13. Hacker Krol haalt net iets teveel uit de kast

Dossiers bij Diagnostiek voor U blijken beveiligd met slechts vijf cijfers

16 april 2012. Een lid van de politieke partij 50PLUS is bij GGZ Eindhoven op bezoek bij zijn psychiater. Daar verneemt hij hoe de arts inlogt bij het Cyberlab van Diagnostiek voor U. Hoe, daar verschillen de meningen over. De een zegt dat hij het wachtwoord van de arts hoorde toen die aan de telefoon zat, een ander zegt dat de arts zijn code zelf aan de patiënt gaf en een derde beweert dat de code met een post-it naast de monitor was geplakt. Hoe dan ook, de psychiater was slordig met zijn vijfcijferige code die hij gebruikte als inlognaam en wachtwoord. En dat voor zo'n site. Hiermee kun je namelijk de resultaten van bloed- en urineonderzoeken raadplegen.

Twee dagen later zit het 50PLUS-lid achter zijn eigen computer en probeert de code uit. Inderdaad, hij kan erin en ziet tot zijn schrik allerlei medische dossiers. Hij belt daarom direct met partijlid en journalist Henk Krol. De volgende dag zitten ze samen achter de computer in Best, waar de redactie van de Gaykrant zit. Krol krijgt ook toegang tot de site en zoekt op zijn eigen naam. Hij staat er zelf niet in, maar ziet wel dossiers van anderen, waaronder ook bekenden. Hij probeert nog wat namen en ziet onder andere uitslagen van drugs- en soa-testen. Als bewijs print hij een aantal dossiers uit en streept de namen door.

Krol belt Diagnostiek voor U en vraagt naar de leidinggevende. De telefoniste zegt dat hij zijn melding schriftelijk moet indienen. Hij voelt zich niet erg serieus genomen en belt daarom een bevriende journalist bij Omroep Brabant voor advies. Die stuurt meteen een cameraploeg. De twee 50PLUS'ers loggen in aanwezigheid van de cameraploeg in bij Cyberlab. Krol bladert weer door de dossiers. De oorspronkelijke vinder van het lek wil niet in beeld, maar print wel negen pagina's aan dossiers uit. Terwijl de journalisten opnames maken van het scherm, gaat ineens de site uit de lucht. Blijkbaar zijn ze gesnapt. Of is de melding dan toch doorgekomen?

Omroep Brabant zendt het item uit op 19 april. We zien Krol aan een bureau zitten achter een computer. De voice-over zegt: "De medische gegevens van duizenden patiënten hebben wij zojuist ingekeken, terwijl wij allebei geen medicus zijn. Jij kwam met een inlogcode en een wachtwoord, hoe ben je eraan gekomen?" Intussen zien we een computerscherm, waarop allerlei variaties van Jansen voorbij komen. Als Krol vertelt hoe "kinderlijk eenvoudig" het is om in te loggen, zien we het inlogscherm van het Cyberlab, waar iemand 12345 intikt. Krol: "Iedereen die op deze site rondspeelt en vijf cijfertjes intikt…" Zo makkelijk dus.

Krol vertelt dat hun leden - spreekt hij hier als provinciaal Statenlid en het gaat over Brabantse patiënten, of bedoelt hij de leden van de Gaykrant? - zich zorgen maken dat iedereen zo bij hun gegevens kan. Bijvoorbeeld verzekeringsmaatschappijen. Dan doorloopt hij de prints met uitslagen: "Je ziet dat mensen veel te veel drinken, drugs gebruiken, dat mensen bepaalde medicijnen gebruiken, dat mensen al dan niet seropositief zijn (…) Gewoon alles wat uit het bloed is af te leiden, is voor heel veel mensen oproepbaar." De verslaggever roept enthousiast: "Gegevens die te misbruiken zijn?!" "Absoluut", antwoordt Krol. "Je zou mensen kunnen chanteren. Als werkgever kun je kijken: wat voor risico's haal ik in huis?" Hij heeft daarom meteen met de provincie gebeld, maar die stelde dat ze daar niet over gaan. Het Ministerie van Volksgezondheid zou er daarom iets aan moeten doen. Krol besluit plechtig met verheven stem: "Dit mag nooit meer zo voorkomen. Het kán niet zo zijn, dat buitenstaanders met slechts het intikken van vijf cijfertjes zo gemakkelijk bij zulke privégegevens kunnen komen. Dat hád niet mogen gebeuren, dat mág niet meer gebeuren en er moet alles aan gedaan worden dat het niet meer kán gebeuren."

Omroep Brabant bericht die dag ook op hun site over de zaak. De redactie krijgt uiteindelijk wel de leiding van Diagnostiek voor U te spreken. Directrice Astrid van der Put vertelt geschokt te zijn en dat ze de site direct uit de lucht hebben gehaald. De dag erna doet ze aangifte bij de politie, want: "Zoals het er nu naar uitziet, is er sprake van computercriminaliteit. Twee mensen van partij 50PLUS hebben zich toegang verschaft tot het systeem door de bestaande inlognaam en wachtwoord van een arts, die

toegang had tot de gegevens van zijn patiënten, te misbruiken." De omroep kopt die dag: 'Diagnostiek voor U wijst vooral naar anderen na lekke website'.

In de berichtgeving komt ook Brenno de Winter aan het woord. Volgens hem overtreedt Diagnostiek voor U de Wet Bescherming Persoonsgegevens. Het gaat immers om "bijzondere gegevens" en dan mag je volgens die wet een hoger beveiligingsniveau verwachten "conform de stand der techniek". Oftewel vandaag de dag voldoen alleen inlognaam en wachtwoord niet meer, maar zou je voor zoiets moeten inloggen met bijvoorbeeld nog een pasje of sms-code erbij. Dit inloggen met meerdere middelen is de zogenaamde meerfactor authenticatie.

Het College Bescherming Persoonsgegevens laat in deze berichtgeving ook van zich horen en noemt het "een ernstige zaak". Het college kan er echter op dit moment niet zoveel aan doen en is dan ook groot voorstander van een meldplicht, waarvoor op dat moment een wetsvoorstel in de maak is. Dan zal de verantwoordelijke het datalek meteen zelf moeten melden en de slachtoffers inlichten. Zo niet, dan mag het CBP een boete uitdelen, tot wel 200.000 euro. Omroep Brabant refereert hier aan het voorstel voor een meldplicht datalekken, dat we al eerder tegenkwamen in de vorige Kamerdebatten als mogelijk nieuw handhavingsinstrument bij helpende hackers.

Zo ook op 20 april, de dag na de uitzending en tien dagen nadat Opstelten in de Kamer een richtlijn heeft toegezegd. Dit keer wordt de meldplicht onder de aandacht gebracht door PvdA-Kamerlid Attje Kuiken. Ze komt zelf ook uit Brabant en kaart de zaak Diagnostiek voor U aan als treffend voorbeeld van datalekken die gemeld moeten worden. "Het wordt tijd dat het College Bescherming Persoonsgegevens behalve alleen blaffen ook eens kan bijten", stelt ze. Het voorstel krijgt ook steun van GroenLinks en CDA, waarmee een Kamermeerderheid is voor een meldplicht datalekken.

Tot een wetsvoorstel komt het echter niet. De dag erna kondigt Rutte namelijk aan dat, na zeven weken onderhandelen in het Catshuis over de begroting voor 2013, het niet was gelukt tot overeenstemming te komen met gedoogpartner Wilders. Het Kabinet valt. Wetsvoorstellen kunnen dan alleen bij hoge uitzondering uitgevoerd worden en de Kamerdebatten gaan dan vooral over een datum voor de verkiezingen. Die zijn 12 september en de partij 50PLUS doet ook mee als landelijke partij, met een nieuwe lijstrekker: Henk Krol. De flamboyante ex-hoofdredacteur van de Gaykrant doet het goed in de media met zijn ferme uitspraken over het lot van de ouderen en komt uiteindelijk als tweemansfractie in de Kamer. De hack verdwijnt dan voor Krol naar de achtergrond, maar niet voor Diagnostiek voor U en justitie.

Het Cyberlab is 2 mei 2012 weer online. De politie is dan ook gestart met onderzoek naar aanleiding van de aangifte van DVU. Het Openbaar Ministerie verhoort de betrokkenen, onder wie ook de psychiater van wie de vijf cijfers afkomstig waren. Dit is pikant, want informatie over patiënten, ook al zijn ze verdachten, valt eigenlijk onder het medisch beroepsgeheim. De Winter weet over dit onderzoek enkele interessante details te melden. De arts zou de gegevens zo hebben gegeven, ook al was er geen vordering. Nog pikanter is dat tijdens het onderzoek blijkt dat medewerkers van justitie al toegang zouden hebben tot Cyberlab. De server waar deze applicatie op draaide, hield geen logboeken bij, dus moest in de applicatie zelf gekeken worden wie wanneer had ingelogd. Daar zouden deze justitiemedewerkers dus kunnen zien wie als behandelaar van wie welke dossiers beheert. Ook dat is medische informatie, verkregen zonder vordering.

Het OM besluit dat Krol voor de rechter moet verschijnen vanwege computervredebreuk. Als hij dit op 4 december verneemt in een brief aan hem, meldt hij dit direct aan Omroep Brabant, die het die dag naar buiten brengt. In de media neemt De Winter het voor hem op: "Ik vind dat mensen die deze zaken aan de kaak stellen zich veilig moeten voelen." Maar bovenal: "Het lijkt wel alsof justitie zaken aanspant om te voorkomen dat misstanden worden aangetoond. Ik snap het niet goed. Het lijkt alsof slecht nieuws niet gehoord mag worden." De psychiater, het medisch centrum, de applicatiebeheerders en justitiemedewerkers gingen allemaal onzorgvuldig om met de medische informatie, terwijl Krol wordt vervolgd. "Ik vind de misstand belangrijker dan de daad", aldus de journalist.

De Winter laat het er niet bij en doet namens NU.nl een rondje langs de net geïnstalleerde Kamerleden. Hij legt hen de vraag voor of de Inspectie voor de Gezondheidszorg de beveiliging van patiëntengegevens beter in de gaten moet houden. De woordvoerders van D66, CDA, PvdA, SP en natuurlijk 50PLUS zijn het met hem eens. Volgens CDA-Kamerlid Hanke Bruins Slot kan de Inspectie voor de Gezondheidszorg "niet zomaar achterover leunen. Op zijn minst verwacht ik dat de IGZ nagaat of de gegevens nu wel voldoende beveiligd zijn". Astrid Oosenbrug van PvdA is ook

nieuw en als ex-systeembeheerder een van de weinige Kamerleden met ICT-ervaring. Ze vindt dat het lek aantoont dat “het algemeen besef rond het belang van goede beveiliging er nog niet is”. De regering zou hebben toegezegd nog dit jaar met kaders rond beveiliging van medische gegevens te komen. Ze wijst naar het Nationaal Cyber Security Centrum, dat de zaak goed in de gaten zou moeten houden. De Winter kopt op 16 december: ‘Kamer wil controle IGZ op beveiliging medische dossiers’.

De dagvaarding volgt 8 januari 2013 en de zitting is op 1 februari. EenVandaag maakt er alvast een item van en opent op 31 januari: “Henk Krol weet niks van computers, maar wordt nu vervolgd voor computervredebreuk”. Krol vertelt beteuterd dat hij bij veroordeling zijn Kamerlidmaatschap en Koninklijke onderscheiding zal kwijtraken. In de beelden die volgen, wordt eerst het item van Omroep Brabant nog eens dunnetjes overgedaan. We zien weer de beelden van de site, afgewisseld met een verongelijkte Krol vanachter de geprinte laboratoriumuitslagen, met commentaar van De Winter.

De EenVandaag voice-over meldt vrolijk dat, nu Krol zich voor de strafrechter moet verantwoorden, hij een graag geziene gast is op hackersbijeenkomsten. Vervolgens zien we de 50PLUS’er vanaf een podium een zaal toespreken: “Ik heb zelf geen enkel nut bij wat je noemt een computerinbraak. Ik heb ook niet dagen achter het scherm gezeten om op een sneaky manier ergens binnen te komen. Nee, ik heb willen aantonen dat de gegevens van heel veel mensen in gevaar waren. Dankjewel.” Als hij na een bescheiden applausje een doos hackersbier krijgt, wil hij nog wel even kwijt: “Vroeger zeiden ze in de buurt, daar heb je die van die ouwelullenpartij. Maar nu kan ik trots door de straat als hacker!”

Even checken via de mail wat enkele bekenden in de zaal ervan vonden. Arda Gerkens, dagvoorzitter en namens HCC medeorganisator van het congres kan er nog steeds wel om lachen: “Henk was redelijk hilarisch omdat hij natuurlijk een echte digibeet is.” Oscar Koeroo (die van ‘Veere’) is kritischer en schrijft: “Mijn mening is dat hij zijn verdiende straf heeft gehad, omdat hij te ver is gegaan. Hij heeft meer dan nodig het lek aangetoond, gedemonstreerd aan diverse mensen en medische informatie ingezien die hij eigenhandig heeft weggestreept. Dit is geen lek verantwoord aantonen, maar de sensatie zoeken.” Hij vond het daarom ook jammer dat Krol tijdens de conferentie zijn verhaal deed en meteen weer wegging. Er was geen ruimte voor vragen of discussie.

Het betreft hier Alt-S, een IT-securitycongres van 22 januari. Op de site, door @legosteentje gemaakt, staat te lezen dat het als doel heeft “de kloof tussen bedrijfsleven en hackers te overbruggen”. Maar eigenlijk is het meer een soort schaduwconferentie. Het NCSC heeft namelijk die dag hun eigen securityconferentie, met prominent op de agenda hun nieuwe leidraad voor responsible disclosure. Het aantal aanmeldingen is echter zo groot, dat het centrum er veel heeft moeten weigeren. Daar is vervolgens druk over getwitterd door hackers die de afwijzing opvatten als uitsluiting en vervolgens zelf een congres zijn gaan organiseren. Het NCSC heeft nog geprobeerd ze te lokken met een grotere locatie, maar dan is ALT-S al een feit.

Een van de eersten die zich aanmeldt bij Alt-S is @meneer, oftewel zelfstandig beveiligingsexpert Andre Koot. Hij spreekt direct na Krol en is daar omdat hij pleit voor ‘trusted dislosure’. Er zou een onafhankelijk meldpunt moeten komen waar je ook anoniem meldingen kunt doen van beveiligingsproblemen. Experts nemen het dan over, zonder tussenkomst van rechtsgang en journalistiek. Hier is het uiteindelijk niet meer van gekomen, maar het was wel een mooi initiatief. Over de zaak Krol versus Diagnostiek voor U vertelt hij mij later: “Dit kan ik met de beste wil van de wereld geen hacken noemen. Door een open deur naar binnenlopen, is ook geen inbreken. Ik denk dat Krol terecht verontwaardigd was en geen idee had hoe hij dit naar buiten kon brengen dan door het zelf maar te laten zien. Het te lage niveau van beveiliging had hij misschien alleen bij het CBP kunnen melden, maar of hij dat kon doen is maar zeer de vraag. Het CBP heeft niet echt een toegankelijk loket.”

Koot maakt zich echter niet zo druk over Krol, maar vooral dat Diagnostiek voor U ermee wegkwam zulke hoogst vertrouwelijke gegevens onvoldoende te beveiligen. Hij begint daarom zelf een actie en vraagt diverse mensen om mee te doen. Op 30 januari 2013 krijg ik van hem deze mail:

“Beste Chris,

Ik heb een handhavingsverzoek ingediend bij het CBP naar aanleiding van de Henk Krol-casus. Ik vind de manier waarop het OM en de Raad van Bestuur om de materie heen draaien niet past, er is alleen aandacht voor de melder van het lek. Dat ging niet goed, maar het probleem is groter. Ik kreeg van Brenno een sjabloon van een verzoek, dat gaat morgen de deur uit.”

Koot vraagt mij om mee te doen. Hij verwacht niet dat we ontvankelijk verklaard worden omdat we geen belanghebbende zijn, maar wellicht helpt het wel om een onderzoek te laten starten. In de bijlage tref ik een brief die is gericht aan Jacob Kohnstam, de voorzitter van het CBP. Na een uiteenzetting van alle gebeurtenissen rondom Diagnostiek voor U wijst Koot de voorzitter op een van hun eigen bepalingen:

"Er wordt naar mijn mening niet voldaan aan artikel 13 Wbp, waarin wordt gesteld dat de beveiliging is voorzien van "passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking". Daarbij moet rekening worden gehouden met de stand der techniek. Daarvan is geen sprake als: bij bijzondere persoonsgegevens eenvoudig te achterhalen authenticatie wordt gebruikt; bij bijzondere persoonsgegevens gebruik wordt gemaakt van zogenaamde éénfactor authenticatie; er onvoldoende waarborgen zijn dat onbevoegden in het dossier van niet eigen patiënten wordt gekeken."

Volgens Koot moet het college daarom handhavend optreden. Zelf voel ik er eerlijk gezegd niet zoveel voor om ook zo'n brief te sturen. Want waarom zou ik me hiermee moeten bemoeien? Maar omdat ik dan net met dit onderzoek ben begonnen, lijkt het me wel interessant om te kijken of ik een reactie kan krijgen. In die zin ben ik dus wel een soort belanghebbende, ook al is het puur eigenbelang. Ik schrijf:

"Geachte heer Kohnstam,

Als het goed is, heeft u al meerdere verzoeken tot handhaving gekregen in de zaak Henk Krol vs Diagnostiek voor U. Daar wil ik deze aan toevoegen. Ik ben niet direct betrokkene in die zin dat het gaat om mijn persoonsgegevens. Wel ben ik betrokken bij deze zaak als onderzoeker. Ik ben namelijk bezig met een boek over responsible disclosure, waarin ik ook aandacht besteed aan deze zaak. Volgens diverse media bent u een onderzoek gestart, maar ontloopt de zorginstelling haar boete als ze binnen een bepaalde termijn orde op zaken heeft gesteld. Dat is vreemd, want er zijn immers al persoonsgegevens gelekt. Deze zaak wordt wel op een presenteerblaadje aangereikt. Het zou mooi zijn als het CBP dit aangrijpt om zorginstellingen op hun verantwoordelijkheden te wijzen."

Om het allemaal wat officiëler te doen lijken print ik de brief uit, onderteken ik hem en doe ik hem op de brievenbus. Uiteindelijk heb ik er niets meer van gehoord. Dat had ik eerlijk gezegd ook niet verwacht, want ik heb eigenlijk niets met de zaak te maken, maar het was wel het proberen waard. Nog zes anderen sturen dan naar aanleiding van Koots vraag een brief, met meer nobele intenties dan ik, dus wellicht hebben zij wel een reactie gekregen. Koot zelf in ieder geval wel, ook al was het pas na enige maanden. Het CBP heeft zijn verzoek inderdaad niet in behandeling kunnen nemen omdat hij geen klant of andere relatie is van Diagnostiek voor U. Het college zegt er wel onderzoek naar te gaan doen. De actie van Koot verschijnt ook in de media. Op 3 februari kopt De Winter op NU.nl: 'Beveiligingsexperts eisen CBP-onderzoek gehackte kliniek', met eronder citaten uit onze brieven.

Aldus: vele experts met meningen in de media, diverse Kamervragen, twee cyber security bijeenkomsten met de zaak op de agenda, een Inspectie voor de Gezondheidszorg die tot de orde wordt geroepen en een handhavingsverzoek naar het CBP... Dit is slechts een greep uit de context waarin de rechtszaak plaatsvindt. Daar komt voor Krol zelf bij dat er niet alleen een strafrechtelijke procedure tegen hem loopt, maar Diagnostiek voor U ook een civielrechtelijke procedure start om de schade op hem te verhalen.

De advocaat van DvU, Henk van Dijk vertelt tegen journalist René Schoemaker van Webwereld dat het gaat om 85.329 euro aan materiële schade. In dit bedrag zit een audit van 23.500 euro die is uitgevoerd door een extern bedrijf en een schade van 10.500 Euro bij de GGZ Eindhoven, waar de vijfcijferige psychiater werkt. De rest bestaat uit de uren die de medewerkers van Diagnostiek voor U hebben gemaakt aan "externe communicatie en het oplossen van het beveiligingsprobleem". Daarnaast zullen veertien personen van wie Krol hun dossier zou hebben ingekeken, elk afzonderlijk ook een schadeclaim indienen. De Winter gaat achter hen aan en krijgt te horen dat het voor deze patiënten niet duidelijk was waar ze hun handtekening onder hadden gezet. Een van de eisers dacht zelfs dat het ging om de verlenging van een behandeling. Een andere had zijn claim voor de zitting ingetrokken, omdat hij onder druk zou zijn gezet door GGZ Eindhoven.

De zitting is 1 februari en op 15 februari 2013 komt de rechtbank Brabant Oost met het vonnis. De hele procesgang, met details over hetgeen de betrokken hebben gedaan, is weer netjes gedocumenteerd in een rechtbankverslag. Daarin is uitgebreid te lezen hoe de officier van justitie haar aanklacht

onderbouwt en welke argumenten de verdediging er tegenover stelt. Wat de twee 50PLUS'ers destijds hebben gedaan weten we nu wel. Voor het doel van dit boek is het vooral interessant om te lezen hoe een standaardformulering uit het Wetboek van Strafrecht wordt vertaald naar een omslachtige beschrijving van hacken:

"Aan verdachte is ten laste gelegd dat hij op een of meer tijdstippen op of omstreeks 19 april 2012 te Best en/of Eindhoven, althans in Nederland, (telkens) tezamen en in vereniging met een ander of anderen en/of alleen, (telkens) opzettelijk en wederrechtelijk in een of meer geautomatiseerde werken, te weten de webserver van [site], of in een deel daarvan, is binnengedrongen, waarbij de toegang is verworven met behulp van een valse sleutel en/of door het aannemen van een valse hoedanigheid, immers heeft/hebben hij, verdachte, en/of zijn mededader(s) meermalen, althans eenmaal, ingelogd op die webserver, met gebruikmaking van inloggegevens en wachtwoord, tot welk gebruik hij en/of zijn mededader(s) niet gerechtigd is/zijn en/of (vervolgens) (medische) dossiers/gegevens bekeken, waarna verdachte vervolgens meermalen, althans eenmaal, gegevens, die waren opgeslagen, werden verwerkt of werden overgedragen door middel van dat/die geautomatiseerd(e) werk(en) waarin verdachte zich wederrechtelijk bevond, voor zichzelf of een ander heeft overgenomen, afgetapt of opgenomen, immers heeft hij, verdachte, meermalen, althans eenmaal, deze (medische) dossiers/gegevens gekopieerd/(uit)geprint."

Het gaat hier dus om computervredebreuk, oftewel artikel 138ab lid 1 en 2 van het Wetboek van Strafrecht. De vraag is of deze onrechtmatige daad geoorloofd is omdat het een hoger maatschappelijk belang dient, in dit geval de privacy van de Brabantse patiënten en de schending daarvan tegen te gaan door het naar buiten brengen van het lek. Dan valt het onder de vrijheid van meningsuiting. Het is wellicht ook daarom dat de officier van justitie juist begint die redenering om te keren en is volgens hem Krol de privacyschender:

"Het recht op privacy van derden was in het geding. Het ging om gevoelige, medische gegevens van derden, die zonder hun goedvinden, zelfs buiten hun medeweten, zijn geraadpleegd. De maatschappelijke relevantie van het aan de kaak stellen van de misstand was veel beperkter dan de verdachte doet voorkomen. Het zogenaamde 'gat' in de beveiliging zat niet zozeer in de technische opbouw van de website, maar in het feit dat door een gebruiker op onzorgvuldige wijze is omgegaan met inloggegevens. Het door de verdachte opgevoerde doel van zijn handelen had ook op een minder vergaande manier bereikt kunnen worden. Verdachte en medeverdachte hadden zich kunnen beperken tot het inloggen in het systeem, zonder verder specifieke dossiers met daarin voornoemde gevoelige gegevens te bevragen. Ze hadden zich in ieder geval kunnen en moeten beperken tot het openen van het dossier van medeverdachte. Zowel voor het geval dat verdachte van mening is dat hij heeft gehandeld als ethisch hacker, als voor het geval hij heeft gehandeld als journalist, heeft hij een zorgvuldige en noodzakelijke stap overgeslagen. Hij heeft gegevensbeheerder niet op een afdoende wijze op de hoogte gesteld voordat hij het hele verhaal naar buiten heeft gebracht. Een telefoontje met een telefoniste was in dat licht niet voldoende."

Volgens de officier van justitie wegen in dit geval "het recht op de bescherming van de integriteit van het geautomatiseerde systeem" en "het recht op privacy van de betrokken derden" zwaarder dan "het recht op de vrijheid van meningsuiting en nieuwsgaring van de verdachten". Artikel 10 van het EVRM staat een strafvervolging, noch een strafoplegging van verdachte in de weg.

De advocaat van Krol keert de redenering weer om: het zijn niet de verdachten, maar de andere betrokkenen die de privacy van de patiënten in gevaar brengen. Ten eerste Diagnostiek voor U, omdat er geen regels werden gesteld aan wachtwoorden. Daardoor was het te makkelijk voor de verdachten om in te loggen vanaf hun eigen computer. Bovendien: "Het systeem hield niet bij vanaf welk IP-adres werd ingelogd. Het hield alleen bij welke dossiers werden geraadpleegd." Krol bracht zijn bevindingen vervolgens zelf naar buiten omdat hij "op dat moment lid van de schrijvende pers en Statenlid was". Hij had bewijs nodig en deed dat door enkele dossiers te printen en te anonimiseren. Ook justitie zelf treft blaam volgens de advocaat, wegen het schenden van het medisch beroepsgeheim: "De identificeerbare gegevens van een patiënt waren voor iedereen met de inloggegevens toegankelijk. Zelfs ook voor justitie, zegt de aangever."

Nu de rechter. Dat er computervredebreuk is gepleegd, daar is iedereen het dus wel over eens. Dat de mede 50PLUS'er zich ervan wilde distantiëren toen Omroep Brabant erbij kwam, doet daar volgens hem niets aan af. Beiden zijn schuldig. Maar, is hier sprake van zeer bijzondere omstandigheden en hogere belangen die een dergelijke inbreuk rechtvaardigen? Volgens hem zijn hierbij drie factoren van

belang. Eerst moet worden beoordeeld of verdachten hebben gehandeld in het kader van een wezenlijk maatschappelijk belang. Zo ja, hebben zij gehandeld volgens de regels van proportionaliteit en subsidiariteit, oftewel gingen ze niet verder dan noodzakelijk om hun doel te bereiken en was er geen andere, minder vergaande, manier om dat te kunnen bereiken?

In het eerste punt kan de rechter volledig meegaan: het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens is zeker een wezenlijk maatschappelijk belang. Dat Krol zelf wilde vaststellen of de bevindingen van de medeverdachte juist waren, vervolgens ging inloggen op de website en enkele dossiers ging raadplegen, begrijpt hij ook. Zo ook de prints als bewijs, want Krol heeft daarbij zorgvuldig gehandeld door ze te anonimiseren. Hiervoor krijgen hij en de medeverdachte dus geen straf.

Maar, en nu komt het, Krol heeft meerdere keren de gegevens geraadpleegd en uitgeprint en dat ook nog in aanwezigheid van de journalisten van Omroep Brabant. Dat is volgens de rechter buitenproportioneel. Bovendien was het "allerminst noodzakelijk om voor de oplossing van het door verdachte gesignaleerde probleem meteen naar de media te stappen". Hij had namelijk geen concrete aanwijzingen dat andere personen over deze inloggegevens beschikten. Het probleem was namelijk niet veroorzaakt door een technisch gebrek aan het computersysteem, maar door een gebruiker die onzorgvuldig met zijn inloggegevens was omgegaan. De onthulling had daarom ook anders en zonder de media gekund, oftewel op subsidiaire wijze. Krol is immers Statenlid en verslaggever, dus mag verwacht worden dat hij in staat is zonder al te veel moeite de juiste persoon binnen de organisatie te benaderen. Krol bedoelde het goed, maar heeft gewoon teveel uit de kast gehaald. Hij krijgt hiervoor een geldboete van 750 euro.

Tot slot de schadevergoeding. Dat is het civielrechtelijk deel van het proces, maar om hiervoor alvast in het strafrechtelijk proces een eerste stap te zetten, heeft de advocaat van Diagnostiek voor U een symbolisch bedrag gevraagd: 1000 euro. De patiënten, waarvan er inmiddels nog negen over zijn ook: 100 euro per persoon. De rechter vindt het echter moeilijk vast te stellen wat de geleden immateriële schade dan is. Verder onderzoek hiernaar vindt hij bovendien "een onevenredige belasting op de strafzaak". Hij stelt de schade daarom op nihil, oftewel geen vergoeding.

Krol komt er gezien de straf die hem boven het hoofd hing nog redelijk vanaf. Hij moet 750 euro en de proceskosten betalen en niet de schadevergoeding van 85.329 euro. Bovendien blijkt eens te meer dat rechters gevoelig zijn voor ethisch hacken, want het aantonen van de lekke site is in dit geval belangrijker dan de computervredebreuk. Alleen moet je dan niet meer dan nodig uit de kast halen. Hier dus een deeloverwinning voor verantwoord onthullen, die wellicht nog interessante jurisprudentie zal blijken voor toekomstige zaken. Bij het NCSC zien ze deze zaak zelfs als een eerste testcase voor hun leidraad responsible disclosure.

Diagnostiek voor U blijkt later ook de positieve kanten van de zaak in te zien. Directeur Van der Put vertelt 10 april 2013 op NU.nl dat hun beveiliging inderdaad tekort schoot en er nu meer aandacht voor is. "Dat systeem wordt ook door andere instellingen gebruikt. Opeens realiseerden veel partijen dat zij ook kwetsbaar waren (…) Je wilt niet weten hoeveel bestuurders van zorginstellingen naar mij toekwamen met vragen of opmerkingen." Artsen moeten nu een betere inlognaam bedenken en inloggen met een extra code die ze via sms ontvangen, oftewel de gewenste tweefactor authenticatie. De Winter concludeert op NU.nl: "Hack Henk Krol vergroot bewustzijn zorgsector."

Dit wordt, anderhalf jaar na dato bevestigd als ik mijn tekst naar Diagnostiek voor U stuur. Yvon van den Berg, manager relatiemanagement, marketing & communicatie schrijft in een reactie: "Deze zaak heeft een bijdrage geleverd ons bewustzijn ten aanzien van informatiebeveiliging te vergroten. Voorziene beveiligingsmaatregelen zijn versneld ingevoerd en hebben een positieve bijdrage geleverd aan onze organisatie."

Mooi, dan is het allemaal toch nog ergens goed voor geweest. Maar wat in de periode na de rechtszaak toch vooral bleef hangen in de publieke opinie is dat Krol wel is veroordeeld en Diagnostiek voor U niet. Oftewel, ethisch hacken loont niet. Ook diverse Kamerleden zijn hierover verontwaardigd. Een VVD-Kamerlid zou zelfs met de pet zijn rond gegaan om Krols boete te betalen. Intussen hebben politie, OM, NCSC, IGZ, CBP en de Kamer hun handen vol aan nog een zaak die dan al een tijdje speelt: de hacker van het Groene Hart Ziekenhuis, die nog veel meer uit de kast haalde. Met ook hier weer een hoofdrol voor Brenno de Winter.

Bronnen

E-mail correspondentie met Brenno de Winter, Andre Koot, Arda Gerkens, Oscar Koeroo, Henk Krol en Yvon van den Berg.

- NOS, (2013, 31 januari) ‘Henk Krol voor de rechter’ *EenVandaag*
- *Omroep Brabant* (2012, 19 april) ‘Medische gegevens duizenden Brabanders op straat’
- *Omroep Brabant* (2012, 19 april) ‘Brenno de Winter: “Medische gegevens op straat mogelijk overtreding wet”’
- *Omroep Brabant* (2012, 20 april) ‘Diagnostiek voor U wijst vooral naar anderen na lekke website’
- *Omroep Brabant* (2012, 20 april) ‘Diagnostiek voor U doet aangifte van diefstal’
- *Omroep Brabant* (2012, 4 december) ‘Henk Krol vervolgd voor hacken medische gegevens’
- *Omroep Brabant* (2012, 5 december) ‘Brenno de Winter over rechtszaak hackende Henk Krol: “Deze rechtszaak zou niet nodig moeten zijn”’
- *Omroep Brabant* (2013, 30 januari) ‘Psychiater schendt beroepsgeheim in hackerszaak Henk Krol’
- *Omroep Brabant* (2013, 15 februari) ‘Diagnostiek voor U laat schadeclaim tegen Henk Krol vallen’
- *Omroep Brabant*, (2013, 26 februari) ‘VVD Kamerlid 'met de pet rond' om boete Henk Krol te betalen’
- Rechtbank Oost-Brabant (2013, 15 februari) *Vonnis, Parketnummer: 01/820892-12*
- Schoemaker, R. (2013, 14 januari) ‘'Gehackt' medisch centrum eist 85.000 euro van Krol’ *Webwereld.nl*
- Winter, B. de (2013, 16 december) ‘Kamer wil controle IGZ op beveiliging medische dossiers’ *NU.nl*
- Winter, B. de (2013, 3 februari) ‘Beveiligingsexperts eisen CBP-onderzoek gehackte kliniek’ *NU.nl*
- Winter, B. de (2013, 9 februari) ‘GGZ Eindhoven stuurt medische gegevens aan ICT-bedrijf’ *NU.nl*
- Winter, B. de (2013, 10 april) ‘Hack Henk Krol vergroot bewustzijn zorgsector’ *NU.nl*