Verantwoorde onthullingen #5

DongIT en het DigiD debacle. Ethisch hacken als businessplan

De meeste ethische hackers die ik spreek doen onthullingen vanuit een mengeling van maatschappelijk belang en individuele kick. Maar vaak volgt ook een zakelijk profijt: de hacker heeft zijn kunnen getoond en kan aan de slag als penetratie tester. Zo ook Wouter van Dongen. Sinds hij diverse lekken bij gemeentewebsites heeft onthuld, runt hij zijn eigen IT security bedrijf aan de Schipholweg in Leiden: DongIT B.V. Daarom aan hem de vraag: is ethisch hacken ook een interessant businessmodel?

Wouter studeerde Systems- en Networkengineering, deed daarnaast aan webontwikkeling en werkte bij het NFI en Fox-IT. En zoals zoveel hackers, haalde hij al vanaf zijn puberteit gekke dingen uit met websites. “Het is de drive om zaken te manipuleren, terwijl ik niet altijd wist wat ik aan het doen was.”, aldus Wouter. Maar, hij heeft het liever niet over zijn jeugdzonden, hij is nu een serieus bedrijf. Die loopbaan begon in 2011 dankzij een kennis die bij een gemeente werkte en net een nieuwe site had. Welke gemeente dan? Dat zegt hij niet. Een van zijn ethische codes is namelijk: noem geen bedrijven of overheidsorganisaties bij naam. “Het gaat mij er niet om mensen of organisaties zwart te maken. Ik wil laten zien dat iedereen fouten maakt en ik vind het belangrijk dat mensen er van leren zodat de digitale veiligheid stap voor stap wordt verbeterd. Dat is mijn doel.”

OK, gemeente X had dus een nieuwe site. De kennis was er erg enthousiast over. Totdat Wouter liet zien dat hij binnen een half uur overal bij kon. Hij deed een SQL injectie op een zelfgemaakte extensie, kon inloggen bij de backend en kwam zo in allerlei mailsystemen en databases. Hij zag ook dat het Content Management Systeem – waarvan hij de naam ook liever niet noemt - allerlei onveilige default instellingen had: wachtwoorden in plain tekst, geen secure cookies, etc. De gemeente zat toevallig in een gebruikersvereniging van nog veertig gemeenten die hetzelfde systeem gebruikten. De vereniging vroeg Wouter of hij een presentatie over webbeveiliging wilde houden om meer bewustwording te creëren onder de gemeenten.

Dat was een mooie gelegenheid om zijn kunnen te tonen. In overleg met de gebruikersvereniging kreeg Wouter toestemming om praktische voorbeelden bij de aangesloten gemeenten te zoeken voor de presentatie. “Geen saai theoretisch verhaal over beveiliging, maar mensen confronteren, wakker schudden en een oplossing bieden”. Wouter schreef een script dat automatisch alle gemeenten testte op de gevonden zwakheden. Hij bracht alle websystemen in kaart, ook verborgen systemen, testsystemen en welke databases, services en versies erop draaide.

Zo kreeg hij toegang tot de backend van tientallen CMS’en, mailsystemen en honderden databases van raadsinformatiesystemen en gemeentewinkels. En duizenden persoonsgegevens van burgers met wachtwoorden. Bij sommige sites kon hij zelfs DigiD sessies overnemen middels Cross Site Scripting (XSS) en het afvangen van cookies. Dit alles kostte hem nog geen week werk. “Het is best leuk om zo’n script te schrijven, maar waarom doen ze dat niet centraal voor gemeenten, bijvoorbeeld via de VNG?”

Zijn presentatie was op 29 september. In de aanloop daar naartoe werd hij al diverse keren benaderd door gemeenten die wilden checken of ze genoemd zouden worden. Een leverancier van gemeentelijke systemen en een gemeente stuurden zelfs advocaten op hem af. Hij ging daarom voorzichtig te werk. Hij had veel screenshots van kwetsbaarheden, maar zorgde ervoor dat de namen van gemeenten, systemen en gebruikers niet te lezen waren. Wachtwoorden waren natuurlijk ook geblurd.

Het verhaal viel goed. “De sfeer kwam meteen los. Het publiek was geboeid en stelde goede vragen”. Wouter liet ook zien welke standaardinstellingen in hun CMS ervoor zorgen dat de wachtwoorden makkelijk te kraken zijn. Hoe hij de DigiD sessies kon onderscheppen, begrepen ze echter niet helemaal. Hij kreeg daarom veel vragen van de gemeentelijke systeembeheerders of hij hun ook even wilde doorlichten. Tevreden ging Wouter naar huis.

Wouter was ondertussen ook benaderd door journalisten, onder andere van Nieuwsuur. De uitzending van 1 oktober begint met onheilspellende muziek. De voice-over zegt: “Wouter van Dongen is veiligheidsexpert en dringt binnen op een gemeentewebsite. Hij gebruikt Cross Site scripting” [1] Hij wilde niet zeggen welke gemeente, maar de journalist weet te vertellen dat het gaat om Amsterdam en stelt dat het geen incident is maar past in een lange reeks ICT blunders bij de overheid. Zelfs Diginotar wordt erbij gehaald.

Vervolgens komt journalist Brenno de Winter in beeld: “Het blijkt dat er zoveel privacygevoelige informatie wordt gelekt, dat we elke dag wel kunnen vullen met een voorbeeld. En dat gaan we komende maand ook eens doen.” Hij had al eerder contact met Wouter en zijn bevindingen waren een mooie start van Lektober, waarin Webwereld een maand lang elke dag een lek meldde. Lek 1: “Blunder Logius maakt DigiD fraude kinderspel” [2] Wouter was niet blij met dit alles, want hij wilde geen namen noemen.

Logius is de Dienst Digitale Overheid van Binnenlandse Zaken, oftewel de IT-ers achter DigiD. Die waren uiteraard ook niet blij met de beschuldiging en namen direct contact op met Wouter. Of hij zijn bevindingen over kwetsbaarheden bij gemeentesites ook daar wilde presenteren. “Als je techneut bent is XSS niet zo moeilijk, maar ik las daar in de implementatierichtlijnen van DigiD niks over. Dus ik had wat tips over http-only cookies, de webserverinstellingen en vulnerabilityscans enzo. Ik was ook wel verbaasd dat ze allemaal druk zaten te schrijven, want wat ik liet zien was toch echt laag hangend fruit.”

Als ik Logius mijn stuk toestuur, krijg ik de volgende reactie. “De fout lag bij de webdiensten van de gemeenten en niet bij DigiD. Dit is in een gesprek op 5 oktober bij Logius bevestigd door DongIT. Nadat een burger met zijn DigiD is ingelogd kon door de lekken aan de kant van de gemeenten de opgebouwde sessie van de webdienst met de burger worden overgenomen.” Bovendien vinden ze dat Logius niet verantwoordelijk is voor de beveiliging van webdiensten die op DigiD aansluiten. “De dienstaanbieder blijft altijd zelf verantwoordelijk voor de veilige en correcte werking van de systemen die op DigiD aansluiten. De implementatierichtlijn (Checklist Testen) is niet bedoeld als norm voor informatiebeveiliging.” Niettemin nam de dienst destijds direct actie: 30 gemeenten die onvoldoende beveiligd bleken werden afgesloten van DigiD.

De kwestie liep zelfs hoog op in de Tweede Kamer. Kamerleden eisten ingrijpen van de minister van Binnenlandse zaken. Donner en later ook zijn opvolger Spies kwamen met maatregelen. De minister verplichtte de gemeenten een ICT-Beveiligingsassessment DigiD te doen, compleet met een audit en penetratietest per aanwezige DigiD-koppeling. Het Kwaliteits Instituut Nederlandse Gemeenten kreeg opdracht een impactanalyse uit te voeren bij de gemeenten. Samen met de VNG richtte het instituut een Informatiebeveiligingsdienst (IBD) voor gemeenten op, dat per 1 januari 2013 van start ging.

Tegen die tijd vindt Wouter het een goed moment om te kijken hoe het ervoor staat bij de gemeenten en hij laat zijn scan over alle gemeentesites gaan. Hij concludeert: “24% van alle gedetecteerde gemeentelijke systemen kan mogelijk beïnvloed worden door de kwetsbaarheden met een hoge of kritische impact rating. De verouderde software op deze systemen zou relatief eenvoudig misbruikt kunnen worden door kwaadwillenden. Het onderzoek toont aan dat de huidige inspanningen om gemeentelijke systemen te beveiligen nog niet afdoende effect hebben gehad.” [3] IBD neemt de melding uiterst serieus, gaat er meteen mee aan de slag, al komen ze naar eigen zeggen tot een iets gematigder conclusie.

Aldus, er is nog veel werk te verrichten bij de gemeenten, maar de bewustwording en zelfs verplichting om meer aan digitale veiligheid te doen is er. Mede dankzij de vrijwillige inzet van DongIT. Maar, is ethisch hacken voor hun nu wel een interessant businessmodel? Eigenlijk niet. Hij werd naar aanleiding van onderzoeken en publiciteit wel vaak benaderd door gemeenten. Dan wilden ze weten of hij ook bij hun lekken hadden gevonden. Vaak wordt er negatief en defensief gereageerd op hun bevindingen. “En dat terwijl de aangetoonde kwetsbaarheden juist behulpzaam zijn bij het verbeteren van de digitale veiligheid van gemeenten en de overheid als geheel.’’ Al met al heeft de hele zaak hem vooral veel tijd gekost, af en toe enkele zorgen opgeleverd, maar ook een leerzame start-up van zijn bedrijf gegeven.

Wouters personeel richt zich nu vooral op bedrijven. Naast veilige web ontwikkeling en uitgebreide pentests biedt hij ook gratis scans aan waarvan het rapport en de details achteraf gekocht kunnen worden. En dat loopt goed. Gemeenten zijn weliswaar verplicht security audits te doen, maar die “worden ingepalmd door het sales apparaat van de grotere partijen, die zetten dan voor veel geld een net afgestudeerde HBO’er aan het pentesten”, aldus Wouter. Die consultants noemen zich vaak ethisch hacker. Maar zo heel erg ethisch is dit eigenlijk niet, want het gaat toch vooral om het binnenhalen van projecten. Kortom, van echt ethisch hacken word je niet rijk, maar het is wel leerzaam.

Volgende aflevering in *Verantwoorde onthullingen* #6: Dismantling Megamos. Hoe Volkwagen de Radboud publicatie over gekraakte autosleutels tegenhield.

Chris van ’t Hof www.cvth.nl

Bronnen:

Interview met Wouter van Dongen 10 oktober 2013
e mail correspondentie met Sonja Kok van KING en Michiel Groeneveld van Logius.
[1] http://nieuwsuur.nl/video/277858-kunnen-hackers-de-overheid-helpen.html
[2] http://webwereld.nl/beveiliging/54887-lek1-blunder-logius-maakt-digid-fraude-kinderspel
[3] https://www.dongit.nl/softwareversies-van-gemeentelijke-websystemen-kaart-gebracht