Column: Verantwoorde onthullingen #4

“I hacked KPN, and all I got was this lousy T-shirt." @stevenketelaar, @bl4sty en de 10 miljoen modems (2013)

Het jaar is net gewisseld als KPN een voorzichtig e-mailtje binnenkrijgt: “We hebben iets gevonden, maar zijn bang dat jullie ons oppakken.” Het is versleuteld en verzonden vanaf een generiek e mail adres. Menig helpdesk zou hier wellicht niet op reageren, maar wel het KPN Cert Team. De melding komt terecht bij Security Officer Martijn van der Heide. Hij stelt de hackers gerust dat ze niet direct worden opgepakt, garandeert hun anonimiteit en nodigt hen uit bij KPN hun verhaal te doen.

In een besloten setting laten ze zien hoe ze het modem van KPN kunnen hacken en al het verkeer afluisteren. Maar ook hoe het lek gedicht kan worden. Het blijkt te gaan om de Zyxel, die wereldwijd door tientallen miljoenen mensen wordt gebruikt. KPN neemt diezelfde dag contact op met de fabrikant en geeft hun een termijn, want de jongens willen begin april hun bevindingen presenteren op Hack in the Box. KPN kan gelukkig de modems op afstand updaten via hun management interface en zorgt ervoor dat ze allemaal voor eind maart gereset zijn. De gebruikers hebben als het goed is niets gemerkt.

Als ik Martijn spreek op het KPN kantoor in Den Haag is er taart voor iedereen. Zijn team is derde geworden bij de Cyberlympics, een jaarlijkse hack competitie in Las Vegas, waar Nederland altijd goed vertegenwoordigd is. Hier dus een groep mensen die begrijpen hoe hackers denken. Van de Heide spreekt dan ook met veel respect over de hackers. Hij begrijpt hun voorzichtigheid ook wel. Toen hij 6 jaar geleden voor het eerst een dergelijke melding binnenkreeg kwam direct de juridische afdeling in actie. Die wilde de identiteit van de hackers weten en een zaak beginnen. Zijn afdeling heeft toen hard moeten strijden om de melders te beschermen. Gaandeweg ontwikkelden ze een Responsible Disclosure beleid en krijgen ze gemiddeld een melding per week die binnen een dag wordt afgehandeld. En de twee modem hackers, die hebben nu een leuke video namens het KPN Guest Hacker Program [1].

Het blijkt te gaan om @stevenketelaar en @bl4sty – ook wel Peter Geissler. Als ik Peter spreek hoor ik een bekend verhaal: school niet interessant, maar uitermate nieuwsgierig, autodidact en probeert van alles uit om te kijken hoe iets werkt. En zo kwamen hij en Steven er bij toeval achter dat ze bij hun modem een hulppagina konden opvragen en daar tekst invoeren. Bij meer dan 58 tekens crashte die. Uit de crashes konden ze afleiden wat er gebeurde. Ze schreven een script om de crash te besturen en vervolgens poort 7676 over te nemen. Dat is de management interface waarmee KPN het modem op afstand voorziet van updates. Na vijf dagen werk, konden ze hun eigen software installeren tussen de gebruiker en het internet. De mogelijkheden zijn legio. Voor hun demo bij Hack in the box kozen ze ervoor een VoIP gesprek af te tappen.

Op 10 april staan beide heren bij Hack in the Box in een soort Star Trek achtige overhemd op het podium met een geïmproviseerd LAN voor zich. De titel van hun presentatie “How I met your Modem. De ZyXEL P-260IHN-FI”[1]. Na een technische verhandeling die ik jullie hier zal besparen, belt Steven iemand via de VoIP en vraagt diegene een vooraf gegeven code te

noemen. Peter rommelt wat aan zijn laptop en jawel, hij tovert het gesprek tevoorschijn. Applaus. En als ze vertellen hoe KPN omging met de melding roept Peter ze erbij. Op het podium verschijn de CISO Jaya Baloo: “On behalf of KPN I would like to thank you for hacking our network”. Ze overhandigt beide heren een T-shirt met daarop de tekst “I hacked KPN, and all I got was this lousy T-shirt”. Nog meer applaus. Jaya: “It shows Responsible Disclosure works!”. Peter: “Yes, some times it does…”

Toch zit iets me nog niet helemaal lekker. De modems worden beheerd vanaf de providerkant via de beruchte poort 7676. Dus als je voor deze onthulling al gehackt was, kon KPN het niet meer patchen. Dat klopt volgens Peter, maar volgens hem zijn zij de eersten die dit ontdekt hebben. Maar zelfs dan nog, Hoe zou het nu vergaan met die 10 miljoen andere modems die niet van KPN zijn? Zou Zyxel alle providers en individuele gebruikers hebben geïnformeerd? Dat zullen we dan vanzelf wel achter komen…

Volgende aflevering in *Verantwoorde onthullingen* #5: “DongIT en het DigiD debacle. Ethisch hacken als businessplan”.

Chris van ’t Hof www.cvth.nl

Bronnen:

Interview met Martijn van der Heide 24 september 2013
Interview met Peter Giessler 19 november 2013
[1] http://www.youtube.com/watch?v=eK8VbFmb0gE
[2] http://www.youtube.com/watch?v=9rBB_Ng7EZA