Mystery Bug Challenge omdat hij, samen met zijn collega Wesley een kwetsbaarheid vond in denhaag.nl. Daarnaast heeft hij een leuke hobby: op het dark web kijken wat voor exploits er worden aangeboden en op welke kwetsbaarheden die zijn gebaseerd. Eén van de groepen die hij volgt, is de zogenoemde Shadow Brokers, vermoedelijk Russische hackers die het Amerikaanse NSA hebben gehackt en hun exploits verkopen. Zo kwam hij erachter waar EternalBlue vandaan komt.

Dat begon op 14 maart van dat jaar, toen Microsoft de kritieke patch MS17-010 uitbracht. Deze zou een bug fixen, zonder vermelding wat het was en wie die had gevonden. Het paasweekend had Rik niet zoveel te doen, dus ging hij kijken wat de patch fixt. Dat doen hackers wel vaker, want als je weet wat de update aanpast, kun je ook zien waar de systemen die nog niet zijn geüpdatet kwetsbaar voor zijn.

Op dat moment komt er net een nieuwe release uit van de Shadow Brokers, met daarin EternalBlue. Rik combineert beide en ziet tot zijn verbazing dat het hier een zeer fundamentele Windows kwetsbaarheid betreft. Sterker nog, elke versie van Windows blijkt kwetsbaar, terwijl de exploit al in 2008 door de NSA is gemaakt. Veel van de NSA-exploitkits zijn gebaseerd op ingekochte of ontwikkelde zero-days. Complexe software dus, maar volgens Rik tegelijkertijd ook uitermate gebruiksvriendelijk. Er zijn immers onvoldoende experts om aan de hackhonger van NSA te voldoen, waardoor ze veel hacktools geschikt maken voor minder getalenteerd personeel. Die blijken er vervolgens slordig mee om te gaan en zo vallen deze tools in handen van anderen, waaronder de Shadow Brokers.

Met EternalBlue kun je de meest fundamentele rechten van een computer overnemen. De exploit maakt namelijk gebruik van een kwetsbaarheid in de Windows-implementatie van Server Message Block (SMB), het netwerkprotocol dat gebruikt wordt om in Microsoft Windows bestandsuitwisseling tussen meerdere computers mogelijk te maken. De kwetsbaarheid kan door malware gebruikt worden om zich direct in het geheugen te nestelen en neemt je hele computer over zonder dat je er iets van merkt. Dat kan met deze exploit bij alle Windows-computers, vanaf XP tot en met Windows 10.

Dit is nogal wat. NSA vindt dus een zeer fundamentele kwetsbaarheid in Windows, meldt dat niet en houdt die achter om een exploitkit te ontwikkelen om anderen te hacken. Vervolgens worden ze zelf gehackt door de Russen die de exploit eerst te koop aanbieden en daarna gratis weggeven, waarschijnlijk gewoon om de Amerikanen te zieken. Pas dan wordt Microsoft ingelicht, waarschijnlijk door de NSA zelf. Microsoft levert een patch, die dan weer niet door iedereen wordt geïnstalleerd, waardoor NotPetya alsnog de hele wereld overgaat. Zo maken staten dus vanuit hun eigen veiligheidsbelangen het internet voor iedereen onveiliger.

Eind dat jaar ben ik weer op het jaarlijkse Chaos Communication Congress. Op het programma zie ik Sebastian Eschweiler staan met een presentatie over ‘Defeating NotPetya’s Cryptography’. Hij is eigenlijk webdeveloper en geen cryptograaf, maar vond het wel interessant om eens onder de motorkap van deze sabotagesoftware te kijken. Hij heeft een versie gedownload en die losgelaten op een bestandje van 1kb om te kijken hoe de versleuteling plaatsvindt. Hij toont de resultaten als rijen hexadecimale code van voor en na de besmetting. Daaruit blijkt, zoals zo vaak bij kwetsbaarheden in cryptografie, dat je makkelijk patronen kunt herkennen. Of anders gezegd: de entropie van het versleutelingsalgoritme wordt onvoldoende benut. Daarmee vindt hij de sleutel.

Na het applaus loop ik naar de microfoon. Ik vertel dat ik in de Rotterdamse haven werk aan cybersecurity. Er wordt hartelijk gelachen in de zaal. Ik vraag Sebastian of met zijn methode ook de computers van Maersk destijds ontsleuteld hadden kunnen worden. Als hij antwoord met “ja” vraag ik hem of hij zijn vondst al heeft gedeeld als Open Source

Intelligence, bijvoorbeeld via nomoreransom.org. “Nee”, antwoordt hij laconiek. Eigenlijk deed hij dit vooral voor de lol. Hij wil niet in de wereld van cybersecurity belanden. Hij is en blijft een webdeveloper…

In de nasleep van de schade in onze haven, vraag ik me steeds meer af of de besmetting bij Maersk met NotPetya toeval was of een geslaagde testcase. Op bijeenkomsten vraag ik aan diverse mensen van de AIVD, MIVD of Defensie of de NotPetya-aanval op de Rotterdamse haven ‘collateral damage’ of een ‘proof of concept’ was. Sommigen doen dit af als een complottheorie, anderen als een waarschijnlijkheid. Maar iedereen is het er wel over eens dat we echt op deze manier aangevallen kunnen worden, dus zijn er al verschillende organisaties die crisistrainingen doen gebaseerd op een vergelijkbaar scenario. Zo ook in de haven van Rotterdam.

Is de cyberoorlog dan al begonnen? Volgens socioloog Albert Benschop allang. In 2013 schrijft hij in zijn boek *Cyberoorlog. Slagveld internet* erover als “een soort koude digitale oorlog die nooit openlijk wordt verklaard, maar die zich voltrekt zonder dat de meeste mensen het doorhebben.” Hij somt hierbij de eerste openlijke cyberconflicten op, zoals de Amerikaanse ‘Legions of the Underground’ die eind jaren negentig zich tot doel hadden gesteld computersystemen te vernietigen in Irak en China, omdat deze staten de mensenrechten zouden schenden. Hier kwam overigens een hele hackersmacht tegen in opstand, dus ver kwamen de Amerikanen niet. In 2003, tijdens de Golfoorlog, lukte het de Amerikanen wel om computersystemen in Irak te saboteren. En ook bij de oorlog in Kosovo in 1998 zetten de strijdende partijen ‘cyberwapens’ in.

Dat zijn echte oorlogen, waar ook met cyberwapens wordt geëxperimenteerd. De eerste, echt pure cyberoorlog is, volgens Benschop en vele anderen, die in Estland in 2007. De regering had besloten een Russisch oorlogsmonument te verwijderen uit het centrum van de hoofdstad Talinn, wat leidde tot een conflict met de Russische autoriteiten. Kort daarop regende het DDoS-aanvallen, op regeringswebsites, nieuwskanalen en banken. Hiermee gingen niet alleen sites plat, maar konden er bijvoorbeeld ook geen banktransacties meer plaatsvinden. In 2008 volgde Georgië, op vergelijkbare wijze en waarschijnlijk ook weer door de Russen.

Deze cybertreiterij valt echter in het niet bij Stuxnet, het eerste echt effectieve cyberwapen, ingezet door de Amerikanen tegen Iran. Kim Zetter beschrijft in zijn boek *Countdown to Zeroday* van 2014 de geschiedenis tot dan toe. De regering Bush zag met lede ogen aan hoe de Iraanse president Ahmadinejad openlijk nucleaire capaciteiten aan het opbouwen was en zag maar twee mogelijkheden: Iran platbombarderen of na verloop van tijd een nucleaire raket ontvangen uit Iran. Volgens de NSA was er nog een derde optie. Ze hadden samen met de Israëlische Mossad (onderdeel geheime dienst) malware in elkaar geknutseld om de nucleaire centrifuges die nodig zijn voor uraniumverrijking te saboteren. Januari 2010 draaide de centrale in Natanz (Iran) zichzelf stuk.

Stuxnet werkte als volgt. Siemens heeft voor allerhande industriële processen zogenoemde SCADA-systemen ontwikkeld: Supervisory Control and Data Acquisition, oftewel een visuele weergave van industriële meet- en regelsystemen. De centrifuges in de Iraanse nucleaire verrijkingsfaciliteit Natanz hebben die ook en ze zijn te zien op een van Ahmadinejads promotievideo's. Uraniumverrijking luistert, zoals te verwachten, zeer nauw en het is van belang dat de centrifuges op constante snelheid draaien. Gaan ze te snel, dan klappen ze uit elkaar. Gaan ze te langzaam, dan raken ze in een resonantie, vliegen ze uit de bocht en klappen ze ook uit elkaar. Het plan was dus dat de malware eerst een week lang alle data zou opnemen en daarna afspelen, terwijl de centrifuges op andere snelheden werden gezet. Daar waren wel een stuk of vier Windows zero-days en een behoorlijke hoeveelheid complexe code voor nodig om dat te maskeren.

Het probleem was echter dat Natanz volledig was afgesloten van het internet. Eigenlijk van de wereld, want het zat onder de grond in een verlaten woestijngebied. Er moest dus iemand met een USB-stick naar binnen en de malware ongezien installeren. Pas eind 2019 brengt journalist Huib Modderkolk naar buiten dat het de AIVD was die dat is gelukt. Eerst via een artikel en later in zijn boek *Het is oorlog en niemand die het ziet*. Daarin lezen we dat Nederland medeverantwoordelijk is voor de inzet van het eerste effectieve cyberwapen, tegen een land waar we formeel niet eens mee in oorlog zijn.

Wel met Rusland. Althans, volgens minister Ank Bijleveld van Defensie. Nadat onze Militaire Inlichtingen- en Veiligheidsdienst een Russische hackaanval op de Organisatie voor het Verbod op Chemische Wapens (OPCW) in Den Haag had verijdeld, zegt ze in WNL op zondag 14 oktober 2018: “Nederland is in een cyberoorlog met de Russen verwikkeld”. De presentator vraagt of ‘cyberoorlog’ wel de juiste omschrijving is van het conflict tussen Nederland en Rusland. De minister: “Ja, dat is het wel”. Het blijkt dat de minister de NAVO Nederlandse cybersoldaten aanbiedt “om te kijken hoe we zelf offensief dingen kunnen doen als het nodig is”. De MIVD waarschuwt namelijk al jaren voor Russische cyberspionage.

In die periode komt aan het licht dat Nederland ook de Russen hackt. Onze AIVD volgde Russische spionnen via een gehackte beveiligingscamera op een universiteit in Moskou. Onze veiligheidsdienst herkende op beeld hun Russische collega’s en ze konden aantonen dat de hack van het Amerikaanse Democratische Congres vanuit die ruimte had plaatsgevonden. Mark Rutte vertelde op televisie dat hij “trots op onze jongens van de dienst” is, maar bond in toen Nederland daarna geteisterd werd door DDoS-aanvallen. Diverse banken en de Belastingdienst gingen enkele uren uit de lucht en veel mensen dachten dat het een vergeldingsactie van Rusland was. We hadden immers ook nog de controverse rondom MH17. Het bleek echter een Nederlandse tiener te zijn die met Webstresser speelde…

Landen hacken elkaar. Dat hebben ze altijd gedaan en zullen ze ook wel blijven doen. Maar waar liggen de grenzen tussen gewoon inlichtingen verzamelen, spionage, sabotage en oorlog? Welke landen zijn daarbij onze vrienden en welke de vijanden? Op 14 mei 2019 hadden we een Hack Talk over deze vragen. Terwijl de dag dat het bombardement van de Rotterdamse binnenstad precies 79 jaar geleden is, hebben we het op dezelfde plek over de volgende oorlog: de cyberoorlog.

Aan tafel een echte cybersoldaat: Jelle van Haaster. Sinds 2014 heeft de Nederlandse krijgsmacht namelijk een Defensie Cyber Commando, een eenheid van een kleine honderd soldaten die getraind worden om digitaal aan te vallen, bijvoorbeeld radarsystemen uit te schakelen of mobiele telefoons van tegenstanders te hacken. Vooralsnog hebben ze dat nog niet

gedaan en richten ze zich vooral op kennisontwikkeling en het verdedigen van Defensie. Ze verzamelen zelf geen inlichtingen. Dat doet de MIVD. Ze hebben ook een pool met IT-securityspecialisten die deeltijd voor Defensie werken, de cyberreservisten.

Een daarvan is Jelle. Van oorsprong is hij jurist en nu zit hij zeven jaar bij Defensie, eerst als luitenant en nu als Researcher Cyber Operations. Hij heeft ook IT-ervaring en zijn CISSP-certificaat gehaald, maar een OSCP-examen ziet hij zichzelf niet zo snel doen. Onder de vlag van de Militaire Academie en de Universiteit van Amsterdam schrijft hij een proefschrift over 'Militair nut van cyberoperaties'.

Hoe ziet het leven van een Nederlandse cybersoldaat eruit? Jelle: "Ik doe onderzoek naar dreigingen en wat dat betekent voor ons arsenaal: 95% is ijzer en die andere 5% is niet allemaal informatie. We hebben nu nog 'security by antiquity', zeg maar. Maar we hebben pentesters, ook onder de reservisten. Die kunnen dan een nieuw voertuig hacken. En we stellen doctrines op. Dat zijn documenten over hoe we in de toekomst militaire operaties moeten uitvoeren. Als er een nieuwe doctrine uitkomt, vragen we de reservisten erop te reageren. Die komen dus niet alleen in actie in oorlogstijd."

Dan de hamvraag: is de cyberoorlog al begonnen? Jelle: "Nee. Het onderscheid tussen spionage, sabotage en oorlog is juridisch vrij duidelijk. Spionage is niet expliciet verboden. Landen leggen wel zichzelf restricties op, zoals in Nederland de Wet op de inlichtingen- en veiligheidsdiensten. Sabotage mag niet volgens het non-interventiebeginsel: soevereine staten mogen niet onderling interventies plegen en geen dingen kapotmaken. Bij cyberspionage in andere landen is die grens echter niet altijd even duidelijk, want is het een verstoring of maak je echt iets kapot? Als landen met elkaar in oorlog zijn, vraag je bij een operatie een Rules of Engagement aan. Bij cyber is dat nog niet gebeurd, omdat we het nog niet in conflictgebieden hebben ingezet."

We hebben non-proliferatieverdragen over de inzet van atoom-, biologische en chemische wapens. Zouden we om een digitale wapenwedloop te voorkomen niet aan die ABC verdragen ook een D moeten toevoegen voor digitale wapens? Jelle: "Hoe effectief zijn die verdragen geweest? Kijk naar chemische wapens… In principe is de

huidige wet- en regelgeving toereikend, al moeten we die wel opnieuw interpreteren."

Hoe dan? Defensie heeft cyber nu als vijfde domein, naast land, water, lucht en ruimte. Waarom? Het is toch niet in tijd en ruimte af te bakenen, het is toch eerder een middel dan een gebied? Jelle: "Laten we daarom eerst het woord 'cyber' definiëren. Het is nogal een breed begrip. Bij ons in de boardroom wordt zelfs het werkwoord 'cyberen' weleens gebruikt. Het komt van het Griekse Kubernetes, wat staat voor 'stuurman' en Plato gebruikte het als 'stuurmanschap in een democratisch systeem'. Norbert Wiener kwam met cybernetics, als besturing van mens en machine. In 1984 verscheen het boek *Neuromancer* van William Gibson met het woord 'cyberspace'. Daarna volgde een 'cyber prefix flood', overal werd 'cyber' voorgezet. Gibson zei hier in 2003 over dat hij het woord alleen maar gekozen had omdat het lekker klinkt en hij het jammer vond dat het een hypewoord werd. Daarom zullen er ook mensen tegen zijn. Nu, in het domein van militair optreden, gebruiken we het omdat het niet alleen gaat over software en hardware, maar ook het gebruik ervan."

Dan de wapenwedloop. Landen schaffen ook wapens aan als afschrikmiddel, om oorlog juist te voorkomen. Werkt dat ook zo met cyber? Jelle: "Dat noemen we 'cyber deterrence'. Je wil als overheid demonstreren en communiceren dat je een super cyberarsenaal hebt en tegelijk wil je het achter de hand houden. Dat is lastig. Bij nucleaire wapens was dat makkelijk, want je kon gewoon kernkoppen tellen. Bij cyber niet. Maar het is nu wel een groot ding in internationale betrekkingen."

Valt die camerahack van de AIVD daar ook onder? Jelle: "Als ze dit deden om de Russen af te schrikken, heeft het niet gewerkt. Het zit ook niet in het aantal manschappen. Bij die 60.000 van het Chinese Peoples Liberation Army zit veel kantoorpersoneel. Het gaat meer om de kwaliteit. In 2013, met Stuxnet, werd cyber gezien als de silver bullet en sprong iedereen op die hype. Nu weten we dat het niet uitmaakt welke fancy wapens je inzet, je gaat toch niet winnen. We doen het, vooral, nog steeds met traditionele inzet van poppetjes en vliegtuigen."

OK, volgens deze cyberrekruut is de cyberoorlog dus nog niet begonnen en hoeven we die ook niet vandaag of morgen te verwachten. Intussen 'cybert' Jelle zelf lekker door. Hij maakt namelijk apps voor Defensie: een

om rangen en standen te herkennen, een voor medisch advies en een social-mediamonitor. Eigenlijk vindt hij dat nog steeds het leukste om te doen.

Cyberspionage is daarentegen wel van alledag. Tijdens de voorbereidingen van deze aflevering kreeg ik van verschillende mensen te horen dat ik het boek *The Cuckoo's Egg* moest lezen van Cliff Stoll. Het boek is weliswaar uit 1989, maar volgens velen nog steeds actueel. Het is een persoonlijk verslag van een Amerikaanse astronoom die op zijn universiteit systeembeheer erbij doet. Hij ontdekt een kleine afwijking in de boekhouding, die leidt tot het spoor van een hacker die via hun universiteit de Amerikaanse defensie hackt. Dat blijkt niet zo moeilijk, want op veel systemen kon je toen als gastgebruiker met standaardwachtwoorden inloggen. Hij zag dat de hacker vanuit dat gastaccount hogere rechten kreeg door malware te installeren. Die noemt Cliff het koekoeksei, vandaar de titel van het boek.

De rest van het boek gaat vooral over hoe Cliff op allerlei manieren het gevaar bij de autoriteiten probeert aan te kaarten, maar die blijken hier niet echt voor open te staan en sturen hem van het kastje naar de muur. Na veel gesprekken met geheimagenten en internationaal getouwtrek, worden de daders uiteindelijk gepakt. Spoileralert: de hackers blijken leden van de Chaos Computer Club die geheimen aan de KGB zouden hebben verkocht.

Het is een spannende cyberthriller, maar de heldenstatus van Cliff Stoll moet wel even gerelativeerd worden. Tijdens het Chaos Computer Congress van 2019 keek historica Anja Drephal terug op de nasleep van *The Cuckoo's Egg*. Inderdaad, enkele van de hackers die toen werden opgepakt waren lid van CCC. Degene die de buitgemaakte informatie verkocht aan de Russische KGB was een heroïneverslaafde met psychische problemen die dit uit geldgebrek deed. De informatie was nep en heeft de staatsveiligheid niet in gevaar gebracht. De CCC wel, want sindsdien werden de hackers van van alles beschuldigd, wat bijna leidde tot het uiteenvallen van de CCC. Maar dat terzijde.

Hoe is het nu gesteld met de Amerikaanse defensie? We zagen al dat de Russen de NSA hacken, maar hoe zit het met de websites van de Amerikaanse defensie? Tijdens de Hack Talk over cyberspionage praten we

hierover met Joel Aviad Ossi. Hij heeft bij verschillende IT-security bedrijven gewerkt en is nu senior IT-security specialist bij Ultimum. Bij Hack Talk is hij als WebSec, zijn eigen bedrijf in pentesten, audits en malwareanalyse en tevens zijn nickname op HackerOne. Daar zien we op de ranglijst dat Joel 151 bugs heeft gevonden en gerapporteerd, waarvan 146 op het .mil domein staan, oftewel Amerikaanse militaire websites.

Vanwaar zijn focus op het hacken van de Amerikaanse defensie? Joel: “Iedereen kan dit doen. Ik had op een gegeven moment geen werk en wilde wat meer ervaring opdoen en een reputatie opbouwen. Het Departement of Defense had een responsible-disclosureprogramma op HackerOne, dus heb ik me aangemeld. Eerst vond ik wat simpele fouten, zoals een XSRF, cross-site request forgery, waarmee ik een wachtwoord kon laten veranderen door een link aan te passen. Daarna wat moeilijkere XSS, cross-site scriptingkwetsbaarheden. Zo gingen mijn findings van medium naar high naar critical. Mijn reputation-index stond op een gegeven moment op 1604 punten. Best verslavend zo’n dashboard.”

Hoeveel heeft hij verdiend aan bug bounties? Joel: “Niets. Het is een vrijwilligersprogramma, dus je krijgt geen bug bounty. Je kunt hiervoor bij HackerOne maximaal zeven punten per programma krijgen terwijl dat bij de bounties kan oplopen tot vijftig. Maar je kunt je wel binnen het programma vergelijken met anderen. Ik deed het vooral om tijdens een sollicitatiegesprek te kunnen zeggen dat ik de beste beveiligingsonderzoeker van de Amerikaanse defensie ben.”

Een van zijn bevindingen is zelfs opgenomen in de lijst van Common Vulnerabilities en Exposures. Dan moet je dus een kwetsbaarheid hebben gevonden die niet alleen op die ene plek zit, maar ook bij veel anderen voorkomt en van zodanig gewicht is dat de rest van de wereld het moet weten. Wat had hij gevonden? Joel: “Een SOAP WSDL Parser SQL Code Execution. Op een website van een ziekenhuis op army.mil kon ik een code invullen in een tekstvakje. Die code werd uitgevoerd op de database achter de website, op administratorniveau. Dan kun je het hele systeem overnemen door een shell te uploaden met SQL-map.”

De Amerikaanse defensie heeft dus nog steeds voldoende plek voor koekoekseieren. De reactie vandaag de dag is echter wel anders. WebSec staat op de vulnerability disclosure website van de US Departement of

Defense onder het tabblad ‘Thanks’. DoD besteedde er een tweet aan. Op 10 januari 2019 meldde @DC3VDP: “Proof that we have the best researchers in the world: Joel Aviad Ossi @websecnl with @Hacker0x01 prevented the loss of an entire DoD website by disclosing a critical SOAP WSDL Parser SQL Code Execution vulnerability (CVE-2018-16803). Bravo sir, and thank you! #OneTeamOneFight.”

Joel had me een screenshot laten zien van de website. Die heb ik meteen verwijderd, want de URL van het slecht beveiligde subdomein was zo slecht geblurred dat die nog leesbaar was, terwijl de kwetsbaarheid nog niet was opgelost. Wat bleek, het screenshot was door de DoD zelf gepubliceerd als proof of concept bij de CVE.

Is het dan echt nog zo’n zooitje bij DoD? Joel: “Het is niet een kwestie van heel goed zijn om daar kwetsbaarheden te vinden. Er zijn zelfs 13-jarigen die meldingen bij hen doen. Hun IT-infra is lang geleden aangelegd, waardoor er nog veel legacy systemen en verouderde websites zijn, waar nooit aan security is gedacht. Als ik heel het .mil domein scan, zie ik duizenden sites en vind ik altijd wel een fout.”

Kwetsbaarheden bij de Amerikaanse defensie kunnen veel waard zijn op de zwarte markt, niet? Joel: “Als iemand tegen mij zegt: ‘Ik geef je 10.000 euro voor die fout’, dan weegt integriteit zwaarder dan het risico dat ik daarmee in problemen kom. Ik weet niet wat de koper ermee gaat doen. Mijn hoofdreden is dat ik een carrière wil maken in security. Dan is het niet verstandig om in de wereld van de zwarte markt terecht te komen.”

Tot zover het aanvalsperspectief. Nu de verdedigers. Op een avond over cyberoorlog en cyberspionage had ik natuurlijk graag iemand van de AIVD aan tafel willen hebben. Bij meer formele, besloten bijeenkomsten heb ik weleens iemand van de dienst mogen aankondigen, maar dan was er vooraf veel gedoe over wie er wel of niet in de zaal aanwezig mochten zijn. Ze komen ook weleens bij open bijeenkomsten, maar dan mogen ze meestal niet zoveel zeggen, want anders zouden ze wellicht iets kunnen verklappen over hun modus operandi. Bij Hack Talk zitten ze weleens in de zaal of doen ze mee aan een hackwedstrijd, uiteraard onder pseudoniem en zonder zich bekend te maken als AIVD’er.

Dan is het beter om mensen te vragen die daar hebben gewerkt. We praten daarom met ex-AIVD'ers Liesbeth Holterman en Pim Takkenberg. Liesbeth is nu zelfstandige en onder andere adviseur bij de brancheorganisatie Cyberveilig Nederland en het Cybersecurity Centrum Maakindustrie. Ze werkte bij de AIVD van 2006 tot 2014. Op haar LinkedIn-profiel staat nog cryptisch dat ze bij het ministerie van Binnenlandse Zaken werkte als 'Security & Policy Analyst'. In die tijd zei ze dan dat ze bij 'BZK2' of 'in Zoetermeer' werkte, maar tegenwoordig zegt ze gewoon 'AIVD'.

Hoe kwam ze terecht bij de dienst? Liesbeth: "Ik werd getipt door iemand die directeur defensieveiligheid was bij TNO. Hij zei: 'Ik vind je een typische inlichtingenofficier en ze hebben een vacature.' Ik ben gewoon historicus, maar het leek me toch wel interessant. Ik kreeg een intelligentietest. Daar valt normaal zo'n twee derde af. Daarna veel gesprekken en een veiligheidsonderzoek naar mijn achtergronden. Pas negen maanden later kreeg ik een brief waarin stond dat ik was aangenomen. Ik ging aan de slag bij de Directie Inlichtingen Buitenland."

Hoe zag je dagelijks werk eruit? Liesbeth: "Je werkt op basis van aanwijzingen. Die worden vastgesteld door de ministeries, op basis van dreigingsanalyses, onderzoek of informatie van andere diensten en partners. Je begint altijd met open bronnen. Al naar gelang de resultaten en de mogelijke dreiging, ga je verder. Ik zag weleens nieuwe medewerkers die dan denken: 'Hier heb ik een telefoonnummer, dat gaan we tappen'. Maar dat kan dus helemaal niet. Het is altijd 'propsub', dus is inzet van het middel wel proportioneel voor het doel en kun je hetzelfde doel bereiken met een minder ingrijpend middel? Zo ja, dan moet je eerst die minder zware middelen inzetten."

De tweede ex-AIVD'er aan tafel is Pim Takkenberg, die we bij Hack Talk nog kennen van het Wiv-debat. Hij is directeur Cyber Security bij Northwave en zelf ken ik hem nog uit de tijd dat hij teamleider was bij Team High Tech Crime van de Nederlandse politie. Toen hij in 2013 bij de AIVD aan de slag ging op het dossier cyberspionage, maakte hij daar zelf geen geheim van. Ik moest dan weleens lachen als hij zich bij de een of andere cyberborrel waar ook hackers kwamen voorstelde als: "Hoi, ik ben

Pim van de AIVD.” Dan zag je ze schrikken. Of ze dachten dat hij een grapje maakte. Na anderhalf jaar had hij het wel weer gezien bij de dienst.

Pim: “Bij Team High Tech Crime had ik weleens te maken met de AIVD. Dan deden we samen een onderzoek. Toen kwamen ze met een vacature en de vraag of ik iemand kende. Ik had bij de politie alle leuke dingen al gedaan en ging toen net als Liesbeth diezelfde sollicitatieprocedure in. Hoe ik door die intelligentietest heen ben gekomen weet ik niet, maar ik kon dus aan de slag met cyberspionage. Ik merkte dat ik ineens veel minder mocht en had de illusie dat ik dat kon veranderen. Ik wilde meer het publieke debat opzoeken om zo meer erkenning en vertrouwen in de dienst te creëren. Dat bleek ingewikkelder dan gedacht. De samenwerking met bedrijven vond ik wel erg leuk, dus na anderhalf jaar dwangbuis heb ik de overstap gemaakt naar het bedrijfsleven.”

Cyberspionage onderzoek, hoe gaat dat in zijn werk? Uit welke landen komen de meeste dreigingen? Pim: “Je krijgt aanwijzingen vanuit het ministerie. Die zijn niet geheim, want die kun je ook lezen in hun jaarverslag. De dreigingen komen uit de bekende landen: China, Iran, Rusland en Noord-Korea. Of je wordt gebeld door een bedrijf dat zegt: ‘We zijn gehackt en vermoeden een Chinese actor, kunnen jullie helpen?’ Dan start je een onderzoek en de middelen die je dan kunt inzetten zijn te lezen in de Wiv: malware reverse-engineeren, hacken, forensisch onderzoek, taps plaatsen, dat soort dingen.”

Een Nederlands bedrijf dat veel last heeft van spionage is ASML. Op een congres sprak ik een van hun securitymensen, die zei: “Ik moet dagelijks Chinezen uit onze systemen gooien. Ik zie ze ook dingen op de markt brengen die wij net ontwikkeld hebben.” Als zo’n bedrijf de AIVD erbij betrekt, dan is dat toch uit een bedrijfsbelang en niet ons landsbelang? Pim: “De primaire opdracht van de dienst is de nationale veiligheid. Economische veiligheid is daar onderdeel van, dus ook de grote, bepalende bedrijven. En het gaat ook niet om dat ene bedrijf, maar vooral om het begrijpen van hoe bepaalde actoren te werk gaan. Het kan heel ingewikkeld worden, want dan kom je uit bij een Indiaas bedrijf als actor, maar dat blijkt dan weer eigendom te zijn van de Chinese overheid.”

Elk land heeft zo zijn eigen dienst of meerdere diensten. In Nederland hebben we de AIVD en de MIVD die samenwerken in de Joint Sigint Cyber Unit (JSCU), respectievelijk 2.000, 800 en 300 medewerkers. In de VS heb je de NSA, die met 38.000 medewerkers nog groter is dan de wat bekendere CIA. In Groot-Brittannië heb je GCHQ, MI5 en MI6. De Amerikanen en Britten vormen samen met de Canadezen, Australiërs en New Zeelanders de Five Eyes, waar wij dan weer als extra oor aan meewerken. De Belgen hebben de ADIV, de Algemene Dienst Inlichtingen en Veiligheid, de Fransen de DGSI, Direction Générale de la Sécurité Intérieure en de Duitsers hun BND, Bundesnachrichtendienst. Bij de Russen had je de KGB en dat is nu FSB, maar vooral de GRU heeft veel hackers in dienst. In Israël heb je de Mossad en binnen hun defensie hebben ze intelligenceafdelingen als Unit 8200. In China noemen de staatshackers zich de People's Liberation Army (PLA). Klinkt leuk, maar er werken maar liefst 60.000 medewerkers bij de grootste dienst ter wereld. Deze namen en getallen komen gewoon van Wikipedia en het is natuurlijk eigen aan geheime diensten om daar in openbare bronnen een beetje mee te spelen om anderen te manipuleren. Maar het geeft wel een indicatie van de wereldwijde dekking.

Wie zijn in dit rijtje onze vrienden en wie de vijanden? Liesbeth: "Dat ligt aan het onderzoek. Gaat het om terrorisme, een chemisch of nucleair wapenprogramma of om digitale spionage? In het ene onderzoek is het je vriend, in de andere je target. Wij hebben een militaire en een algemene inlichtingen- en veiligheidsdienst en die werken samen. In andere landen, zoals de VS en het Verenigd Koninkrijk, hebben ze elk hun eigen technische diensten." Pim: "We hebben partners met gelijke omvang en doelen binnen Europa. VS, Verenigd Koninkrijk en Canada gaan meer hun eigen weg, maar hebben vaak wel dezelfde doelen. Verder naar het Oosten en het Zuiden wordt het vijandiger. Wat je ook ziet, is dat landen die fysiek niet zoveel macht hebben, digitaal snel groeien."

Weten andere diensten meer dan wij? Pim: "Ja, aan de lopende band. Veel inlichtingendiensten hebben bronnen in andere landen, met taps of onderzoeksystemen. Ze schermen hun bronnen goed af, want als iemand bekend wordt, kan hij dat met zijn leven moeten bekopen." Liesbeth: "Het

is vaak een optelsom. Een losse bron zegt niet zoveel, maar met elkaar verbonden juist weer wel."

De AIVD-hack op die Russische camera werd in de media gebracht. Zelf heb ik het idee dat de hack niet zo bijzonder is, want je vindt toch wel vaker beveiligingscamera's die slecht beveiligd online staan. Maar dat Mark Rutte dat dan zelfs met trots op tv vertelt, vind ik toch raar. Zo lok je toch een tegenreactie uit? Pim: "Wat ik daarvan weet komt ook gewoon uit de krant, maar ik vond het wel een rete-gave strakke actie. Ze waren in staat om vanuit de beginpuzzel een universiteitscamera te hacken en die te linken aan de mensen die daar naar binnen gaan. Het was bekend geworden en in de krant gekomen. Dan houd je het niet tegen. Het is ook wel goed om je tanden te laten zien. Net als die wifihack van GRU. Gewoon rijbewijsnummers vrijgegeven, zodat iedereen kan zien wie dat zijn. Ze worden steeds brutaler en dan is het wel goed om wat terug te doen." Volgens Liesbeth had Nederland nog een strategisch belang bij de bekendmaking: "Anders waren de Amerikanen er zelf mee op de borst gaan kloppen."

Eerder hadden we bij Hack Talk het debat over de nieuwe Wet op de inlichtingen- en veiligheidsdiensten (Wiv). In de tussentijd begreep ik van iemand van de dienst dat ze het eerste jaar vooral bezig waren hun administratie hiervoor op orde te brengen. De Toetsingscommissie Inzet Bevoegdheden meldde dat in de eerste maanden 5,5% van de verzoeken werd afgewezen, waarop Bits of Freedom concludeerde dat de diensten zich dus niet aan de wet houden. We zijn nu een jaar verder en in haar eerste jaarverslag schrijft de TIB dat "de extra inspanningen die de AIVD heeft verricht om groen licht te krijgen voor de inzet van bepaalde bijzondere bevoegdheden zijn vruchten heeft afgeworpen." Het percentage afwijzingen daalde naar 2,1%. Maar wat zegt dat eigenlijk? Is dat hoog of laag?

Liesbeth: "Je weet niet wat is afgewezen. De ingewikkelde of de simpele onderzoeken? Of alleen terrorisme? Het werk van inlichtingenofficieren is er in ieder geval niet makkelijker op geworden, maar we hebben nu wel meer waarborgen." Pim: "Ik vind het een redelijk percentage. Een afwijzing betekent niet per se dat het verzoek voor inzet van middelen in strijd is met de wet. De TIB stuurt ook weleens iets terug omdat het te kort door de bocht is of slecht geformuleerd. De waarborgen

zorgen wel dat het stroever verloopt. Overigens is de grootschalige interceptie waar zoveel om te doen was, nog niet ingezet en dus ook nog niet geëvalueerd."

Tot slot: werkt hun ervaring bij de dienst nog door in hun huidige werk? Pim: "Als ik bij Northwave op het Security Operations Center zit en we doen malwareanalyse, dan zien we indicaties van statelijke actoren. Die indicatoren stoppen we in onze technologieën om onze klanten te beschermen." Liesbeth is voor Cyberveilig Nederland een advies aan het schrijven over postkwantum crypto, oftewel hoe we moeten versleutelen als er straks kwantumcomputers zijn.

Die avond hebben we nog lang nagepraat over cyberoorlog en -spionage. Dat deze ex-AIVD'ers nu zo openlijk over hun verleden bij de dienst kunnen vertellen, is volgens mij een bijvangst van het Wiv-debat het jaar ervoor. Immers, wil je meer bevoegdheden als geheime dienst, dan zal je ook meer openheid moeten geven over wat je ermee gaat doen. Die bevoegdheid zullen de diensten nodig hebben om Nederland te verdedigen tegen hackaanvallen van vijandige staten.

Terug naar de vraag die ik aan het begin van dit hoofdstuk stelde: Was de NotPetya aanval op de Rotterdamse haven collateral damage of een proof of concept? Het antwoord op die vraag kunnen we afleiden uit het boek van Andy Greenberg dat eind 2019 uitkwam: *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlins Most Dangerous Hackers*. Hij reconstrueert vrij minutieus de verschillende oorlogsdaden van Rusland tegen buurland Oekraïne, waarbij gaandeweg steeds meer digitale wapens worden ingezet. De analyse van netwerkverkeer, de samenstelling van de code in NotPetya en de historische samenloop van aanvallen wijzen allen in één richting: de GRU.

Deze Russische geheime dienst zou het Oekraïense bedrijf M.E.Doc gehackt hebben om NotPetya te verspreiden. Volgens Greenberg niet alleen om de Oekraïners te treiteren, maar ook om de rest van de wereld te laten zien waar Rusland toe in staat is, of zoals Jelle dat noemt 'cyberdeterrence'. Dat daardoor ook containerterminals APM 1 en 2 platgingen, zal niet het doel geweest zijn van deze malware, maar het kwam de Russen wel goed uit. Het was dus beide, zowel collateral damage als een proof of concept…

Daar zullen we er nog wel meer van krijgen. Net als in de Koude Oorlog zullen andere landen niet achter willen blijven en ook sabotagesoftware ontwikkelen, testen en loslaten op elkaar, zonder te weten wie ze ermee raken. Al is Nederland momenteel formeel niet met een ander land in oorlog, we zijn zeker kwetsbaar. Al was het alleen al omdat we zowel digitaal als logistiek een belangrijk knooppunt zijn in de wereld. Of onze geheime diensten kunnen voorkomen dat Nederland bij zo'n aanval offline zal worden geblazen, vraag ik me af. We kunnen ons daarom maar beter, met z'n allen, zo goed mogelijk voorbereiden op het einde van het internet.

15. Het einde van het internet

Er komt een moment dat het internet het niet meer doet. Dat kan door bewuste sabotage van een groepering, een staat of misschien zelfs een individu. Of door een wereldwijde cyberoorlog. Of doordat we het internet zo ingewikkeld hebben gemaakt dat we wel zien dat er iets mis is, maar niet begrijpen wat. Het mooiste zou natuurlijk zijn dat het internet ophoudt te bestaan, omdat we iets nieuws hebben gemaakt dat het vervangt. In al deze gevallen zullen we de creativiteit van hackers nodig hebben om ons te beschermen, de boel te fixen of, beter, een alternatief te ontwerpen.

De afgelopen tien jaar heb ik in verschillende gremia mogen meedenken over rampscenario's. Onder andere in het Analistennetwerk. Dat was een club van ongeveer honderd experts die rondom verschillende thema's regelmatig bijeenkwam om eerst op deelthema's rampen te bedenken, die in scenario's uit te werken en vervolgens te toetsen of de overheid voldoende capaciteit heeft om dergelijke rampen onder controle te krijgen. Ik deed dan mee aan sessies over bijvoorbeeld cyberspionage of satellietuitval, of bedacht een methode om de experts flink uit hun comfortzone te halen en meer open te brainstormen. Dan riep ik weleens: "We gaan er telkens vanuit dat het internet het blijft doen. Maar stel nu dat het internet het op de een of andere manier niet meer doet. Wat is dan onze back-up?" De reactie was dan steevast: "Het internet kan niet stuk, daar is het op ontworpen."

Ik mocht een keer deelnemen aan de Shell Future Scenario's, met een bijdrage over de toekomst van het internet. De planningshorizon van Shell reikt ver: van nu tot 2100. We kregen dus mooie futuristische scenario's over AI, kernfusie, robotica en genetica. Ik had vier scenario's voor de toekomst van internet. Ten eerste, het groeit door zoals het nu doet, met steeds meer netwerken, apparaten en problemen van routing en congestie

van dien, maar die zijn oplosbaar. Twee: internet wordt splinternet. In dat scenario scheiden enkele landen en grote bedrijven hun netwerken af waarbinnen alles gecontroleerd verloopt, maar er dus geen verbindingen meer zijn naar anderen. Het derde scenario was: internet wordt vervangen door iets anders. Aangezien we er vijftig jaar over hebben gedaan om het internet te maken wat het nu is, zou die vervangende technologie nu al bedacht moeten worden om op tijd klaar te zijn. Maar ik zie die nog niet. Of wordt dat een netwerk van kwantumcomputers misschien? Wie weet. Het laatste scenario was, je raadt het al: het internet gaat stuk en er is geen alternatief. Die zagen ze volgens mij niet aankomen. In alle toekomstvoorspellingen die we die twee intensieve dagen op het Londense hoofdkantoor voorbij zagen komen, werd verondersteld dat we online konden blijven communiceren. Gewoon, omdat het internet niet stuk kan, toch?

Een veelgehoorde reactie van techneuten is: “Het internet is ooit ontworpen door de Amerikaanse defensie als een communicatiesysteem dat zelfs een nucleaire aanval kan weerstaan.” Ze bedoelen daarmee het DARPA-project van halverwege vorige eeuw, dat inderdaad ooit die doelstelling had, maar anders uitpakte. Het idee was informatie niet van een punt naar een ander te sturen over een lijn, maar op te knippen in kleine pakketjes met het adres van bestemming, zodat die via verschillende netwerken kunnen worden doorgestuurd. ‘Distributed Communication’ en ‘Packet Switching’ noemen we dat en in principe werkt het internet nog steeds zo. Alleen werd dat toen vooral gedaan om de belasting over verschillende computers en netwerken te verdelen en niet om het robuuster te maken. Het draaide om openheid en kostenreductie, niet om veiligheid. Sterker nog: het beschermen van de inhoud van de communicatie speelde tijdens het ontwerp van het internet nauwelijks een rol en daar hebben we in toenemende mate problemen mee.

Om de vraag of internet stuk kan te beantwoorden, eerst de vraag: wat is internet? Het eerste antwoord is: internet is een netwerk van netwerken. Dat zijn er volgens de samenwerkende internet registries, de onafhankelijke partijen die de domeinnamen uitgeven, momenteel wereldwijd tegen de 100.000. Nederland heeft er 1.546. Zo hebben bijvoorbeeld KPN,

Rijkswaterstaat en de universiteiten zo'n eigen netwerk. In kleine landen kan, bijvoorbeeld, een telecombedrijf de enige zijn met een netwerk. Binnen die netwerken heeft elke aangesloten computer een adres, waar de informatiepakketjes hun weg naartoe vinden. De meeste netwerken liggen in de VS: 28.185. Ook niet verwonderlijk, want daar is het internet ooit begonnen. Al die netwerken adverteren dus volgens protocol continue aan elkaar welke adressen ze hebben en worden ook wel Autonomous Systems genoemd.

Overigens vliegen de pakketjes niet meer, zoals vroeger, over alle netwerken heen, maar worden ze binnen datacenters van het ene naar het andere netwerk overgezet. Als twee partijen vaak data uitwisselen, zeg Google en Facebook, kan dat via de internet exchanges. Een van de grootste ter wereld is onze AMS-IX, de Amsterdam Internet Exchange, een soort grote rotonde in het wereldwijde internetverkeer. En nee, als je die platgooit, gaat niet het internet uit. Mocht dat je al lukken, het zijn immers dertien verschillende, zwaarbeveiligde locaties, dan nog komen de pakketjes op hun bestemming via de traditionele wegen.

Het tweede antwoord op de vraag wat internet is: internet is een protocol, een reeks afspraken over hoe we communiceren. Het belangrijkste protocol is TCP/IP, het Transmission Control Protocol, dat gebruikmaakt van het Internet Protocol, dat het bovenstaande verkeer beschrijft, maar er zijn er veel meer. We spreken vandaag de dag ook wel van de Internet Protocol Suite, omdat het een reeks protocollen is die telkens wordt aangevuld. De protocollen beschrijven hoe de informatiepakketjes worden samengesteld, geadresseerd, verstuurd en ontvangen. Dat adverteren van IP-adressen door AS-en is het Border Gateway Protocol. Als je daarmee knoeit, kun je wel het hele internet plat krijgen, omdat de pakketjes dan hun weg niet meer kunnen vinden. Maar daarover later meer.

Het derde antwoord is: internet is een samenwerkingsverband van verschillende, veelal onafhankelijke organisaties. Er is dus niet een bedrijf of overheid die het internet beheert, maar een bonte stoet van stichtingen, verenigingen en losse vrijwilligers die in allerlei samenwerkingsverbanden de protocollen aanpast om problemen tijdelijk op te lossen, ook wel aangeduid als The Internet Community. Overheden en bedrijven mogen meepraten, maar zijn niet de baas in dit gezelschap. Dit wordt ook wel het

multi-stakeholdermodel genoemd en is zowel de kracht als de zwakte van de organisatie van het internet.

Die Internet Community is heel open. Heb je een goed idee om het internet beter te laten werken, dan dien je dat idee in als RFC, Request for Comments. Daar wordt dan door een groep experts over gediscussieerd en als de meesten het een goed idee vinden, gaan ze het testen. Dat moeten dan twee of meer onafhankelijke partijen zijn, om te kijken of de specificaties aan zowel de zender- als de ontvangstkant kloppen. Werkt alles naar tevredenheid, dat wordt de RFC opgenomen in de reeks van standaarden.

Die internetexperts zijn georganiseerd in non-profitorganisaties als Internet Engineering Task Force (IETF), the Internet Research Task Force (IRTF), the Internet Architecture Board (IAB) en the Internet Society (ISOC). Maar eigenlijk kan iedereen een RFC indienen. De eerste RFC stamt uit 1969. Sindsdien krijgen ze een uniek nummer en datum mee, zodat je op de websites van de deelnemende organisaties de hele geschiedenis van veranderingen kunt teruglezen. Belangrijk voor de discussie hier: je kunt iets toevoegen aan de protocollen, maar al het oude moet wel blijven werken. ‘Backward compatibility’ heet dat en dat beperkt dus de mogelijkheden om internet echt anders in te richten.

Een andere belangrijke club van non-profits zijn de organisaties die het Domain Name System beheren. Zij koppelen dus een internetadres aan een naam. De registers van namen en nummers worden wereldwijd bijgehouden door organisaties die samenwerken in de ICANN, de Internet Corporation for Assigned Names and Numbers. Binnen Europa is dat RIPE, de Réseaux IP Européens, vrij vertaald Europese IP-netwerken, die bijhoudt wie welke netwerken gebruikt en beheert. Binnen Nederland hebben we SIDN, de Stichting Internet Domeinregistratie Nederland. Net als BGP is het DNS een essentieel onderdeel van internet: maak je dat stuk, dan kunnen internetgebruikers niet meer surfen op het www.

Je zou het internet ook kunnen beschrijven in hiërarchische lagen, volgens het zogenoemde OSI-model. Of je kunt op de filosofische toer gaan en het internet beschrijven als een levend organisme met een neuraal netwerk dat zich voedt via knooppunten en ons bestuurt in plaats van andersom… Laten we het er voor nu op houden dat internet een netwerk van netwerken is, dat we gebruiken volgens protocollen die zijn ontwikkeld

in een samenwerkingsverband van veel onafhankelijke organisaties die problemen oplossen naar beste kunnen.

Het probleem dat telkens blijft terugkomen, is dat we het internet vandaag de dag gebruiken voor zaken waar het niet voor is ontworpen: betalingen, geheime informatie en belangrijke beslissingen. We hangen er ook steeds meer dingen aan: auto's, industriële processen en consumentenelektronica. Optimisten zijn enthousiast over dit Internet of Things, terwijl securityspecialisten het hebben over The Internet of Shit vanwege de slechte beveiliging van die apparaten.

We kunnen niet van de ene op de andere dag opnieuw beginnen. Het internet kan niet uit of overgedaan worden, we kunnen er alleen nog meer dingen aanhangen. Alternatieven voor internet worden ondertussen afgeschaft. De oude telefoonlijnen, PSTN, zijn allemaal vervangen door Digital Service Lines, DSL. Tv en radio gaan over op internet. Alles wordt internet en een back-up is er dus niet meer. Om deze enigszins beknellende gedachte eens goed uit te werken, hebben we hierover een Hack Talk georganiseerd.

Hack Talk van 10 juli 2018 gaat over 'Het einde van het internet'. Ik heb dertien scenario's ontwikkeld om het internet kapot te maken en tien experts uitgenodigd om hierover te discussiëren: vijf die weten hoe je online dingen kapot kunt maken en vijf die in het dagelijks leven het internet draaiende houden, oftewel aanvallers versus verdedigers. Om het abstracte thema wat op te leuken, hebben we ook allerhande handsonactiviteiten die we zouden kunnen doen als er geen internet meer is. We hebben een heuse telex, waarmee het publiek analoog kan meechatten tijdens de discussie. Club Worm heeft een fysieke versie van The Pirate Bay, het online platform voor het al dan niet illegaal delen van content. Bij hun Pirate Bay kun je dvd's, cd's, boeken en games lenen en ter plekke kopiëren. Worm heeft een Pirate Box ontwikkeld, een LAN-filesharingsysteem, om zonder toegang tot internet toch bestanden met elkaar te kunnen delen via een lokaal netwerk. Onze dj, die normaal zijn muziek van een USB-stick speelt, is vervangen door Akim die op een oud analoog orgeltje easy tunes speelt.

We eindigen de avond met Jeux de Cyber: gooien met oude mobieltjes, tablets en andere digitale elektronica op een echte jeu-de-boulesbaan. VJ

Pleun schakelt over van haar Mac naar een authentieke sheet projector om de score te projecten. Als muzikale begeleiding krijgt Akim versterking van de samengeraapte Anti Cyber Analogue Assembly. En als er geen internet is, hebben we uiteraard ook geen blockchaintechnologie meer. Om toch alle gebeurtenissen in een feilloze administratie vast te leggen, hebben we een analoge, offlineversie. We noemen het Bloktj1.

Maar eerst dus het debat. Aan de kant van de hackers hebben we onze Guild of Grumpy Old Hackers: Victor Gevers, Edwin van Andel, Mattijs van Ommeren en Hans van de Looy, samen goed voor minstens honderd jaar hackervaring en regelmatig bij ons programma om commentaar te geven op allerlei onderwerpen. Hans heeft daarom zijn toepasselijk shirt aan met Statler en Waldorf, de oude mannetjes van The Muppet Show. Als GGOH begeleiden ze jonge hackers om ze op het goede pad te houden, zoals we lazen in het stuk over Hack_Right. Eigenlijk zijn deze mannen verdedigers van het internet, want ze weten hoe aanvallers denken.

De vijfde man, Daan Archer, heeft een bijzondere positie. Hij is geen hacker in de zin van aanvaller, maar meer als maker. Ik ken hem nog uit mijn tijd in Japan, waar hij Technisch Wetenschappelijk Attachee was. Als we dan langs bedrijven gingen, had hij ‘de baksteen’ bij zich: een satelliettelefoon, voor het geval alles in Japan zou uitvallen en de ambassade Nederlandse burgers zou moeten mobiliseren. Nu, terug in Nederland, is hij bezig met een startup in blockchaintechnologie. Hij doet dus de Bloktj1 en staat met de doos blokjes, rekenmachine en viltstiften klaar naast het scherm om elke opkomende gast voor eeuwig vast te leggen in onze houten administratie.

Bloktj1 werkt als volgt. Net als de huidige blockchaintechnologie, wordt elke transactie vastgelegd met een uniek nummer, dat met voorgaande transacties een onveranderbare reeks vormt en openbaar is voor iedereen om te checken. Als een gast opkomt, wordt het tijdsstip genoteerd en opgeteld bij de datum van die dag. Dit getal wordt gedeeld door de naam van de gast, alfabetisch omgezet in cijfers, dus: Daan is 41114. Het geheel wordt vermenigvuldigd met de uitkomst van de vorige transactie, de zogenoemde ‘nounce’. Op zijn blokje staat dus de uitkomst van mijn nounce x (180710+191043)/41114. Deelnemers uit het publiek kunnen met

hun rekenmachine checken of de berekening klopt en krijgen voor dit ‘minen’ een drankje.

Tot zover de overeenkomst met de huidige blockchaintechnologie. Maar we gaan analoog, letterlijk met houten blokjes. Die heb ik uit een houten balk gezaagd en zijn dus, door de houtnerf, uniek van opmaak en te controleren als enige blokje op die plek in de ketting. De uitkomst van het sommetje van Daan is echter te groot om op de blokjes te schrijven, dus nemen we alleen de eerste negen getallen. Hiermee creëren we tegelijkertijd een one-way encryption function. Het getal is uniek, maar je kunt niet terugrekenen welke naam ervoor is gebruikt. Daarmee is de Bloktj1 niet alleen praktisch uitvoerbaar, maar ook nog eens privacyvriendelijk zoals de echte blockchain.

Daan is druk aan het rekenen en schrijven om voor elk van de Grumpy Old Hackers een eigen blokje in de Bloktj1 te maken.

Dan komen de verdedigers van het internet erbij. De eerste is Frank Breedijk, maker van de vulnerabilityscanner Seccubus en Security Officer bij Schuberg Philis, een bedrijf waaraan je je IT-omgeving kunt uitbesteden als je zeker wilt weten dat het blijft draaien. Frank heeft ook een toepasselijk T-shirt aan met de tekst “Looking for Trouble”. Want dat is wat hij doet: problemen oplossen. Hij heeft ook de telex meegenomen, geleend van stichting Noodnet. Het zijn twee grote beige kasten met elk een typemachine. Als je aan een kant iets intypt, worden de toetsenaanslagen als analoog signaal via een klein koperdraadje naar de andere machine gestuurd, die het op een rol papier uitprint.

Wat is zijn grootste nachtmerrie als het gaat om het internet draaiende houden? Frank: “Als een of andere wizzkid een manier weet te vinden om een heel lang getal te ontbinden in twee priemgetallen. Dan kan ik als securityman wel inpakken.” Veel cryptografie is namelijk gebaseerd op puzzeltjes, die versleuteling makkelijk maken en ontsleuteling moeilijk. Twee priemgetallen vermenigvuldigen is makkelijk, maar om het resultaat weer te ontbinden moet je alle mogelijkheden afgaan. Als het getal maar lang genoeg is, lukt het computers niet om dat binnen korte tijd uit te rekenen. Veel cryptografie is gebaseerd op dat principe en naarmate computers sneller worden, nemen we gewoon langere getallen. Weet je

echter een andere manier te verzinnen om makkelijker die ontbinding te doen, dan is al die versleutelde informatie alsnog te lezen.

Terwijl Frank dit uitlegt, begint de grote beige kast naast hem te ratelen. Een berichtje vanuit het publiek. Op de rol papier staat echter een onleesbare combinatie letters en getallen. Frank gaat het meteen fixen, dus we gaan door naar de volgende gast.

Michiel Steltman is onder andere directeur van stichting DINL, de Digitale Infrastructuur Nederland, een samenwerkingsverband van organisaties die zorgen dat de netwerken, datacenters, clouds en domeinen, kortom de basisstructuren van het internet, het doen. Michiel is een veel geziene spreker op IT-congressen en noemt zich daarom “IT-nerd die door omstandigheden in de public affairs is terechtgekomen”. Hij had al e-mail in 1987 en heeft vanuit zijn werk meegemaakt hoe het internet is geworden tot wat het nu is.

Hoe kan, volgens hem, het internet kapot? Michiel: “Mijn grootste zorg is niet technisch van aard. Het internet is zo ontworpen dat het niet stuk kan, juist omdat het, zeg maar, met plakband aan elkaar zit. Dat doen we al 25 jaar zo en zo zullen we ook wel blijven doen. Mijn grootste zorg is de zogenoemde Master Switch. Als er nog maar een paar organisaties aan de knoppen zitten, kan iemand het internet uitzetten. Met het grote geld dat omgaat met internet komt er machtsconcentratie, versterkt door overheidsregulering, waardoor alleen zulke grote bedrijven het nog aankunnen.” De open cultuur van samenwerkende non-profits kan dus, volgens hem, steeds meer vervangen worden door een klein besloten clubje van giganten dat dan kan besluiten het internet aan of uit te zetten.

De overheid zelf, in de vorm van het NCSC mag natuurlijk op deze avond ook niet ontbreken. Op mijn verzoek een afgevaardigde te sturen, krijgen we Jeroen van der Ham aan tafel. Goede keuze, want hij is niet alleen security expert bij het Nationaal Cyber Security Center, maar ook een bekende in het hackerswereldje. Jeroen was vrijwilliger bij hackerskamp SHA, lid van de Utrechtse Hackerspace Random Data en securitydocent aan de UvA. Hij komt op met een toepasselijk T-shirt, met de tekst: “The only winning move is not to play”. Dit verwijst naar de film War Games, waar een hacker bijna een nucleaire oorlog ontketent via een

defensiecomputer, die hij per abuis aanziet als spelcomputer. Is dat ook zijn rampscenario voor het internet? Jeroen: “Nee. Dat is BGP.” Typisch Jeroen: kort en bondig.

We praten nog wat door over de Diginotar-affaire, de certificatenverstrekker die in 2011 werd gehackt, wat leidde tot de grootste cybercrisis tot dan toe. Midden in de nacht verscheen minister Donner op tv, met de boodschap dat we de overheidssites niet meer konden vertrouwen. De man begreep zelf niet echt wat er aan de hand was, maar toen was wel goed te zien hoe de Nederlandse overheid opereert in dergelijke crises. GovCERT, de voorloper van NSCS, betrok iedereen erbij, van hackers tot Microsoft, om zo snel mogelijk certificaten te vervangen en Nederland weer veilig online te krijgen. Dat was de wake-upcall, waardoor we nu beter zijn voorbereid op grote internetcrises volgens Jeroen. De overheid heeft sindsdien meer voelhoorns voor komende cyberellende. Onder andere in de Information Sharing and Analysis Centers (ISACs) waar de vitale sectoren dreigingsinformatie delen.

Maar, zoals gezegd, wordt het internet vooral draaiende gehouden door onafhankelijke non-profits. We zijn dan ook trots dat we iemand aan tafel hebben van ICANN, de club die het wereldwijde DNS-register bijhoudt. Het is voormalig D66-leidster Lousewies van der Laan, die nu bij ICANN in de International Board of Directors zit. Over een rampscenario hoeft ze niet lang na te denken, want ze heeft er net een meegemaakt. Ze is namelijk net voor haar werk in Puerto Rico geweest. Lousewies: “Daar hingen de internetkabels gewoon aan de palmbomen. Een orkaan rukte al die draden los en het eiland ging offline. Een draadloos internet opzetten lukte niet, vanwege de hoge bergen. Iedereen in rep en roer, want in al hun rampscenario’s hadden ze geen rekening gehouden met een falend internet. Toen kwam er zo’n gast van Google, een vent met dreadlocks. Die liet grote luchtballonnen op met microgolftechnologie eraan en Puerto Rico was weer online.”

Interessant geval en een mooie illustratie van hoe vanzelfsprekend internet is voor iedereen, maar geen realistisch scenario voor het dichtbekabelde, vlakke Nederland. Het rampscenario van Lousewies ligt meer in lijn met dat van Michiel. Ook zij is groot voorvechter van een vrij internet volgens het multi-stakeholdermodel: “Internet is het enige wat

wereldwijd werkt zonder overheidsbemoeienis. Iedereen werkt met elkaar om beleid te maken. ICANN heeft wel een Governmental Advisory Committee (GAC), waarin de regeringen van alle landen kunnen meepraten. Maar die begrijpen niet dat ze niet de baas zijn en proberen dan toch grip te krijgen op die technische laag. Mijn angst is: ze begrijpen het niet, dus gooien ze er veel wetten tegenaan. Dat is wat het internet kapotmaakt."

Tot slot hebben we ook bij de verdedigers een vijfde lid met de bijzondere positie om, net als Daan, met een back-up te komen voor ons falende internet. René van der Velde is zelfstandige en adviseert bedrijven en overheden met dreigingsstrategieën. Hij is ook de eigenaar van de laatste Noodnet-bunker van Nederland. Van hem heeft Frank dus de telex geleend, die inmiddels aan de praat is. Maar ik heb René vooral gevraagd om met hem te praten over Noodnet, onze enige back-up voor als alle communicatie faalt.

Hij komt echter niet aan tafel, maar neemt als een echte crisismanager meteen de leiding en richt zich tot het publiek. "Ga allemaal even staan" roept hij handgebarend. "OK, kijk nu op je telefoon. Is je batterij minder dan 50%, ga dan zitten." Meer dan de helft gaat zitten. "Wie heeft nog 60% over? Wie 80%, wie 90%?" Uiteindelijk staat er van alle 140 bezoekers nog een jongen, met lang haar, baard en telefoon. Hij zegt: "Ik heb geen smartphone, maar een oude Nokia. Met deze batterij gaat die nog een week mee." De hippie krijgt applaus.

René vervolgt: "Kijk, in tijden van crisis is het eerste wat je wilt doen het thuisfront bellen. Of alles OK is en dat het nog weleens laat kan worden. Dan moet je dus wel kunnen bellen. Ik heb daarom een telefoon van T-Mobile, een van Vodafone en deze." Hij houdt een smartphone omhoog met een dikke rubberen bekleding en smijt hem hard op de grond. Dan wenkt hij de barvrouw, die aan komt lopen met een emmer water. René gooit de telefoon erin, laat hem tien seconden onder water en haalt hem er dan weer uit. "Waterdicht, schokvast en met powerbank. Gaat vier dagen mee."

Dan het Noodnet, waar de telex vandaan komt. René laat een oude kaart zien van Nederland, met daarop 23 punten die onderling verbonden waren

door staatsbedrijf PTT. Elk van die punten was een bunker, waar in tijden van nationale crisis een team van 21 mensen zich kon terugtrekken. Er waren in Nederland in totaal 5.500 mensen aangewezen die onder alle omstandigheden met elkaar moesten kunnen blijven communiceren. Via die telexteams dus. In 2010 besloot de Nederlandse overheid echter dat deze miljoenen kostende voorziening niet meer rendabel was. Noodnet werd overgezet naar internet en omgedoopt tot de NCV, Nood Communicatie Voorziening. De bunkers konden worden gesloopt. Behalve een, die in Arnhem. René diende samen met twee anderen een voorstel in om de laatste Noodnet-bunker te kopen voor een symbolisch bedrag en om te toveren tot een museum. Dat kun je nu nog steeds bezoeken.

Noodnet was dus onze allerlaatste back-up voor als het internet het niet meer doet. Je zou nog iets kunnen proberen via het C2000 van de hulpdiensten, maar dat werkt nog steeds niet zoals het zou moeten. Of via zendamateurs, of met Software Defined Radio, maar dat wordt nog te weinig gebruikt en is niet echt betrouwbaar. We hebben dus eigenlijk geen alternatieven meer.

Daarom nu het debat: hoe waarschijnlijk is het dat het internet stukgaat? De gasten kunnen stemmen op dertien scenario's die bestaan uit een technisch deel, dus wat kapot kan, een mogelijke aanvaller met bepaald motief en een inschatting van de totale schade. Om alvast een voorschot te nemen op het offline gaan, hebben we geen stemkastjes maar papieren emoji's. Elke gast krijgt een geel rondje, waar een gezichtje op kan worden getekend dat zegt: dit is een realistisch scenario. De een maakt er een smiley van, de ander een huilend gezicht en een derde zet er een zonnebril op. De andere emoji is een papieren drol. Als je die omhooghoudt, zeg je: "dit is een waardeloos shitscenario". Het publiek chat mee via de telex.

Scenario 1: ModderDoSSers. Dit rampscenario is gebaseerd op de actualiteit. Nederland werd kort voor deze aflevering opgeschikt door een reeks DDoS-aanvallen. Eerst gingen een paar sites van banken uit de lucht en vervolgens ook die van de overheid. Veel mensen dachten dat we werden aangevallen door de Russen, maar het bleek achteraf de 18-jarige Jelle S. die het wel grappig vond om te spelen met Webstresser. Dat is een online tool die je voor 25$ per uur kunt huren om heel veel aanvragen op je

website af te laten vuren om te kijken of je een DDoS kunt weerstaan. Je kunt daar echter elke URL invullen, dus eigenlijk is het een DDoS as a Service.

We trekken dit scenario door en hebben het niet over een jongen met Webstresser, maar een groepje gamers dat op zoek is naar een flinke uitdaging: wie krijgt de meeste sites plat. We noemen ze de ModderDoSSers. Ze zijn erg competitief, jutten elkaar online flink op en zijn bereid om over allerlei grenzen heen te gaan. Uiteindelijk lukt het niet om het hele internet uit te zetten, maar ze kunnen wel het merendeel van de Nederlandse websites voor enkele dagen platleggen.

Bij de hackers zie ik alleen maar drollen. Edwin: “Heel Nederland is niet te doen. Dan moet je te veel machines aanvallen.” De rest knikt instemmend. Ze krijgen bijval van Michiel, die als directeur DINL zich ook heeft ingezet voor NaWas – de Nationale Wasstraat tegen DDoS-aanvallen. “DDoS is een oplosbaar probleem. We houden grote aanvallen bij en mitigeren die. Alleen bedrijven die hun netwerkrouting niet onder controle hebben, zijn de sjaak.” De rest van de verdedigers houdt hun smiley omhoog. Frank: “Ik zie de technieken om veel verkeer te generen wel verder evolueren.” Lousewies: “Ja, joh, al die IoT dan?” Jeroen: “Inderdaad. Stel je voor dat het Mirai-botnet op Nederland gericht wordt…”

Mirai is een botnet van gehackte consumentenelektronica, vooral webcams met standaardwachtwoord zijn gewillige slachtoffers. In de VS is met 300.000 gehackte webcams eens een Internet Service Provider platgelegd, en daarmee een deel van het Amerikaanse internet. OK, schoorvoetend verdwijnen de drollen en kunnen we met z’n allen concluderen dat in het ModderDoSSers-scenario het internet niet stuk gaat, maar je wel delen van het Nederlandse internet voor enkele dagen onbereikbaar kunt maken.

Scenario 2: Master Switch. Overheden gaan in samenwerking met grote bedrijven proberen het internet te reguleren, bijvoorbeeld om auteursrechtwetten af te dwingen. Dat gebeurt nu al en blijkt niet zo effectief. Experts zeggen dan: “The internet interpretates censorship as just another routing problem”. Het bijzondere in dit scenario is echter dat de internet community, die nu het internet telkens verbetert en draaiend houdt,

het gedoe zat is en besluit af te haken. Dan valt het multi-stakeholdermodel dus uiteen.

René steekt enthousiast zijn smiley in de lucht. “Tijdens de Koude Oorlog had je een boek met daarin dertig bedrijven waarmee je alles kunt uitzetten. Als de overheid daartoe besluit, kan dat.” Hij is echter de enige. De rest houdt de drol op. Lousewies: “Er zijn landen die maar een paar kabels hebben, dan kan dat. Je ziet ook wel in Iran en China dat de overheid streng reguleert, maar dan spreek je meer van fragmentatie van het internet, geen Master Switch.” Zij en Michiel hadden Master Switch als hun meest gevreesde rampscenario, en er is hen dus alles aan gelegen het te voorkomen. Dat is immers hun werk.

Telexbericht vanuit het publiek. “DNS. Als je SIDN oplegt alles uit te zetten. Kan ook met .com via Verisign. Cripple Switch.” Jeroen doet nog een duit in het zakje: “Alternatieven verdwijnen. Jongeren gebruiken internet alleen voor social media. Die kun je uitzetten.” OK, laten we dan concluderen dat als je echt wilt, je bepaalde diensten kunt uitzetten en daarmee het internet flink kan saboteren. Maar de kans dat de overheid dat ook echt gaat doen, is niet heel erg waarschijnlijk.

Scenario 3: Cryptopocalyps. De geschiedenis van cryptografie gaat terug tot de klassieke oudheid. Oorlog en spionage is van alle tijden, zo ook geheimschrift. In die geschiedenis zie je dat er telkens iemand de code weet te kraken en iemand anders een nog ingewikkeldere versleuteling bedenkt. In het huidige digitale tijdperk is het vooral een kwestie van steeds langere sleutels maken, zodat de computers er te lang over doen om die te raden.

Frank noemde al het ontbinden in priemgetallen. Als iemand daar een makkelijk sommetje voor bedenkt, kan het veel sneller. Een andere uitdaging wordt de komst van kwantumcomputers. Die kunnen meerdere berekeningen tegelijk doen en heel snel, waardoor het aantal ontsleutelmogelijkheden exponentieel toeneemt. De NSA, die nu een kwantumcomputer aan het bouwen is, zegt ook niet voor niets: “Collect now, decrypt later.” In dit scenario doet het internet het dus nog wel, alleen kunnen we niks meer geheimhouden en er niet meer op vertrouwen dat online informatie klopt.

Lousewies: “Vertrouwen is de basis van het internet. Ook als mensen alleen al het gevoel hebben dat ze internet niet meer kunnen vertrouwen, ben je ze kwijt. En de NSA levert de meeste crypto…” Jeroen: “Crypto zit overal in. Als je dat wilt vervangen, moet je nu beginnen, voordat er kwantum is.” Michiel: “Als het een wiskundig probleem is, dan is het op te lossen. Maar ik vertrouw overheden niet die achterdeurtjes in willen bouwen.”

Hacker Hans weet de gemoederen te bedaren, volgens hem klopt de redenering wel, maar zijn we al druk bezig al die cryptografische problemen op te lossen. De rest van de hackers stemt in. De geschiedenis van crypto breken en maken gaat dus onverminderd door. Belangrijkste crypto is momenteel SHA256. Ook die zal er ooit aan gaan en dan komen we weer met wat nieuws.

Nog een laatste poging via de telex: “Nobody but the US has safe crypto. Zal ook gelden voor Chinese crypto. Phil Zimmermann deed aan wapenhandel…” Dan loopt de papierrol vast. Terwijl Frank het probleem oplost, komt een gast uit het publiek tevoorschijn. Het blijkt Oscar Koeroo te zijn, securityman bij KPN en hij licht zijn bericht toe: “Wat dacht je van het verlies van de sleutels voor DNSSEC. Als je een foutje maakt in de key rollover, gaat alles daarna op zwart.” Ik vraag de deelnemers wat ze hiervan vinden, maar niemand reageert. Behalve Daan. “Moet hij ook een blokje krijgen?” roept hij wanhopig. Hij was namelijk nog bezig de hele Bloktj1 van de gasten tot nu toe door te rekenen. O ja, handmatige crypto… “Mag ik mijn laptop gebruiken?” Ja hoor, zolang je maar niet online gaat. Oscar krijgt ook een Bloktj1 en we laten crypto even voor wat het is: een onoplosbare puzzel…

Scenario 4: Het Code Leger, oftewel Rusland, gooit ons internet plat. Nederland heeft zich natuurlijk niet echt populair gemaakt bij het Kremlin toen onze AIVD aantoonde dat Russische hackers hadden ingebroken bij het Amerikaans Democratisch Congres. Ook zijn vier leden van de Russische geheime dienst GRU het land uitgezet. Onze MIVD had ze namelijk op heterdaad betrapt toen ze de wifi van het hoofdkantoor van de Organisation for the Prohibition of Chemical Weapons (OPCW) stonden af te tappen. Rutte sprak trots dat onze jongens van de dienst knap werk

hadden geleverd, maar daar zal Poetin anders over denken. Het conflict escaleert als het Internationaal Gerechtshof in Den Haag oordeelt dat Rusland achter het neerhalen van MH17 zat.

Omdat de spanningen tussen Rusland en de NAVO toenemen, gaan Amerikaanse troepen zich bewegen van west naar oost, via de Rotterdamse haven. Dat is natuurlijk diezelfde haven waar twee containerterminals platgingen in juni 2017 door de Russische sabotage software NotPetya. Eigenaar van die terminals Maersk had toen wereldwijde schade, maar heeft, toeval of niet, de Amerikaanse defensie als grootste klant. Kortom: NotPetya was slechts een proof of concept en het ergste moet nog komen.

De Russen hebben de middelen en motivatie om ons land als vijand en internationaal knooppunt lam te leggen. En ze hebben een belangrijke troef: een cyberaanval is moeilijk te herleiden naar een dader, dus ze kunnen blijven ontkennen dat ze erachter zitten. Is het de GRU, de FSB, het Kremlin, patriottistische Russische splintergroeperingen of iemand die zich voordoet als Rusland? Hoe dan ook, ze blijken over meer kwetsbaarheden te beschikken: in industriële systemen, auto's en elektriciteitsnetwerken. En die zetten ze nu in om Nederland op de knieën te krijgen.

Ik ben nog niet uitgepraat of ik zie bij alle hackers de smileys omhooggaan. Ja, waarschijnlijk scenario. Ook bij de verdedigers gaan, na wat twijfels, de gele rondjes omhoog. Behalve bij Michiel, altijd optimistisch over de weerbaarheid van de Nederlandse infrastructuur: "Zo'n aanval moet wel worden voorbereid en dan is de ontdekkans redelijk aanwezig." Victor: "EternalBlue komt weer terug. Let maar op. Het is gewoon wachten tot het misgaat." Daarmee is het pleit beslecht: Het Code Leger is een realistisch scenario om het internet in Nederland, en zelfs daarbuiten, plat te krijgen.

Scenario 5: BGP-hijacking. In de voorbereiding van dit programma vroeg ik aan Victor hoe je volgens hem het internet kapot zou kunnen krijgen. Net als Jeroen gaf hij deze mysterieuze drieletterafkorting als antwoord. Ik dacht dat ik wel wat wist van internet, maar van het Border Gateway Protocol (BGP) had ik nog niet gehoord. Dat terwijl het al sinds 1994 bestaat (RFC1771) en een belangrijke achilleshiel is van het internet. Als informatiepakketjes hun weg vinden van het ene IP-adres naar het andere,

moeten die pakketjes dus ergens te weten krijgen in welk Autonomous System dat adres zich bevindt. Omdat dat nog weleens verandert, adverteren die AS-en continu aan elkaar welke adressen zich binnen hun netwerken bevinden, zodat de routers ertussen kunnen beslissen waar de pakketjes naartoe moeten.

Dat is in het verleden weleens misgegaan. In 2008, bijvoorbeeld, wilde de Pakistaanse overheid haar burgers de toegang tot YouTube blokkeren, omdat daar opruiende video's te zien zouden zijn. Hun landelijke telecomoperator kreeg de opdracht om via hun AS al het YouTube-verkeer naar een doodlopend IP-adres te sturen. Toen streden dus binnen BGP twee adressen om voorrang. Dat van Pakistan won en het wereldwijde YouTube-verkeer verdween in hun dode adres.

De geschiedenis van BGP kent wel meerdere van dergelijke incidenten. Tijdens een presentatie bij de AMS-IX hoorde ik iemand spreken over Ghost BGP, oftewel niet-bestaande AS-en die roepen dat ze bepaalde IP-adressen hebben. Zijn dat spionagenetwerken of saboteurs, vroeg ik de spreker. Hij dacht dat het gewoon ruis op de lijn was en een oplosbaar probleem. Fouten in BGP zijn vooralsnog vooral storingen en geen opzettelijke verstoringen.

Aldus: wie zouden we kunnen bedenken die wel bewust BGP zou verstoren om het internet plat te krijgen? Vergelijkbaar met het boek *Black-out* van Marc Elsberg gaan we uit van een mondiale groep anarchisten, die de huidige samenleving willen ontwrichten om een vrij Utopia te stichten. Ze hebben verschillende netwerkbeheerders gehackt en gaan dan via BGP de IP-adressen adverteren van veel gebruikte sites: Google, Facebook, etc.

Michiel voelt wel iets voor het rampscenario. "Dit kan langdurige shit veroorzaken, maar niet voorgoed. Waarschijnlijk komt er dan een versnelde invoering van een nieuw routing manifesto." Oftewel, ook hier staat de Internet Community klaar om het probleem meteen op te lossen. Hans is niet overtuigd: "De meeste BGP-problemen zijn fouten, niet hacktivisten." Op de telex verschijnt: "Injecteer alle AS /24 met more specifics." Frank legt uit: "De meest specifieke route wint. Maar dat moet je dan wel doen vanaf een plek waar men je niet vindt, anders word je van internet gehaald." Kortom, dit scenario blijft vooralsnog theoretisch. Laten we hopen dat dat zo blijft.

Scenario 6: Aanval op de datacenters. We gaan nog even door met de mondiale hacktivisten. In dit scenario hebben we te maken met een antikapitalistische beweging die de grote Amerikaanse techbedrijven wil dwarsbomen door hun datacenters te saboteren. Google, Amazon, Microsoft en Apple hebben in die datacenters niet alleen veel data staan, maar routeren ook binnen die datacenters veel verkeer, oftewel private peering. Een manier om die datacenters plat te krijgen, is via de koelsystemen die, net als veel industriële systemen, weleens kunnen draaien op verouderde software, terwijl ze wel online te benaderen zijn. Zet eerst de noodsystemen uit, gooi de temperatuur een paar graden omhoog en de servers raken oververhit. Dan gaan niet alleen de diensten van de techreuzen plat, maar gaat ook veel netwerkverkeer weer zoals vroeger over de openbare netwerken en kunnen andere delen van het internet overbelast raken, zeg voor een paar dagen.

Ik zie vooral drollen. Hans: “In de meeste datacenters zitten mensen. Die voelen of het te warm is.” Frank, die verantwoordelijk is voor de veiligheid van het datacenter van Schuberg Philis: “In geval van storing is er altijd iemand op de zaak. Pas bij autonome datacenters zou je zoiets kunnen doen.” De enige die een smiley ophoudt, is René. Hij vindt het scenario wel wat en voegt eraan toe: “Je zou ook het brandalarm af kunnen laten gaan.” Hij krijgt bijval van Mattijs: “Of zout in het reservoir van het koelsysteem.” Kortom, ook dit scenario blijft te theoretisch. Datacenters zijn mensenwerk, van techneuten die weten hoe ze problemen moeten oplossen. Vooralsnog wel…

Scenario 7: Zonnestormen. Dit is een scenario waar ik zelf eerder bij betrokken was vanuit het Analistennetwerk en het gaat als volgt. Onze zon straalt een behoorlijke hoeveelheid elektromagnetische straling uit. Onze elektronische apparatuur is bestand tegen een dergelijke dosis. De zon straalt echter niet continue, maar is grillig. Dat komt door grote explosies op het oppervlak van de zon. Soms vindt er een hele grote uitbarsting plaats en als die net richting aarde gaat, hebben we in een keer heel veel straling, een zonnestorm.

De laatste zonnestorm was in 1859 en legde destijds het telegraafsysteem plat. Er zou er zomaar weer een kunnen plaatsvinden en

onze apparatuur verstoren. Als eerste gaan de satellieten die om de aarde draaien eraan. Dan zijn we niet alleen GPS kwijt, maar ook onze tijdsbepaling. Computers zouden namelijk hun interne klok synchroniseren op de satellieten en als dat niet meer kan, gaat er van alles mis in de communicatie tussen die computers. Dat is: als ze het nog doen na zo'n overdosis straling…

René is meteen enthousiast. "Als die satellieten uitvallen, zal de VS ze herschikken, maar dan natuurlijk in hun eigen belang. In Europa hebben we er niet genoeg om dat op te vangen." De rest van het gezelschap is wat minder onder de indruk. Michiel: "Het kan en de voorspelbaarheid is niet groot, maar de kans ook niet. En als het een grote storm is, dan ligt ook het elektriciteitsnetwerk plat en hebben we nog grotere problemen." Jeroen: "We hebben vanuit het NCSC contact met het KNMI, dat meldt het als er zo'n storm aankomt. De stroom zal eerder uitvallen, want computernetwerken zijn beter geïsoleerd. Maar de kans is inderdaad niet zo groot. Uiteindelijk bereikt zo'n sunflare alleen dat (kleine) deel van de aarde, dat naar de zon toe gericht is." Kortom: het scenario kan, maar de kans erop is klein. Vooralsnog dan.

Scenario 8: Kabelbreuk door platentektoniek. We gaan nog even door met moeder natuur als hacker. René heeft een kaart van West-Europa met zeekabels. Is er een aardbeving en de aardplaten verschuiven, dan breken enkele van die kabels en zal, bijvoorbeeld, internetverkeer tussen Nederland en Groot-Brittannië of Denenmarken, of tussen Europa en de VS afgebroken worden. Zo'n kabelbreuk zou ook veroorzaakt kunnen worden door een statelijke actor, bijvoorbeeld China of Rusland die het Westen wil dwarszitten, of Amerika dat Europa wil afstraffen.

Nee, de rest is eensgezind: geen realistisch scenario. Vroeger had dat misschien gekund, toen we nog maar enkele kabels hadden. De kaart van René is achterhaald. Nu hebben we zoveel kabels, die inderdaad weleens breken, maar dan zijn er altijd nog genoeg over om al het verkeer op te vangen.

Scenario 9: Black-out. Het is al enkele keren ter sprake gekomen: als de elektriciteit uitvalt, dan valt ook het internet uit. Daar hebben we in

Nederland al eens kleine voorbeelden van gehad en meerdere grote in het buitenland. En we hebben er ook een Hack Talk over gedaan, aflevering 8: Hack the grid. De conclusie was toen en nu: in de oude situatie, met enkele grote centrales kan het wel, maar met de toenemende decentralisering niet meer. De grote centrales worden aangevuld met kleine energie-opwekkers, zoals zonnepanelen, windmolens en biocentrales. Energieconsumenten worden producenten en het geheel wordt steeds meer een smart grid met energievraag en - aanbod. Mocht er een verstoring in het net optreden, dan kunnen we makkelijker delen afkoppelen die autonoom verder draaien. Kortom: ons elektriciteitsnetwerk wordt juist robuuster, omdat het steeds meer op het internet gaat lijken. De vele datacenters en zendmasten hebben backupstroom om dagen door te gaan. Wie het elektriciteitsnetwerk wil platleggen, moet dus snel zijn nu het nog kan.

Scenario 10: Einde van Moore's Law. Het aantal transistoren op een chip verdubbelt elke twee jaar, aldus Gordon Moore in 1975. Daarmee krijgen computers dus exponentieel meer rekenkracht. Deze wetmatigheid blijkt tot op de dag van vandaag nog steeds op te gaan. Of Moore nu echt zo'n vooruitziende blik had of dat zijn uitspraak vooral een selffulfilling prophecy is, laat ik even in het midden. Feit is wel dat een groot deel van de IT-industrie deze exponentiele groei in hun businessmodellen heeft verankerd. Ze maken zwaardere besturingssystemen omdat de chips meer aankunnen en verkopen die voor dezelfde prijs. Ze bouwen nieuwe datacenters in de veronderstelling dat er steeds meer data wordt gebruikt. Ze draaien zwaardere algoritmes om meer waarde te generen met al die data. Enzovoort, enzovoort… Al die businessmodellen gaan uit van groei, waardoor veel kan voor weinig en ze houden elkaar in stand. Maar wat nu als de groei afgeremd wordt en die businessmodellen elkaar gaan tegenwerken?

Een belangrijke rem op Moore's Law is dat we tegen fysieke beperkingen aanlopen: er kunnen gewoonweg niet nog meer transistoren op de vierkante millimeter. Ze worden te klein. Een andere beperking is dat de transistoren nu al zo dicht op elkaar staan, dat ze elkaar kunnen beïnvloeden. De VU-onderzoeksgroep van professor Herbert Bos heeft bijvoorbeeld een techniek ontwikkeld waarmee je door eentjes en nulletjes

in een chip te wijzigen, ook die in naastgelegen bits kunt beïnvloeden: bitflips door rowhammering noemen ze dat. De enige oplossing is de transistoren verder uit elkaar te plaatsen en dat zou dus het einde van Moore's Law betekenen. Je zou ook meer theoretisch kunnen redeneren: exponentiële curves kunnen niet oneindig doorgaan, ze zullen altijd ergens gaan afvlakken, of zelfs de andere kant op gaan.

De deelnemers zijn vooralsnog optimistisch over Moore's Law. Edwin: "Chips ontwikkelen blijft gewoon doorgaan." Michiel: "Exponentiële groei stopt altijd ergens, maar dat zie ik hierbij niet op korte termijn gebeuren." De enige die nog twijfelt is Jeroen. Hij voelt wel wat voor die elkaar beïnvloedende businessmodellen. Als alleen al de verwachting van groei afneemt, zal dat impact hebben. "Stel je voor dat alles wat nu online gratis is ineens wel wat gaat kosten. Het einde van het internet is als we ervoor moeten gaan betalen…" Dat is eigenlijk best een trieste conclusie, maar ik zie aan de rest dat ze zich hierin wel kunnen vinden.

Scenario 11: Onoplosbare kwetsbaarheden. Rowhammering is er zo een. Laten we dat wat breder trekken. Hackers vinden wel vaker kwetsbaarheden die alleen te verhelpen zijn als je de hardware vervangt. Stel nu dat die hardware wijdverbreid is of fundamenteel is aan de werking van het internet en niet te vervangen is. Recentelijk hadden we Meltdown en Spectre, die hiervoor in aanmerking kwamen, al waren die kwetsbaarheden moeilijk uit te buiten en kwam er toch nog een soort van softwarematige oplossing. Of wat te denken van al die netwerk hardware van Cisco? Als daar iets mis mee blijkt, kunnen we ze niet in een keer allemaal vervangen, want het zijn er gewoon te veel.

Jeroen protesteert: "Dit is mijn werk. Als iets fundamenteel is, informeren we iedereen. Al die dingen die je noemt, hebben we overleefd." De hackers hebben echter allemaal smileys omhoog. Mattijs: "Als je echt gemotiveerd bent, lukt het je altijd wel een lek te vinden waar niemand van gehoord heeft." Victor: "Hoeveel oude kwetsbaarheden zie je nu nog op het internet? Veel, en het worden er steeds meer. Telkens als we iets opgeruimd hebben, komt het weer terug. Overheden doen veel goede dingen: ze waarschuwen, raden patches aan, alleen rebooten ze niet."

De telex rapporteert: “Stimuleer transparantie, voorkom monocultuur.” Volgens Michiel klopt het beeld van een monocultuur niet: “Er is niet een stukje dat alles beïnvloedt. Die netwerkswitches en routers zijn niet alleen van Cisco, maar ook van Juniper.” Hij herhaalt nog maar eens: “Juist omdat het internet met plakband aan elkaar zit, is het weerbaarder.” Ik concludeer: we hoeven niet te vrezen dat er nu een fundamentele kwetsbaarheid is die het hele internet platgooit, maar we moeten er wel voor blijven waken dat de totale hoeveelheid kwetsbaarheden niet te groot wordt.

Scenario 12. We maken het internet zo ingewikkeld, dat er op een gegeven moment iets misgaat waardoor het internet het niet meer doet en we niet weten waarom. Dit is mijn favoriete scenario. Eigenlijk is het niet echt een scenario, maar een aanname die niet te bewijzen of te weerleggen is. Je weet immers niet wat je niet weet… De deelnemers reageren daarom wat gelaten op deze stelling. Frank doet nog een poging: “Complexiteit is de aartsvijand van veiligheid en vertrouwen. We hebben niet genoeg checkboekjes om te internetbankieren. Het aantal AS-nummers en IP-adressen schaalt niet oneindig…” De hackers zijn resoluut en eensgezind: Nee. Dit is een shitscenario. Jeroen valt hen bij: “Ik ben onder de indruk van hackers die willen begrijpen hoe de dingen werken. Zij zullen ervoor zorgen dat de dingen ook blijven werken.” OK, ik geef toe: deze blijkt te ver gezocht.

Scenario 13. Wat denkt het publiek? Is er iemand met een rampscenario dat we nog niet hebben besproken? Iemand roept iets over monocultuur. “Er zijn maar een paar vendoren. Wat als die nu niet meer te vertrouwen zijn?” Iemand anders roept: “Een astroïde die de aarde raakt!” Tsja, dan hebben we wel wat andere zorgen dan een goed werkend internet… Net als ik denk dat we het wel hebben gehad voor deze avond, grijpt onze orgelman Akim de microfoon: “Het internet zoals we dat nu kennen, houdt op te bestaan als we iets beters hebben ontwikkeld. Een heel ander protocol, misschien niet eens binair, maar iets echt fundamenteel anders.”

Een beter einde van het debat kan ik me niet voorstellen, dus we gaan over naar het minder serieuze deel. Akim mag met zijn orgel naar de borrelruimte van Worm, waar inmiddels ook gitaren en een analoog

elektronisch drumstel worden ingeplugd. Pleun klapt haar laptop dicht en volgt Akim met een sheetprojector, een stapel doorzichtige plastic velletjes en stiften. De grote plastic grasmat ligt klaar voor Jeux de Cyber. Edwin, al vaker juryvoorzitter bij hack events legt de regels uit. “Wie heeft er oude mobieltjes, tablets of andere digitale meuk meegenomen? Die smijt je op de mat. Wie het dichtst bij de target zit, wint een ronde en wie de meeste rondes wint, is de winnaar.” Ik gooi de target op de mat: een oude Toon, de slimme thermostaat, die ik nog over had van Game of Toons. Rond middennacht wordt Jeroen uitgeroepen tot winnaar. Hij krijgt een grote roze opblaasbokaal. Hopelijk neemt hij die mee naar zijn werk, het NCSC. Wie weet halen ze hem nog eens tevoorschijn als het internet wel ooit eens platgaat en zeggen: “Weet je nog? Toen dachten we dat dit nooit zou gebeuren.” We zullen zien…

16. Niet lullen maar patchen

1 oktober 2019. De One Conference wordt ook dit jaar geopend door de minister van Justitie en Veiligheid, Ferd Grapperhaus. Op hetzelfde podium, waar hij in 2018 eerst te laat kwam en vervolgens opriep om de deuren op slot te doen omdat hij gehoord had dat hier ook hackers komen, zien we nu een minister die voorzichtig zijn woorden kiezend over het podium schuifelt. Hij onderstreept het belang van updates en maakt zich zorgen over bedrijven die patches niet meteen installeren. Hij vraagt zich hardop af: “Of moeten wij dat anders doen?” Maar hij beantwoordt de vraag niet.

Dat heeft hij die dag al gedaan in Het Financieele Dagblad. Daarin lezen we dat hij niet begrijpt dat bedrijven software-updates uitstellen omdat ze dan bijvoorbeeld het productieproces moeten stilleggen. “Als dat je excuus is om de noodzakelijke veiligheidsmaatregelen niet te nemen, ben je echt een ongelooflijke oliebol. Als je niet zonder problemen kunt updaten dan heb je iets in je bedrijfsvoering niet op orde.” Aldus de minister. Hij stelt zelfs: “Wij moeten kunnen zeggen tegen een bedrijf: ‘Als je het zelf niet regelt, dan komen wij het wel doen’.” Blijkbaar heeft een van zijn ambtenaren hem intussen teruggefloten, want hier op de One Conference geen spierballentaal, maar eerder onzekerheid bij de minister.

De aanleiding voor de oliebollenuitspraak was een artikel van Huib Modderkolk in de Volkskrant van 27 september met de titel ‘Reconstructie Pulse Secure. Intern netwerk honderden bedrijven en ministerie lag maandenlang wagenwijd open’. Matthijs Koot, IT-beveiligingsspecialist bij Secura en onderzoeker aan de Universiteit van Amsterdam had namelijk ontdekt dat veel organisaties in Nederland een belangrijke update in hun VPN van het merk Pulse Secure niet hadden geïnstalleerd. Een Virtual Private Netwerk gebruik je juist om op een veilige manier op afstand in je kantooromgeving te kunnen werken. Is dat lek, dan kan iedereen erin, data

stelen of wijzigen, malware installeren, kortom, je organisatie binnenstebuiten keren. Pulse had al in april een patch geleverd die de kwetsbaarheid CVE-2019-11510 verhelpt, maar toen Matthijs op 24 augustus de Nederlandse IP-adressen scande, zag hij dat er nog 538 kwetsbaar waren. In zijn scanresultaten zag hij ook een aantal organisaties die van vitaal belang zijn voor de nationale veiligheid.

Matthijs had zijn bevindingen aan cert@ncsc.nl gestuurd en zag dat de vitale organisaties vrij snel werden geüpdatet. De rest niet. Het NCSC liet weten dat zij alleen verantwoordelijk is voor de Rijksoverheid en organisaties die zijn aangemerkt als 'vitaal', zoals energievoorziening, financiële instellingen of waterhuishouding. Matthijs scande bijna dagelijks de adressen opnieuw en zag het aantal kwetsbare organisaties maar langzaam dalen.

Op 2 september publiceerde hij zijn bevindingen op een blog en werd de zaak opgepakt door de media. De journalisten gingen vervolgens zelf op zoek naar scanresultaten van andere onderzoekers en onthulden welke specifieke organisaties kwetsbaar waren. Zo kopte Huib Modderkolk op 28 september in de Volkskrant: 'Netwerk honderden bedrijven, waaronder KLM, Shell en Schiphol, maandenlang lek.' In het stuk lazen we dat ook het ministerie van Justitie en Veiligheid haar Pulse VPN niet direct had geüpdatet. Grapperhaus bleek dus zelf ook een oliebol.

Voorafgaand aan deze onthulling had Matthijs al met behoorlijk wat mensen contact gezocht om te helpen kwetsbare organisaties erop te wijzen dat ze moeten updaten. Op 24 september kreeg ik ook een bericht van hem. Ik was namelijk bezig met een groepje hackers om een nieuw onderzoeksinstituut op te richten: DIVD, het Dutch Institute for Vulnerability Disclosure. De lancering was gepland op de eerste dag van de One Conference. We hadden al een naam, logo, website en Twitteraccount, maar moesten nog naar de notaris om de stichting op te richten. Eerst orde op zaken stellen en dan pas onthullingen, dacht ik, dus hield ik Matthijs zijn verzoek af. In de berichtenwisseling die volgde, zag ik dat hij veel organisaties aan het mobiliseren was, dus had ik toen al kunnen weten dat er iets groots aan zat te komen.

De aanleiding voor DIVD was Victor Gevers. Zijn bijna manische manier van lekken opsporen en melden ging steeds meer mensen opvallen, die vervolgens hun hulp aanboden. Daar heeft iemand ooit eerder een stichting voor opgezet, om subsidie binnen te halen en een gezamenlijk identiteit te creëren, maar die functioneerde niet. Victors maten van de Guild of Grumpy Old Hackers, Edwin van Andel, Mattijs van Ommeren en Hans van de Looy, hadden al eens laten weten dat ze ook wilden helpen de boel te organiseren, zodat hij zich meer op zijn scan- en meldwerk kan richten. Toen ik vernam dat Astrid Oosenbrug ook al met Victor hierover in gesprek was, sloot ik aan. Astrid is voormalig politica, oprichtster van de Cyberwerkplaats, betrokken bij Hack_Right, altijd wel aanwezig bij hackerevents en iemand die dingen kan regelen. Ze wilde vooral ook jongeren betrekken om het werk van Victor over te nemen en die waren er zeker. Maar ook de ervaren hackers stonden klaar om Victor te helpen.

Tijdens de zomer van 2019 kwamen we meerdere keren samen in wisselende formaties. De behoefte aan een gezamenlijke identiteit was er zeker. En aan geld. Hackers doen hun scan- en meldwerk dan wel als vrijwilliger, maar het vreet servercapaciteit en softwarelicenties die toch op de een of andere manier betaald moeten worden. Bovendien komt het veel professioneler over als je als hacker een melding doet namens een instituut en niet als individu. En mocht dan toch een of ander bedrijf het niet leuk vinden dat je meldt dat ze lek zijn en een advocaat of de politie op je afsturen, dan sta je er niet alleen voor.

Hoe moesten we dan gaan heten? Er mag geen ‘cyber’ in onze naam voorkomen, daar was iedereen het wel over eens. Liefst iets met ‘vulnerability’ en ‘disclosure’. Moeten we dan het woordje ‘responsible’ of ‘coordinated’ ervoor zetten? Nee, dat wordt weer zo’n eindeloze discussie. Ik herinnerde me ineens dat ik de domeinnaam divd.nl nog had, om ooit nog eens de Democratische Inlichtingen- en Veiligheidsdienst op te zetten, een soort wiki voor dreigingsinformatie. Dat was bedoeld als grap en als naam van een serieus onderzoeksinstituut kon dit natuurlijk niet. We moesten ook een Engelse naam hebben, want het internet houdt zich niet aan landsgrenzen. Maar met een vier letterige .nl URL lijkt het wel alsof je al lang bestaat, want de meesten daarvan zijn allang vergeven. Puzzelend met de vier letters kwam ik tot Dutch Institute for Vulnerability Disclosure.

We doen onderzoek, onthullen kwetsbaarheden en doen het op z'n Nederlands: open, eerlijk en gratis. Daar kon iedereen zich wel in vinden.

Ik moest natuurlijk nog wel even checken of ik met deze naam geen gedonder zou krijgen met de AIVD en MIVD. De eerste die ik vroeg was Pim Takkenberg, die daar ooit heeft gewerkt. Volgens hem kon het wel. Bij een van de whiskyleaks die zomer kwam ik Ronald Prins tegen, de ex-Fox-IT baas en op dat moment de technische man in de Toetsingscommissie Inzet Bevoegdheden. Hij beoordeelt de onderzoeken van de diensten, dus kent ze goed. Ook volgens hem zou onze naam geen problemen opleveren. Ik wist dat hij en Victor elkaar goed kennen, dus vertelde ik enthousiast dat we met onze nieuwe stichting Victors onderzoeken gaan ondersteunen. Dat vond hij een goed initiatief en vroeg: "Heb je al een goede Raad van Toezicht? Daar wil ik best wel in zitten hoor."

Daar hadden we eigenlijk nog niet over nagedacht. Bij stichtingen controleert een Raad van Toezicht het bestuur of zij wel het doel van de stichting dient en zich aan de regels houdt. Dat lijkt me in de hackerswereld geen overbodige luxe, want veel initiatieven vliegen nogal eens alle kanten op. Zo'n raad adviseert ook het bestuur en kan het ook voor ons opnemen, dus is het zaak om daar ervaren mensen in te hebben die elk een andere achterban vertegenwoordigen. Met Ronald hadden we al iemand vanuit de overheid. Om de cybersecurity bedrijven te vertegenwoordigen vroegen we Petra Oldengarm, directeur van brancheorganisatie Cyber Veilig Nederland. Vanuit de academische wereld vroegen we Herbert Bos, professor in cybersecurity, met al behoorlijk wat vulnerability disclosures op zijn naam. Lodewijk van Zwieten vroegen we omdat hij als Officier van Justitie Cybercrime het beste de justitiële wereld kan vertegenwoordigen en de grenzen van de wet kan aangeven. Allemaal zeiden ze meteen 'ja'. Ze wezen Lodewijk aan als voorzitter.

Op 27 september zaten Astrid, Victor en ik bij een notaris in Rotterdam om de akte van oprichting te ondertekenen. Uiteraard gingen we meteen moeilijk doen dat onze identiteitsbewijzen werden gescand bij een publieksbalie, op een apparaat waarvan je je afvraagt wie het beheert en er toegang toe heeft. Maar goed, zo zijn notarissen nu eenmaal. En wij hadden haast, want 1 oktober op de One Conference was ons lanceringsmoment. En ik werd al actief benaderd door hackers die graag via DIVD hun gevonden

kwetsbaarheden wilden onthullen en anderen die op de een of andere manier wilden meehelpen. Tegen elk van hen zei ik: “Kom tijdens de lunch naar ons toe en dan kijken we hoe we kunnen samenwerken.” Matthijs was er helaas niet bij, maar zijn onthullingen klonken nu dus luid door op het hoofdpodium tijdens de opening van de One Conference.

Na de speech van Grapperhaus betreedt een forse Amerikaan met grote baard het podium. Het is Robert Lee, op dat moment de baas van securitybedrijf Dragos, maar de meesten kennen hem uit zijn tijd bij de NSA waar hij zich bezighield met het hacken van industriële systemen. Na een uitweiding over Advanced Persistent Threats die hele energiecentrales hebben gehackt, komt hij met een opmerkelijk ontnuchterende conclusie: “Patches close down more power plants than the Russians and Chinese combined.” Veel industriële controlesystemen zijn oud en helemaal niet voorbereid op de snel veranderende softwarewereld. Al die updates werken verstorend en leveren dus momenteel meer schade dan de doelgerichte aanvallen. Ik weet niet of de organisatie van de conferentie er zich van bewust is dat we hier een topexpert hebben die de minister openlijk tegenspreekt of dat het gewoon toeval is, maar de zaal vindt het erg vermakelijk. Na Lee volgt een bijdrage van Marijn Fraanje, de CIO van Den Haag, die graag wil vertellen dat Hâck The Hague weer een succes was, maar hij ziet ook wel in dat de zaal vooral denkt aan de verantwoordelijk wethouder die die ochtend is opgepakt op verdenking van fraude. Kortom, het is weer een onvergetelijke opening van de One Conference.

Tijdens de lunch zit ik klaar in het restaurant van het Worldforum met een stapel DIVD T-shirts en laptopstickers. De eerste die naar me toekomt, is Frank Breedijk, de CISO van IT-bedrijf Schuberg Philis, die ook had meegedaan met de Hack Talk over het einde van het internet. Hij vertelt dat hij een soortgelijk initiatief wil beginnen, een Security Meldpunt. Daar kunnen mensen als Matthijs en Victor terecht met hun scans, zodat hij de meldingen kan doorzetten. Hij heeft al een klein team geformeerd en een website, maar nog geen juridische entiteit zoals een stichting. Astrid en Victor vinden het prima als het Security Meldpunt onder onze stichting komt te vallen.

Al snel loopt de plek vol met bekenden. Sommige hackers hebben nog wat databases met lekken liggen, die ze via ons willen onthullen. Anderen bieden aan om te helpen een platform te bouwen om meldingen af te handelen. Astrid vertelt enthousiast dat ze zich vooral wil inzetten voor de jongeren, die bij DIVD een opleiding kunnen krijgen. Victor zit rustig op zijn laptop te typen om zijn presentatie voor straks klaar te krijgen. Hij, onze Raad van Toezicht en enkele anderen die bij de oprichting betrokken waren, krijgen een zwart T-shirt met knalgeel DIVD-logo. Als iedereen weer zijn weg vervolgt, zie ik de opvallende shirts zich mengen in de menigte. Telkens word ik in de gang aangesproken over wat we doen en wie we zijn. De guerrillamarketing werkt.

Op de tweede dag van de conferentie mag ik een sessie leiden over Hack_Right. Ik doe mijn DIVD-shirt aan. De politie vindt dat prima, want wellicht kunnen ook wij op de een of andere manier jonge cybercriminelen op het goede pad krijgen. Ik stuur hen door naar Astrid, die op dat moment al actief is binnen Hack_Right.

Ons belangrijkste publieksmoment is op de derde dag van de conferentie. Victor heeft namelijk een plek gekregen op het grote podium, bij een sessie met de titel: ‘Strengthening our Resilience: the Compelling Case for a Vulnerability Management Program’. Hij heeft zijn DIVD-shirt aan, een mooi overzicht klaarstaan van de vele kwetsbaarheden die hij heeft gevonden en wil de opsomming afsluiten met hoe we dat als DIVD gaan oppakken. De sprekers voor hem nemen echter zoveel tijd in beslag en de moderator van het NCSC grijpt niet in, waardoor er slechts enkele minuten voor hem overblijven. Haastig klikt hij door zijn slides om toch nog iets van onze boodschap over te krijgen.

Tot slot mag ikzelf aan het einde van de conferentie op het grote podium. Er is nog ongeveer een derde van het publiek over. De voorste rij ziet zwart-geel van de DIVD-shirts. De NCSC-directeur Hans de Vries kijkt wat verrast naar het kleine legertje lekkenmelders als hij binnenkomt en gaat met een brede glimlach naast hen zitten. Dan is het showtime en ik kom op vanachter de coulissen. Ik heb een DIVD-shirt aan en lig op een brancard, voortgeduwd door twee ambulancebroeders. De broeders doen verslag aan twee mannen in verplegerskleding en een vrouw met een doktersjas. De dokter vraagt me hoe het met me gaat en ik vertel dat ik me

niet zo goed voel en wat duizelig ben. De verplegers brengen een infuus en monitorsensoren aan en zeggen dat ik vooral even rustig moet blijven liggen. De arts begint een vraaggesprek over mijn gezondheid, begeleid door het bliepje van de hartmonitor.

De dokter leidt af uit mijn verhaal dat ik een hartritmestoornis heb en besluit wat calcium in het infuus te doen. Als de verpleger me voor de tweede keer bij de schouder pakt en vraagt of het wel goed gaat, weet ik dat dit mijn teken is. Ik probeer nog een keer overeind te komen, mompel iets onverstaanbaars en val achterover. De monitor laat een luide aanhoudende piep horen. Ik word van de brancard gehesen en op de grond gelegd. De verplegers beginnen met reanimeren en spuiten allerlei stoffen in me. Niets helpt. Ik ben dood…

De broeders brengen me met spoed weg van het podium. Achter de coulissen probeer ik, schuddend van de lach, alle slangen en draden van me af te krijgen en hoor ik Joshua Corman het woord nemen. Hij vertelt dat deze infuuspomp wereldwijd wordt gebruikt in ziekenhuizen. Hij trof er een aan toen hij zijn dochter naar het ziekenhuis bracht en vroeg zich af of die pomp te hacken was. Dat kon vrij eenvoudig en om de een of andere reden staat het ding ook nog online. Als je de waardes die de pomp doorgeeft aan de monitor aanpast, kun je, zoals in dit geval, de dosis calcium die normaal over een langere tijd in de bloedstroom wordt gebracht, in een keer in de patiënt pompen. Zie hier het resultaat.

Joshua bedankt vervolgens de arts, die niet op de hoogte was van ons scenario en alleen had meegekregen dat het een oefening was. De verplegers, twee Amerikanen, zaten wel in het complot. Vooraf hadden ze, tot in elk detail, het scenario wel vijf keer met me doorgenomen. We moesten de arts richting de calciumpomp krijgen, anders zou alles mislukken. Ik mocht ook tegen niemand vertellen wat er ging gebeuren, maar mocht mijn vrienden op de voorste rij wel waarschuwen dat er iets raars op het podium zou gebeuren en ze niet moesten schrikken.

Achteraf vraag ik Hans de Vries of hij het niet erg vindt dat we zo uitgebreid gebruik hebben gemaakt van hun conferentie om aandacht te trekken voor DIVD. Nee, hij is blij met ons initiatief en vindt dat mensen als Victor enorm belangrijk werk verrichten.

Drie maanden later is onze eerste grote zaak: Citrix. De aanleiding was een officiële bekendmaking van Citrix zelf over serieuze kwetsbaarheden in hun Citrix Application Delivery Controller, Citrix Gateway en Citrix SD-WAN WANOP. Deze worden gebruikt om op afstand in te kunnen loggen in kantooromgevingen. Ene Mikhail Klyuchnikov, Web Application Penetration Tester bij securitybedrijf Positive Technologies, had ontdekt dat hij door deze kwetsbaarheid codes zou kunnen invoeren op de server, zonder enige authenticatie en zo data downloaden en gebruikers binnen het netwerk aanvallen. De kwetsbaarheid werd opgenomen in de lijst van Common Vulnerabilities and Exposures als CVE-2019-17781.

Bijzonder aan deze onthulling is dat Citrix zelf aankondigde dat hun product kwetsbaar was, nog voordat ze een patch beschikbaar konden stellen. Waarschijnlijk hadden ze bedacht dat Mikhails vondst toch wel naar buiten zou komen en het daarom zelf maar gedaan, om te laten zien dat ze hun verantwoordelijkheid nemen. Of ze waren onder druk gezet. Wie weet. Wat Citrix nog wel kon doen, was een paar mitigerende maatregelen adviseren om aanvallen te voorkomen, maar die bleken al snel niet te werken. Vervolgens konden onderzoekers uit de voorgestelde maatregelen afleiden wat de kwetsbaarheid inhield. Echter, een kwetsbaarheid in een systeem hoeft niet per se te betekenen dat je er meteen in kunt. Je hebt een exploit nodig om succesvol code uit te voeren op de server en die was er toen nog niet.

Intussen scande Positive Technologies het hele internet naar de oude Citrix-versies en maakte de inschatting dat op 23 december zo'n 80.000 organisaties, verspreid over 158 landen, kwetsbaar waren. Victor had al op de dag dat de kwetsbaarheid bekend werd een scan gedaan met Nmap en zag 128.777 kwetsbare servers online. Hoeveel er ook werkelijk kwetsbaar waren, was lastig te valideren, maar het was wel duidelijk dat, als er een exploit beschikbaar zou komen, in een klap heel veel bedrijfsnetwerken gehackt zouden kunnen worden. CERT's van over de hele wereld zagen dat het massaal scannen van kwetsbare servers zorgwekkend toenam. Volgens het Common Vulnerability Scoring System hadden we te maken met een kwetsbaarheid met een impactscore van 9,8 van de 10. Heel veel servers waren dus zeer kwetsbaar, te veel om zo eventjes te melden en op te volgen.

Matthijs Koot, die zich inmiddels heeft aangesloten bij DIVD, besluit daarom op 9 januari de Nederlandse IP-adressen te scannen op de kwetsbaarheid en vindt er een kleine 600. Dat is nog wel te overzien. Net als bij Pulse VPN stuurt hij zijn bevindingen naar het CERT van het NCSC. Hij krijgt te horen dat ze alleen de getroffenen melden die onder vitaal of Rijk vallen. Wie daar wel of niet onder vallen, kan het NCSC niet zeggen omdat die informatie niet zomaar gedeeld mag worden.

Op 11 januari 2020 komt de exploit beschikbaar. Zowel Project Zero India als Trusted Sec publiceren tegelijkertijd een code op Github waarmee je de Citrix-kwetsbaarheid kunt uitbuiten. De patch van Citrix is dan nog niet beschikbaar. Om de cyberellende compleet te maken, blijkt dat een aanvaller die zich eenmaal toegang heeft verschaft tot het kwetsbare systeem, die gewoon kan blijven gebruiken nadat de update is geïnstalleerd. De Citrix-server blijft het gehackte account gewoon zien als die van een legitieme gebruiker, ook al is hij gepatched. Het enige wat eigenaren van de Citrix-systemen nog kunnen doen, is actief monitoren en proberen aanvallen af te slaan. Of beter nog: de server offline halen. Tenminste, als ze al weten dat ze kwetsbaar zijn.

Dit is voor Frank Breedijk het moment om zijn Security Meldpunt te activeren. Eerst checkt hij met de rest van DIVD of we er klaar voor zijn en op 13 januari kondigt hij aan op onze site dat we alle getroffenen gaan waarschuwen. Eerst doet het Meldpunt dat geautomatiseerd. Met een scriptje zetten ze de IP-adressen van de lijst van Matthijs om in de URL's van de sites en sturen ze e-mails naar info@, abuse@ en security@ van die sites. In die mail staat de waarschuwing, wie wij zijn en wat te doen.

Vervolgens kijken Frank en een groeiend groepje onderzoekers binnen welke netwerken de IP-adressen zich bevinden. Zoals te lezen in het vorige hoofdstuk, is het internet een netwerk van netwerken en adverteren die via het Border Gateway Protocol welke IP-adressen ze hebben en van wie het netwerk is. Het grootste netwerk in Nederland is dat van KPN. Frank neemt contact op met enkele bekenden daar en geeft ze de IP-adressen van de lijst die binnen hun netwerk valt, met het verzoek de organisaties erachter te waarschuwen. Veel van de andere Nederlandse netwerken bereikt hij via de serviceproviders die zich verenigd hebben via NBIP, de Nationale

Beheersorganisatie Internet Providers. Wie kwetsbaar is, ontvangt dus een melding van zowel ons meldpunt als hun provider.

De Citrix-crisis wordt intussen opgepakt door de media. Frank en Matthijs worden aan het woord gelaten op de radio bij BNR en RTLZ en in de kranten Het Financieele Dagblad en NRC Handelsblad. Iemand die ik ken van de Z-CERT, het Computer Emergency Response Team voor zorginstellingen hoort zo van onze veegactie en belt me met de vraag of er ook kwetsbare zorginstellingen op onze lijst staan. Ik stuur hem door naar Frank, die binnen een uur een lijst met IP-adressen van zorginstellingen doorstuurt aan Z-CERT, waarna zij onze meldingen doorzetten.

Matthijs blijft vervolgens dagelijks scannen en monitort zo of het aantal kwetsbare systemen afneemt. Op 13 januari zijn dat er nog 546, op 15 januari nog maar 294 en op 17 januari 112. Dat schiet dus al aardig op. Of dat komt door onze meldingen, die van hun providers, de media-aandacht, of de adviezen die het NCSC op haar website zet, is moeilijk te bepalen. Maar vergeleken met andere landen uit de mondiale scan van Victor, doen we het hier in Nederland best goed met het dichten van de lekken in Citrix.

Met al dit scannen en melden bereiken we wel de ethische en juridische grenzen van ons werk. Je kunt van een afstand kijken welke versie een systeem draait en daarmee een inschatting maken of iets kwetsbaar is of niet. Nu eigenaren ook mitigerende maatregelen nemen, moet je net een stapje verder gaan en een code sturen om te kijken of er wat gebeurt. Een ‘non-weaponised exploit’ noemen we dat. We maken niets kapot, maar plegen in feite een beetje computervredebreuk omdat we “het systeem benaderen onder een valse identiteit of sleutel”, zoals dat heet in de Wet computercriminaliteit III.

Een andere juridische frictie is de Algemene Verordening Gegevensverwerking. Een mailadres of zelfs een IP-adres kan opgevat worden als een persoonsgegeven. Volgens de AVG moet je eerst degene die achter dit adres zit om toestemming vragen of je diens gegevens mag verwerken. Maar dat doen we niet, omdat we pas weten van wie we de gegevens verwerken nadat we die verzameld hebben. We verwerken hun gegevens dus ongevraagd en sturen ze ook nog eens door aan derden. Frank wijdt hier daarom een tekst aan op Security Meldpunt, waarin hij stelt dat

we doen aan ‘slachtoffernotificatie’ en we van mening zijn dat het onder de huidige omstandigheden moet kunnen wat we doen.

Kortom, we betreden dus openlijk de grenzen van de wet. Maar gezien de jurisprudentie in Nederland, moet zo’n beetje computervredebreuk best kunnen vanwege het hogere doel Nederland veiliger te maken (proportionaliteitsbeginsel) en is er momenteel ook geen andere manier om dit doel met minder ingrijpende middelen te bereiken (subsidiariteitsbeginsel).

Op 19 januari komen eindelijk de eerste van de langverwachte patches van Citrix beschikbaar en op 24 januari de laatste van deze reeks. Maar ja, als je in de tussentijd al gehackt bent, kan de aanvaller nog steeds onopvallend binnen je netwerk blijven, ook na het installeren van de update. Frank raadt op zijn blog aan Citrix-servers te onderwerpen aan goede forensische analyse, of beter nog: alles te wissen en opnieuw te installeren.

Begin februari zien we nog zeventig IP-adressen van de oorspronkelijke lijst aan kwetsbare servers binnen de Nederlandse IP-range. Ervan uitgaande dat die inmiddels wel gehackt zijn, blijft ons meldpunt waarschuwingen sturen naar hun algemene e-mailadressen. Begin maart zijn het er nog maar vijf. Enkele van onze nieuwe vrijwilligers nemen de taak op zich de organisaties te bellen. Vier gesprekken leiden tot directe actie. Slechts één strandt bij een receptionist die niet echt begrijpt wat we bedoelen.

De werkelijke schade wordt uiteindelijk langzaam maar zeker zichtbaar. Fox-IT rapporteert op 1 juli dat ze in Nederland 36 gehackte Citrix-servers hebben gevonden. Wereldwijd horen we verhalen van organisaties die eerst gehackt waren en vervolgens door de aanvallers zelf gepatched werden, zodat andere aanvallers niet meer binnen kunnen komen. Al die gevallen moeten nog aan het licht komen…

Voor DIVD is Citrix onze eerste grote zaak en een goede testcase voor onze manier van werken. Je kunt dus heel Nederland scannen op een CVE en kwetsbare organisaties melden. Al snel volgen meer zaken. De tweede is een bijvangst van de Citrix-veegactie. Veel van de servers blijken namelijk met certificaten te werken die misbruikt kunnen worden om andere onderdelen in de organisatie aan te vallen. De derde zaak betreft een lek in

Microsofts Remote Desktop Protocol. In de vierde zaak scannen we op apparaten die besmet zijn met een virus waarmee het apparaat onderdeel wordt van een botnet. De vijfde gaat over een kwetsbaarheid in Apache-servers. De zesde SMBv3… Telkens gooit een van onze onderzoekers een beschrijving van een gevonden kwetsbaarheid op ons chatkanaal met de vraag of dit interessant is om verder uit te zoeken. Dan volgt er een hele discussie en vormt zich spontaan een onderzoeksgroepje dat het oppakt. De scans worden meestal uitgevoerd door Victor en Matthijs. De andere onderzoekers valideren de gegevens, zetten meldingen door en informeren de getroffenen.

Als secretaris van de stichting probeer ik bij te houden wie aanhaakt bij DIVD. Daaronder bekenden uit dit boek, zoals Barry van Kampen, Zawadi Done en Wietse Boonstra, en veel nieuwe mensen. Er haken vrijwilligers aan die helpen met het onderhouden van de website, juridische zaken uitzoeken, connecties aangaan met andere organisaties, etc. Een maand na de Citrix-zaak, hebben we in totaal dertig deelnemers in onze nieuwe stichting. Zelf probeer ik vooral de boel een beetje bij elkaar te houden door regelmatig vergaderingen te organiseren en het overzicht te houden van wie wat doet. Samen met Astrid schrijf ik een subsidieaanvraag voor het SIDN Fonds die wordt gehonoreerd.

Citrix heeft ook geholpen DIVD bekend te maken. Dankzij Frank hebben we waardevolle contacten opgedaan bij netwerkbeheerders die onze meldingen kunnen doorzetten en opvolgen. Samen met andere partijen die helpen het internet veilig te houden, organiseren ze op 14 februari een bijeenkomst, waar ook wij zijn uitgenodigd. Als Frank, Astrid, Matthijs en ik tijdens het voorstelrondje vertellen dat we van DIVD zijn, horen we links en rechts: “Ah, zijn die meldingen van jullie. Dank. Goed werk.”

Om ons heen zitten dertig anderen die elk een organisatie vertegenwoordigen met een naam die buiten de internetwereld wellicht niet veel zegt, maar voor insiders partijen zijn die het internet draaiende houden: NBIP, ISPConnect, AbusIO, Deloitte, DHPA, DINL, SIDN, ECP, RIPE NCC, A2B internet, LMIO, Connect2Trust, EOKM, VVR, DTC, Schuberg Philis, AIE, Secura en Cyberveilig Nederland. Daar komen later nog KPN, TuDelft, de AMS-IX en nog wat andere organisaties bij. Vanuit de overheid haken het ministerie van Economische Zaken, DTC, de politie en het

Openbaar Ministerie aan. Na deze eerste bijeenkomst op Valentijnsdag spreken we af voortaan dreigingsinformatie te delen. Na enkele vruchtbare bijeenkomsten besluiten we ons voortaan AAN te noemen, het Anti Abuse Netwerk. Inge Bryan, voormalig topvrouw bij de politie en op dat moment director Cyber Risk Services bij Deloitte, zit elke vergadering voor en wordt het gezicht van de club. De grote afwezige in dit netwerk is het NCSC.

Anno augustus 2020, een jaar na de Pulse VPN-rel die Matthijs in gang had gezet, kan het NCSC nog steeds niets anders doen dan onze lijstjes in ontvangst nemen, zonder iets terug te melden. De schade van het niet-patchen van de kwetsbaarheden wordt echter gaandeweg steeds meer zichtbaar in het aantal gehackte organisaties. Het chagrijn onder onze onderzoekers en de discussie in de media en de Tweede Kamer over de houding van het NCSC neemt toe. “Nationale cyberwaakhond blaft lang niet voor iedereen” kopt Het Financieele Dagblad op 27 augustus 2020. Ook Frank komt in het stuk aan het woord. Hij legt uit dat we onze scans delen met het NCSC en dat deze er vervolgens alleen iets mee doet als het betreffende bedrijf vitaal is.

Het NCSC neemt verschillende keren contact op met ons, laat weten dat ons werk gewaardeerd wordt, maar dat het zelf niet meer kan en mag doen volgens haar mandaat. Dreigingsinformatie kan alleen gedeeld worden met organisaties die onder het zogenoemde Landelijk Dekkend Stelsel vallen. Als we de status van CERT krijgen of als OKTT (Objectief Kenbaar Tot Taak) mogen we meedoen, maar daarvoor moeten we eerst de nodige bureaucratische hoepels door. Tot die tijd mogen we onze lijstjes met IP-adressen opsturen, maar krijgen we er vooralsnog niets voor terug.

Deze opsomming van onderzoeken, namen van mensen en organisaties en kreten in de media is waarschijnlijk weinig relevant meer als je dit boek leest. Zoals dat gaat in cybersecurity en al helemaal in de hackerswereld, kan alles snel samenkomen en ook zo weer uiteenvallen. Wellicht staat DIVD nog een rechtszaak te wachten, valt de hele club uiteen, beginnen de deelnemers iets nieuws of groeien we uit tot een bekend instituut waarvan ik hier een korte ontstaansgeschiedenis heb beschreven.

Hoe anders gaat het bij de overheid. We hebben jarenlang discussie gehad in de media, het Parlement en op congressen, maar daardoor wel als geen land ter wereld coordinated vulnerability disclosure erkend gekregen als een legitieme en noodzakelijke praktijk. Zo zal het ook gaan met het grootschalig delen van kwetsbaarheden. Je kunt zeggen dat we een beetje de wet overtreden en dat het NCSC zich eenmaal aan haar wetten heeft te houden. Omgekeerd laten we zien dat de wet niet klopt en die dus best een beetje mag veranderen. Ik heb er wel vertrouwen in dat vroeg of laat de Nederlandse overheid ook hierin zal meegaan met de hackers en inziet dat we anders het internet nooit veiliger krijgen.

Laten we daarom stoppen met de eindeloze discussies over wie waarvoor verantwoordelijk is in cybersecurity en gewoon kwetsbaarheden delen om ze samen op te lossen, oftewel: niet lullen maar patchen. Daarom hebben we bij DIVD een leidraad opgesteld, die dient als code of conduct voor onze onderzoekers en voor iedereen die wil meehelpen het internet veiliger te maken. Ik vind de code of conduct een mooie afsluiting van dit boek, omdat hierin samenkomt wat we doen, waarom we dat doen en hoe we dat doen.

Code of conduct

We aim to make the digital world safer by scanning the internet for vulnerabilities

These vulnerabilities are most likely CVE (Common Vulnerabilities and Exposures) or CWE (Common Weakness Enumeration), which should already be known by the people responsible for the vulnerable systems and might be actively exploited. We do not hack websites, we only scan IP ranges, using, for example, Masscan, ZMap or Nmap to identify hosts with the aim to notify the owners.

We validate our findings

For further investigation and to prevent reporting false positives, we sometimes need to verify if a vulnerability is actually present. We use custom-made scripts, based on publicly available proof of concepts or non-

weaponized exploit code. So, we take care we don't damage systems, download personal data or create backdoors. Similarly, we don't patch vulnerable systems. That remains the responsibility of the owner.

We report these vulnerabilities to the ones who are responsible for fixing them

Our researchers will send their report to your info@ and abuse@ mail address and hope your IT department catches up. You may also receive our report through your CERT (Computer Emergency Response Team), PSIRT (Product Security Incident Response Team) or ISP (Internet Service Provider). Reports are accompanied by advice on how to mitigate or fix vulnerabilities. In the Netherlands reports are send out by Security Meldpunt.

We expect a response

If you are responsible for a digital system, we expect you to: have a point of contact where researchers can file their report, promise to respond, provide updates on the progress and warn others who might be affected. It is highly valued if you credit our researchers for helping you out.

We log our research as long as a case is active

After reporting our findings, we repeat our scans in order to track progress. We, therefore, need to store data and log our activities. We may also need this data in case of a dispute. We minimise the amount of personal data we gather and store and are aware of the fact that an IP address can also be perceived as personal data. We believe that our processing of personal information is proportional to our aim to protect much more sensitive personal data in the systems at stake.

We share our findings

During our research we inform the broader security community and the media on our findings on a statistical basis. We only provide the total numbers, no names, or other identifiable information.

And we stick to these rules

DIVD is responsible for reminding researchers of these rules, while it's the responsibility of each individual researcher to stick to them. If they don't, their DIVD account will be revoked.

So, in short

We perceive vulnerability disclosure as a societal need. To prove you are vulnerable we use minimal invasive tools (subsidiarity principle) and collect the minimal amount of data (proportionality principle). We don't go naming and shaming, don't report you to Data Protection Authorities or law enforcement, don't serve any company's interests and don't make any money from this. We are just a group of volunteers who help out victims of online vulnerabilities.

Dank

Dit boek is voor een groot deel geschreven tijdens de coronacrisis, die mij eigenlijk wel goed uitkwam. Eerst was het even slikken, na de beruchte persconferentie van 12 maart 2020 waarin Mark Rutte vertelde dat het voorlopig gedaan was met alle evenementen. Maar het was het voor mij eerlijk gezegd ook een opluchting. Voorheen had ik elk voor- en najaar veel evenementen en de zomer en winter om te schrijven. Zoals je hebt kunnen lezen, organiseren hackers hun evenementen juist in die downtime momenten en was ik al snel het hele jaar rond bezig. En al die evenementen leverden nieuw materiaal op voor mijn boek. Totdat dus in een klap mijn agenda voor het komende halfjaar werd leeg geveegd en ik eindelijk weer toe kwam aan schrijven.

Mijn dochter Lena ook. Ze kreeg op 24 maart te horen dat ze niet meer naar school hoefde en vanwege haar goede cijfers bij voorbaat was geslaagd. Ook zij had veel losse flarden voor haar volgende boek liggen en ging direct aan het werk om er een geheel van te maken. Samen kwamen we in een steevast dagelijks ritme van uren achtereen schrijven, afgewisseld door wandelingen door een verlaten stad, pratend over ons schrijfwerk. Hoe bouw je een verhaal op? Wat is ervoor nodig om een personage tot leven te wekken? Hoe kun je spelen met sprongen in tijd en ruimte? Wat laat je bewust weg om het spannend te maken? Geen normale vragen voor een achttienjarige, maar voor Lena dagelijkse kost. Mijn dank gaat dus allereerst uit naar jou, Lena, voor alle goede gesprekken en inspiratie voor het schrijven. Ik weet zeker dat je meer lezers zult krijgen dan ik.

Ik had vooral nog veel onuitgewerkte opnames liggen van Hack Talk. Dit praatprogramma heb ik in het leven geroepen om gewone mensen te laten zien dat hackers best aardige mensen zijn en om hackers te laten zien dat gewone mensen ook best interessant kunnen zijn. Gaandeweg ging ik

het podium steeds meer gebruiken om interviews te doen voor dit boek. Dat kon omdat ik volledig vrij was om de inhoud van de programma's zelf te bepalen. Dank dus aan de sponsoren die me die vrijheid hebben gegeven en ons programma onvoorwaardelijk hebben gesteund: Luisella ten Pierik van Stedin, Juul Brouwers van dcypher, Sarah Olierook van het Havenbedrijf Rotterdam en Annelies van der Meer van de gemeente Rotterdam. Dank ook aan club Worm voor de gastvrijheid en aan mijn vaste VJ Pleun Gremmen die als kunstenares de hackergemeenschap feilloos aanvoelt.

Op 10 september 2020 was het manuscript van dit boek klaar. Ik had tien bekenden bereid gevonden het als proeflezer te beoordelen en hen een geprinte versie gestuurd. Op de valreep bedacht ik dat het misschien toch wel zo netjes zou zijn om het NCSC te laten weten wat ik over hen schrijf. Een van de medewerkers had me verteld dat het niet echt waarschijnlijk zou zijn dat het centrum met een officiële reactie zou komen op een boek, maar het leek me wel het proberen waard. Dus mailde ik het document naar directeur Hans de Vries, in de hoop dat iemand van zijn secretariaat het zou oppakken en ik hen in ieder geval in kennis had gesteld. Tot mijn verbazing kreeg ik diezelfde avond nog een reactie van Hans zelf: "Hi, Chris. Heb je boek gelezen. Morgen even bellen?"

In het gesprek nam Hans het uiteraard op voor zijn eigen centrum, dat nu eenmaal in haar taak beperkt is tot het helpen van haar doelgroep: Rijksoverheid en vitaal. Ze kunnen niet, zoals DIVD, heel Nederland gaan scannen en melden. Dat begrijp ik inmiddels. Hans nam het vooral op voor de helpende hackers en zei: "Het is geen spielerei met alleen maar feestjes en conferenties! Hackers zijn een belangrijke steun in moeilijke tijden, dus wat wil je bereiken met je boek? Je eigen communityglazen ingooien?" Eh, nou nee. Ik wil juist laten zien hoe waardevol die community is. Aan de lezer het oordeel of dat is gelukt. Aldus, Hans: dank voor je betrokkenheid, bij mijn werk en dat van de hackers.

In de daaropvolgende maand kwamen de geprinte manuscripten terug, de een vol gekrast en de andere met slechts een pagina commentaar. De een had het in een keer uitgelezen, met alleen het commentaar: "Leest lekker weg". Anderen hadden spellingscorrecties en feitenchecks gedaan. Sommigen wilden er graag kopjes tussen en een slot aan het eind, maar die

waren toch in de minderheid, dus heb ik het lekker als doorlopend verhaal gelaten. En als je tot hier bent gekomen met lezen, dan was dat voor jou blijkbaar ook geen onoverkomelijk probleem. Mocht je nog wel iets willen schrappen of toevoegen, laat me dat weten voor de volgende druk.

Dank reviewers voor jullie eerlijkheid en betrokkenheid: ‘Unicorn’ Hans van de Looy, ‘schooljuf’ Marjolijn Bonthuis, mijn geliefde Ingrid Hille Ris Lambers, ‘Mister CVD’ Jeroen van der Ham, ‘hackerakela’ Astrid Oosenbrug, ‘taalvirtuoos’ Jacoba Sieders, Esther Makaay die er een geheel eigen boek van maakte, ‘cyberpresentator’ Peter Zinn, ‘onthullende verslaggever’ Gerard Janssen, ‘Miss Privacy’ Rachel Marbus en ‘Eindbaas’ Thijs Bosschert. Jullie commentaar was zeer waardevol, maar soms ook tegenstrijdig.

Vele lezers zijn jullie voorgegaan in het becommentariëren van dit boek. Dat zijn de meer dan honderd mensen wiens verhalen ik heb geselecteerd voor dit boek en hun stuk van commentaar hebben voorzien. In alfabetische volgorde: Ad Buckens, Akim Moiseenkov, Alex Scherphof, Ancilla van de Leest, Anne Ardon, Antoinette Hodes, Arnd Marijnissen, Attilla de Groot, Barry van Kampen, Bart Jacobs, Bart Roos, Bob Hoogeboom, Brenno de Winter, Chantal Stekelenburg, Cynthia Schouten, Daan Archer, Daniel Bakker, Daniel Scheper, Diederik de Vries, Edwin van Andel, Elger Jonker, Elina van ’t Zand-Kurtovic, Elmer Leger, Erik van Oosbree, Falk Garbsch, Floor Jansen, Frank Breedijk, Frans de Bie, Gerhard de Koning-Gans, Hans van de Looy, Henk Krol, Herbert Bos, Inge Bryan, Ingeborg van der Geest, Janneke van den Brand, Jelle Niemantsverdriet, Jelle van Haaster, Jeroen Schipper, Jessica Conquet, Joel Aviad Ossi, Joeri Jungschlager, John Fokker, John Sinteur, Jorik Berkepas, Karl Lovink, Karsten Nohl, Kas Clark, Kees Verhoeven, Liesbeth Holterman, Lodewijk van Zwieten, Lousewies van der Laan, Manon de Vries, Marie Gutbub, Marijn Fraanje, Martin Knobloch, Mary-Jo de Leeuw, Matej Skello, Matthijs Koot, Mattijs van Ommeren, Melanie Rieback, Michiel Prins, Michiel Steltman, Mieke van Heesewijk, Mischa van Geelen, Nick Brands, Nina Boelsum, Oscar Koeroo, Owen Vogelaar, Patricia Zorko, Patrick de Brouwer, Peter Beverloo, Peter Geissler, Peter van Eijk, Peter van Hofweegen, Petra Oldengarm, Pieter Jansen, Pim Takkenberg, Rabin Baldewsingh, Rachid Guernaoui, Remco Verhoef, Remko Sikkema, Remon Klein Tank, René van

der Velde, Ricardo ten Cate, Rickey Gevers, Rik van Duijn, Rob de Charro, Roel Verdult, Ronald Prins, Sanne Maasakkers, Saskia Hoogma-Ton, Sjoerd van der Maaden, Stef van Dop, Tabitha Vogelaar, Thamar van Vlaanderen, Thomas van Ruitenbeek, Tobias Groenland, Tom Kooijman, Ton Siedsma, Ton Starrenburg, Victor Gevers, Vincent Ossewaarde, Walter Belgers, Wesley Neelen, Wietse Boonstra, Wouter van Rooij, Wytske van der Wagen, Ymkje Lugten en Zawadi Done. Dank voor de wonderlijke reis in jullie belevingswereld en de verhalen die jullie me hebben toevertrouwd.

De cyberwereld is dankzij jullie inzet niet alleen veiliger, maar vooral ook veel leuker geworden.

Chris van ’t Hof
Rotterdam, februari 2021

Over de auteur

Chris van ’t Hof (1972) is internetsocioloog, schrijver en presentator. Met zijn bureau Tek Tok maakt hij ingewikkelde zaken in wetenschap en technologie toegankelijk voor iedereen. Als spreker en dagvoorzitter doet hij veel congressen, webinars en crisismanagement trainingen. Hij heeft een eigen live-praatprogramma: Hack Talk, een praatprogramma voor en door de hackers community. Daarnaast is hij secretaris en medeoprichter van DIVD, het Dutch Institute for Vulnerability Disclosure, om helpende hackers te steunen.

Dit boek is een vervolg op *Helpende hackers. Verantwoorde onthullingen in het digitale polderlandschap* (2015). In zijn tijd bij het Rathenau Instituut verschenen mede van zijn hand: *Voorgeprogrammeerd. Hoe internet ons leven leidt* (2012), *Check in/Check out. The Public Space as an Internet of Things* (2011) en *RFID and Identity Management in Everyday Life* (2007). Daarnaast schreef Chris meer dan honderd artikelen, waaronder een reeks over hackers in *De Correspondent.*

Profiel: www.cvth.nl
Bedrijf: www.tektok.nl
Praatprogramma: www.hacktalk.nl
Boek: www.cyberellende.nl
Twitter: @cvthof

Weer dat f*ckingW@CH7W00rD vergeten…
Opdringerige updates wanneer je het druk hebt…
Altijd die spam met phishingmails…
En zelfs als je alle veiligheidsadviezen opvolgt,
kun je alsnog gehackt worden.
Dat is wat cybersecurity is voor de dagelijkse gebruiker:
vooral ellende.

Dit boek laat de andere kant zien.
Cybersecurity is namelijk ook een heel open wereld,
met hackers die juist helpen ellende te voorkomen.
Ze stellen hun kennis en vaardigheden gratis beschikbaar
en organiseren daarvoor de leukste feestjes.

Organisaties staan steeds meer open voor deze helpende hackers
en begrijpen dat we pas veilig zijn als we een keer goed gehackt zijn
en we beter onze kwetsbaarheden kunnen delen
om zo samen sterker te worden.

TEK TOK