Jouw data is zelden veilig bij een beheerder

Het parkeren van data in de vorm van een website, e-mails of in de *cloud* is niet van risico's gevrijwaard. Jouw data staat altijd ergens anders op een computer geparkeerd, of die nu in beheer is van een commercieel bedrijf of een kleine activistische provider.

De meeste mensen vertrouwen erop dat bedrijven of personen die hun data op het internet beheren dit netjes doen. Tot een paar jaar geleden was er nog nauwelijks besef over die vertrouwelijkheid en de beveiliging van data. Recente discussies over privacy, maar ook datalekken en hackers, hebben bijgedragen aan een iets groter bewustzijn. Daarnaast zijn de afgelopen tijd in binnen- en buitenland diverse servers en data van activisten in beslag genomen.

Het is logisch dat de discussie over de veiligheid van opslag moeizaam verloopt, data op het internet is ongrijpbaar. De ontwikkelingen gaan snel, men is schijnbaar afhankelijk en de online services van Google, Yahoo, Hotmail en Facebook lijken niets te kosten. Over grote bedrijven wordt echter veel vaker bericht zodra er sprake is van veiligheidslekken, privacyschendingen of andere zaken. Ook voeren individuen actie tegen privacyschendingen door internetgiganten, zoals het vergeetrecht van Google en persoonsdata van Facebook.

De actievoerder online

Inlichtingendiensten beleven hoogtijdagen met '*big data*', zo maakte klokkenluider Edward Snowden de wereld duidelijk aan de hand van gelekte overheidsdocumenten van de Amerikaanse datastofzuiger NSA (National Security Agency). Activisten daarentegen zijn massaal overgestapt op het voeren van online-campagnes en mobilisatie voor protest via Twitter, Facebook en Google. Traditionele actiemethoden, zoals het verspreiden van papieren pamfletten, kranten en brochures, zijn veelal op de achtergrond geraakt.

Met de digitale oplossingen hebben zij vaak hun autonome informatiestructuur losgelaten en uitbesteed aan dominante technologische bedrijven. Het is kostenbesparend en het bereik zou groter zijn, maar het zicht op de data zelf en de gegevensverwerking van gebruikers, ondersteuners en sympathisanten van de campagne is volledig verdwenen. Veel van de commerciële internetbedrijven nemen het namelijk niet zo nauw met zowel de veiligheid als de privacy van haar gebruikers. Daarnaast hebben deze digitale multinationals nauwe contacten met overheden, zoals Snowden met zijn gelekte documenten

heeft aangetoond. Kleinere internetbedrijven verschillen meestal nauwelijks van de grote jongens.

In de artikelen 'Met de billen bloot op Facebook' en 'FB inlichtingendienst' uit *Observant #65* wordt dieper ingegaan op de werking van sociale media en de wijze waarop Facebook met data van haar gebruikers omgaat. Daarin wordt niet alleen gewaarschuwd voor de werkwijze van de multinationals, ook de gebruikers, waaronder activisten, dienen in deze hun verantwoordelijkheid te nemen. Zij delen zoveel informatie op sociale media en nodigen anderen uit dit ook te doen, waardoor er in wezen organogrammen van actiegroepen, campagnes of netwerken kunnen worden samengesteld.

Dat is ideaal voor zowel bedrijven die geld willen verdienen aan advertenties en data op internet, als voor inlichtingen- en veiligheidsdiensten. De internetgiganten bieden om die reden steeds meer gratis toepassingen aan, zodat gebruikers naast sociale media ook hun e-mails, foto’s, chats, documentenopslag kunnen overhevelen naar de computers van deze bedrijven. De vraag of die data daar veilig geparkeerd staat, is meestal van ondergeschikt belang. 'Het zal wel goed geregeld zijn', is de doorsnee gedachte.

Een enkele keer haalt de in beslagname van een server of data de media. Microsoft wil bijvoorbeeld bepaalde data niet overhandigen aan de Amerikaanse FBI omdat deze data in Ierland geparkeerd staat en de Amerikanen daar geen jurisdictie hebben. Zulke berichten zijn echter spaarzaam. De meeste bedrijven willen dit niet aan de grote klok hangen, omdat gebruikers zich dan zullen afvragen of die gratis diensten niet ten koste gaan van allerlei rechten. Of dat je documenten van je opleiding niet in een datacentrum in Nederland, maar elders in de wereld geparkeerd blijken te staan.

Veiligheid essentieel

Voor activisten is veiligheid van data eigenlijk essentieel wanneer je acties, campagnes, etc. voorbereid. Misschien willen donateurs of activisten anoniem blijven, wil je niet dat bekend wordt dat een bepaald e-mailadres aan jou als persoon is gekoppeld, of dat je woonadres te traceren valt. Data is meestal een goudmijn voor de overheid en een in beslag genomen server of dataset kan veel onthullen, niet alleen over een persoon, maar ook over groepen, netwerken, campagnes etc.

De afgelopen tijd zijn er enkele acties van overheden geweest waarbij servers en data van activisten in beslag zijn genomen. In 2011 werd in Nederland een dataset in beslag genomen bij *Animal Rights Media*, een

zelf beheerde server voor dierenrechtenactivisten. In de zomer van 2014 werd de server van de linkse DIY-website *Indymedia Bristol* in beslag genomen door de Engelse politie. Ook vorig jaar werd een server van de Amerikaanse links-radicale groep Mayfirst door de FBI in beslag genomen op last van de Griekse overheid.

In alle gevallen bleef het in eerste instantie onduidelijk wat er precies aan de hand was. De beheerders van de websites en servers traden niet meteen naar buiten met het nieuws. Bij het Engelse en Nederlandse voorbeeld kun je je afvragen waarom er niet direct een verklaring is uitgegaan van de beheerders. De Amerikanen van Mayfirst mochten niets naar buiten brengen, er gold een *Gag Order.* Zij moesten van de politie zwijgen over de zaak, anders zouden ze zelf vervolgd worden.

Het Nederlandse voorbeeld draait om *Animal Rights Media* (ARM). Enige jaren geleden beheerde een groep activisten vanuit Nederland een server in Denemarken waarop verschillende dierenrechtengroepen hun websites lieten draaien met eigen e-mailadressen. Het achterliggende idee was dat je met servers in eigen beheer zelf zicht kon houden op de content en kon reageren op eventueel ingrijpen door de overheid. Het onderhoud van de oorspronkelijke ARM-server was goed geregeld.

De Amerikaanse FBI echter zette de provider waar de server zich bevond onder druk bij een politieoperatie tegen de Amerikaanse actiegroep LAKills.net. Wat er precies met de data is gebeurd, is onduidelijk. Ook Animal Rights Media kreeg een brief, maar deelde die niet met de activistische achterban. De mensen die de server beheerden, hebben geen verklaring doen uitgaan, ook niet toen zij de server verplaatsten naar Nederland.

Er is door de groep nog wel onderzoek gedaan om een nieuwe server in een ander land op te zetten, maar dat bleek niet haalbaar. Enerzijds was dat het gevolg van een financieel verhaal, anderzijds hielden de technische mensen die de server onderhielden ermee op.

'Activepaulus'

Dit betekende echter niet het einde van Animal Rights Media. De Nederlander Paul alias 'activepaulus', een van de personen van de oorspronkelijke groep, ging in z'n eentje verder met een nieuwe server. Hij bood hosting en e-maildiensten aan en verschillende Nederlandse groepen en personen, zoals de organisatie van het jaarlijkse anarchistische actiekamp PinksterLanddagen en activiste Joke Kaviaar, maar ook buitenlandse groepen, maakten gebruik van zijn diensten. Paul presenteerde zich uitdrukkelijk als een activistische hoster met kennis

van zaken. Slechts een enkele gebruiker heeft Paul ooit gevraagd hoe het met de veiligheid van de server zat, of iemand anders benaderd om naar de server te kijken.

De website van Joke werd lange tijd door Paul gehost. Zij is gevraagd naar haar ervaringen met hem: 'Tot 7 december 2011 werd mijn website en daaraan gekoppelde e-mailadres gehost door Paul, ofwel Animal Rights Media. Paul heeft me dit in 2004 aangeboden. Hij presenteerde zich als *reseller*, dat wil zeggen: hij huurde een server bij een groot hostingbedrijf, Flexwebhosting. Ook deed hij het voorkomen alsof hij wist wat hij deed. Voor mij als leek was hij een 'techie'. Het zou veilig zijn, beweerde hij, de overheid ofwel justitie zou er niet bij kunnen.'

Niet alle gebruikers van ARM wisten dat Paul zelf geen server bezat, hij had niet de beschikking over een fysieke machine. De server waar hij gebruik van maakte, draaide in de *cloud.* Het was misschien een virtuele server, maar eerder *cloud* waar hij een aantal websites op kon draaien. Een *cloud* is zeg maar een term die wordt gebruikt indien je een server laat draaien op een harde schijf van een computer van iemand anders. Over de hardware had Paul dus niets te zeggen. Flexwebhosting schrijft op haar website bij *reseller*: 'Zelf uw hostingdiensten verzorgen: Met *reseller* hosting van Flexwebhosting kunt u zelf eenvoudig hostingpakketten voor u zelf of voor uw klanten samenstellen.'

Een ingevoerde in de technische status van de service die Paul aanbood zegt hierover: 'Paul gebruikte een VServer of OpenVZ opstelling als 'prefab' server. Bij een virtuele server wordt een gehele machine (computer) gesimuleerd bij het bedrijf waar je internetruimte huurt. Je moet het zo zien dat een OpenVZ/VServer geen eigen dienst is. De bestanden staan als het ware niet op je eigen machine maar in een map op de *host*. Hierdoor is het dus veel moeilijker om je gevoelige data te beschermen tegen toegang van het hostingbedrijf.'

In antwoord op vragen van Jansen & Janssen zegt Paul dat 'de servers nooit slecht hebben gefunctioneerd. Waar dat verhaal vandaan komt vind ik zeer bijzonder, er zijn altijd geschoolde IT'ers bij betrokken geweest.' Hij presenteert zichzelf als IT-specialist in zijn contacten met mensen en zijn cv op zijn persoonlijke website. In antwoord op vragen geeft hij aan dat hij bij 'een gerenommeerd ICT-bedrijf werkt dat gespecialiseerd is in cloud-servers.' Hij zou daar Senior Network Programmer zijn. In zijn cv staat dat het enige ICT-bedrijf waar hij nu nog werkt 'W. K. Computerhulp' is (de naam van de persoon is geanonimiseerd). Of zijn verhaal over zijn kennis ten aanzien van serveronderhoud klopt, is niet vast te stellen. Toch zijn er grote vraagtekens te zetten bij de veiligheid van de service die hij aanbood.

DDoS-aanvallen

Joke Kaviaar wist dat Paul niet zelf een server beheerde, maar die huurde bij Flexwebhosting. 'Door de jaren heen waren er wel eens problemen. Zo is er menig DDoS-aanval geweest waardoor mijn site offline raakte en hij de boel moest resetten', schrijft zij. Paul verzekerde haar echter dat hij wist wat hij deed en dat haar data, website en e-mail veilig bij hem waren.

Paul kon dat echter nooit met zekerheid beweren. De fysieke server was eigendom van Flexwebhosting waardoor derden in ieder geval eenvoudig bij de server konden komen en, indien nodig, ook naar de virtuele server van Paul konden kijken. In het geval van Joke bleken die derden politie en justitie te zijn. Haar data werd door de overheid in beslag genomen.

Paul zelf beweert dat hij een server draaide met 'CentOS en als webbeheer een *customized* versie van Direct Admin. Deze *customized* versie hebben we zelf aangepast om alle vormen van beveiligingslekken dicht te gooien.' Joke, en waarschijnlijk ook anderen, waren geïmponeerd door deze termen en zullen niet verder hebben doorgevraagd.

Iemand die heel lang met Paul heeft gewerkt schrijft ons: 'Hij heeft zich in onze tijd nooit echt bezig gehouden met de technische zaken aangaande de server. Eigenlijk is het zo dat, als ik erover terugdenk, hij alleen dingen via een webpanel kon instellen.' Specifiek over de DDoS-aanvallen op de server van Animal Rights Media stelt deze bron: 'Van DDOS-aanvallen weet ik niets af via de Deense server. Ik heb het idee dat dat verhaal met een korrel zout moet worden genomen.'

Aanhouding Joke K.

De onveiligheid van de server van Paul hadden grote gevolgen voor Joke. 'Op 13 september 2011 vielen rechercheurs van de Nationale Recherche mijn woning binnen. Er werd vanwege een viertal teksten die ik geschreven en gepubliceerd had huiszoeking gedaan waarbij ik tevens werd aangehouden wegens opruiing '*met terroristisch oogmerk*'. Ze hebben me drie dagen in Zwolle in volledige beperking vastgehouden. Het heeft nog tot voorjaar 2012 geduurd voor ik erachter kwam dat er nog veel meer schade was aangericht door de onveilige server van Paul. Ik kreeg toen het procesdossier van de zaak in handen, door de Nationale Recherche 'Gulkana' genoemd.'

In de drie dagen dat Joke in volledige beperkingen in Zwolle gevangen

werd gehouden, zat de overheid niet stil. 'Justitie had een '*vordering bevriezing van gegevens*' en een '*vordering verstrekking historische gegevens*' ingediend bij Flexwebhosting, de host waar Paul de server huurde. Uit het dossier blijkt dat ze meer dan 4700 e-mails in handen hebben gekregen. Flexwebhosting had met de '*vordering verstrekking historische gegevens*' eveneens het bevel gekregen '*geheimhouding in acht te nemen omtrent al hetgeen u terzake van de vordering bekend is*'. De host had dus zwijgplicht en voldeed aan bevriezing en verstrekking.'

Omdat Paul niet zelf over de fysieke server beschikte, maar harde schijfruimte huurde van een extern bedrijf, had hij niets te zeggen over de data en kon tevens geen enkele veiligheid garanderen. 'Paul heeft niets van de acties van justitie en de medewerking van Flexwebhosting gemerkt. Het is gebeurd zonder dat er bij hem alarmbellen afgingen. Een aantal e-mails met daarin opgenomen de gewraakte 'opruiende' teksten zijn in het procesdossier terechtgekomen en maakte deel uit van de bewijsvoering', stelt Joke.

Paul zelf over de acties van politie en justitie: 'Die ochtend heeft justitie contact opgenomen met Flexwebhosting en deze ertoe aangezet enkel de website van Joke Kaviaar plat te leggen. Flexwebhosting heeft geen enkel contact met ons daarover opgenomen. Tevens was het een verzoek en dus niet een gerechtelijk bevel. We hebben hier contact over opgenomen met Flexwebhosting. Deze was, hoewel zij altijd op de hoogte waren van de inhoud van de websites, ineens van mening veranderd omdat dit criminele activiteiten zouden zijn.'

Op vragen waarom zijn verhaal over zijn contacten met FLexwebhosting en het nauwe contact met Joke over de zaak in tegenspraak zijn met de verhalen van anderen, waaronder dat van Joke zelf, wil Paul niets zeggen. 'Wij hebben daarna de hele server uitgepluisd en geconstateerd dat er geen data van andere websites was meegenomen.' Hoe Paul dit heeft kunnen constateren, kan hij niet duidelijk maken.

Bristol Indymedia

De constructie die Paul gebruikte voor zijn server werd ook toegepast door Bristol Indymedia (BIM), een alternatief mediaproject dat in 2001 online ging. Ook deze club had een virtuele server gehuurd bij een commercieel bedrijf. Op de website konden mensen zelf hun bijdragen posten, zoals bij Indymedia Nederland.

Augustus 2014 ging de website van BIM offline. Een week lang was er sprake van onrust vanwege de onduidelijkheid wat er aan de hand was. Op 27 augustus 2014 bracht BIM een verklaring uit: *'Last week we heard*

from our web hosts that the police had a court order to access the Bristol Indymedia server. […] We consider this server to be compromised, users should assume that from this point on the Police have access to the IP address of anyone accessing this site.'

Wederom bleek naderhand dat de fysieke server niet in bezit was van de beheerders van BIM, maar elders werd afgenomen van een Engelse hostingpartij. Bristol Indymedia stelt: '*We don't know for sure, but assume that our web hosts have complied with the order and given the police this access*.' Hoe het met de IP-loggegevens van de gebruikers van de site was gesteld, bleef onduidelijk. Indymedia UK: '*The false claim is that IP logs were kept for the last 16 months. As the site only launched, with a brand new CMS, on March 21st, 2014, this clearly cannot be true.*'

Iemand reageert op libcom.org: '*It sounds like Bristol Indymedia weren't storing IP addresses, so previous users should be okay, I think. In general it'd be good practice to hide your IP using a proxy or VPN if you really must post online about something illegal (or don't post at all, preferably).*' Het team van BIM heeft echter zelf verwarring gezaaid door in haar verklaring te stellen dat '*users should assume that from this point on the Police have access to the IP address of anyone accessing this site*.'

Naast kritiek op het beleid aangaande het bewaren van historische gegevens, volgde er een discussie over het lekken van IP-adressen door de DIY-website. Indymedia UK meldde dat Bristol Indymedia werd gehost op een 'Bytemark Debian virtual server.' Vanaf maart 2014 draait de website op het gebruiksvriendelijke gratis Wordpress publicatie platform. Een van de gebruikers stelde na de inbeslagname door de politie de vraag of het gebruik van Wordpress wel zo'n veilige optie was. Omdat Indymedia ook reacties van gebruikers toelaat, is de vraag gerechtvaardigd waarom de website niet voldoende beveiligd wordt door bijvoorbeeld een versleutelde verbinding (https).

Hoe lang en wat er van de gebruikers is vastgelegd, blijft onduidelijk, maar Bristol Indymedia had in ieder geval de moed om te verklaren wat er gebeurd was. Mede omdat het bedrijf waar zij hosten hen had ingelicht. Paul van Animal Rights Media meed elke verantwoordelijkheid, of hij nu wel of niet wist wat er plaatsgevonden had.

Nieuwe dreiging

Joke over de dagen voordat haar website offline ging: 'Mijn arrestatie werd pas na mijn vrijlating bekend toen justitie het met een persbericht,

voorzien van citaten uit mijn teksten, de wereld in slingerde. Ik heb Paul ook zelf gebeld en gemaild, de teksten stonden immers op zijn server. Binnen een week na mijn vrijlating begon justitie te dreigen mij opnieuw te zullen arresteren omdat de teksten waarover het ging nog op mijn site stonden. Ik heb geweigerd die te verwijderen en stelde Paul op de hoogte van deze ontwikkeling.'

Of Paul de kennis en vaardigheden bezat om het hoofd te bieden aan de complexe technische en juridische situatie, is onduidelijk. Joke was echter verbaasd over het offline gaan van haar website. 'Op 7 december 2011 belde iemand mij dat justitie mijn site ontoegankelijk had laten maken. Ik was verbaasd, want wist van niks. Ik belde als eerste Paul om te vragen of het klopte en zo ja, hoe dat dan kon. Hij zei dat hij kon zien dat de rechten anders waren gezet door onbekenden en zei dat ie dat kon fiksen. Even later belde hij dat het probleem was opgelost.'

Paul bleek echter niet lang in staat om de website online te houden. Joke belde hem daarover en kreeg de indruk dat hij niet wist wat er aan de hand was. 'Hij reageerde alsof hij er niks van begreep en zei dat hij het niet kon oplossen.' Wat iedereen had kunnen weten, was dat omdat Paul niet over een eigen fysieke server beschikte en slechts prefab serverruimte huurde bij een internetbedrijf en weinig zeggenschap had over het beheer van die server. Daarnaast wist hij eigenlijk niet wat hij deed, bleek de ‘achterkant’ van de server lek en kon Flexwebhosting op last van justitie de website van Joke Kaviaar offline halen.

Paul zelf zegt over het offline gaan van de website: 'Het bleek dat de website wel op de server bleef staan, maar dat de rechten waren veranderd waardoor de *public map* steeds op privé werd omgezet. We hebben dit eerst handmatig aangepast, met als resultaat dat de website enkele minuten weer online was. Echter na enige tijd klapte deze weer uit. We zijn toen op onderzoek uit gegaan waarna bleek dat Flexwebhosting een proces had geïmplementeerd om dit automatisch weer aan te passen.'

Paul zegt dat hij juist wel veel verstand van zaken heeft en tevens veel contact met Flexwebhosting. 'Toen wij dit proces eruit haalden, volgde het eerste telefonische contact met Flexwebhosting (hiervoor hadden we per mail wisselende communicatie). De provider dreigde de complete server er helemaal uit te trekken. Om onze andere klanten niet te duperen, hebben we dit aan Joke uitgelegd en de opties besproken.' Hoe Paul bij dat 'proces' kon komen, maakt hij niet duidelijk. Joke beweert echter dat Paul reageerde alsof hij er niks van begreep en dat hij het niet kon oplossen. Waarom Paul niet aan de bel heeft getrokken is onduidelijk, alsmede waarom hij geen persverklaring heeft verspreid.

Veiligheidsrisico

In tegenstelling tot Bristol Indymedia en ook Mayfirst hebben Paul en Animal Rights Media nooit iets geschreven over wat er gebeurd is met de e-mails en de website van Joke Kaviaar. Dat is kwalijk, want niet alleen die data werd op zijn server gehost, ook die van andere groepen uit binnen- en buitenland, zoals de Pinksterlanddagen. Die liepen eveneens gevaar omdat de server van Paul een veiligheidsrisico was. Joke schrijft hierover dat 'Paul wat lacherig gereageerd heeft, alsof het hem niets kon schelen.'

Omdat de diensten die Paul aanbood onveilig waren, besloten enkele mensen de server onschadelijk te maken. Dit werd overigens niet meteen gedaan. Een jaar lang is geprobeerd Paul meer te laten doen aan de veiligheidsaspecten van zijn diensten. Een van de betrokken mensen: 'De server van Animal Rights media is neergehaald omdat deze een paar keer het middelpunt vormde van een justitieel onderzoek naar activisten. Met het onder ogen krijgen van het strafdossier van Joke Kaviaar bleek (en later in de rechtszaak) dat de VPS/Server lek was en via de achterkant benaderbaar voor inlichtingendiensten en justitie.'

Paul is door diverse mensen benaderd om zijn server beter te beveiligen of om internetdiensten aan andere organisaties over te dragen en in ieder geval mensen te waarschuwen. Eén van de betrokkenen: 'Paul was nooit benaderbaar. Hij gaf aan dit onnodig te vinden. Bij activisten bakte hij zoete broodjes en liet hen geloven dat zijn server goed beveiligd was.' De situatie was onhoudbaar, al helemaal nadat bleek dat justitie mogelijk ook tegen anderen juridische stappen zou ondernemen. 'Wij waren nog in volledige voorbereiding toen het nieuws kwam dat er weer een actiegroep in het vizier lag bij justitie vanwege de server', stelt een van de betrokkenen.

Helaas kon niemand van de gebruikers worden ingelicht. Volgens een betrokkene was daar geen tijd voor. 'De server en Paul stonden waarschijnlijk onder observatie vanwege Joke Kaviaar en 'anonymous' die haar website weer overeind hielp. Het van tevoren waarschuwen van mensen konden we niet doen, omdat we niet wisten of iemand in paniek zou raken waardoor ons de toegang tot de server afgesneden kon worden.' Er was dus geen tijd om mensen en groepen te waarschuwen die eigenlijk al lang op de hoogte waren van het feit dat er iets mis was met de diensten die Paul aanbood. Zij hadden zelf geen stappen gezet om zowel hun eigen data als de data van hun gebruikers veilig te stellen.

In het geval van Paul met zijn Animal Rights Media server was er zoveel

mis dat het voor de overheid en de commerciële partij erg gemakkelijk was om van zijn onwetendheid gebruik te maken. Bij Bristol Indymedia kun je achteraf ook vraagtekens zetten over de in acht genomen veiligheid ten aanzien van haar gebruikers. BIM valt misschien te verwijten dat zij niet helder communiceerden over het loggen van gegevens en het ontbreken van enige versleuteling bij het communiceren op de nieuwssite.

Aan de andere kant plaatste BIM zo snel mogelijk informatie over de in beslag genomen server en werd er gecommuniceerd over mogelijke data van gebruikers die in het bezit waren gekomen van de overheid. Paul daarentegen heeft totaal niet gecommuniceerd met allerlei gevolgen voor zeker één individu, Joke Kaviaar, maar misschien ook voor anderen. Naast de onveiligheid van de server, het niet inschakelen van mensen met kennis om de beveiliging te verbeteren, is hem aan te rekenen dat hij niet heeft gecommuniceerd over wat er plaats gevonden heeft.

Mayfirst

Een andere groep die niet met de buitenwereld communiceerde nadat het offline ging is Mayfirst, maar in tegenstelling tot Paul wisten zij wél waar ze mee bezig waren en was het hen door de Amerikaanse autoriteiten verboden te communiceren over het voorval. Mayfirst bezit haar eigen fysieke infrastructuur. Kort na de in beslagname van de Bristol Indymedia server werd in Amerika ook een server uit een serverkast getild. De zaken hebben echter niets met elkaar te maken. Deze server was van het internetcollectief Mayfirst/People Link. Mayfirst host veel NGO’s in Amerika, maar ook daarbuiten, zoals van groepen in Griekenland.

Aan het einde van de zomer van 2014 was het plots niet meer mogelijk te mailen en mail te ontvangen via de Mayfirst server. De groep staat echter bekend om haar open karakter en publiceert altijd als er problemen zijn met een server. Dit keer gebeurde dat niet en dat was erg vreemd. Mayfirst gaf geen enkele verklaring tot eind vorig jaar toen de 67-jarige activist Alfredo Lopez meldde dat hij drie maanden lang gedwongen was door de Amerikaanse overheid om te zwijgen over de inbeslagname van de server.

Mayfirst werd onderworpen aan een *Gag Order*, een verbod om over een juridische zaak te spreken in de openbaarheid. Pas eind 2014 werd duidelijk wat er aan de hand was nadat de zwijgplicht was opgeheven. Alfredo maakte bekend dat MayFirst het internationale bekende Indymedia Athene host. Op verzoek van de Griekse overheid was de server waarop IMC Athene draaide door de FBI uit een serverkast getild.

Het gevolg was dat niet alleen Indymedia Athene offline werd gehaald, maar ook allerlei andere websites en e-mail accounts.

Hoewel het om IMC Athene ging, waren andere gebruikers ook de klos. Of Mayfirst dit had kunnen voorkomen, is niet geheel duidelijk. Mensen die hun website of e-mail bij Mayfirst draaiden, hadden ook zelf een back-up kunnen maken van zowel hun website als hun e-mail. Dat is uiteraard niet alleen de verantwoordelijkheid van de aanbieder, hoewel die ook helder moet communiceren over wat er aangeboden wordt en of er een back-up is die, als een server in beslag wordt genomen, nog toegankelijk is voor de klanten.

Daarnaast heeft een aanbieder, commercieel of activistisch, ook de verantwoordelijkheid te communiceren over het optreden van de overheid tegen servers of websites. Mayfirst wilde dat wel, maar mocht het niet. De groep maakte na drie maanden duidelijk wat er was gebeurd en gaf daarbij aan dat de server van Mayfirst geen loggegevens bijhield zodat de politie niet wist wie en wanneer een website bezocht werd. E-mails waren wel in beslag genomen.

Conclusie

Bristol Indymedia maakte de inbeslagname van de server na een aantal dagen openbaar en attendeerde de gebruikers op de risico's. Hoewel BIM daar misschien niet heel helder over communiceerde, was het voor gebruikers direct duidelijk dat mogelijk hun loggegevens in bezit waren gekomen van de politie. Paul van Animal Rights Media had alle mogelijkheid om te communiceren, maar deed dat niet. Zelfs niet om aan te geven dat hij niet wist wat er aan de hand was.

Door de strafzaak van Joke K. is inmiddels bekend dat alle 4700 e-mails van haar in handen van justitie terecht zijn gekomen. Of er loggegevens van bezoekers van haar website door de overheid zijn bemachtigd, is niet duidelijk. Naar alle waarschijnlijkheid wel, want Paul gebruikte veel standaard-instellingen. Daarnaast draaiden er veel meer websites op de server van Paul en hadden ook veel meer mensen een e-mail account bij hem afgesloten. Hoewel de server van Paul niet in beslag is genomen, is duidelijk dat een ieder die gebruik maakte van zijn diensten gevaar liep. Dat was minder het geval bij Mayfirst en Bristol Indymedia.

Deze drie voorbeelden maken duidelijk dat het parkeren van data in de vorm van een website, e-mails of in de *cloud* niet van risico's is gevrijwaard. Jouw data staat altijd ergens op een computer geparkeerd van iemand, of die nu in beheer is van een commercieel bedrijf of een kleine activistische provider. Facebook kan ook je profiel plotseling op

slot doen of verwijderen. Dan ben je als actiegroep niet alleen je website, data en tijdlijn maar ook je contacten kwijt. Joke dacht dat zij goed zat bij Paul, maar raakte uiteindelijk haar website en haar e-mails kwijt doordat hij zijn zaken niet goed op orde had en daarover niet communiceerde.

Buro Jansen & Janssen, augustus 2015

Statement on Federal Gag Order Against MF/PL
https://linksunten.indymedia.org/node/130060

'Gagged' by the Government: a Police State Story
http://thiscantbehappening.net/gagged?page=2

Statement on Justice Department Subpoena of Athens
https://mayfirst.org/athens-imc-subpoena

A National Security Gag Order
http://bubbamuntzer.blogspot.nl/2015/02/a-national-security-gag-order.html

Security is Not a Crime—Unless You're an Anarchist
https://www.eff.org/deeplinks/2015/01/security-not-crime-unless-youre-anarchist

Anarchist website Bristol Indymedia to close following police raid
http://www.bristolpost.co.uk/Anarchist-website-Bristol-Indymedia-close/story-22848036-detail/story.html

Police serve Bytemark with production order for Bristol Indymedia information
http://indymedia.org.uk/en/2014/09/517868.html

Police action against Bristol Indymedia
https://www.indymedia.org.uk/en/2014/08/517810.html?c=on#comments

Police investigating the incendiary anarchist minority raid Bristol IMC, who shut down their project (UK)
http://325.nostate.net/?tag=indymedia-bristol

https://libcom.org/blog/sources-police-raid-bristol-indymedia-290820141