Patrick de Brouwer, van hacker naar ethical hacker:

‘Dit leer je niet **op school**; ervaring doe je alleen op in de **praktijk’**

Ethical hacker Patrick de Brouwer trainde zichzelf van zijn vijftiende tot zijn twintigste nachtenlang in hacken. Die ervaring maakte hem een zeer kundig hacker – aantrekkelijk voor de ‘white side’ maar ook voor de veel lucratievere ‘dark side’. Hij koos toch de kant van het bedrijfsleven. “Het geeft een kick iemand te helpen zijn systeem veiliger te maken.”

door: TANJA DE VREDE / T.D.VREDE@AUTOMATISERINGGIDS.NL

Hoe word je een hacker? Patrick de Brouwer geeft zelf cursussen over ethical hacken, maar hij zal de eerste zijn die je vertelt dat je met het volgen daarvan nog geen ethical hacker bent. Zeker 25.000 uren stak hij van zijn vijftiende tot zijn twintigste in zijn ‘training’. Eigenlijk begon die training al op zijn elfde, toen internet zijn intrede deed in huize De Brouwer. Hij mocht een paar uur per dag op internet en kwam terecht in chats via IRC, een protocol voor (groepsgewijze) communicatie over het internet. Al snel leerde hij met scripten aanpassingen te bouwen waardoor het chatten sneller en beter kon. Binnen een jaar kwam hij op andere IRC-netwerken terecht waar hij mensen leerde kennen ‘die meer deden met scripten dan mag’. “Er werd veel gespamd. En dan werd er wat gebouwd om de spammers er vanaf te gooien.”

Op zijn vijftiende had hij eigen servers thuis en maakte hij contact met serieuze hackers. “Ik zat in de filesharing-scene, dat ging om films en zo. De activiteiten in die scene waren niet helemaal legaal. Er werden gehackte servers gebruikt; ik zat bij de groep die scande op bruikbare servers. Daarbij zag ik code voorbij komen waarvan ik vond dat die wel wat beter kon. Ik heb hun scripts geheel herschreven, met positieve resultaten.”

Zijn prestaties leverden hem hoge waarderingen op in de hackersscene en dus werd hij geïntroduceerd bij ‘de echte hackers’. “Ik keek tegen hen op, maar merkte ook dat daar wat minder leuke mensen bij zaten. Zij hielden zich bijvoorbeeld bezig met creditcardfraude. Niet prettig, want mijn vuistregel was ‘do no harm’.” Ook hield De Brouwer zich strikt aan ongeschreven regels en aan de ‘Do-not-touch-lijst’. “Dat is een lijst met ip-nummers die je niet moet benaderen. De kans dat je dan gepakt wordt, is te groot.”

Genoeg andere makkelijkere doelwitten bovendien, universiteiten bijvoorbeeld: snelle verbindingen en een minimale pakkans.

De sfeer bij de ‘echte hackers’ was minder prettig. Er was sprake van zware competitie. De hackers draaiden botnets en konden daar heftige ruzies over hebben – die dan weer uitmondden in onder meer DDoS-aanvallen op elkaar. “In 2005 zag je wat kleinere botnetjes, maar in 2007 ging het al om grote botnets waar tot anderhalf miljoen systemen in zaten. Hackers vonden het een kick om zoveel mogelijk machines te infecteren, want het was hún virus dat dat deed.” Hij zag hoe een Russische hacker – “met wie ik wel eens wat geknutseld had” – met cash een splinternieuwe BMW kocht.

“Ik was altijd wat achterdochtig en zag ook af en toe mensen achter de tralies verdwijnen.” Zelf is hij ook zeker acht keer door zijn provider afgesloten wegens ‘mogelijke aanvallen en hackpogingen’. Zijn verklaring dat het vast een virus moest zijn, werd de achtste keer niet meer geloofd. Hij ontving mailtjes van Microsoft, want dat zag verdachte activiteiten op zijn DNS en wilde daarop toegang om ‘systemen te kunnen cleanen.’ Hij weigerde, maar bij toeval ontdekte hij later dat Microsoft zijn activiteiten bleef volgen tot 2013.

Naar de good guys

Die steeds negatievere ervaringen plus positieve acties vanaf de ‘witte’ kant, zorgden er voor dat De Brouwer bewust de kant van de ‘good guys’ koos. “Ik vond bijvoorbeeld een kwetsbaarheid waardoor remote overname van de systemen mogelijk was. Het was leuk om bij hun machines naar binnen te gaan en hen dan te vertellen wat er aan de hand was en hoe ze dat konden fixen. Dat was een feel-good-momentje.”

Het definitieve keerpunt kwam in 2007. Hij vond op gehackte systemen een mapje waarin de configuratiebestanden te vinden waren van alle servers en de versleutelde wachtwoorden van een grote provider uit een Oostblokland. De provider had door het hele land wifipunten draaien die met elkaar verbonden waren. “Een paar maanden later vond ik een programma voor die configuratiebestanden. Een paar keer dubbelklikken was genoeg geweest om in duizenden machines te komen.”

De Brouwer deed niets, maar in de nacht voordat hij die maand op vakantie zou gaan lag zijn internetverbinding er ineens uit terwijl hij zelf aan zijn machine zat. “Ik heb onmiddellijk de computer uitgezet en de harddisk mee genomen op vakantie. Mijn moeder heb ik de volgende dag gezegd de stekker uit het modem te trekken. Achteraf was er niets aan de hand, gewoon een storing. Voor mij was het een alarmbel. Ik vond het allemaal wat te ver gaan.”

Alarmerend was ook dat zijn kennissen steeds vaker bezoek kregen van de autoriteiten. Hij had ondertussen ook wat aangenamere mensen leren kennen op de IRC-netwerken. “Die werkten aan Metasploit en aan Kali, software voor penetratietesten. Zij gebruiken het hacken om mensen te helpen. Kijk, alle hackers doen nog wel eens iets wat niet mag, maar dat doen ze om te leren. Bij iets als Stuxnet wil ik ook het liefst in een Iraans systeem kunnen werken om te zien wat dat virus doet. Ik ben met die mensen gaan omgaan.”

Ethical hacker

Ondertussen volgde hij ook nog een opleiding. Eerst het VMBO en toen een jaar MBO programmeren/netwerkbeheer. Dat hield hij een jaar vol. “Ik ben maar werk gaan zoeken, want ik moest daar als eerstejaars de vierdejaars lesgeven in Linux.” Hij werkte in een reparatiecentrum – waar hij om zijn productie op te voeren een botnetje bouwde – en later in een computerwinkel. Een baan als IT-beveiliger kon hij niet krijgen omdat hij geen diploma’s had. Toen leerde hij zijn ‘goede’ hackersvrienden pas echt kennen. “Via IRC kende ik een docent van het SANS Institute, dat toen in Nederland een cursus gaf van vijf dagen. Ik mocht die cursus doen op zijn kosten. Een ander betaalde mijn reiskosten. En ik ken ze alleen van de computer! Dit was voor mij het bewijs dat dit groepje hackers heel anders was; zij helpen elkaar. Ik doe nu ook dingen terug, bijvoorbeeld als vrijwilliger bij Attack Research, een Amerikaans bedrijf dat onderzoeken doet na aanvallen. Ik help hen als ze iets nodig hebben. We helpen elkaar.”

In 2010 trad hij in dienst bij de Security Academy als ethical hacker. Hij is nu de man achter het ethical hacking-portfolio van de opleider: een tweedaagse, een driedaagse en een vijfdaagse cursus. “Het gebrek aan kennis is enorm. Dit leer je niet op school. Ervaring doe je alleen op in de praktijk.” De Brouwer heeft het uitgerekend: hij stak er van zijn 15e tot zijn 20e zeker 25.000 uur in. Elke dag zat hij zeker 15 uur achter zijn systemen en dat vijf jaar lang. “Ga dat maar eens in de baas zijn tijd doen. Je kunt nooit zo goed worden met alleen wat cursussen.”

Je kennis en ervaring bouwde je op in die 25.000 uur. Hoe blijf je nu bij?

“Dat is lastig. Bepaalde contacten heb ik afgesloten. Voor een baan als ethical hacker is een verklaring van goed gedrag essentieel. Ik kan dus niets verkeerds doen. Maar ik hoor nog wel eens wat hier en daar en daarmee blijf ik anderen een stapje voor.

Ook lees ik de nieuwsberichten, volg soms wat fora, vooral de publieke. Kwetsbaarheden als Heartbleed probeer ik zo veel mogelijk uit op geïsoleerde systemen zodat ik weet hoe het werkt.

Daarnaast is er wel wat tijd om het hacken bij te houden, maar ik kan bepaalde dingen niet meer zo volgen als vroeger – ik wil het ook niet meer zoals vroeger. Ik ontwikkel nu lesmateriaal en doe pentesten. Ik heb er voor gekozen om mijn kennis met anderen te delen en uitsluitend ethical hacker te zijn.”

Wat merk je nog van de zwarte kant van het hacken?

“Er wordt onderling tussen hackers veel gedreigd, maar dat is stoerdoenerij achter het toetsenbord. Ik houd niet van ruzies. Ik blijf daar van weg. Ook breken ze in en dat is strafbaar. Het is een grens die snel is overschreden. Ik krijg vooraf overal toestemming voor en bij elke pentest krijg ik een vrijwaringsverklaring, zodat ik niet verantwoordelijk kan worden gesteld als de boel bij een klant wordt platgelegd.”

Is het grote geld aan de zwarte kant niet verleidelijk?

“De bounty’s van bedrijven als Google zijn ook heel goed. Goed voor je imago, hun imago en voor de beveiliging. Ik ben niet op zoek naar lekken om die te kunnen verkopen. En zou ik er één vinden. dan zou ik die niet verkopen aan de onderwereld. Ik heb een gezin. Het is interessanter voor mij om een lek aan een partij als Google te verkopen, want dat helpt me verder in mijn carrière.

Ik ben lang geleden wel grenzen over gegaan, maar daar heb ik van geleerd. Dankzij die kennis lig ik een stap voor op de gemiddelde pentester. Mijn praktijkervaring zorgt ervoor dat ik dingen sneller zie. Een collega zei ooit: in de tijd dat ik één kwetsbaarheid vind, heeft Patrick er al drie gevonden.”

Hoe ga je te werk bij een ethische hack?

“Aan mijn opdrachtgevers vraag ik altijd wat volgens hen het ergste is dat zou kunnen gebeuren. Dat is dan mijn doel. Dát wil ik dan voor elkaar krijgen. Het is mijn evil mindset uit het verleden en die maakt mij effectiever dan wanneer ik volgens het boekje werk.

Eigenlijk gaat er geen pentest voorbij zonder een leuk resultaat. Soms lijkt alles goed op orde bij een pentest. Daar kan ik dan niet tegen. Ik heb in die situaties wel eens succes gehad met een ARP-poisoningaanval. Daarbij loopt al het verkeer via mij voordat het zijn daadwerkelijke doel bereikt. Zo zie je op de transportlaag binnen vijf minuten een niet-versleuteld wachtwoord voorbij komen.

Mijn insteek is dat ik een mens, een applicatie of een systeem iets kan laten doen waar het niet voor is bedoeld. Ik blijf er zo lang tegenaan schoppen dat het omvalt, dat ik het kan kantelen om ermee te doen wat ik wil. En lukt het niet op de digitale manier, dan ga ik mailen of bellen. Er is altijd wel iets te vinden. Ik blijf het leuk vinden om ergens binnen te komen, maar het geeft me nu vooral een kick om iemand te helpen zijn systeem veiliger te maken.”

Waar ben je als ethisch hacker het meest trots op?

“Ik ben trots op de cursussen die ik heb neergezet en de strategische samenwerking tussen de Security Academy en EXIN, die hebben geleid tot het Ethical Hacking Foundation-examen wat gebaseerd is op mijn cursussen. Een training heeft blijvende gevolgen en is ook beter voor mijn naamsbekendheid. Een pentest laat veel minder achter. Als het klaar is, is het klaar. Een pentest moet altijd stilgehouden worden. Er is veel dat je niet mag laten weten.”

Altijd maar lekken vinden, nooit eens een super beveiligd netwerk dat niets doorlaat. Maakt je dat niet moedeloos?

“Welnee. Ik vind wel dat ethical hackers meer bewustwording moeten creëren. Gooi je USB-sticks door de gang, dan blijven mensen die oprapen en gebruiken. Ook sticks die je systeem doorbranden en dus fysiek vernietigen. Ja, die zijn er ook, maar daar denkt niemand aan.

Ook zie je in de trein mensen die een sticker op de webcam van hun camera hebben geplakt. Maar om daar misbruik van te maken, moet iemand eerst toegang tot je systeem hebben. En die persoon die die camera afplakt heeft 10 tegen 1 al jaren hetzelfde wachtwoord... Persoonlijk vind ik het spannender dat ze mijn rekening kunnen plunderen dan dat iemand me in mijn onderbroek voor mijn computer ziet zitten.” «

Patrick de Brouwer is als docent verbonden aan de Security Academy (www.securityacademy.nl). De Brouwer verzorgt de afsluitende bijeenkomst van de **Masterclass Security-Business Alignment 2.0** van AutomatiseringGids, Nyenrode Business Universiteit en Security Academy.
In zes bijeenkomsten praten specialisten op dit terrein u in deze Masterclass - tussen 6 maart en 11 april - bij over wat u anno 2016 moet weten van security.

Meer informatie: **www.ag-events.nl**