Verantwoorde onthullingen #8

Toen @iliaselmatani een studieboek kocht, kreeg hij er 1643 gratis. Authorisatie Infinitas Uitgeverijen makkelijk te omzeilen

Deze aflevering van Informatiebeveiliging gaat over de beleving van de hacker. Eigenlijk gaat deze column daar altijd wel over, dus deze keer een aspect dat nog onvoldoende belicht is: je moet als verantwoorde hacker vooral heel veel geduld hebben. Zo ook @iliaselmatani die maar liefst een jaar moest wachten totdat een ogenschijnlijk eenvoudige fout in de site van Noordhoff Uitgevers werd gedicht. Waarom? Ze hadden het al zo druk met andere dingen…

Alweer een jaar geleden zag ik op Twitter een uitnodiging voorbijkomen van een zogenaamde #fristileaks. Dat is de jongeren variant van #wiskyleaks, een open informele bijeenkomst waar hackers onder Chatham House rules hun geheimen delen. Oftewel: je mag alles doorvertellen, als je maar niet zegt van wie je het hebt. Naast dat het altijd wel leuk is jonge hackers te ontmoeten, had ik een doel: minstens een goede case voor mijn onderzoek naar Responsible Disclosure. Ik dus daar naartoe.

Aan het einde van de avond realiseerde ik me dat ik vooral zelf vanachter een groot glas Triple aan het woord was geweest. Ik weet niet of de verlegen jongens – en een meisje – met hun Fristi's zich hadden vermaakt met de praatgrage onderzoeker, maar ik had gefaald: geen interessante onthulling. Jammer. Onderweg naar de trein komt echter @iliaselmatani naar me toe. Hij beweert dat hij alle boeken van Noordhoff Uitgevers zomaar kan downloaden. El Matani had dit al eerder willen onthullen via Webwereld, maar die hadden het laten liggen. Of ik wilde bemiddelen tussen hem en de uitgever. Graag.

De volgende dag krijg ik een mail met uitgebreide documentatie. Ilias schrijft dat hij voor zijn studie een online boek had aangeschaft bij Noordhoff. Je logt dan in met een (voucher) code en kan er dan online in bladeren. Pagina's opslaan kan niet. Dat is best lastig als je bijvoorbeeld in de trein wilt lezen. Hij ontdekt echter dat de pagina's steeds geladen worden vanaf een url die eindigt op "page" met een nummer erachter. Als hij nummer handmatig aanpast krijgt hij een foutmelding. Hm, dat zou ook te eenvoudig zijn.

Als hij in de cache van zijn Firefox browser kijkt, ziet hij dat de inhoud van de pagina steeds geladen wordt vanaf een andere url. Als hij hier een van de nummers verandert komt hij wel gewoon uit bij de gevraagde pagina. Maar het boek heeft ook een nummer zo te zien. En als hij dat veranderd…jawel, komt er een ander boek tevoorschijn. Hij heeft zo dus toegang tot alle boeken van deze uitgever. Ilias laat zijn bevinding zien aan @sander2121. Samen schrijven ze een script in Python waarmee de urls automatisch worden aangepast. En ja, het werkt. Maar aan losse pagina's in SWF formaat heb je ook niet zoveel, dus het script zet ze netjes op volgorde achter elkaar in pdf. En zo zouden ze dus maar liefst 1643 boeken kunnen downloaden.

Wat zou jij doen als je zoiets ontdekt? Ikzelf zou het meteen aan mijn medestudenten doorgeven en zo iedereen trakteren op gratis boeken. @iliaselmatani en @sander2121 niet. Ze willen de slechte beveiliging op een verantwoorde manier melden. Maar hoe zal die uitgever reageren? Zal hij aangifte doen? Ze besluiten het via de media te doen en sturen

hun melding op 21 april naar Webwereld. Daar wordt het echter niet opgepakt en daarom komt Ilias nu bij mij.

Best spannend, zo'n uitgever benaderen dat hun site lek is. Er zijn dan wel geen persoonsgegevens gelekt. Je zou zelfs kunnen stellen dat systematisch urls afgaan niet gezien kan worden als hacken. Maar toch, ze zouden een zaak kunnen starten - alleen al om ons af te schrikken. De uitgever zou immers een flinke reputatieschade kunnen oplopen door deze onthulling. Het miljarden investeringsbedrijf Bridgepoint achter deze uitgever, heeft hoogstwaarschijnlijk een flinke batterij aan advocaten klaar staan om ons het leven zuur te maken – ook als ze geen zaak hebben. Ik begin daarom met een voorzichtig mailtje waarin ik het lek meld en me aanbiedt als bemiddelaar tussen hun en de hacker.

Binnen een dag krijg ik een reactie van Jean Pierre Miani, Technology Officer bij Infinitas Learning. In de CC zie ik nog drie mensen van de technische afdeling. Mooi. Hij zegt de melding zeer serieus te nemen en vraagt met spoed om aanvullende informatie. Even bellen dan maar. Ik vertel Miani over de urls en de boeken. "Oh, dat. Nou, dat is geen hacken toch? Hebben we in april al gehoord en dat is nu gefixed. Is dit nu weer diezelfde jongen?" Dat wil ik natuurlijk niet zeggen. Infinitas kan alle details krijgen, maar eerst moeten ze via een PGP gesigneerde mail beloven niet tot vervolging over te gaan. Miani reageert geërgerd: "Nee, ik ga geen vrijbrief geven."

Ilias is onaangenaam verrast. "Tsja, hier gaan mijn nekharen van overeind staan. Het is inderdaad geen hacken, eerder ongeauthoriseerde toegang. Maar als je dit op Twitter gooit kunnen ze de tent wel sluiten. Dat scriptje heeft me twee uur gekost en zelfs met een gewone verbinding kun je in een nachtje alle boeken downloaden. Kun je je eigen uitgeverij beginnen." Hij begrijpt ook niet hoe de melding al bij hun is gekomen. Ze hebben dit nog met niemand gedeeld, ook niet bij #fristileaks. Vervolgens kijkt hij even op de site van Noordhoff. Nee, het lek is nog niet gedicht. Wat volgt is een langdurige woordenwisseling tussen Ilias en Jean Piere, via mij.

Als we er niet uitkomen besluit ik voor te stellen elkaar dan maar te ontmoeten zonder vrijwaring. Ilias is gelukkig bereid het risico te lopen. Jean Pierre draait bij: "Ik vind dat white hat hackers beloond moeten worden, kan er zelf ook van leren." Op 6 januari sta ik samen met Ilias in het kantoor van Infinitas in Houten. De Technology Officer steekt direct van wal. Security is zijn hoogste prioritiet. Als educatieve uitgever hebben ze vaak aanvallen te verduren van scholieren die vanuit school proberen te hacken en DDoS aanvallen lanceren. Ze verzamelen daarom een minimum aan persoonsgegevens met het idee: als je ze niet hebt, kun je ze ook niet kwijtraken. Het abonnement waarmee je de boeken kunt inzien is dan ook alleen maar een nummer.

Ze hadden dus al in april gehoord van het lek, via een leverancier van hun. Maar om het te dichten moest wel het hele systeem op de schop. En als educatieve uitgever moet alles in juni goed draaien, want dan schaffen de scholen de nieuwe uitgaven aan. Je kunt dan niet het hele systeem omgooien. De aanpassing zou worden meegenomen in het groot onderhoud, maar toen werd het druk en verdween het probleem weer naar de achtergrond. Zo spannend is het niet, dat iemand een pagina kan downloaden, vindt de uitgever. En nee, er is daarom geen enkele reden om een rechtszaak tegen ons te beginnen.

Ik opper dat Ilias ook zijn tool aan andere studenten had kunnen geven en er dan veel meer boeken gratis zouden worden gedownload. De auteurs lopen dan hun royalties mis en zouden die op Infinitas willen verhalen. Volgens Jean Pierre leven niet al hun 6000 auteurs van royalties, maar ze zouden inderdaad een zaak kunnen starten. “Hoe dan ook”, stelt hij trots, “er wordt aan gewerkt en de nieuwe versie wordt binnenkort uitgerold.” “Mag Ilias het dan testen?” opper ik enthousiast. Jean Pierre twijfelt: “Eh, nu nog niet, we zijn er nog mee bezig. Geef ons nog en paar weken. Ik zal wat documentatie sturen waar hij naar kan kijken”.

De weken worden maanden, zonder bericht van Infinitas. Ilias heeft het inmiddels gehad met de trage uitgever, maar ik wil natuurlijk wel mijn stukje publiceren. Ik wacht daarom maar tot de truuk met de urls niet meer werkt, anders zou deze onthulling ook niet erg verantwoord zijn. Het is inmiddels juni en jawel: de geconstrueerde links leiden slechts naar dode pagina’s. Blijkbaar is het Jean Pierre toch gelukt. Op de home page staat trots: “Infinitas Learning re-affirms market leadership by launching e-book platform Classmate".

And what’s new? De inmiddels 2000 boeken zijn nu eindelijk ook te downloaden - mits je een voucher hebt gekocht natuurlijk - zodat je ze off line kunt lezen. Niet dat @iliaselmatani daar nu nog wat aan heeft, want hij is inmiddels klaar met zijn opleiding. Hij werkt nu als security specialist bij Securelabs en krijgt, net als de uitgever, eindelijk gewoon betaald voor zijn werk.

Chris van ’t Hof, @cvthof
De voorgaande case studies zijn te vinden op www.cvth.nl/vo