Column: Verantwoorde onthullingen #3

Toen @UID_ de kazerne belde met een fabriekswachtwoord. Het Teleconferentiesysteem van Defensie (2012)

Beroepshacker Rickey Gevers, ook wel @UID_, kreeg een tip van iemand van Anonymous: het Nederlandse Ministerie van Defensie zou gebruik maken van een videoconferentie systeem, waarvan niet alle gebruikers hun wachtwoord hebben aangepast. Met het standaard fabriekswachtwoord, dat is te vinden in een handleiding die op internet, opende hij de inlogpagina van een topman bij de Defensie. Hij toonde dit aan een journalist van de Volkskrant, die eerst zijn advocaat en daarna Defensie belde. Een woordvoerder zei dat het Defensienetwerk veilig was. Maar, als de krant bij de drukker ligt, ziet Rickey dat het systeem uit de lucht is gehaald. Had @UID_ gelijk?

Gevers is, zoals zijn Twitter profiel meldt, een “criminal brought to justice”. In 2008 werd hij, na een tip van de FBI, opgepakt door Team High Tech Crime van de Nederlandse politie. Voor het hacken van o.a. de Michigan University heeft hij 18 dagen in de gevangenis gezeten. Daarna heeft hij zijn hackersvaardigheden vooral ingezet om anderen te helpen hun beveiliging op orde te brengen. Soms vrijwillig, maar ook voor commerciële tarieven via het bedrijf Digital Investigation. Niettemin heeft hij nog veel contact met het schemergebied van de hackerswereld, zoals Anonymous.

Op maandag 20 februari 2012 krijgt @UID_ een bericht van de Nederlandse anarchistische hacker @ntisec. Hij had een tip gekregen van Anonymous, maar vindt het lek van dermate hoog kaliber dat hij zijn vingers hier liever niet aan wil branden. Daarom had hij twee journalisten benaderd om het te onthullen, maar dat deden ze niet. Of @UID_ ernaar wilde kijken. Dat wilde hij wel en hij kreeg de handleiding van het CISCO video conference system, een ip adres en de opdracht in te loggen met het default wachtwoord.

Rickey logt in en ziet tot zijn verbazing de pagina van directeur marine bedrijf A.J. de Waard. Hij checkt vervolgens de IP adressen, telefoonnummers en namen of dit wel echt het systeem van Defensie is. Het klopt. Vervolgens probeert hij nog wat andere pagina’s in het systeem. Het blijkt dat hij eindeloos veel wachtwoorden kan intypen en dus andere accounts gewoon met brute force zou kunnen openen. Gevers is geschokt en weet niet goed hoe hij dit naar buiten moet brengen. Hij wil natuurlijk niet weer de gevangenis in. Hij schakelt daarom, net als @ntisec, een journalist in: Victor de Kok van de Volkskrant. Rickey weet namelijk dat deze krant goede advocaten heeft.

Die woensdag ontvangt Rickey journalist De Kok op zijn studentenkamer om samen in te bellen. Rickey achter de laptop en de journalist continue aan de telefoon met zijn advocaat. Ze loggen in als de directeur marine bedrijf en bellen de directie van de Jan de Noordazaal, een kazerne in Den Helder. Helaas, er wordt niet opgenomen. Ze zouden ook kunnen bellen naar warroom@denhaag NL of testsite@US, maar dat lijkt ze te link. De journalist belt daarom zelf met de gewone telefoon naar de kazerne om het lek te melden. Daar wordt hij direct doorverbonden naar een woordvoerder die in eerste instantie niet begrijpt wat er aan de hand is en later terug meldt dat er niets aan de hand is omdat het betreffende systeem niet in gebruik is.

Rickey ziet echter aan de logfiles dat het systeem een uur geleden nog is gebruikt en zeker niet door de minsten. Daar heeft de woordvoerder geen weerwoord op. De Kok gaat over tot de onthulling en kopt vrijdag 24 februari “Communicatie Defensie eenvoudig te kraken“. Dit wordt direct overgenomen door andere journalisten, waaronder ook een parodie van GeenStijl die het bekijken waard is. Bij Defensie zijn ze er inmiddels achter wat er aan de hand is, want Rickey ziet dat het systeem offline is gehaald.

Wat is er gebeurd? Ik heb daarom ook contact opgenomen met Defensie. Het bleek te gaan om woordvoerder Maarten Hilbrandie. Die heeft direct na het telefoontje van de journalist naar hun communicatiesystemen gekeken en zag niets vreemds. Die staan ook niet online. Pas toen kwam hij erachter dat er nog een ander systeem was, dat wel via internet ging. Dat was inderdaad tegen de regels in en het systeem werd donderdagavond 21.25 offline gehaald. Dat was maar goed ook, want de krant lag toen al bij de drukker. Niet echt een verantwoorde onthulling dus. Maar het heeft wel geholpen.

Hoe is het eigenlijk afgelopen met Arjen de Waard, de directeur die tegen de regels in het onveilige systeem gebruikte? Als ik hem bel reageert hij vrij luchtig: “Ja, ze hadden weleens dat fabriekswachtwoord moeten veranderen. Was niet zo netjes”. En nee, de hack heeft voor hem geen negatieve consequenties gehad.

Volgende keer *Verantwoorde onthullingen #4*: “I hacked KPN, and all I got was this lousy T-shirt. @stevenketelaar, @bl4sty en de 10 miljoen modems”

Chris van ’t Hof www.cvth.nl

Bronnen:

Interview met Rickey Gevers 5 augustus 2013
[1]http://rickey-g.blogspot.nl/2012/02/maandag-de-20ste-word-ik-getipt-door.html?spref=tw
[2]http://www.volkskrant.nl/vk/nl/2694/Tech-Media/article/detail/3199980/2012/02/24/Communicatie-Defensie-eenvoudig-te-kraken.dhtml
[3] http://www.geenstijl.nl/mt/archieven/2012/02/communicatiesysteem_defensie_g.html