## M.H. Elferink en M.J.M. Kortier

Mirjam Elferink en Martijn Kortier zijn beiden advocaat bij KienhuisHoving Advocaten en Notarissen te Enschede. Zij zijn werkzaam in de sectie Intellectuele eigendom, ICT-recht & Privacy.

# Cybercrime: wat is het en wat kunt u ertegen doen?

*Mirjam Elferink* en *Martijn Kortier*

## Inleiding

De vele berichten in de media winden er geen doekjes om: wij zijn met z'n allen in hoge mate afhankelijk van digitale dienstverlening en daardoor ook steeds kwetsbaarder. Wie het boek *The Circle* van Dave Eggers heeft gelezen weet dat het door hem geschetste toekomstbeeld dichter bij is dan gedacht. In feite zitten we er al midden in. Het thema van het Jonge Baliecongres: *The sky is the limit? past ons inziens goed bij de huidige digitale en technologische ontwikkelingen. Of is panta rhei van alle tijden?*

Volgens het Amerikaanse Center for Strategic and International Studies (CSIS) loopt de Nederlandse economie jaarlijks 8,8 miljard euro schade op door de gevolgen van cybercrime.[1] En volgens een recent rapport bedraagt de schade wereldwijd ten minste 325 miljard euro.[2] Cybercriminelen weten op steeds grotere schaal (klant)gegevens van bedrijven te stelen[3] en bankrekeningen te plunderen en ze worden steeds bedrevener in de verspreiding van allerlei malware op computers. DoSS-aanvallen gericht op specifieke sectoren komen steeds vaker voor.[4] Kortom: cybercrime komt niet voor niets bijna dagelijks in het nieuws, het is een serieuze bedreiging van onze samenleving.

Maar wat is het eigenlijk? En hoe erg zijn de gevolgen? Is het vooral een ver-van-mijn-bed-show of kan het mij ook treffen? De laatste vraag lijkt bevestigend te moeten worden beantwoord, want ook datalekken, waarbij inbreuk op onder andere uw persoonsgegevens wordt gemaakt, vormen dagelijkse kost. Een greep uit recente nieuwsberichten: medische gegevens uit personeelsdossiers op straat[5], klantgegevens van

1 P. van der Beek, *Cybercrime schaadt Nederland voor 8,8 miljard*, 9 juni 2014, www.computable.nl/artikel/nieuws/security/5108294/1276896/cybercrime-schaadt-nederland-voor-88-miljard.html.

2 J. Kraan, *De drie dingen die nodig zijn om cybercrime te bestrijden*, 9 juni 2014, www.nutech.nl/cybercrime/3795898/drie-dingen-nodig-cybercrime-bestrijden.html.

3 M. Rademaker, *Omvangrijke hack treft meerdere bedrijven in energiesector*, 30 juni 2014, www.nu.nl/internet/3816193/omvangrijke-hack-treft-meerdere-bedrijven-in-energiesector.html.

4 *Gegevens 600.000 klanten Domino's gestolen*, 16 juni 2014, www.nu.nl/internet/3803987/gegevens-600000-klanten-dominos-gestolen.html.

5 Zie o.m. J. van Bentum, *VCD blundert met online verzuimregistratie*, 20 april 2012, *www.computable.nl/artikel/nieuws/security/4492289/1276896/vcd-blundert-metonlineverzuimregistratie.html*.

Twitteraars uitgelekt via een app[6] en een ziekenhuis dat medische dossiers lekt via een nauwelijks beveiligde computer.[7] De gevolgen voor betrokkenen kunnen aanzienlijk zijn en de maatschappelijke impact hiervan is soms groot.

Volgens het Cybersecuritybeeld Nederland (CSBN), dat op 10 juli 2014[8] werd uitgebracht, blijven cybercrime en digitale spionage de grootste dreiging op het gebied van cyber security. Door snelle digitalisering neemt de potentiële impact van cyberaanvallen en verstoringen toe. Daarnaast is er volgens het rapport gebrek aan ICT-Duurzaamheid. Hieronder wordt verstaan het risico dat een toenemend aantal apparaten aan het internet is verbonden, terwijl de apparaten en de bijbehorende software niet voor langere tijd door de leveranciers onderhouden kunnen worden. Verder wordt benadrukt dat ook privacy onder druk kan komen te staan door de verregaande technische mogelijkheden om data te verzamelen.

Alleen al uit de vele maatregelen die de overheid treft om cybercrime tegen te gaan mogen we afleiden dat cybercrime een steeds groter probleem wordt. Nu ons leven zich meer dan ooit op de digitale snelweg afspeelt, neemt ook de kans op criminaliteit via die route toe. Naar mate wij meer gebruik zullen gaan maken van de mogelijkheden die de digitale vooruitgang ons biedt, zal cybercrime navenant toenemen.
In dit artikel zetten we uiteen wat cybercrime is, waarom het een probleem is en wat de mogelijkheden zijn om u juridisch te wapenen.

## Wat is cybercrime?

Er zijn verschillende definities van cybercrime in omloop. In feite is dit een containerbegrip. Zo definieert de Nederlandse politie cybercrime als "criminaliteit met ICT als middel én doelwit"[9], het Openbaar Ministerie als "criminele activiteiten, waarbij gebruik wordt gemaakt van ICT"[10] en Wikipedia meent dat het gaat om "alle vormen van criminaliteit waarbij gebruik van internet een hoofdrol speelt".[11] Tot slot gebruikt de KLPD Dienst Nationale Recherche in 2009 de definitie: "cybercrime omvat elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is."[12] De Nederlandse wet hanteert overigens het begrip computercriminaliteit. Daaronder valt elke vorm van criminaliteit met betrekking tot computers.

6 *'Twitter ontkent hack van gebruikersaccounts'*, 22 augustus 2013, www.informatiebeveiliging.nl/nieuws/twitter-ontkent-hack-van-gebruikers.

7 B. de Winter, *Groene Hart Ziekenhuis lekt medische dossiers*,7 oktober 2012, www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medischedossiers.html.

8 Nationaal Cyber Security Centrum, *Cybersecuritybeeld Nederland CSBN-4*, te downloaden via: www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-4.html.

9 Zie: www.politie.nl/onderwerpen/cybercrime.html.

10 Zie: www.om.nl/onderwerpen/cybercrime.

11 Zie: www.nl.wikipedia.org/wiki/cybercrime.

12 *Cybercrime: van herkenning tot aangifte*, National Cyber Security Centrum, 2012, te downloaden via: www.ncsc.nl/actueel/nieuwsberichten/publicatie-cybercrime.html.

We kunnen concluderen dat cybercrime weliswaar niet eenvoudig te definiëren is, maar dat er wel een rode lijn valt te ontdekken in de verschillende definities. Er moet sprake zijn van *criminaliteit,* waarbij op enigerlei wijze gebruik wordt gemaakt van *ICT.* Nu bijna elke device, waaronder mobiele telefoons, is aangesloten op een (internet) netwerk, wordt het in theorie steeds makkelijker om criminele activiteiten te ontplooien met gebruikmaking van ICT. De overheid neemt cybercrime zeer serieus aangezien de enorme koppeling van apparatuur en programmatuur, via allerhande netwerken, er in theorie voor zou kunnen zorgen dat criminelen een groot deel van Nederland kunnen platleggen, met alle gevolgen van dien.

Welke vormen van cybercrime bestaan er dan zoal? De bekendste soorten kan iedereen wel opnoemen; phishing, waarbij men met valse e-mails persoonlijke gegevens probeert los te krijgen van internetgebruikers, en hacken, waarbij websites en computernetwerken worden platgelegd of worden misbruikt voor andere doeleinden. Naast cybercrime kennen we 'gedigitaliseerde criminaliteit'. Denk bijvoorbeeld aan het verspreiden van kinderporno, alsmede het seksueel benaderen van minderjarigen in chatboxen. Deze 'ouderwetse' criminaliteit maakt gebruik van computertechnologie. Ook het zaaien van haat via internet en het aanzetten tot terrorisme zijn vormen van 'gedigitaliseerde criminaliteit'. Daarnaast vindt veel identiteitsfraude plaats via het internet. Bovendien wordt het internet regelmatig gebruikt voor heling, witwassen, valsheid in geschrifte, fraude, bedreiging, smaad en laster. En denk tot slot ook aan het Project-X feest in Haren, waarbij door middel van het internet een grote groep mensen werd opgeroepen tot relschoppen, waarmee het ook als een vorm van cybercrime in ruime zin kan worden aangemerkt.

## Een cybercrime-aanval en nu?

En dan gebeurt het ondanks alle voorzorgsmaatregelen: het netwerk van uw bedrijf wordt getroffen door een cybercrime-aanval. Uw (bedrijfs)gegevens liggen op straat en, erger nog, ook de privacygevoelige gegevens van al uw klanten bent u kwijt. Wat doet u dan? Welke mogelijkheden biedt het recht om de dader(s) te pakken en de schade te verhalen?

Het is in ieder geval raadzaam om melding te maken van het incident. Dit kan bij de politie.
Vervolgens is het van belang voor zoveel mogelijk te bepalen wat de schade is van de aanval en wat de consequenties daarvan zijn.

Aangezien er in dit geval sprake is van computervredebreuk, zuivere cybercrime, is het raadzaam gelijk aangifte te doen bij de politie. Justitie kan, met de middelen die haar in het Wetboek van Strafrecht en het Wetboek van Strafvordering ter hand zijn gesteld, onderzoek doen naar de dader van dit strafrechtelijke voorval. De mogelijkheden van Justitie reiken verder dan die van een particulier rechercheburéau. Wanneer Justitie de daders vervolgens gepakt heeft, wilt u uiteraard uw schade - voor zover dat te vergoeden valt - vergoed zien. Dat kan door u te voegen in de strafzaak, doch het kan zich lonen om, na afloop van die strafzaak, een civiele vordering jegens de daders in te stellen. De hoogte van de schadevergoeding zal in casu immers niet eenvoudig vast

te stellen zijn waardoor een gang naar de civiele rechter een meer geëigende weg lijkt. Bovendien staat bij een veroordeling in de strafzaak de onrechtmatigheid in een civiele zaak in de meeste gevallen immers vrijwel vast.

Als er persoonsgegevens zijn ontvreemd gelden binnenkort speciale eisen. Daarover in paragraaf 4 meer. In het navolgende bespreken we eerst de mogelijkheden die de wet biedt om cybercriminelen aan te pakken, zowel strafrechtelijk als civielrechtelijk, en te achterhalen wie de dader is.

## Juridisch kader

In het Wetboek van Strafrecht is de mogelijkheid van criminaliteit met behulp van computers erkend en opgenomen. De Wet Computercriminaliteit I is in 2006 vervangen door de Wet Computercriminaliteit II. Deze wetgeving is op dit moment nog van toepassing. De politiek is momenteel bezig met een ontwerp voor een Wet Computercriminaliteit III. Nu dit nog slechts een ontwerp is, laten wij dit ontwerp in het kader van dit artikel buiten beschouwing. Ons Wetboek van Strafrecht kent de term cybercrime niet; er wordt gesproken over computervredebreuk.

### Computervredebreuk

Wat wordt verstaan onder computervredebreuk in de zin van de wet? *Elk opzettelijk en wederrechtelijk binnendringen in computersystemen* waarvan men weet dat men er niet hoort te zijn is strafbaar als computervredebreuk. Het maakt daarbij niet uit of het systeem of netwerk beveiligd is. Ook binnendringen in een onbeveiligd netwerk is strafbaar. De wet noemt vier vormen van binnendringen. Hiervan is sprake indien de toegang tot het werk wordt verworven:

a. door het doorbreken van een beveiliging,
b. door een technische ingreep;
   denk bijvoorbeeld aan een SQL-injectie
c. met behulp van valse signalen of een valse sleutel;
   denk bijvoorbeeld aan het inloggen op het systeem van een oud-werkgever

Wanneer een van deze handelingen worden verricht, is er sprake van computervredebreuk.

### Opsporing?

Hoe komt u er dan achter welke personen en/of organisaties het feit hebben gepleegd of -doen plegen? Daarvoor zijn de nodige opsporingsmaatregelen voorhanden. De Officier van Justitie kan in een aantal specifieke gevallen opgeslagen en al dan niet identificerende gegevens opvragen bij diegene die daar redelijkerwijs voor in aanmerking komt of van wie redelijkerwijs kan worden vermoed dat hij toegang heeft tot die opgeslagen of vastgelegde gegevens.[13] Tevens is het de Officier van Justitie onder voorwaarden toegestaan telecommunicatieverkeer op te nemen of gegevens van tele-

13 Zie o.a. artikel 126nc en artikel 126nd Wetboek van Strafvordering.

communicatieverkeer op te vragen.[14] Overigens is daarbij interessant om te vermelden dat de Wet bewaarplicht verkeersgegevens sinds enige tijd van kracht is.[15]

## Wet bewaarplicht verkeersgegevens

In de Telecommunicatiewet is voor aanbieders van een openbaar telecommunicatienetwerk of –dienst (waaronder onder andere internetservice providers) de plicht opgenomen verkeers- en locatiegegevens te bewaren. Deze gegevens zijn (bijna) letterlijk gegevens over het verkeer van de communicatie en de locatie waar de gebruiker zich bevindt, daaronder valt in ieder geval niet de inhoud van correspondentie.[16][5]

Artikel 13.2 a van de Telecommunicatiewet regelt dat deze gegevens slechts worden bewaard ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven. Gegevens dienen, in verband met telefonie, gedurende een periode van twaalf maanden bewaard te worden en gegevens in verband met internettoegang etc., zes maanden.

## Civielrechtelijke aansprakelijkstelling

Overigens is het ook in een civiele context denkbaar dat men achter de gegevens en identiteit van personen kan komen indien die personen bijvoorbeeld inbreuk maken op uw systemen of zich anderszins onrechtmatig gedragen (met gebruikmaking van computerapparatuur of het internet).

Om iemand aansprakelijk te kunnen stellen voor computervredebreuk, moet u zijn identiteit kennen. In de meeste gevallen heeft alleen zijn provider die gegevens. Op grond van jurisprudentie zijn providers onder omstandigheden verplicht deze NAW-gegevens af te geven. Dit geldt mits de eiser daar een redelijk belang bij heeft.

14 Zie artikel 126s e.v. Wetboek van Strafvordering.

15 Overigens heeft het Oostenrijkse Constitutionele Hof prejudiciele vragen gesteld over de werking van de Dataretentierichtlijn (de richtlijn op grond waarvan de bewaarplicht in de Nederlandse wetgeving is geïmplementeerd). In Oostenrijk had men met name moeite met het feit dat ook de gegevens van personen worden bewaard, die daar generlei aanleiding toe gaven - de niet-criminelen zo gezegd -. Die gegevens worden echter wel opgeslagen en bewaard en daarmee zijn zij kwetsbaar voor misbruik en verlies. De Oostenrijkers vragen zich af of een en ander in harmonie is met het Handvest van de grondrechten van de Europese Unie.

16 Zie Artikel 11.1 van de Telecommunicatiewet definieert verkeersgegevens als volgt: "gegevens die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan" en locatiegegevens als: "gegevens die worden verwerkt in een openbaar elektronisch communicatienetwerk of een openbare elektronische communicatiedienst, waarmee de geografische positie van de randapparatuur van de gebruiker van een openbare elektronische communicatiedienst wordt aangegeven."

## Afgifte NAW-gegevens door provider?

In het arrest Lycos/Pessers[17][6] heeft de Hoge Raad een zogenaamde vier-stappentoets geïntroduceerd waarna, als aan alle vier de stappen is voldaan, de websitehouder/provider NAW-gegevens van hun klanten zouden moeten verstrekken. De Hoge Raad heeft daartoe de volgende vier cumulatieve vereisten geformuleerd:

(I). de mogelijkheid dat de informatie, op zichzelf beschouwd, jegens de derde onrechtmatig en schadelijk is, voldoende aannemelijk is;
(II). de derde een reëel belang heeft bij de verkrijging van de NAW-gegevens;
(III). het aannemelijk is dat er in het concrete geval geen minder ingrijpende mo gelijkheid bestaat om de NAW-gegevens te achterhalen, en
(IV). de afweging van de betrokken belangen van de derde, de serviceprovider en de websitehouder (voor zover herkenbaar) met zich meebrengt dat het belang van de derde behoort te prevaleren, dan dient degene die daarover beschikt, of wel de websitehouder of wel de provider, de NAW-gegevens van iemand die met gebruikmaking van de website onrechtmatig handelt jegens een ander, aan die ander openbaar te maken.

Is er aan al deze eisen voldaan, dan is het volgens de Hoge Raad redelijk dat de provider een verzoek om afgifte van adresgegevens van een klant honoreert.

## Inbreuk op persoonsgegevens

Bijzondere aandacht in dit verband verdient het wetsvoorstel 'meldplicht datalekken' dat momenteel in behandeling is bij de Tweede Kamer.[18] In dit wetsvoorstel wordt een meldplicht voorgesteld in het geval zich een 'datalek' heeft voorgedaan. Uit privacyoverwegingen moeten betrokken personen in zo'n geval snel worden ingelicht. Dit betekent dat organisaties worden verplicht diefstal, verlies of misbruik van persoonsgegevens te melden aan de betrokken personen en aan het College Bescherming Persoonsgegevens (CBP). Deze meldplicht zal worden opgenomen in de Wet bescherming persoonsgegevens (Wbp). Wat is men verplicht te doen qua preventie? En welke juridische instrumenten kunnen worden aangewend om de schade van een datalek zoveel mogelijk te beperken? Als het wetsvoorstel in de huidige vorm wordt aangenomen en een datalek niet of niet tijdig wordt gemeld, kunnen organisaties namelijk een boete opgelegd krijgen van maximaal € 450.000.
Overigens heeft het Europees Parlement recent een voorstel voor een nieuwe Privacyverordening aangenomen, waarin ook een meldplicht is opgenomen. Deze verordening bepaalt onder meer dat organisaties bij het niet tijdig melden van een datalek een geldboete opgelegd kunnen krijgen tot 2% van de wereldwijde jaaromzet. Het voert in het kader van dit artikel te ver om hier uitgebreid op in te gaan, derhalve verwijzen wij

17 [6] HR 25 november 2005, NJ 2009, 550 m. nt. P.B. Hugenholtz.

18 Het voert te ver om genoemd wetsvoorstel in dit artikel te behandelen. Diegenen die geïnteresseerd zijn in de achtergrond verwijzen wij graag naar het artikel dat beide auteurs eerder hebben gepubliceerd: M.H. Elfennk & M.J.M. Kortier, *'Brede' meldplicht datalekken, preventie en privacy*, Huisorgaan van het Platform voor InformatieBeveiliging, 2013 nummer 7, p. 13.

naar ons artikel waarin wij op hoofdlijnen de belangrijkste wijzigingen uit de verordening bespreken.[19]

## Preventie

Teneinde cybercrime effectief te kunnen bestrijden, is er dus de nodige wet- en regelgeving opgesteld. Maar wat kunnen ondernemingen doen om dergelijke grote inbreuken op hun netwerken in de toekomst te voorkomen? Immers, een doelbewuste hack teneinde zeer privacygevoelige gegevens, alsmede bedrijfsgeheimen te achterhalen kan aanzienlijke schade voor ondernemingen met zich meebrengen. Om van reputatieschade nog maar te zwijgen. En wat kunnen ondernemingen preventief doen om zich voor te bereiden op een geval van cybercrime?

### Bewustwording en tijdige herkenning

In de eerste plaats raden wij aan om bewustwording te kweken bij het eigen personeel. Niet zelden wordt immers de mogelijkheid tot inbraak op een systeem geboden doordat werknemers van een onderneming onvoorzichtig zijn, bijvoorbeeld doordat zij wachtwoorden laten slingeren of (delen van) het systeem per ongeluk openstellen en/of niet weer afsluiten.

### Vaststellen van kwetsbaarheden

In sommige gevallen kan een particulier recherchebureau dat forensisch (digitaal) onderzoek kan verrichten, uitkomst bieden. Het loont overigens de moeite om zo'n bureau vooraf in te schakelen om ervoor te zorgen dat organisaties "forensic ready" zijn. Dit houdt in dat organisaties onverwachte incidenten kunnen managen. Incidenten vinden nu eenmaal in iedere organisatie plaats, dus men kan er maar beter op voorbereid zijn. Welke digitale sporen zijn er in uw organisatie? Een forenisch onderzoek legt de zwak- en kwetsbaarheden van de digitale infrastructuur van organisaties bloot. Dat kan op het eerste gezicht pijnlijk zijn, anderzijds helpt het organisaties enorm bij het (her)beveiligen van hun infrastructuur en bij het protocolleren - als hierna genoemd. Men weet dan immers waar de zwakke plekken liggen en wat derhalve extra aandacht verdient. Het behoeft nauwelijks vermelding dat het uiteraard van belang is om een gedegen cybersecurity beleid op te stellen, opdat de hardware en software goed beveiligd is en blijft.

Daarnaast is het raadzaam, zeker voor organisaties, om allerlei interne protocollen op te stellen die in werking kunnen treden op het moment dat er, ondanks alle getroffen maatregelen, toch sprake is van een cybercrime-aanval. Bewustwording van werknemers en het vaststellen van kwetsbaarheden in de eigen organisatie is daarbij een niet onbelangrijk onderdeel.

19 M.H. Ellerink & M.J.M. Kortier, '*Bent u er klaar voor? De nieuwe Europese privacyregels*', Globe Magazine, juli/augustus 2014, nr. 389.

## ICT-protocol en cybercrime-protocol

Een ICT-protocol, waarin werknemers erop wordt gewezen hoe zij om moeten gaan met de ICT-voorzieningen van een bedrijf, alsmede hoe zij zich op het internet moeten gedragen, met gepaste sanctionering, kan behulpzaam zijn bij het vergroten van bewustzijn van de medewerkers van een organisatie. Op het moment dat zich toch een cybercrime-aanval voordoet, is het aan te raden dat er een intern draaiboek klaarligt waaruit blijkt hoe men moet handelen. Zo'n intern draaiboek, of cybercrime-protocol waarin o.m. vastgelegd wordt bij wie de cybercrime-aanval gemeld moet worden, of en hoe er aangifte gedaan moet worden, of (er delen van) het systeem afgesloten moet worden of herbeveiligd, etc. kan daarbij helpen.

## Datalek-protocol

Verder is het raadzaam om een datalekprotocol te hanteren. Cyercrime-aanvallen zullen niet zelden tot doel hebben het verkrijgen van (persoons)gegevens, zodat naast alle strafrechtelijke gevolgen, tevens consequenties op grond van de Wbp zich zullen openbaren. In sommige gevallen zou een bedrijf zelf subject kunnen worden van het informatieverzoek en/of inval van opsporingsinstanties. Op dat moment is het goed om te weten wat te doen. Ook daaromtrent kunnen protocollen worden opgesteld.

Voor hostingproviders kan tot slot nog worden gedacht aan een "Inval (bezoek) opsporingsinstanties-protocol en een zogenaamd "Inlichtingenverzoek-protocol".

## Derden/dienstverleners

Veel ondernemingen maken gebruik van 'cloud computing'.[20] De leverancier levert in de meeste gevallen een totaaloplossing voor de ICT-voorzieningen van bedrijven. Dit brengt mee dat er een nieuwe leveringswijze van ICT-diensten plaatsvindt. Deze nieuwe diensten brengen juridische vraagstukken met zich mee waarover bij voorkeur in de contractfase afspraken moeten worden gemaakt. Gevoelige bedrijfsdata en ook persoonsgegevens worden immers naar de cloud verplaatst en staan daarmee niet meer binnen de muren van het eigen kantoor, maar 'zweven' in de datacentra van de cloudleverancier. Dat is praktisch en bespaart tevens een hoop geld dat anders zou zijn gespendeerd aan hardware en personeel.

Maar wat als een cybercrime-aanval niet zozeer bij u, maar bij uw cloudleverancier plaatsvindt? Uiteraard zullen de daders daarvoor verantwoordelijk gehouden moeten worden. Maar wat als deze niet zijn te traceren? Wie draait op voor de schade? En wie is er eigenlijk verantwoordelijk als er privacy gevoelige en / of bedrijfsinformatie wordt gelekt? Uw onderneming loopt immers reputatieschade, schade wegens verlies of verminking van gegevens of stagnatieschade op. Met andere woorden: welke juridische risico's loopt u en hoe voorkomt of beperkt u die risico's?

In ieder geval is het zeer aan te raden goede afspraken te maken met de leverancier. Dat dient bovendien meerdere doelen. Als verantwoordelijke in de zin van de Wbp besteedt

20 Het begrip 'cloud computing' is in feite een verzamelnaam van allerlei vormen van ICT-dienstverlening via het internet. Denk bijvoorbeeld aan het gebruik van Gmail, Google Apps of andere clouddiensten.

de onderneming, door het afnemen van de clouddienst, een deel van de verwerking van de persoonsgegevens uit aan de cloudleverancier. Wanneer zich aan de kant van de leverancier een incident voor doet met een lek tot gevolg, zal de verantwoordelijke het lek nog steeds moeten melden en is hij eventueel boeteplichtig. Hij zal die boete willen verhalen op de leverancier - wanneer de schuld van het lek althans aan diens zijde ligt. Welke contractuele afspraken dienen organisaties dan te maken? In dit kader kan er een onderscheid gemaakt worden in soorten afspraken. Uiteraard zijn er afspraken van technische, praktische en organisatorische aard. Daarnaast dienen er ons inziens meer juridische afspraken gemaakt te worden in de trant van aansprakelijkheden, vrijwaringen en toepasselijk recht.

## Aanbevelingen

Wij raden aan om in ieder geval over de volgende onderwerpen passende afspraken te maken en uw rechten en plichten goed vast te leggen in een contract:

***Technisch, organisatorisch en juridisch:***

- Service Level Agreement (SLA): maak in het contract goede afspraken over het dienstenniveau. In een SLA kunnen bepalingen worden opgenomen over de beschikbaarheid en bereikbaarheid van de dienst en de data alsmede over de betrouwbaarheid, vertrouwelijkheid en het gebruiksgemak.
- Worden er periodiek back-ups gemaakt?;
- Wordt er gelogd? Wie kan, en komt, wanneer bij de data;
- Onder welke omstandigheden worden er incidenten gemeld aan de afnemer;
- Welke oplossingen zal de leverancier hanteren in het geval van incidenten;
- Welke organisatorische en technische beveiligingsmaatregelen en -niveaus zal de leverancier hanteren?;
- Maakt de leverancier op zijn beurt gebruik van de diensten van derden?;
- Hoe lang worden de data bewaard?;
- In geval van een public cloud: wat zijn de waarborgen dat andere gebruikers van de public cloud geen toegang hebben tot de gegevens van de afnemer;
- Audit-recht voor de afnemer ter controle van de uitvoering van de afspraken en dienstverlening?;
- Toegankelijkheid data?;
- Controle over fysieke locatie van de data?
- Bij wie rusten de (intellectuele) eigendomsrechten op de gegevens?
- Van wie zijn de servers (eigendom) en waar zijn ze gevestigd (jurisdictie)
- Wie is waarvoor aansprakelijk? Denk daarbij met name aan dataverlies, datalekken en data-recovery. Boete en schade bij ondeugdelijke uitvoering dienstverlening. Evt. sole remedy clause.
- Meldplicht in het geval van datalekken?

- Waarborgen met betrekking tot de continuïteit van de dienstverlening, zoals ondersteuning van de leverancier bij migratie van bestaande ICT-oplossingen en het leggen van koppelingen met andere systemen en / of diensten. Voorkom een 'vendor lock-in': zorg ervoor dat de data ook beschikbaar zijn na het einde van de overeenkomst (waaronder faillissement, verhuizing naar een andere leverancier). Vergewis u ervan op welke locatie de data worden opgeslagen?
- Toepasselijk recht. Cloud is immers per definitie niet grensgebonden, dus het is niet ondenkbaar dat u met buitenlandse partijen contracteert. Kijk dus welk recht van toepassing wordt verklaard in de contracten. Voor wat betreft persoonsgegevens geldt bovendien dat u ervoor moet waken dat de gegevens in landen buiten de Europese Unie worden opgeslagen. Dat mag namelijk niet zonder meer. Bovendien is het inmiddels een fact of life dat de Amerikaanse Patriot Act haar klauwen ver uit heeft geslagen? [21]

21 De reikwijdte van de Patriot Act, waarmee de VS overheidsinstanties in beginsel inzage kunnen krijgen in data, is niet geheel duidelijk. Er zijn echter gevallen bekend dat de VS overheid daadwerkelijk haar macht heeft doen laten gelden en inzageverzoeken deed. Aangenomen wordt in ieder geval dat wanneer een Nederlands bedrijf op enigerlei wijze (op regelmatige basis) zaken doet met VS bedrijven, dat de Patriot Act van toepassing is. Voor meer informatie over de Patriot Act verwijzen wij de lezer naar het artikel: M.H. Elfernk, *De implicaties van de Amerikaanse Patriot Act*, Fenedexpress, Januari 2013 nr. 379, p. 14.