Verantwoorde onthullingen #2

A man in the middle of money and media. ING weigert ontwerpfouten te erkennen in de Mobiel Bankieren app (2012)

Herinnert u zich de campagne “3x kloppen” nog? Die werd in 2007 gelanceerd door de Nederlandse Vereniging van Banken en is sindsdien onderdeel van het standaardrepertoire om klanten te wapenen tegen internetcriminelen. Stel jezelf bij online betalingen de volgende drie vragen: klopt mijn pc-beveiliging, klopt de website en klopt de betaling? Hacker @floorter ontdekte begin 2012 dat de bankierenapp van de ING dat zelf onvoldoende deed en kwetsbaar was voor een man-in-the-middle-attack. Dat terwijl al 800.000 mensen de app hadden gedownload en ongeveer 300.000 hem dagelijks gebruikten. Hij meldde het lek, maar er gebeurde niets. Pas toen hij er een blog over schreef en EenVandaag erbij kwam, luisterde de bank en werd de bug gefixed. Zonder enige erkenning voor Terra’s vondst.

Floor Terra is een prototype ethische hacker. Hij is zowel handig in het begrijpen van complexe systemen als betrokken bij het maatschappelijk welzijn. Bij het NIKHEF deed hij data-analyse en onderhield hij de controle- en meet software. Hij was ook een tijdje docent. Op zijn blog floort.net/blog snijdt hij regelmatig actuele veiligheidskwesties aan. Hij heeft ook een blauwdruk gepubliceerd voor verantwoorde onthullingen op responsibledisclosure.nl. Als hij een beveiligingsprobleem vindt, meldt hij het eerst bij de eigenaar van het systeem en niet zoals anderen wel eens doen bij de pers.

De bankierenapp van de ING hoefde hij niet eens te hacken. Hij zag al aan het ontwerp hoe kwetsbaar de app was en belde de ING helpdesk. De medewerker aan de lijn stelde dat de app wel echt veilig was en nam de melding in ontvangst. Terra hoorde weken niets en zette daarom zijn vermoedens 15 januari op zijn blog [1]. Met de vraag: “Mag ik concreet aantonen dat de applicatie slecht beveiligd is om mijn stelling te onderbouwen?” want hij wilde niet de wet overtreden. Toen reageerde de bank wel. Terra werd uitgenodigd om uit te leggen wat hij had gevonden. EenVandaag wilde ook uitleg. Dat kon, maar eerst wilde hij als ethische hacker ING de tijd geven om het lek te dichten. Half maart was de bug eindelijk gefikst. De journalist kon over gaan tot onthulling.

In de uitzending van 21 maart 2012 [2] komt Terra aan het woord: “In eerste instantie dacht ik, ze zullen toch niet *dit* vergeten zijn? Dat heb ik gecontroleerd en binnen een uurtje had ik het zo uitgewerkt dat ik kon afluisteren wat voor verkeer er over ging en mijn eigen server er tussen zetten en te doen alsof ik de ING was.” Wat hij ontdekt zou hebben, wordt verbeeld met een animatie van een bank, mobiel en slot dat doorgekruist wordt. Vervolgens komt professor Bart Jacobs in beeld. Na lof voor Terra’s werk, legt hij uit dat een man-in-the-middle bedragen en rekeningnummers zou kunnen veranderen. “Dit is een blammage. Hierom wordt ING in security kringen hard uitgelachen” ING zelf reageert alleen schriftelijk, stelt dat de app wel veilig is, zonder melding van Terra’s tips. Slechte bank dus.

De avond van de uitzending van EenVandaag twittert @mount_knowledge aan @floorter: “ING app SSL issue is oud nieuws. Ik schreef hier in November al over” En inderdaad, in deze blog [3] van Richard van den Berg werd het probleem al netjes uitgelegd. @floorter: “In dat

geval heeft de ING dus keihard tegen mij gelogen toen ze zeiden dat er nooit eerder zoiets gemeld was." En "Als dit soort security meldingen niet centraal gecoördineerd worden is dat op zichzelf ook een probleem."

Maar wat was er nu werkelijk mis met de app? ING gebruikte een standaard SSL, die geen controle deed op een reeks attributen van het certificaat. Je zou dus kunnen doen alsof je de server van de ING was met een nep certificaat. Of je dan ook werkelijk kon frauderen, kon Terra echter niet testen, omdat hij daar geen toestemming voor kreeg. Wel kon hij zien aan de update die erop volgde, dat de bank precies dat had aangepakt. Hij had dus gelijk, zonder dat de bank dat wilde erkennen. Dat is jammer, want ING mist hiermee gratis advies en zullen hackers in het vervolg meteen naar de media stappen.

Vlak voor de deadline van deze column krijg ik nog een DM van @floorter. De bank heeft nu ook een meldpunt. Heb mijn tekst direct gemaild naar responsible-disclosure@ing.nl met de vraag of @floorter de aanleiding was. Diezelfde dag antwoordt ING: "De invoering van responsible disclosure is een actie vanuit de verschillende Nederlandse banken in samenwerking met de NVB." Komt het toch nog goed in Nederland.

Chris van 't Hof www.cvth.nl

Volgende aflevering in *verantwoorde onthullingen*: "Toen @UID_ de kazerne belde met een fabriekswachtwoord."

Bronnen:

[1] Floor's Blog: http://floort.net/blog/verantwoordelijkheid-voor-beveiliging.html
[2] EenVandaag: http://www.eenvandaag.nl/binnenland/40032/mobiel_bankieren_ing_maandenlang_onveilig
[3] Mount Knowledge blog: http://www.mountknowledge.nl/2011/11/09/ing-mobiel-bankieren-authenticatie/
[4] Meldpunt ING: http://www.ing.nl/de-ing/veilig-bankieren/veiligheidsbeleid-van-de-ing/meldpunt-kwetsbaarheden/index.aspx