Verantwoorde onthullingen #12
Trots op onze digitale polderoplossingen

Op 19 december j.l. kregen we weer een brief van Ivo Opstelten over hoe het ervoor staat met responsible disclosure, oftewel "beleid voor het op verantwoorde wijze openbaar maken van ICT-kwetsbaarheden in informatiesystemen en softwareproducten die door goedwillende melders of hackers worden ontdekt en gemeld." Het gaat goed met dat beleid, want steeds meer partijen doen eraan mee. Bij de Rijksoverheid, telecom, banken, hosters, verzekeraars en nog vele anderen zijn nu meldpunten voor gevonden kwetsbaarheden. Het NCSC is hierin de spil. Het centrum bemiddelt bij meldingen en heeft er zelf ook 136 afgehandeld. Er is veel gebeurd sinds het verschijnen van hun leidraad responsible disclosure twee jaar geleden.

Ook toen kregen we een brief van onze minister van Veiligheid en Justitie. Hij schreef op 5 december 2012: "Centraal bij het werken met responsible disclosure staat het verhelpen van de kwetsbaarheid en het verhogen van de veiligheid van informatie- systemen. Daarbij gelden een aantal algemene uitgangspunten, zo is het bijvoorbeeld niet gepast om onnodige schade aan te richten of verder te gaan dan het aantonen van de kwetsbaarheid. In een dergelijk geval is het niet gepast om onnodig grote databestanden te ontvreemden als al is aangetoond dat het databestand benaderbaar is." Dat standpunt is niet veranderd en werd bevestigd door de rechtszaken die erop volgden.

Aanleiding voor de brief was destijds de onthulling van beveiligingsproblemen bij het Groene Hart Ziekenhuis. Een hacker had aangetoond dat hij bij persoonlijke data kon omdat het netwerk verouderd was. Brenno de Winter onthulde dit op 7 oktober 2012 op NU.nl. Het ziekenhuis stelde meteen een crisisteam in werking en liet onderzoek doen. Toen bleek dat er malware was geïnstalleerd en grote hoeveelheden patiëntengegevens waren gedownload, deed het ziekenhuis aangifte en werd de hacker opgepakt.

In diezelfde periode moest ook Henk Krol voor de rechter verschijnen. Hij had enkele patiëntendossiers gedownload om te laten zien dat hij met slechts vijf cijfers in de database van Diagnostiek voor U kon en bracht dat direct in de media. Ook DvU deed aangifte en Krol werd vervolgd. Beide zaken leidden tot veel protesten in de media en de Tweede Kamer. Waarom werden de melders aangepakt en niet de organisaties die slecht omgingen met de persoonsgegevens? Net op dat moment kwam de leidraad uit.

Voornaamste kritiek op de leidraad was dat die ethische hackers geen garanties geeft. Organisaties zijn vrij om hun eigen regels op te stellen voor verantwoorde onthullingen, zonder dat ze verplicht zijn iets met de meldingen te doen. Het OM behoudt zich ondertussen het recht om onderzoek te starten naar de rechtmatigheid van de ethische hack. Uitgangspunt daarbij is dat computervredebreuk is toegestaan als het een hoger maatschappelijk doel dient en de hacker handelt volgens de principes van subsidiariteit en proportionaliteit. Oftewel: hack alleen om aan te tonen dat de beveiliging niet klopt, doe het met de minst ingrijpende middelen en download zo min mogelijk persoonsgegevens.

De zaak Krol diende in januari 2013. De rechter vond dat Krol wel ethisch had gehandeld door in te loggen, dossiers uit te printen, te anonimiseren en zijn vondst in de media te brengen – ook al gaf hij DvU nauwelijks tijd om voorbereidingen te treffen. Wat hij deed was nodig om de misstand in de beveiliging van persoonsgegevens aan te tonen en hij voldoet daarmee aan de subsidiariteitseis. Maar dat hij diverse keren had ingelogd en ook voor het oog van journalisten dossiers downloadde, vond de rechter disproportioneel. Hij kreeg hiervoor een boete van 750 Euro. DvU had nog een fikse schadevergoeding geëist, maar daar ging de rechter niet in mee.

Chris van 't Hof

TEK TOK

18 februari 2015

De zaak Groene Hart duurde wat langer, want op de in beslag genomen computer werd ook kinderporno gevonden, wat leidde tot een nieuwe zaak. Gelukkig heeft de rechter in haar oordeel van 17 december 2014 de twee zaken gescheiden, anders zou het wel rommelige jurisprudentie zijn geworden. De hacker handelde volgens haar in eerste instantie ethisch omdat hij geen financieel belang had bij de hack en het lek heeft gemeld via een journalist die bekend staat om onthullingen. Zo hebben ze een beveiligingsprobleem geagendeerd bij een ziekenhuis dat hierin tekortschoot en dienden ze een hoger maatschappelijk belang.

De rechter ziet het als noodzakelijk voor dit doel dat hij een server heeft gehackt en als bewijs enkele dossiers heeft gedownload met een programmaatje dat gezien kan worden als malware. Dat kon niet met minder ingrijpende middelen. Dat hij echter de dagen erna weer inlogde en dossiers ging downloaden, gewoon uit nieuwsgierigheid, was niet noodzakelijk en een disproportionele inbreuk op de privacy van de patiënten. Daarvoor wordt hij veroordeeld tot 120 uur taakstraf wegens computervredebreuk.

De leidraad responsible disclosure laat dus veel open en die ruimte wordt nu ingevuld door de rechtspraak. Bij gebrek aan wetgeving, moeten we het voorlopig doen met de vorderende jurisprudentie. Dat is heel naar voor de hackers en gehackten die zo'n ingrijpend proces moeten doormaken. Maar ik zie ook niet direct een wet komen die opgaat voor alle gevallen, omdat de situatie telkens zo anders is. Responsible disclosure blijft een polderoplossing waarbij iedereen zich wel een beetje, maar niemand helemaal in kan vinden. Dat is ook inherent aan cyber security: iedereen is een beetje verantwoordelijk voor een deel en daardoor uiteindelijk niemand echt voor het geheel. Hopelijk kunnen rechtszaken voorkomen worden door goed overleg en hebben strijdlustige advocaten en activistische journalisten het nakijken. De leidraad en bemiddeling van het NCSC helpen daar zeker bij, want steeds meer meldingen worden achter de schermen afgehandeld.

Dit is de digitale polderlandschap zoals het erbij ligt begin 2015. Ook dit jaar staat er veel op de agenda voor responsible disclosure. De leidraad wordt geactualiseerd, getoetst bij de ICT community en verder uitgedragen. Onder andere bij twee conferenties: de Global Conference on CyberSpace en de NCSC One Conference. Hiervoor wordt ook onderzocht hoe ethisch hacken zich verhoudt tot de rechtssystemen van andere landen. In 2016 zal Nederland zijn EU voorzitterschap gebruiken om responsible disclosure internationaal uit te dragen. Het is dan wel een digitale polderoplossing, maar we zijn wel het eerste ter wereld dat het zo doet. Daar mogen we best trots op zijn.

Intussen zit ik tijdens de Kerstvakantie mijn boek hierover af te ronden, want 11 maart krijgen alle bezoekers van Security Bootcamp een exemplaar van "Helpende Hackers". Misschien volgend jaar maar een versie 2.0?

Chris van 't Hof
www.helpendehackers.nl