Zaterdag

De verhalen achter het nieuws

De eerlijke hacker

Cybersecurity-bedrijven houden hun klanten dom en zijn alleen maar uit op winst, zegt **Melanie Rieback**. Ze biedt een ethisch alternatief.
P2

Onveilige haven: waarom containerbedrijf APM plat kwam te liggen
P6

Foto Aisha Zeijveld

Column

Huilers

ESTHER GERRITSEN

De jonge zeehondjes die worden opgevangen in zeehondencrèches blijken daar niet allemaal beter af te zijn. Sinds kort weten we dat de kleine zeehondjes, de huilers, die achtergelaten lijken te zijn op het strand, meestal gewoon weer door hun moeder worden opgehaald. Zelfs de prematuren kunnen prima acht uur alleen zijn. Maar voor die uren voorbij zijn, worden ze gered door voorbijgangers. De afgelopen jaren hebben vele zeehondenmoeders dagenlang tevergeefs naar hun kind gezocht.

Ik dacht meteen aan Peter Pan, die als baby het raam uit vloog. Ik was mijn 8-jarige dochter de originele *Peter Pan* gaan voorlezen. Het begon allemaal prachtig met dat vliegende kind, tot we bij het hoofdstuk aankwamen dat Peter terug naar zijn moeder wou. Hij was al eens eerder naar haar slaapkamerraam gevlogen maar toen toch weer vertrokken, de vrijheid was hem te lief. Tot hij besloot definitief terug te keren. Maar juist die nacht, aangekomen bij haar slaapkamer, zag hij haar met een ander kind in haar armen en om dit kind te beschermen had ze tralies voor het raam gemaakt.

'Peter riep: 'Moeder! Moeder!' Maar ze hoorde hem niet en vruchteloos sloeg hij met zijn kleine armen en benen tegen de ijzeren staven.' Naast mij barstte mijn dochter in huilen uit en huilen doet ze zelden.

> **Op een dag behandelen ze op school de onderwerpen waarvan je pas echt wakker ligt**

Ik las door: 'Hij moest wel snikkend terugvliegen naar de Tuinen. Nooit zag hij zijn liefste weer, en hij had zo'n geweldige zoon voor haar willen zijn!'

'Nee', riep mijn dochter, 'hij moet terug naar haar!' en zij sloeg al even zo woest als Peter Pan met haar armen en benen om zich heen.

Maar J.M. Barrie ging nog verder: 'Ach Peter! Wij allen die de grote fout hebben gemaakt, wat zouden we niet allemaal anders doen als we een tweede kans kregen...' om te besluiten: '... maar er is geen tweede kans, voor de meesten in ieder geval niet.'

Precies, wanneer die zeehonden weer worden uitgezet is mama zeehond allang vertrokken, er is geen tweede kans.

Ik las ter geruststelling nog maar een ander verhaal voor, zo vlak voor het slapen gaan.

Toen ik de volgende dag zei: 'Zullen we maar niet meer uit *Peter Pan* lezen?', zei ze: 'Jawel, want als ik dan overstuur raak, lees je nog een verhaal.'

In het najaar is het Kinderboekenweek, het thema is Griezelen, met als motto Gruwelijk Eng! Veel scholen en ouders schijnen daar niet blij mee te zijn. Schrijver Rian Visser schreef er dinsdag over in *de Volkskrant* en zij nam het met recht op voor enge en nare verhalen. Ik herinner me met genot alle nare jeugdboeken die ik vroeger las.

Maar met pijn herinner ik me de waargebeurde verhalen die me werden verteld. Op een dag behandelen ze op school de onderwerpen waarvan je pas echt wakker ligt en waarvan niemand troostend kan zeggen dat het niet werkelijk is gebeurd. De eerste oorlogsverhalen die ze je vertellen, de foto's erbij, ik weet nog precies van welke beelden ik niet kon slapen. Later dacht ik: had iemand me niet tegen die verhalen kunnen beschermen? Om me nog weer later te realiseren dat dat onmogelijk is. Op een dag hoor je waartoe de mens in staat is. Te beginnen bij de tragiek van de goede bedoelingen, met wanhopig zoekende zeehondenmoeders als gevolg. Van daar verder naar het echte kwaad. Op een nacht lig je wakker, en het is niet van *Peter Pan*.

Samenwerken tegen **hackers**

Topgeek: we zijn extreem kwetsbaar

Met Radically Open Security test Melanie Rieback de computersystemen van grote bedrijven. Klanten kijken mee als ze het ene lek na het andere blootlegt. Geheimhouding helpt de goede zaak niet, vindt ze.

Door **Gerard Janssen** Foto's **Aisha Zeijpveld**

Dit verhaal begint niet in een verlaten loods in een buitenwijk van een grote stad, met op de achtergrond het geluid van druppelend water. Geen fabriekshal met opgestapelde blikjes Monster Energy en beeldschermen met groene lettertjes. De hackers van Radically Open Security werken niet samen in een fysieke ruimte, maar in een chatroom.

Het moet geheim blijven welk bedrijf vandaag het doelwit is van de hack, of *penetration test*, zoals een hack in opdracht genoemd wordt. Het moet zelfs geheim blijven in welke branche het opereert. 'Maar er werken de capabelste en technisch best opgeleide mensen die er zijn', verzekert Melanie Rieback, oprichter van Radically Open Security. Ik spreek haar op een Amsterdams terras. Rieback praat snel, soms Amerikaans en soms Nederlands. En ze grinnikt vaak na een zin. Soms zucht ze. Soms zucht ze heel diep, als het over Donald Trump gaat.

Rieback is zo'n beetje de Wonder Woman van de computerbeveiligingswereld. Met haar internationale team van vijfendertig tophackers test ze de beveiliging van computernetwerken en websites. Ze heeft klanten in uiteenlopende sectoren, van verzekeraars tot universiteiten en van mediabedrijven tot de politie.

Overal waar een internetaansluiting is, kan een 'pentester' van Rieback aan het werk. Haar team kan freelancers bevatten uit Australië of Azië.

Nu heeft ze twee hackers uit Berlijn aan het werk gezet: Pierre Pronchery en Stefan Gronke. Vanachter haar laptop volgt Rieback hun verrichtingen. De avatarfoto van Pronchery is die van een piloot met een microfoontje voor de mond en een zonnebril op. Gronke heeft korte blonde haren en draagt een overhemd. Op haar eigen avatarfoto zit Rieback op een racefiets met een opblaasdolfijn in haar handen.

De hackers plaatsen zakelijke berichten, met astronaut-achtig jargon.

'We could do a connect scan via a socks proxy over SSH…'
'I can do that. Let me check the device capacity to see if that works.'

Het werk is te vergelijken met het in kaart brengen van een wijk. Welke straten zijn er, wat zijn de adressen van de huizen. Vervolgens is het aan de deurtjes rammelen en door de ramen naar binnen kijken. Of er oude software draait bijvoorbeeld. De klanten, die 'slachtoffer' zijn van de hack, mogen meekijken en vragen stellen terwijl de hackers van de ene naar de andere kamer lopen.

'Het is een beetje als Indiana Jones die een grot onderzoekt', vertelt Pronchery op de chat, we vinden nutteloze dingen, schatten, raadsels, doorgangen die naar nieuwe kamers leiden, met daarin nieuwe voorwerpen.'

Het wordt al snel duidelijk dat Pronchery en Gronke razendsnel werken. Ze zien raampjes waar niemand anders ze ziet en oude deurtjes die mensen vergeten zijn. 'Folks als Pierre en Stephan zijn echt a-typisch', zegt Rieback, 'het duurt zeker tien jaar voor je zo goed bent. En dan niet tien jaar van 9 tot 5. *It's a passionate thing.*'

Al binnen een dag zijn de hackers het systeem van het bedrijf binnengedrongen.

Pierre: *I have good news and bad news: unicorn123 (root)*
Klant: *Bingo*
Melanie: *Is that what I think it is?*
Pierre: *It's a password for the local root account on the machine I dumped yesterday*
Melanie: *Ouch… that was quick*
Pierre: *I'll be off for lunch.*

Binnen een paar dagen hebben de twee Berlijners volledige controle over het netwerk.

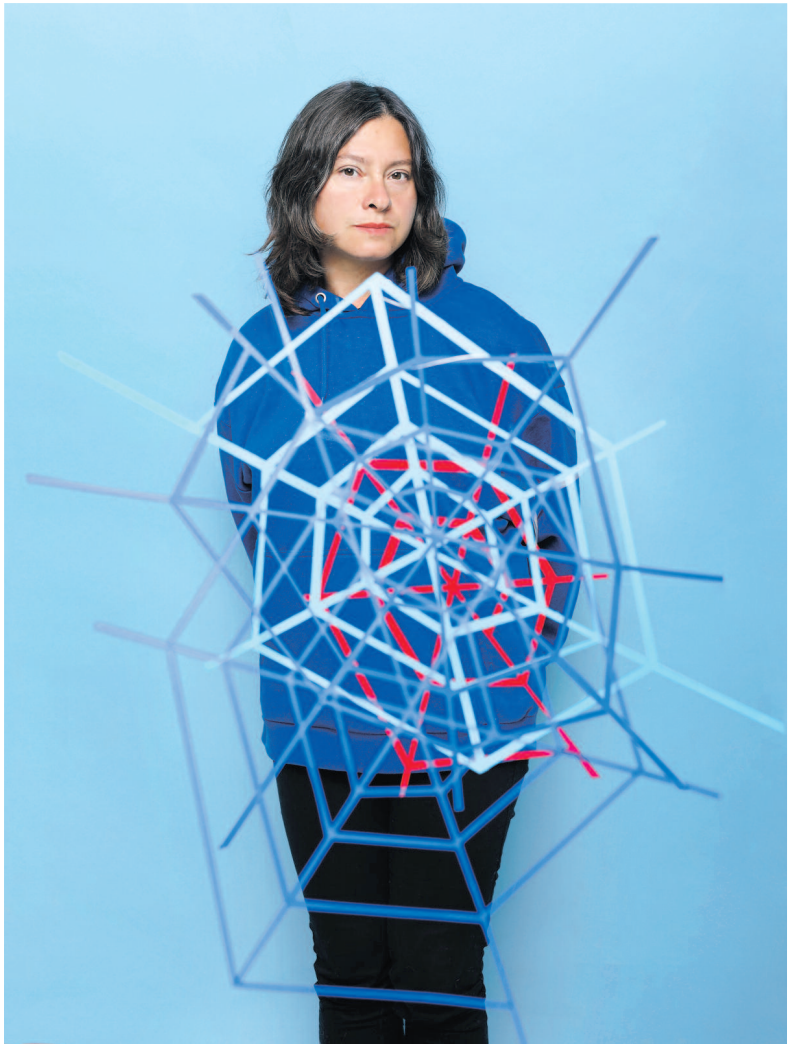
'Het was een totaal verlies voor de klant', zegt Rieback later lachend, '*we pretty much destroyed it*. Je kijkt ernaar en … *get the popcorn*. En als je nagaat wie het doelwit was. Als deze goede mensen al deze fouten maken. Bedenk dan eens welke fouten er worden gemaakt door minder technische mensen bij andere bedrijven.'

Ze is niet verbaasd dat haar team de beveiliging gekraakt heeft. Dat lukt namelijk altijd. In het uiteindelijke rapport, grotendeels automatisch geschreven door een robot in het chatprogramma, staat een opsomming van vijftig kwetsbaarheden, variërend in dreigingsniveau. Zeventien dragen het label 'extreem'.

Als geen ander weet ze hoe kwetsbaar onze samenleving is, met een economie die volledig draait op internet. Kijk alleen al naar de ransomware-aanvallen in de Rotterdamse haven. 'Een groep hackers met tijd en geld komt overal binnen', zegt Rieback. Met de nadruk op overal. Elektriciteitsbedrijven, politieke partijen, de politie, gemeenten, ziekenhuizen. 'Grote netwerken zijn zo complex en *the devil is in de detail*. Mensen moeten begrijpen dat alles kwetsbaar is en moeten nadenken over de datasporen die ze overal achterlaten. Er is weinig te doen aan een goed gemaakte phishing mail. Ik kan er ook intrappen.'

Het is schokkend, wat ze soms bij bedrijven aantreft, beaamt Rieback. 'We hebben pentests gedaan waarbij de resultaten zelfs binnen een kleine groep technici in het bedrijf geheim moesten blijven, omdat het zo gevoelig was. Als het uitgelekt was naar mensen zoals jij hadden we een groot publiek schandaal gehad. Ha ha.'

Reden te meer voor computerbeveiligers om samen te werken en open te zijn over de methoden, zegt Rieback. Cybercriminelen werken immers ook samen en innoveren razendsnel. Om nog maar te zwijgen van de *state actors*, hackers die gesteund worden door bijvoorbeeld de Amerikaanse, Russische of Chinese overheid.



MELANIE RIEBACK **Eerder dit jaar door het blad *CIO Magazine* uitgeroepen tot innovatiefste ict-leider van Nederland.**

> Bij het beveiligen van computers moeten we samenwerken en we moeten open zijn over onze methoden. **Ook de cybercriminelen werken immers samen**. En ze innoveren razendsnel

Maar het gros van de cybersecuritybedrijven is helemaal niet gericht op samenwerking, zegt Rieback. Zij willen vooral zo veel mogelijk geld verdienen. Sommige van hen werken ook samen met overheden, niet altijd de *good guys* waar gaat het om computerveiligheid. Veiligheidsdiensten als de NSA en de AIVD hebben er juist baat bij dat bij een bedrijf soms een raampje blijft openstaan.

Een onbekende opening in het laatste besturingssysteem van een computer of telefoon kan een waardevol wapen zijn. Maar een wapen kan in verkeerde handen vallen. De ransomware die vorige week in Rotterdam containerbedrijf Maersk trof en de wereld-

LEES VERDER OP **PAGINA 5**

Samenwerken tegen **hackers**

VERVOLG VAN **PAGINA 3**

handel verstoorde, gebruikte luikjes die de NSA geheim had gehouden en vijf jaar geleden al had kunnen sluiten.

Rieback zag het licht toen ze werkte bij het Computer Security Incident Response Team (CSIRT) van de ING. Daar werd het zaadje geplant van haar bedrijf Radically Open Security. Het was de tijd dat er mysterieuze dingen gebeurden bij de ING. In 2013 lag de bank een paar keer plat door zogenoemde DDoS-aanvallen. Het waren de hoogtijdagen van Russische criminele hackersgroepen die de ene na de andere bank beroofden.

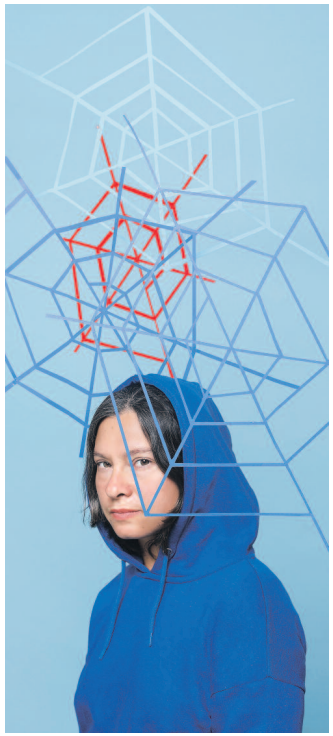
Rieback lacht mysterieus. Het Traffic Light Protocol (TLP) is haar tweede natuur. 'Groen betekent dat iedereen het mag weten. Oranje informatie moet in een kleine kring blijven en rood betekent dat het zo gevoelig is dat je het niet eens ergens op mag schrijven.' Het stoplicht springt op rood als het over de ING gaat. Van haar geen smeuïge verhalen. Ze heeft een hoge stapel *non disclosure agreements* getekend.

Maar het stoplicht springt op groen als het over externe cyberbeveiligingsbedrijven gaat. ING huurde deze bedrijven in om hun systemen te testen. Om te kijken of ze hackproof waren. Rieback, die zelf bij wijze van spreken geblinddoekt en met een hand op de rug computervirussen programmeerde, wilde graag meekijken. Maar de laptopjes klapten dicht als ze in de buurt was. En de adviseurs 'vergaten' de beloofde logbestanden te saven en door te sturen.

Rieback: 'Ze willen je onwetend houden en zo min mogelijk kennis overdragen. Ze zijn als een brandveiligheidsbedrijf dat zijn werk opzettelijk niet al te goed doet, omdat het bang is anders niet meer gebeld te worden. Ze willen de klanten niks leren, want dat zou ten koste gaan van hun bedrijfsvoering. Alles wat ze deden was ultracommercieel en hielp niets.' Rieback wil geen namen noemen. 'Maar bijna alle grote cybersecuritybedrijven maken zich eraan schuldig.'

Rieback merkte dat ze niet de enige was die zich hieraan stoorde, ook collega's van andere bedrijven klaagden erover. Tegelijk wist ze dat sommige hackers die ingehuurd werden door de traditionele beveiligingsbedrijven worstelden met hun geweten. Of zoals de Berlijnse hacker Stefan Gronke het verwoordt: 'Het is als toekijken hoe mensen lijden en tegelijkertijd het vaccin geheimhouden.'

Een plus een was drie voor Rieback. In mei 2014 begon ze Radically Open Security. De allerbeste hackers ter wereld willen voor haar werken.



Ik ben een socialist die een bedrijf begonnen is. **Ik ben een activist, maar probeer niet de gemeenschap omver te werpen**. Soms is de beste manier om tegen onrecht te strijden de structuur te omarmen

Rieback heeft de beschikking over een club mensen, onder wie ook Nederlanders, waarmee de NSA of de Russische veiligheidsdienst dolblij zou zijn. Met dit dreamteam bedient ze zo'n vijftig klanten.

Met Radically Open Security, ook wel ROS, wil Rieback het helemaal anders doen. Ze laat haar opdrachtgevers meekijken als haar hackers de computernetwerken binnendringen en zet alle tools die ROS gebruikt gratis op haar site. Zo krijgen bedrijven een veel beter inzicht in de manier waarop hackers te werk gaan. Want, zo meent Rieback, de beste computerbeveiligers zijn niet alleen technisch capabel, ze kunnen ook denken als hackers: creatief, sluw, gemeen, humoristisch en out of the box.

Per opdracht bekijkt Rieback of ze het ethisch verantwoord vindt. Bedrijven die data aan inlichtingendiensten doorgeven helpt ze niet. Een opdracht voor de politie doet ze alleen als er geen *non disclosure agreement* getekend hoeft te worden. En ze bouwt geen surveillancesystemen.

De winst van Radically Open Security gaat voor 90 procent naar goede doelen. Rieback keert zichzelf het wettelijk minimum uit.

Ze ziet haar bedrijf als een vorm van activisme, vergelijkbaar met bedrijven die fairtradeproducten verkopen. 'Zij maken het je makkelijker de wereld te verbeteren door je aankoopbeleid te beïnvloeden. Ik geef bedrijven en overheidsinstellingen een ethisch alternatief.'

Melanie Rieback werd op 26 oktober 1978 geboren in Ohio en verhuisde naar Naperville, Illinois, een voorstad van Chicago, waar haar beide ouders werkten bij Bell Labs, de legendarische laboratoria waar de transistor, de laser en het computerbesturingssysteem Unix ontwikkeld werden. Als klein kind rammelde ze al op de machines van haar ouders. Ze leerde op haar zevende programmeren en leefde in een wereld van groene lettertjes en floppy disks. 'Super oldskool.' Op haar 9de verhuisden ze naar Florida. Als ze uit school kwam was het huis leeg, haar ouders werkten dan nog.

'Als je in de buitenwijken van Florida geen rijbewijs hebt, moet je creatief zijn in hoe je in contact komt met mensen.' Gelukkig had ze een computer en een internetaansluiting. Ze maakte vrienden op bulletinboards, sites waar je berichtjes kunt achterlaten. En daarop zaten toen ook hackers. Zelf durfde ze het niet. Maar ze verslond de verhalen die ze er las, over het hacken of over phreaking, het met hoge tonen manipuleren van het telefoonsysteem.

'Ik was altijd een beetje een geek, met alle voordelen en nadelen die erbij horen. Een loner. Ik had vrienden, maar ik was nooit super-superpopulair dus ja… Om eerlijk te zijn… Het was niet mijn favoriete tijd.' Het TLP-stoplicht springt op oranje. 'Ik wil niet te veel in persoonlijke details treden.'

Ze ging biologie studeren in Miami, en raakte door haar handigheid betrokken bij het Human Genome Project op het MIT in Boston, waar het eerste menselijke dna in kaart werd gebracht. Ze loste er computerproblemen op, 'blusklusjes', zoals ze het zelf noemt. Ze wilde graag naar Europa en kwam via de TU Delft in Amsterdam terecht, waar ze haar promotiewerk deed bij de legendarische Andrew Tanenbaum, een grootheid op het gebied van computers en netwerken.

'Bij hem promoveren en met hem werken was een van de gelukkigste dingen in mijn leven.' Ze werkte aan de chipkaart, zoals die in het openbaar vervoer wordt gebruikt. Op zo'n kaart zit een chip met een piepklein computertje. Het lukte Rieback een miniatuurvirusje te schrijven dat van de chipkaart kon overspringen naar de database-systemen. Dit kunststukje haalde de nieuwssites van CNN en de BBC. 'Het ging viraal voordat zoiets viraal gaan genoemd werd.'

Na vier jaar als universitair docent aan de VU en een uitstapje naar het Canadese bedrijfsleven belandde ze in 2013 bij de ING in Amsterdam. Nu is ze dus ceo van ROS en tevens een van de oprichters van het Nederlandse Girls Geek Dinner, een netwerkbijeenkomst voor vrouwen in de technologiesector. 'Ik wilde graag al die vrouwen laten zien die opzienbarend werk in 'tech' doen, om andere vrouwen, jong en oud, te inspireren.

'Het is ironisch. Ik ben een socialist die een bedrijf begonnen is. Ik ben een activist, maar ik probeer niet de gemeenschap omver te werpen. Soms is de beste manier om tegen onrecht te strijden de structuur te omarmen. Omdat ondernemingen zo veel vrijheid krijgen. Een bedrijf kan alles doen zolang het maar legaal is, en zolang het de eigen kosten maar dekt. Een bedrijf heeft daardoor meer bewegingsvrijheid dan een liefdadigheidsinstelling of een stichting.'

Volgens Rieback is de sociale onderneming het beste antwoord op wat ze de 'post-Trumpwereld' noemt. 'Het probleem is dat zakendoen voor veel activisten een vies woord is. Ik denk dat we in de toekomst de sociale onderneming als nooit tevoren moeten omarmen. Een bedrijf is een uitstekend middel voor politiek activisme.'

Dit voorjaar won ze de jaarlijkse TIM Award voor de innovatiefste ictleider van Nederland, uitgereikt door *CIO Magazine*. De jury was unaniem lovend: 'Ze steekt op een unieke manier de nek uit om veranderingen teweeg te brengen.'

Dat vitale infrastructuur vandaag de dag zo makkelijk te hacken is, bezorgt Rieback geen slapeloze nachten. 'Wat me wakker houdt, is wat er nu aan de hand is in de Verenigde Staten. Het hacken van de verkiezingen. Hoe Trump er nu op reageert. Hij zwakt het af omdat hij er beter van wordt. Hij bagatelliseert buitenlandse inmenging in de verkiezingen. Ik bedoel … Wow… Hoe zijn we hier beland? Wat betekent het voor de democratie, als we niet meer kunnen vertrouwen op de integriteit van onze verkiezingen? Welke implicaties heeft dat voor onze samenleving? Wat betekent het dat een zakenman toegang heeft tot het grootste afluisterapparaat van de wereld? Daar maak ik me ernstige zorgen over.'