Bijlage 2 – Jurisprudentie en praktijkvoorbeelden bij de OM-beleidsbrief Coordinated Vulnerability Disclosure December 2020

Jurisprudentie

In jurisprudentie is reeds enkele malen geoordeeld[1] dat elke inbreuk op een geautomatiseerd werk zonder toestemming van de rechthebbende strafbaar is, tenzij er bijzondere omstandigheden zijn die deze inbreuk kunnen rechtvaardigen. Om deze bijzondere omstandigheden te kunnen toetsen, moet de verdachte wel een verklaring hebben afgelegd over wat zijn intenties waren bij het plegen van de inbreuk. [2] Hier volgen enkele voorbeelden:

Casus 1: Niet proportioneel en subsidiair[3]

Tijdens een bezoek aan Diagnostiek voor U heeft de verdachte onbedoeld een inlogcode en een bijbehorend wachtwoord voor de website gehoord. Op 18 april 2012 heeft de verdachte op zijn computer, met de door hem gehoorde inlogcode en wachtwoord met succes ingelogd op de desbetreffende website. Hij heeft vervolgens in het systeem een aantal medische dossiers/gegevens bekeken.
De volgende dag is er, samen met een medeverdachte, nogmaals ingelogd en zijn er nogmaals medische gegevens/dossiers bekeken. Daarnaast werden medische gegevens van verschillende personen uitgeprint en geanonimiseerd. De medeverdachte heeft het kantoor van de gegevensbeheerder gebeld en zijn bevindingen met betrekking tot een kwetsbaarheid van de website gedeeld.
Direct hierna heeft de medeverdachte naar Omroep Brabant gebeld om diezelfde bevindingen te delen.

Naar het oordeel van de rechtbank was er gehandeld in het kader van een wezenlijk maatschappelijk belang, namelijk het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens.
Echter wordt het handelen van de verdachte als disproportioneel bestempeld. Het was voldoende geweest als er 1 á 2 medische dossiers waren geraadpleegd.
Daarnaast werd geconcludeerd dat er niet voldaan is aan het subsidiariteitsvereiste. Verdachte had de tijd en had deze ook moeten nemen om de psychiater, diens werkgever en/of de gegevensbeheerder gericht te benaderen en had het geconstateerde probleem op een adequate manier daar onder de aandacht moeten brengen. Indien op zijn melding niet adequaat zou zijn gereageerd, hadden mogelijk andere wegen open gelegen, waaronder de thans gevolgde weg om Omroep Brabant te benaderen. Door anders te handelen heeft verdachte daarbij de grenzen van de subsidiariteit overschreden, en was reeds om die reden zijn aandeel in de computervredebreuk wederrechtelijk.

Casus 2: Niet proportioneel en subsidiair[4]

---

[1] Zie onder meer: Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1163 ; Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611.

[2] Rb. Den Haag 11 juni 2020, ECLI:NL:RBDHA:2020:5654.

[3] Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1163.

De verdachte heeft met behulp van valse signalen weten binnen te dringen in een webserver, waarna hij eerst enkele persoons- en betalingsgegevens handmatig heeft verkregen en later door middel van het schrijven en uitvoeren van een script, de voormelde gegevens van 80.000 personen heeft overgenomen. De verdachte heeft zijn bevindingen niet gemeld bij de benadeelde, maar anoniem bij verschillende media via een klokkenluidersplatform.

De rechtbank oordeelt dat de verdachte een wezenlijk maatschappelijk belang heeft gediend, door een bijdrage te leveren aan het beveiligen van een groot aantal privacygevoelige gegevens.
Het handelen van de verdachte overschreed echter wel de grenzen van de proportionaliteit. Hij had het bij de enkele handmatig verkregen records kunnen laten en de benadeelde zelf de omvang van het beveiligingslek kunnen laten onderzoeken.
Ook zou er niet subsidiair gehandeld zijn. De rechtbank is van oordeel dat de verdachte niet de benadeelde had mogen passeren. Uitgangspunt is dat een datalek eerst gemeld wordt bij de desbetreffende instantie.
De strafbaarheid kan dus niet worden weggenomen en dus is de verdachte veroordeeld voor computervredebreuk.

Casus 3: Niet proportioneel[5]
Op 26 september 2012 ontdekte de verdachte door middel van een softwareprogramma dat het computersysteem van het Groene Hart Ziekenhuis op verouderde software draaide. Hij heeft vervolgens een commando naar de server van het ziekenhuis gestuurd om de gebruikersnaam en het bijbehorende wachtwoord te achterhalen. Dit slaagde, waarop de verdachte op verschillende dagen heeft ingelogd, rondgekeken, bestanden gedownload en screenshots van die bestanden aan een journalist heeft doorgestuurd. In totaal heeft hij inzicht gehad in twee medische dossiers en de gegevens van 496.064 patiënten.

De rechtbank erkent dat de verdachte het wezenlijke maatschappelijk belang heeft gediend. Ook is de rechtbank van oordeel dat de verdachte subsidiair gehandeld heeft. Hij heeft zijn bevindingen bij een journalist gemeld bij wie hij eerder bevindingen had gemeld, met wie hij een vertrouwensrelatie had opgebouwd en van wie hij wist dat deze, voordat hij de bevindingen zou publiceren, het GHZ eerst de gelegenheid zou bieden adequate maatregelen te treffen om te voorkomen dat gevoelige gegevens in de openbaarheid terecht zouden komen. Ook neemt de rechtbank mee dat de verdachte heeft verklaard de volgende keer NCSC, die ten tijde van de onderhavige hack nog niet bestond, als intermediair te laten fungeren.
De rechtbank valt in deze zaak over de proportionaliteitsfactor. Het was niet nodig om na de succesvolle inlogsessie en de melding van het beveiligingslek bij de journalist, opnieuw in te loggen in het computersysteem van het Groene Hart

[4] Rb. Den Haag 30 augustus 2018, ECLI:NL:RBDHA:2018:10451.
[5] Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611.

Ziekenhuis. Ook was het niet nodig om in de medische gegevens te zoeken naar een bekende Nederlander, zoals verdachte zelf heeft verklaard te hebben gedaan. De verdachte heeft wederrechtelijk gehandeld en zich aldus meerdere malen schuldig gemaakt aan computervredebreuk.

In de praktijk:
Voornoemde casus tonen aan dat er steeds een wezenlijk maatschappelijk belang was gediend bij de openbaring. De moeilijkste beoordelingsfactoren betreffen proportionaliteit en subsidiariteit. Onder ogen moet worden gezien dat dit ook voor de 'ethisch hackers' moeilijk af te wegen criteria zijn. Ook dient onder ogen te worden gezien dat deze personen in korte tijd diverse beslissingen moeten nemen, zonder dat deze personen altijd kennis hebben van de diverse beleidslijnen over CVD. Die omstandigheden dienen te worden meegewogen bij het nemen van een beslissing tot het instellen van een feitenonderzoek en/of strafrechtelijk onderzoek, alsmede bij het nemen van een vervolgingsbeslissing.

Indien een door de officier van justitie aangemerkte verdachte na het onderzoek blijkt te hebben gehandeld in de lijn van het CVD-beleid, ligt een sepot 01 voor de hand en niet een sepot 02. Immers heeft de verdachte in dat geval gehandeld conform daarvoor ontwikkelde beleidsregels en binnen de in de jurisprudentie ontwikkelde maatstaven. Dat levert een situatie op waarin het feit op zichzelf wel strafbaar is, maar daarvoor een rechtvaardigingsgrond bestaat en verdachte dus, achteraf bezien, ten onrechte als verdachte is aangemerkt.

CVD Praktijkvoorbeelden uit 'Helpende Hackers' van Chris van 't Hof[6]

Marktplaats
De website om tweedehands goederen te kopen en verkopen heeft al zeer vroeg een CVD-beleid vastgesteld. Op de website wordt al in 2012 vermeld dat hackers een veiligheidslek kunnen melden en daar zelfs een beloning voor kunnen krijgen. Als je maar handelt volgens het protocol: meld ons het lek zonder het eerst met anderen te delen, geef ons de tijd om het te dichten en veroorzaak geen schade. Een van de hackers die dat begin 2012 deed, was de toen 19-jarige Pieter Vlasblom, ook wel @legosteentje.

Vlasblom gaat aan de slag met een applicatie die automatisch advertenties plaatst op Marktplaats. Hij zet in plaats van gewone tekst HTML-code met Java-Script in de advertenties, oftewel Cross Site Scripting (XSS). Het werkt: de advertentie gedraagt zich nu als een site en Vlasblom zou nu bezoekers van Marktplaats met pop-ups naar een andere site kunnen leiden. Op 2 maart 2012 plaatst hij een voorzichtige tweet: "Heb een securityprobleempje bij Marktplaats gevonden". Bas Anneveld (Manager Site Operations bij Marktplaats) reageert: "We komen graag

[6] De e-pub van het boek 'Helpende Hackers, Chris van 't Hof, Tek Tok Uitgeverij 2016', met meer voorbeelden uit de praktijk is gratis te downloaden op http://www.cvth.nl/helpendehackers.epub

met je in contact indien je een bug gevonden hebt. We hebben een responsible disclosure program.' Vlasblom denkt eerst dat hij in de problemen kan komen, maar Anneveld benadrukt dat hij vooral uitleg wil en ze beginnen te mailen. De kwetsbaarheid wordt binnen een dag opgelost. Vlasblom krijgt 350 euro voor zijn vondst en een pakje: een Classified White Hat in a Black Box.

KPN

Begin 2013 ontdekken twee jonge beveiligingsonderzoekers hoe ze een ZyXEL-modem kunnen hacken. Ze hebben zelf een KPN-modem en doen hun melding onder een pseudoniem. De hackers krijgen meteen een reactie van KPN dat het telecombedrijf geen aangifte zal doen. Ze worden zelfs uitgenodigd bij KPN om in besloten setting hun verhaal te doen. De hackers geven op het hoofdkantoor een PowerPointpresentatie waarin ze laten zien hoe ze de controle over de modem hebben overgenomen, maar ook hoe het lek gedicht kan worden. KPN security officer Martijn van der Heide heeft het CVD-beleid bij KPN mede ontwikkeld. Hij begrijpt direct dat deze melding van grote waarde is, omdat de ZyXEL modems wereldwijd door tientallen miljoenen mensen gebruikt wordt. KPN neemt daarom diezelfde dag nog contact op met de fabrikant en geeft die een termijn om de modems te patchen. De hackers willen namelijk begin april hun bevindingen presenteren op de hackersconferentie Hack in the Box. KPN zal in de tussentijd de modems op afstand updaten en zorgen dat ze allemaal voor eind maart gereset zijn. De hackers ontvingen van KPN een t-shirt met de tekst: 'I hacked KPN, and all I got was this lousy t-shirt.'