Verantwoorde onthullingen #1

Hoe @legosteentje een witte hoed verdiende. Marktplaats.nl als voorloper in ethisch hacken (2012)

Marktplaats is een interessant doelwit voor hackers. De site trekt gemiddeld 1,3 miljoen bezoekers per dag en er gaat veel geld in om. Alleen al de vele inlognaam en wachtwoordcombinaties kunnen interessant zijn voor criminelen. Veel mensen gebruiken immers nog steeds één wachtwoord voor verschillende sites. De beveiliging van Nederlands grootste veilingsite wordt daarom regelmatig getest. Intern, zoals tijdens de Beer, Pizza & Hacking avonden, waar ontwikkelaars proberen de zwakke plekken in elkaars code vinden en zo te leren waar men voortaan op moet letten. En van buiten de organisatie, door hackers die gaten in de beveiliging vinden en dat op een verantwoorde manier willen onthullen. Voor hen is er een speciaal Responsible Disclosure beleid.

De initiatiefnemers van dit beleid zijn Robin Schuil (medeoprichter en Innovation Program Manager) en Bas Anneveld (Manager Site Operations). Vind je een veiligheidslek dan kun je dat dus melden en zelfs een beloning krijgen. Als je maar wel handelt volgens protocol: meld ons het lek zonder het eerst met anderen te delen, geef ons minimaal 30 dagen om het te dichten, geef de volledige gegevens en veroorzaak geen schade, etc.

Een van de hackers die erin slaagde was Pieter Vlasblom, ook wel @legosteentje, een 19-jarige scholier van het Rijn IJssel MBO. School vond hij eigenlijk maar niks. Geen uitdaging. Stage vond hij leuker. Daar werkte hij met een applicatie die automatisch advertenties plaatste op Marktplaats. Maar hij kwam er al snel achter dat hij beter zelf iets in elkaar kon knutselen, in de open-source taal Ruby. Vervolgens deed hij wat hackers van nature doen: er van alles in stoppen om te kijken wat er gebeurde. Zo zette hij in plaats van gewone tekst HTML code met JavaScript in de advertenties, oftewel Cross-Site Scripting (XSS). Het werkte. De advertentie gedroeg zich als site en @legosteentje zou zo bezoekers van Marktplaats pop-ups naar een andere site leiden.

Hij meldde 2 maart 2012 op Twitter dat hij een security probleempje had gevonden. Prompt reageerde @basanneveld: “We komen graag met je in contact indien je een bug gevonden hebt. We hebben een responsible disclosure program tinyurl.com/7orv6ap”. Pieter dacht eerst dat hij in de problemen zou komen. Maar Bas wilde vooral uitleg en ze begonnen te mailen. De site was binnen een dag weer gefixed. Pieter kreeg tot zijn verbazing 350 Euro voor zijn vondst en een pakje: een Classified White Hat in a Black Box, oftewel een witte hoed in een zwarte doos. De tegenstelling white hat – black hat komt uit oude cowboy films waar de goeden een witte hoed en de slechten een zwarte droegen. Deze term is alom bekend in de hackerwereld. @legosteentje was nu een erkende white hat hacker.

Zijn stage opdracht zat erop maar hij wilde ook niet terug naar school. Hij ging daarom op de koffie bij Bas. Of hij stage kon lopen bij Marktplaats. Jazeker. Vanaf juni 2012 ging hij aan de slag om een applicatie te schrijven die Marktplaats test op zwakheden: SQL injections, poortscan, XSS, etc. Een soort geautomatiseerd @legosteentje. In Ruby uiteraard. En als hij wat vindt, dan meldt hij dit meteen. Zijn stage werd in juli 2013 omgezet in een baan.

Ondertussen rommelde het in politiek Den Haag. Er bleken veel gevallen van ethisch hacken, met als bekendste voorbeeld Kamerlid Henk Krol die dossiers van “Diagnostiek voor u” had ingekeken. Het ministerie van V&J kwam daarom in januari 2013 met hun richtlijn Responsible Disclosure. De ambtenaren hadden het protocol van Marktplaats als voorbeeld genomen. Minister Opstelten werd vanuit de kringen van beleid, handhaving en bedrijfsleven geprezen voor zijn kordate optreden. Maar er was ook kritiek op de richtlijn. Zo heeft het OM alsnog de bevoegdheid over te gaan tot vervolging, ook als hacker en getroffene er onderling uit zijn gekomen. Dat bleek voor veel hackers onverteerbaar, maar is wellicht logisch vanuit het perspectief van mogelijk getroffen derden.

Dat geldt dus ook voor de klanten van Marktplaats. Toen Schuil zijn verhaal over @legosteentje op 26 maart 2013 presenteerde tijdens een bijeenkomst van Deloitte, kreeg hij weerwoord van juriste Annika Sponselee. “Stel dat een van jullie klanten zich aangetast voelt in zijn privacy, omdat jullie hackers uitlokken? Die zou een zaak kunnen beginnen.” Daar wist Robin niet echt een antwoord op. Maar ja, het gebeurt toch wel en dan kun je dat beter goed doen. @legosteentje gaat in ieder geval door, ook buiten zijn werk. Laatst heeft hij Spotify ge-cross-script. Ook dat leverde hem een mooi pakket met goodies op.

Beleid en richtlijnen voor ethisch hacken kunnen helpen, maar de praktijk blijkt toch altijd weerbarstig. Daarom vanaf heden deze column. Volgende aflevering in *verantwoorde onthullingen*: “A man in the middle of money and media. ING weigert ontwerpfouten te erkennen in de Mobiel Bankieren app”

Chris van ’t Hof www.cvth.nl

Bronnen

Interview met Pieter Vlasblom 5 augustus 2013
Seminar “Security Intelligence 2013” van Deloitte in De Beukenhof 26 maart 2013
RD policy: http://statisch.marktplaats.nl/help/responsible_disclosure_policy_en.html