↑ Melanie Rieback, Radically Open Security

HOE IK...

IT VEILIGER MAAK (DOOR OPEN TE ZIJN)

MELANIE RIEBACK (35) test met RADICALLY OPEN SECURITY

hoe veilig IT is voor aanvallen van buiten. Haar bona fide hackers doen dat op een radicaal andere manier dan de gevestigde orde: "Bij alles wat wij doen, mag de klant over onze schouder meekijken. Uiteindelijk wil ik de veiligheidsindustrie dwingen tot dezelfde openheid."

Philip Bueters Jorn van Eck 0.00 min.

Het idee voor Radically Open Security is geboren in mijn tijd bij ING, waar ik tot begin 2014 verantwoordelijk was voor het antwoord op cyberaanvallen. Daarvoor schakelden we ook security-experts van buiten in, maar ik werd kwaad over de manier waarop zij werkten. Ze komen binnen met een air van: 'Wij nemen de boel hier wel even over, we gaan niet uitleggen wat we doen want dat is toch veel te ingewikkeld.' Nou, dat valt wel mee. Ik programmeer zelf al vanaf mijn zevende en heb informatica gestudeerd in Miami, Delft en Amsterdam. Aan de VU ben ik gepromoveerd op de veiligheid van RFID, de draadloze chips die onder meer in de OV-Chipkaart zitten. We hebben daar nog veel publiciteit gehaald door te bewijzen dat die kaart helemaal niet zo veilig was.

Ik ben jarenlang universitair docent geweest, tot ik het zat was om eindeloos subsidievoorstellen te schrijven om onderzoeksgeld binnen te halen en besloot over te stappen naar het bedrijfsleven. Bij ING kwam ik terecht nadat ik een jaar bij Citrix in Canada had gewerkt: ik miste Nederland gewoon te erg, de vrienden die ik hier had gemaakt. Als securitymanager bij ING leek het me verstandig om mee te kijken met de security consultants. Hoe pakten zij de aanvallen aan? 'Ik wil zo veel mogelijk van jullie leren,' zei ik. Dat vonden ze niet leuk. Ze 'vergaten' me toegang te geven tot hun logbestanden en probeerden hun werkwijze te verbergen. Terwijl ik ervan overtuigd ben dat alleen als je een klant laat zien wat je doet en hoe je het doet, je hem kunt leren hoe hij zelf zijn systemen veiliger kan maken. →

FACTS & FIGURES

WERELDWIJD WORDT **75 MLD** DOLLAR UITGEGEVEN AAN IT-BEVEILIGING, **4,7%** MEER DAN HET JAAR ERVOOR

VERZEKERAAR LLOYDS SCHATTE DE TOTALE SCHADE VAN CYBERCRIME IN 2015 WERELDWIJD OP **400 MLD** DOLLAR

BIJ DE CYBERAANVAL OP DATINGSITE ASHLEY MADISON KWAMEN DE PERSOONLIJKE GEGEVENS VAN **37 MLN** VREEMDGANGERS OP STRAAT TE LIGGEN

SONY PICTURES LEED **85 MLN** SCHADE, MAAR VOORAL GEZICHTSVERLIES NADAT HACKERSGROEP GUARDIANS OF PEACE EIND 2014 FILMS, SCRIPTS EN E-MAILS OPENBAARDE

'DE KLANT ZOU ZOVEEL VAN ONS KUNNEN LEREN DAT HIJ ZONDER ONS KAN'

Ik vroeg collega's bij andere bedrijven wat ze vonden van die geheimzinnigheid. Hun antwoord was meestal: 'Ik vind het ook niks, maar wat moeten we anders?' Dat bracht me op het idee voor Radically Open Security.

Ik legde het plan voor aan een vriend, die meteen enthousiast was. Binnen twee weken besloot ik mijn baan bij ING op te zeggen en startten we Radically Open Security, ofwel ROS. De naam voor het bedrijf en onze vijf kernwaarden had ik op dag twee bedacht: ik ben begonnen vanuit het *why*. Heel belangrijk voor ons is het *teach to fish*-principe: geef iemand een vis, en hij heeft een dag te eten. Leer hem vissen, en hij heeft de rest van zijn leven te eten. Vervolgens stelde ik mezelf de vraag: wie zijn de beste hackers die ik ken? Ik ging ze stuk voor stuk langs, en ze wilden bijna allemaal meedoen. Binnen anderhalve maand na mijn vertrek bij ING hadden we onze eerste klant voor onze pen-testen, de penetratietesten waarmee we – met toestemming natuurlijk – proberen in te breken in de systemen van onze klant. Dat is voor 10 procent een kwestie van software en voor 90 procent menselijke creativiteit.

Vanaf de start ging de groei eigenlijk vanzelf – aan sales doen we bij ROS niet, mond-tot-mondreclame doet zijn werk en ik spreek regelmatig op congressen. Mijn bedrijf heeft snel een reputatie opgebouwd en dat is ook niet gek want wat we doen valt nogal op in de IT-wereld. ROS is echt radicaal anders. Om te beginnen is het het enige not-for-profit securitybedrijf ter wereld, als zogeheten fiscale fondsenwervende instelling: we schenken onze winst onbelast aan een maatschappelijk doel. In Nederland werkt bijvoorbeeld Regina Coeli zo, beter bekend als de Nonnen van Vught. In ons geval gaat 90 procent van de winst naar stichting NLnet, die steunt maatschappelijk relevante open source- en onderzoeksprojecten rond internet. De overige 10 procent verdelen we over alle medewerkers, naar rato van de uren die ze hebben gedraaid. De medewerkers van ROS zijn allemaal freelancers: van de administratie tot de hackers, van de mensen die de rapportage schrijven tot de businessmedewerkers. Ze willen zelf bepalen waar en wanneer ze willen werken. We zijn superschaalbaar doordat we alleen met freelancers werken. Hackers kennen ons goed, we zijn een aantrekkelijke partij om voor te werken. Ze zijn het een beetje zat te werken voor securitybedrijven die zich ook laten betalen door overheden die de burger bespioneren. Als ik een extra kracht nodig heb, is dat hét

DE **5 PRINCIPES** VAN ROS

Geen schimmig gedoe
We bouwen geen bewakingssystemen, gaan niet achter activisten aan, verkopen geen lekken aan veiligheidsdiensten. Als een klus ethisch gezien ook maar enigszins twijfelachtig is, doen we hem niet.

Leer vissen
We delen niet alleen onze resultaten met onze klant, maar beschrijven ook stap voor stap hoe je zonder ons dezelfde audit of procedure kunt doorlopen. Wat we doen is geen rocket science, en we willen echt helpen je bedrijf veiliger te maken... zelfs als dat ons toekomstige omzet kost.

Open source
Alle software die we bouwen zetten we als open source op onze website.

Gratis IOC's
We zetten alle tekens die wijzen op een veiligheidsinbreuk, de zogeheten Indicators of Compromise, in een gratis te gebruiken database.

Zero days
We verkopen geen zero-days, de lekken in software die onmiddellijk moeten worden gedicht. We nemen onze verantwoordelijkheid en maken ze openbaar!

NETAIDKIT

Vraag het maar aan Edward Snowden: zodra je internet gebruikt, ben je niet zomaar veilig voor meeloerende overheden. Melanie Rieback en de haren zijn nogal voor individuele vrijheid en werken daarom met ROS mee aan de ontwikkeling van de NetaidKit. De wifirouter die ook digibeten in staat stelt onbespioneerd gebruik te maken van internet is een initiatief van Free Press Unlimited, dat zich ermee richt op journalisten en bloggers die onder moeilijke omstandigheden hun werk moeten doen. De open source software is af, de handzame router zou elk moment leverbaar moeten worden.

moment om ons netwerk weer eens uit te breiden. Ik ben net zelf twee weken in Zuid-Afrika op reis geweest en werk het liefst vanuit huis. We zijn wat je noemt een *distributed* online organisatie: onze experts werken vanuit locaties over de hele wereld. We houden contact met elkaar via ons eigen online samenwerkplatform, dat gaat prima.

Onze open aanpak is natuurlijk wat ons echt onderscheidt: bij elke stap die we zetten, elke softwareregel die we checken of bouwen, mag de klant meekijken. Hij krijgt toegang tot ons chatplatform en ontwikkelplatform, zodat hij alles kan volgen. De software die we gebruiken, is open source en kan hij zelf ook gebruiken. Wij doen niet geheimzinnig, we zetten nergens een black box neer die dingen met je data doet waar je geen zicht op hebt. In principe zou de klant zo veel van ons kunnen leren, dat hij zonder ons kan. Maar de ervaring leert dat ze allemaal regelmatig terugkomen.

Ons doel is onze klanten en de maatschappij tot nut te zijn, bij de meeste concurrenten is de klant het middel en geld het doel. Dat is het principiële verschil tussen ons en de gevestigde orde. Wij zijn idealisten en werken bijvoorbeeld tegen kostprijs mee aan projecten als de NetAidKit, een veilige wifirouter die wordt ontwikkeld door Free Press Unlimited.

ROS is nu met veertig man en we hebben meer dan twintig klanten, uit de energiesector, het onderwijs, de verzekeringswereld, de overheid en de non-profitsector: dwars door alle branches heen. We hebben op dit moment een stuk of vijftien offertes in de pijplijn zitten en winnen ongeveer de helft van alle aanbestedingen. Onlangs heb ik een deal getekend met een klant in de VS, die is in zijn eentje al goed voor een omzet vergelijkbaar met heel 2015.

Winst maken we nog niet, deels doordat we veel tijd investeren in onze eigen infrastructuur en processen. En onze snelle groei kost ook geld. We hebben niemand op de loonlijst staan, maar alle offertes en testrapportages opstellen kost ontzettend veel tijd.

Op korte termijn wil ik ROS tot een stabiel en productief bedrijf maken. Op middellange termijn wil ik de securitymarkt disrupten met onze aanpak. Ik hoop dat ons succes ertoe leidt dat de rest van de branche de lat gewoon hoger legt, ik wil ze dwingen zélf opener te worden.

Mijn grootste droom is dat Radically Open Security als not-for-profitbedrijf een schoolvoorbeeld wordt voor andere ondernemers die, in welke branche dan ook, maatschappelijk nuttige doelen willen koppelen aan hun bedrijf. Ergens in de geschiedenis is het verkeerd gegaan en begon alles om het geld te draaien. Maar in mijn ogen is een onderneming ooit bedoeld als een samenwerkingsverband om de maatschappij te dienen.” ■

radicallyopensecurity.com