Verantwoorde onthullingen #10

Terugkijken

Verantwoorde onthulling nummer tien alweer… Tijd voor wat reflectie. Ik heb nog een paar cases en een flinke analyse te gaan voor mijn boek “Helpende Hackers” (2015), maar hier alvast een van de conclusies: algemene principes voor ethisch hacken zijn goed, maar casuïstiek is beter. Want of een onthulling verantwoord is, hangt vooral af van de context. En die is voor elk van de betrokkenen weer anders.

Een hacker is ethisch bezig als hij een gevonden kwetsbaarheid netjes meldt bij de eigenaar van het systeem, verder geen gekkigheid uithaalt (malware plaatsen, data downloaden of aanpassen, etc.) en iedereen de tijd geeft het lek te dichten. Gelukkig zijn er steeds meer organisaties die voor Responsible Disclosure beleid hebben om hier goed mee om te gaan: snel de juiste technici inschakelen, communiceren over de voortgang en uiteindelijk credits voor de melder. Zo bereiken steeds meer meldingen de media uiteindelijk niet.

Maar bij veel organisaties is er nog steeds geen RD beleid, of zelfs geen aanspreekpunt. De helpdesk begrijpt niet wat de jongen toch allemaal uitkraamt over vulnerabilities, de systeembeheerder heeft geen tijd, want hij zit al in een lange migratiefase en het management heeft te weinig manuren ingezet op security. Even geduld a.u.b., volgend jaar beter. Dan gaat de hacker met zijn melding maar naar een journalist, of nog erger naar een andere hacker die ermee verder gaat.

Dan is er ineens een CTO of CISO die het incident met open armen ontvangt. Al jaren heeft hij gepleit voor beter patchmanagement en wachtwoordenbeleid. Nu weten ze waarom. Hij weet iemand in het bestuur te overtuigen het gesprek aan te gaan met de hacker en de juridische afdeling op afstand te houden. Een crisisteam wordt samengesteld dat snel werk maakt van het dichten van het lek. De hacker wordt zelfs uitgenodigd een presentatie te houden. Andere organisaties die met hetzelfde beveiligingsprobleem zijn ook uitgenodigd. Mooi!

De geest is echter al uit de fles en er volgen Kamervragen. De oppositie grijpt het bericht aan om de minister aan de tand te voelen: dit lek is geen incident, maar weer het zoveelste voorbeeld dat overheidsinstellingen hun beveiliging niet op orde hebben. Toezicht heeft blijkbaar gefaald. De minister heeft ook het bericht in de krant gelezen. Eigenlijk vindt hij dat de instellingen vooral zelf verantwoordelijk zijn voor de beveiliging, maar hij wil wel het maatschappelijk belang onderstrepen en verschuilt zich achter de toezichthouders die toch echt wat meer tijd nodig hebben.

De politie is ondertussen onderzoek gestart want het OM wil weten wat er precies is gebeurd. De hacker heeft weliswaar ethisch gehandeld en is eruit gekomen met de instelling, maar er blijken nu meer gedupeerden: de andere organisaties met hetzelfde lek en die hebben aangifte gedaan. De hackers is dan wel geen verdachte, maar wordt wel gehoord om uit te zoeken met wie hij de kennis heeft gedeeld. Als hij dit vertelt op een hackersconferentie, ontploft de scene: waarom wordt hij nu gepakt en niet die instellingen die de data lekken?! Weer volgen er kritische mediaberichten en Kamervragen.

Deze fictieve casus is een samenraapsel van dingen die ik tegenkom in mijn onderzoek. Ik kan me goed voorstellen dat ethische hackers zich vaak onbegrepen voelen en natuurlijk hebben journalisten haast met een pakkend verhaal. Ik snap ook dat de ICT afdeling, het management al genoeg aan hun hoofd hebben, Kamerleden willen debatteren en Justitie wil checken of alles wel klopt. Wie van hen heeft gelijk? Allemaal en daarmee niemand.

Moeten we dan maar lekker relativistisch achterover hangen omdat men elkaar toch niet begrijpt? Nee. Wat we nodig hebben is casuïstiek, zodat we patronen kunnen zien in de handelingen van de betrokken actoren en hun uiteenlopende belevingswerelden. Oftewel: verhalen vertellen. Dat kweekt niet alleen begrip, maar voegt ook een dimensie toe die we nogal eens vergeten bij controversen: de tijd.

De tijdsbeleving van de hacker en systeembeheerder lopen nogal uiteen. De ontdekker ziet meestal vrij direct wat er mis is en hoe het gefixed kan worden, maar ziet niet hoeveel ander werk de systeembeheer nog heeft. Het is niet de enige bug op zijn lijst en bovendien werkt hij met systemen die op een onlogische, maar historisch verklaarbare wijze gekoppeld zijn. Liefst wacht hij op de migratie die over een half jaar plaats vindt. Maar daar kunnen zowel de hacker als de journalist niet op wachten, want ondertussen worden er wel gevoelige persoonsgegevens gelekt.

Of de melding van een lek nieuws is, hangt af van al het andere nieuws en hoe snel het medium is. Nu.nl en Tweakers kunnen binnen een dag publiceren, terwijl Eenvandaag soms wel weken nodig heeft om de juiste beelden te vinden voor een TV item. Dan is er even veel aandacht. Staat kort na de uitzending toevallig een Kamerdebat gepland over ICT, dan is het voorval munitie voor de oppositie en is er meer nieuws. De minister zal moeten antwoorden, maar kan best nog een paar maanden wachten als dat beter uitkomt. Toezichtsorganen komen in de regel ook pas na een paar weken of maanden in actie. Het NCSC is meestal wat vlotter, maar kan uiteindelijk alleen informeren en bemiddelen want zij heeft geen handhavende bevoegdheden. De tijdslijn voor strafrechtelijk onderzoek is nog langer. Dat duurt soms wel jaren.

Als uiteindelijk alle details aan het licht komen, is de media aandacht alweer verdwenen. Door deze wir war van tijdslijnen springen de meningen alle kanten op. Die blijven hangen in de onderbuik, van waaruit bij een volgende hack weer wordt gereageerd. “Zie je wel dat ze altijd weer de hacker pakken” roept de een. “Nee joh, die hackers zijn gewoon niet te vertrouwen” roept de ander. Wel zijn ze het er over eens dat de overheid altijd te kort schiet. Zo blijven we een ritueel debat voeren. Totdat we terugkijken en zien dat het eigenlijk best de goede kant opgaat met ethisch hacken in Nederland. Steeds meer meldingen worden achter de schermen opgelost. Dat is jammer voor de media, maar goed voor mijn boek.

Chris van ’t Hof @cvthof
Voor meer verantwoorde onthullingen, zie www.cvth.nl/vo