Verantwoorde onthullingen #9

Te goedkoop voor security? @1sand0s vindt geen gehoor bij de Youfone helpdesk

Als ik naar een bijeenkomst ga waar ook hackers zijn, dan gooi ik er meestal even een tweet uit: “Nog tweeps aanwezig?” Zo kom ik aan cases voor deze column. 28 april was er weer zo’n bijeenkomst: #hackdetoekomst @De_Zwijger. Diverse bekenden reageren op mijn tweet. Zo ook @1sand0s, die ik die avond zie in de bar van Pakhuis de Zwijger. Hij heeft een zwart T-shirt aan met de tekst “I hacked my ISP and all I got was this lousy shirt”. Dus ik roep: “He, heb jij een ethische hack op je naam?” Inderdaad. Hij kon bij zijn telecomprovider Youfone vrij eenvoudig accounts overnemen en heeft dit gemeld. Niet dat hij van hun dit T-shirt kreeg. Dat is van het NCSC, zoals te zien is aan het logo op zijn mouw.

@1sand0s is volgens zijn Twitter profiel “researcher and teacher on the arts moving of 1s and 0s (preferably securely and privately) — RCX”. Het blijkt te gaan om Jeroen van der Ham van de UvA. Hij studeerde en promoveerde daar en was er vier jaar Post Doc. Nu is hij onderzoeker en docent System and Network Engineering en begeleidt ongeveer 35 studenten in hun onderzoek. Die doen natuurlijk veel verantwoorde onthullingen, dus heeft hij met twee collega’s nu een ethische commissie opgericht die de onderzoeken toetst. Ze kijken al bij de opzet van het onderzoek hoe de studenten omgaan met gevoelige persoonsgegevens en of hun onthulling verantwoord is. Elk onderzoek wordt voorzien van een risico classificatie, voor adequate begeleiding. Dat gaat over het algemeen goed.

Deze onthulling niet. Die kwam ook niet uit de opleiding, maar uit zijn persoonlijke omgeving. Zijn vriendin heeft namelijk een mobiel abonnement bij Youfone. Als ze oktober vorig jaar op haar persoonlijke pagina wil inloggen lukt dat niet. Ze probeert een nieuw wachtwoord aan te vragen, maar de site herkent haar e mail adres niet. Of Jeroen er even naar wil kijken, het is immers zijn werk. Maar het lukt hem ook niet het wachtwoord aan te passen. Vreemd. Zelf heeft hij ook een Youfone abonnement, dus hij probeert of hij bij zijn eigen account wel een nieuw wachtwoord kan instellen. Dat lukt wel.

Tot zijn verbazing ziet hij dat hij zijn e mail niet hoeft te verifiëren en er een wachtwoord wordt gegenereerd dat bestaat uit zijn postcode en huisnummer. Als je dus het e mail adres en postcode van een andere Youfone gebruiker hebt, kun je dus zo een account overnemen. Vervolgens kun je het abonnement aanpassen, het rekening nummer zien, hoeveel er gebeld is en ook met wie en wanneer… Hij graaft wat dieper in de browser en ziet dat de communicatie niet versleuteld is en de interactie plaatsvindt met een sessie cookie. Dat betekent dat je er tussen kan gaan zitten en wachtwoorden af vangen. Dit is wel een hele reeks standaard security fouten.

Hij stuurt daarom meteen een mailtje naar de Youfone klantenservice. Vanaf zijn werkadres, want dan weten ze meteen dat ze hier te maken hebben met iemand die er verstand van heeft. Geen reactie. Dan maar openbaar. @1sand0s tweet aan @youfone: “Ik heb via contactformulier een bericht gestuurd, maar nog geen reactie. Het is best ernstig en zou zsm antwoord willen zien!”. Dan volgt wel een reactie: “Beste Jeroen, je krijgt binnen maximaal 5 werkdagen een reactie op je ticket. Stuur je 06 nummer in een pb, dan kijken wij alvast wat er aan de hand is.” In de discussie die volgt via de DM, stelt de helpdeskmedewerker dat het lek niet echt een probleem is. Jeroen vraagt of hij het aan de media kan melden. Hij doet maar…

Dan maar naar het NCSC. Het is inmiddels vrijdagavond. Jeroen weet dat hun response team ook in het weekend werkt, maar dan alleen op de meest urgente meldingen reageert. Maandag krijgt hij een reactie. Het centrum ziet dit niet als haar primaire verantwoordelijkheid, maar omdat er ook burgers getroffen kunnen worden willen ze wel helpen. Een medewerker meldt dat Jeroen het beste

contact kan opnemen met de directie secretaresse en geeft hem haar e-mail adres. De secretaresse reageert op de mail dat ze ernaar zullen kijken. Als hij woensdag nog geen reactie heeft, mailt hij nogmaals…

Ondertussen benadert Jeroen de bouwer van de site, maar die reageert geïrriteerd: “je moet ons niet lastig vallen, dit is iets wat Youfone zelf moet oplossen”. Hij benadert ook verschillende journalisten die wel eens onthullingen hebben gedaan, maar die tonen geen interesse. Jeroen: “Zo’n melding is blijkbaar niet sexy meer”. Dan maar weer wachten. Anderhalve week later heeft hij nog steeds geen reactie van Youfone. Hij blijft via de mail aandringen om een belafspraak met de directeur. Die belt na een paar dagen zowaar zelf terug. Hij vraagt: “hoe erg is dit nou? Hoe zou je dit kunnen uitbuiten?” De directeur luister geïnteresseerd wat iemand met dit lek zouden kunnen en belooft dat de site gefixed wordt.

Dat gebeurt inderdaad. Jeroen moet het vernemen via de Youfone nieuwsbrief, waarin staat dat de site vernieuwd is, zonder vermelding van het incident of Jeroens melding. Als hij de site checkt blijkt er nog steeds geen e mail verificatie te zijn. Er wordt gelukkig nu wel een random wachtwoord gegenereerd en niet een postcode. Ook de encryptie en de sessie cookie is aangepast. Vreemd is wel dat het certificaat dat erachter hangt dateert van 22 juli 2013, drie maanden voor zijn melding. Ze hadden dus al een oplossing klaar liggen, maar om de een of andere reden niet ingevoerd.

Jeroen vond het al met al erg frustrerend. Hij is er drie weken mee bezig geweest, zonder enige reactie van hun kant. “Er moet begrip zijn voor persoon die de melding doet want die doet dat vrijwillig, zonder belang. Je zou snel afspraken moeten maken met de melder over vrijwaring van vervolg en hem op de hoogte houden van de voortgang” Hij stuurt Youfone tot slot nog een mailtje waarin hij schrijft blij te zijn dat het nu is opgelost en krijgt een kort bedankje. Dan stuurt @1sand0s 7 november zijn laatste tweet over de zaak: “Na een responsible disclosure procedure (met dank aan @ncsc_nl) heeft @youfone nu een veiligere klantenportal.”

Responsible Disclosure beleid zou volgens de andere telco’s die ik tegenkom in mijn onderzoek sector-breed zijn ingevoerd. Bij deze blijkbaar niet. Op www.youfone.nl (een site die ongevraagd cookies plaatst) staan vooral “superrrrr goedkope aanbiedingen”, maar nog steeds geen e mail adres waar je veiligheidsproblemen kunt melden, laat staan een richtlijn. Geen zin, geen tijd, geen prioriteit? Of zijn sommigen zijn gewoon te goedkoop voor security?

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