Verantwoorde onthulling #11

Beg en de Bug Bounty

Laatst was ik bij een bijeenkomst over de toekomst van het cybersecurity onderwijs. Een hoogleraar begon met de bekende klaagzang: te weinig studenten, leraren te oud en verkokering van academische specialismen. De oplossing: meer samenwerking met bedrijven, multidisciplinair en iets leuks met jongeren. Daar zullen we het allemaal wel mee eens zijn. Maar wat te doen met briljante jonge hackers, die op de een of andere manier het vwo zijn misgelopen en de sector zeker veel te bieden hebben? Is er een soort zijinstroom programma?

Nee, dergelijke moeilijke materie moet je wel op niveau behandelen volgens de hoogleraar. Liefst universitair. Aan de hbo wordt gewerkt, maar dat loopt nog wat moeilijk. Een van de weinige hackers in het gezelschap riep enthousiast: doe iets met hackerspaces, daar ligt zoveel kennis en dat vinden jongeren leuk! Iedereen keek haar glazig aan: “Hackerspaces, waar zijn die dan?” Zucht. Lieve mensen: H4ck3rs z13N d3 d1ng3N v44k g3w00N N3t 13ts 4Nd3rs d4N 4Nd3r3N. Moeite met deze zin? Lees dan vooral even door, want dit is vooral belangrijk voor gewone security specialisten als jij.

In mijn onderzoek naar ethisch hackers komt ik vaak dit levensverhaal tegen: slechte cijfers ondanks uitzonderlijke intelligentie, dan maar naar het vmbo, misschien nog een mbo certificaat of een cursusje erachteraan, gevolgd door een stage. Dan ineens gebeurt het: bingo, ze zijn de bink want het blijkt dat niemand computers zo goed begrijpen zoals zij. OK, er zitten jongens bij met ADHD of Asperger. Vooral dyslexie komt vaak voor. Maar eigenlijk zijn dit vooral labels vanuit een maatschappij die niet weet wat ze aan moet met mensen die anders denken en hen daarom maar pathologiseert. Volgens mij hebben ze niet iets tekort, ze hebben juist iets extra’s en dat komt pas op latere leeftijd echt goed aan het licht.

Hier een voorbeeld: @smiegles, ook wel Olivier Beg. Hij is net 18 jaar geworden en nummer 1 in de Hall of Fame van Yahoo. School ging niet makkelijk vanwege zijn dyslexie en hij vond de lesstof verre van interessant. Dus werd hij naar het vmbo gestuurd. Daar ging hij tijdens de les zitten hacken, vooral uit verveling en omdat de school een snelle internetverbinding had. Als hij beveiligingsproblemen in het schoolnetwerk ontdekte, meldde hij dat netjes. Verder zei niemand er wat van als hij tijdens de les op zijn laptop werkte. Ook zijn ouders begrepen niet echt wat hij deed, maar lieten hem zijn gang gaan.

Tijdens ons gesprek kom ik erachter dat hij een van de melders was tijdens Lektober, de maand oktober 2011 waarin Webwereld elke dag een lek meldde. Ik zal niet zeggen welk lek, want hij bleef toen, net als de meeste melders, liever anoniem. Wel weet hij me vertellen dat het CMS van Webwereld zelf niet helemaal veilig was. Hij ontdekte namelijk dat hij via Cross- Site Forgery de account van de journalist kon overnemen. Het zou best grappig zijn geweest als hij dan namens die journalist een artikel op de site had gezet, maar hij was volwassen genoeg om dat niet te doen. Hij was toen dus nog maar 14 jaar.

In de jaren daarna treedt Olivier steeds meer naar buiten met zijn meldingen en dat zijn er heel wat. Zo’n beetje alle grote Nederlandse banken: ABNAmro, ING, SNS, RABO, ASN,

Regiobank, Van Lanschot bank. Meestal kreeg hij wat VVV bonnen en een spreekverbod. Bij de Telco's had hij ook veel onthullingen. Upc, Ziggo en KPN namen zijn meldingen netjes in ontvangst, zonder beloningen te geven. Bij XS4all kreeg hij nog wel een appeltaart. Zijn melding bij T-mobile is nog echter nog steeds onbeantwoord.

Hij ontdekte ook kwetsbaarheden bij de Nederlandse overheid, bijvoorbeeld op de site van de Belastingdienst. Daar bleek een oude Adobe Flash Player te draaien waar je een XSS zou kunnen doen. Deze videoapplicatie werd bovendien gebruikt bij verschillende andere overheidssites, waaronder ook het NCSC. Hij meldde het daarom bij het centrum. Het was zondagavond 22.50, kreeg een reactie om 23.10 en zag dat het om 23.30 gefixed was. Ook bij de Belastingdienst. Opmerkelijk, want zo'n vlotte reactie verwacht je niet van de overheid. Als dank kreeg Beg een beker van de Belastingdienst, met de tekst: "I hacked the state government and never got a refund." En natuurlijk een T-shirt van het NCSC, waarvan hij er inmiddels acht heeft.

Vergeleken met de Lektober periode is er veel veranderd. Bij zowel de overheid als het bedrijfsleven is er nu beleid om verantwoorde onthullingen op een goede manier af te handelen. Sommigen reiken zelfs beloningen uit, maar dan niet te scheutig, want we zijn natuurlijk wel Hollanders. Hoe anders verging het dit jonge talent bij Yahoo. Ook daar kon hij een XSS doen en het netjes melden. Tot zijn verbazing hier geen VVV bon, T-shirt of beker, maar gewoon keiharde cash: $ 1000,- per melding. Hij deed er zeventien, dus tel uit je winst. Het Parool kopt begin dit jaar trots: "17-jarige Amsterdammer voert hackerslijsten aan". En inderdaad, bij Yahoo staat hij op 1. Maar we treffen hem ook aan in de Hall of Fame van Google, Microsoft, Nokia, Apple, Adobe, AT&T, eBay…

Als ik hem vraag of hij liever gaat voor de bounty's of zich ook nog wel wil inzetten voor het Hollandse vrijwilligerswerk, zegt hij me dat het hem eigenlijk niet zoveel uitmaakt. Hij doet het vooral voor de erkenning. Hij wil de puzzel oplossen en aan anderen laten zien. Momenteel heeft hij overigens niet meer zoveel tijd voor ethisch hacken, want hij doet al de hele dag aan informatiebeveiliging op zijn stage. Nog een paar maanden en dan is hij klaar het mbo. Wat gaat hij dan doen? Liefst een reisje door de VS om wat hackerscongressen te bezoeken. Daarna ziet hij wel verder. Hopelijk komt hij wel weer terug.

Mijn vraag aan jullie is dus: hoe houden we jongens als Olivier in Nederland? Aangepast onderwijs, een hackers gilde, bigger bounty's… Laten we beginnen met wat meer waardering voor hun werk. Bij deze.

Chris van 't Hof @cvthof
Voor meer verantwoorde onthullingen, zie www.helpendehackers.nl