'BREDE' MELDPLICHT DATALEKKEN, PREVENTIE EN PRIVACY

Mr. dr. M.(Mirjam) H. Elferink is werkzaam als advocaat bij KienhuisHoving in Enschede in de praktijkgroep Intellectuele Eigendom, ICT-recht en Privacy. Zij is sinds jaren gespecialiseerd in Intellectuele Eigendom, ICT-recht en privacy. Mirjam publiceert en doceert regelmatig over deze onderwerpen. Zij is te bereiken via mirjam.elferink@kienhuishoving.nl of @MirjamElferink.

Mr. M.(Martijn) J.M. Kortier is werkzaam als advocaat bij KienhuisHoving in Enschede in de praktijkgroep Intellectuele Eigendom, ICT-recht en Privacy. Hij is gespecialiseerd in Intellectuele Eigendom, ICT-recht en privacy. Martijn is te bereiken via martijn.kortier@kienhuishoving.nl of @MartijnKortier.

Medische gegevens uit personeelsdossiers op straat [1], klantgegevens van Twitteraars uitgelekt via een app [2] en een ziekenhuis dat medische dossiers lekt via een nauwelijks beveiligde computer [3]. Datalekken zijn aan de orde van de dag. De gevolgen voor betrokkenen kunnen aanzienlijk zijn en de maatschappelijke impact hiervan is soms groot. De politiek zit niet stil en heeft wettelijke maatregelen voorgesteld om eventuele schade van datalekken te beperken c.q. te verminderen. Op 21 juni jl. is het langverwachte wetsvoorstel 'meldplicht datalekken' naar de Tweede Kamer gezonden [4]. In dit wetsvoorstel wordt een meldplicht voorgesteld in het geval zich een 'datalek' heeft voorgedaan. Vanwege 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? In dit artikel zal worden ingegaan op de vraag welke consequenties dit wetsvoorstel voor organisaties heeft en hoe de verplichtingen daaruit moeten worden geïmplementeerd in protocollen en contracten. 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.

Aanleiding meldplicht

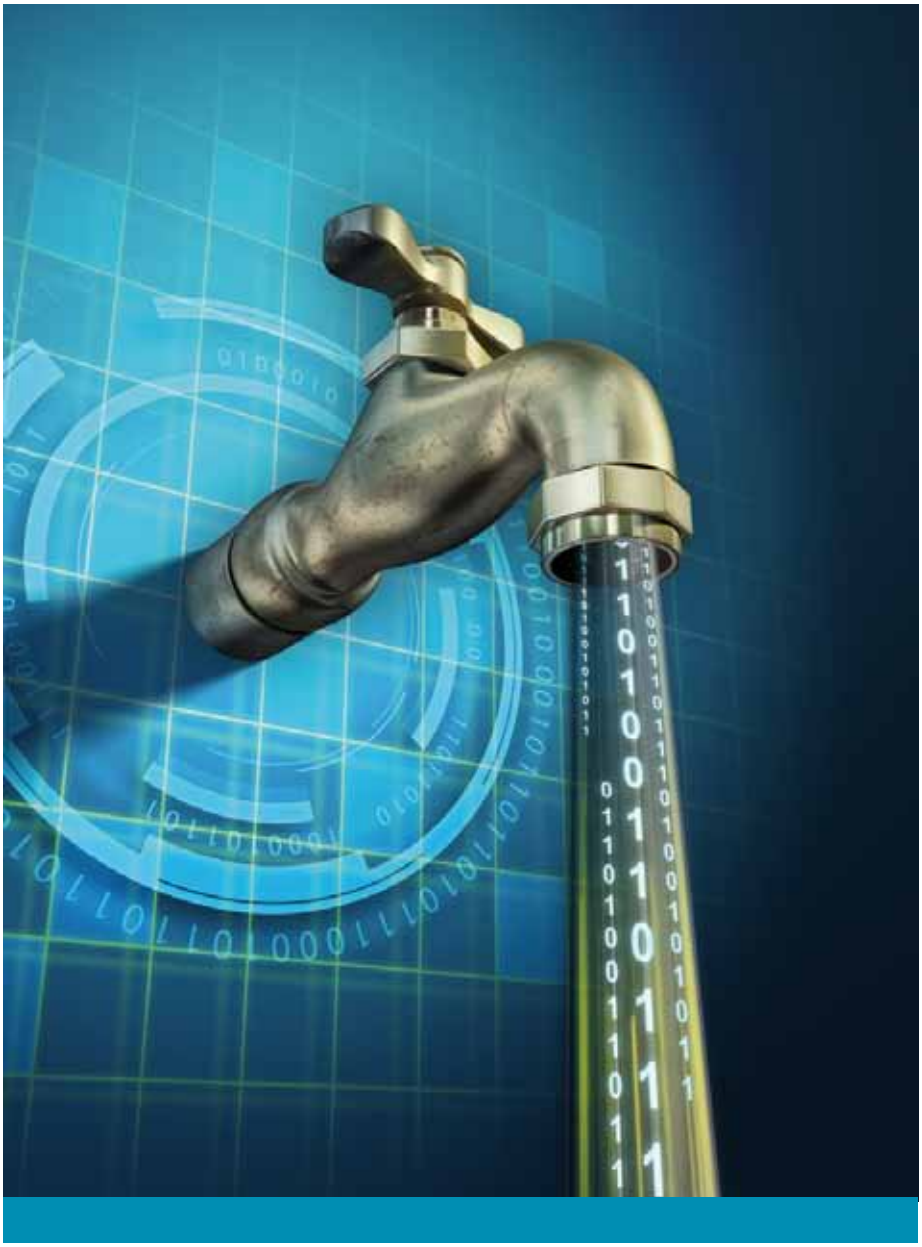
De aanleiding voor het wetsvoorstel is een groot aantal incidenten waarbij sprake is van inbreuken op persoonsgegevens. Sinds juni 2012 geldt al een meldplicht voor telecommunicatiebedrijven en internet servers providers op grond van de Telecommunicatiewet, ook wel de 'smalle' meldplicht genoemd. Deze meldplicht ziet op inbreuken op de beveiliging die nadelige gevolgen hebben voor de bescherming van persoonsgegevens. Daarnaast bestaan al andere meldplichten in verschillende wetten en is er ook nog diverse wetgeving in de maak [5]. Verder is in dit kader van belang dat de Europese Commissie op 25 januari 2012 een voorstel heeft gepresenteerd voor een Algemene verordening gegevensbescherming [6]. Deze ontwerpverordening zal de Wbp op termijn (grotendeels) buiten spel zetten. Ook in deze ontwerpverordening is een meldplicht van datalekken aan de toezichthouder en/of betrokkenen opgenomen. Indien de meldplicht niet wordt nageleefd wordt een boete van 1 miljoen Euro of 2% van de wereldwijde jaaromzet geriskeerd. Vanwege de ontwerpverordening zijn stemmen opgegaan om de aanpassing van de Wbp uit te stellen en volledig op die verordening toe te snijden. Hier is niet voor gekozen, omdat de ontwerpverordening naar de mening van de wetgever nog in een prematuur stadium verkeert en het nog lang niet zeker is of deze in de huidige vorm gehandhaafd zal worden. Naar verwachting treedt de verordening pas in 2016 in werking.

> De meldplicht ziet dus niet op situaties als die rond DigiNotar

De voorgestelde meldplicht is overigens beperkter dan de roepnaam van het wetsvoorstel - 'meldplicht datalekken'- doet vermoeden. Het wetsvoorstel ziet namelijk slechts op 'doorbrekingen van maatregelen voor de beveiliging van persoonsgegevens'. "*De meldplicht ziet dus niet op situaties als die rond DigiNotar waarin fouten*

werden gemaakt in de beveiliging van certificaten waardoor deze onbetrouwbaar waren, of op andere meldplichten met een min of meer verwant karakter (cybersecurity-incidenten)," aldus de memorie van toelichting [7].
Alvorens nader in te gaan op de voorgestelde meldplicht is het van belang enkele aspecten uit de Wbp onder de loep te nemen.

Enkele begrippen uit de Wbp
Verantwoordelijke - bewerker: De meldplicht gaat gelden voor degene die het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In de terminologie van de Wbp de *verantwoordelijke*.



Denk bijvoorbeeld aan een werkgever. Onder het begrip *verwerking* valt elke handeling die betrekking heeft op persoonsgegevens, van het moment van verzameling tot vernietiging. Daaronder valt ook het opslaan van gegevens door een derde. Deze derde 'verwerkt' de gegevens in opdracht van de verantwoordelijke en wordt aangeduid als *bewerker*.

> Nieuw is om de verantwoordelijke op te leggen dat de bewerker de verplichtingen nakomt

Wanneer een onderneming zijn debiteurenadministratie uitbesteedt aan een bureau dat zich volledig onderwerpt aan de instructies van de desbetreffende onderneming en uitsluitend onder diens verantwoordelijkheid gegevens verwerkt, is eveneens sprake van bewerkerschap.

Persoonsgegevens: Wat valt er onder het begrip 'persoonsgegeven'? Volgens de wet gaat het om alle gegevens die informatie kunnen verschaffen over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit kan geschreven informatie zijn, maar ook informatie in beeld en geluid, zoals camerabeelden of stemopnamen. In de praktijk is men zich er vaak niet van bewust dat deze definitie meer behelst dan informatie waarvan alleen al uit de aard blijkt dat het om persoonsgegevens gaat, zoals de combinatie van naam-, adres- en woonplaatsgegevens. Ook gegevens waardoor een persoon indirect kan worden geïdentificeerd vallen hieronder. Denk bijvoorbeeld aan een taxicentrale die ritgegevens bijhoudt. In feite is de verwerking gericht op het registreren van routegegevens, waardoor men in eerste instantie niet snel aan persoonsgegevens zal denken. Dit wordt echter anders indien met behulp van deze routegegevens individuele chauffeurs kunnen worden getraceerd.

Beveiligingsplicht uit hoofde van de Wbp: Wat houdt de meldplicht in? Een verantwoordelijke is gehouden een melding te doen bij het CBP en/of de betrokken persoon, indien zich een inbreuk op getroffen beveiligingsmaatregelen voordoet en wanneer het aannemelijk is dat deze inbreuk een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens met zich meebrengt, die door de verantwoordelijke worden verwerkt. Kort gezegd: indien sprake is van diefstal, verlies of misbruik van persoonsgegevens moet dit gemeld worden. De voorgestelde

meldplicht staat dus in nauw verband met de beveiligingsverplichting die is neergelegd in artikel 13 van de Wbp. Op grond van deze bepaling is de verantwoordelijke verplicht om passende technische en organisatorische maatregelen ten uitvoer te (laten) leggen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. De maatregelen moeten bovendien een passend beschermingsniveau garanderen, gelet op de stand van de techniek en de kosten van de tenuitvoerlegging en gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Het CBP geeft in richtsnoeren aan wanneer er sprake is van een blijvend, passend beveiligingsniveau [8]. Daarin wordt uitgelegd hoe het CBP bij het onderzoeken en beoordelen van beveiliging van persoonsgegevens in individuele gevallen deze open beveiligingsnorm uit de Wbp toepast. Daartoe geeft zij een zogeheten plan-do-check-act-cyclus waarin zij allereerst aanraadt om de risico's goed in kaart te brengen en te beoordelen, en om gebruik te maken van algemeen geaccepteerde beveiligingsstandaarden. Bovendien adviseert het CBP om regelmatig te controleren en te evalueren. Periodiek dient beoordeeld te worden of het beveiligingsniveau nog steeds past bij de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen. Deze richtsnoeren kunnen verder worden toegepast in samenhang met algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van informatiebeveiliging zoals de code voor informatiebeveiliging (NEN-ISO/IEC 27002:2007 NL).

Een datalek valt pas onder de meldplicht indien de technische en organisatorische beveiligingsmaatregelen niet hebben gefunctioneerd en wanneer er sprake is van een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens. Denk aan een hack van een ICT-systeem of een gestolen laptop uit een afgesloten locker, aldus de memorie van toelichting bij het wetsvoorstel. Het is dus niet noodzakelijkerwijs zo dat er sprake moet zijn van tekortschietende beveiligingsmaatregelen. Het gaat er om dat de getroffen beveiligingsmaatregelen teniet worden gedaan of omzeild. Het kan ook gaan om menselijke fouten of een niet adequate beveiliging van bestanden of gegevens, bijvoorbeeld het slordig omgaan met het beheer van wachtwoorden die toegang geven tot informatiebestanden.

Gevolgen brede meldplicht voor organisaties

Organisaties krijgen volgens het huidige wetsvoorstel een aantal nieuwe verplichtingen opgelegd. Dat leidt in ieder geval tot onder meer de volgende veranderingen:

1. Noodzaak tot aanpassen van de bewerkersovereenkomst
2. Protocolplicht verantwoordelijke
3. Opstellen 'datalek'-protocol
   - Aard en inhoud van de melding
   - Kennisgeving aan betrokkenen
   - Kennisgeving aan het CBP
   - Wijze van melden

Noodzaak tot aanpassen van de bewerkersovereenkomst

Wanneer een verantwoordelijke persoonsgegevens te zijnen behoeve laat verwerken door een bewerker, dient hij in een zogenaamde bewerkersovereenkomst een aantal zaken vast te leggen. Dit is een wettelijk vereiste die volgt uit artikel 14 Wbp. Zo moet worden geregeld dat de bewerker de persoonsgegevens slechts in opdracht van en conform de instructies van de verantwoordelijke verwerkt. Verder moet de bewerker de verplichting opgelegd krijgen om de persoonsgegevens adequaat te beveiligen conform de beveiligingsverplichting die voortvloeit uit de Wbp. Op grond van artikel 14, lid 5 van de Wbp is de verantwoordelijke namelijk verplicht om de getroffen beveiligingsmaatregelen ex artikel 13 Wbp schriftelijk vast te leggen. Deze regel is opgesteld in zowel het belang van de betrokkene als de verantwoordelijke. Dit zijn zaken die nu al gelden.
Nieuw is het voorstel om de verantwoordelijke op te leggen er zorg voor te dragen dat de bewerker de verplichtingen nakomt die op de verantwoordelijke rusten ten aanzien van diens meldplicht. Dit betekent dat deze verplichting in de bewerkersovereenkomst zal moeten worden opgenomen. Dit is ook noodzakelijk omdat de verantwoordelijke anders geen weet heeft van een eventueel datalek en hij derhalve eenvoudigweg niet in staat zou zijn om dat te melden.

Protocolplicht verantwoordelijke

De verantwoordelijke zal worden verplicht een overzicht bij te houden van alle inbreuken. Dit betreft niet alleen de meldingsplichtige inbreuken, maar alle geconstateerde inbreuken. Ook als deze niet zijn gemeld. In de memorie van toelichting wordt het belang van dit protocol benadrukt, omdat de toezichthouder achteraf vragen kan stellen aan de verantwoordelijke. Met behulp van dit protocol kan de verantwoordelijke aantonen welke inbreuken hij heeft geconstateerd en welke maatregelen er zijn genomen. Daarnaast moeten de gegevens die aan het CBP zijn verstrekt, alsmede de tekst van de kennisgeving die de verantwoordelijke aan de betrokkene doet, in dit protocol worden opgenomen. Digitale burgerrechtenorganisatie Bits of Freedom heeft ervoor gepleit om

Boete van 1 miljoen Euro of 2% van de wereldwijde jaaromzet wordt geriskeerd

deze protocollen openbaar te (laten) maken. De wetgever gaat daarin echter niet mee, omdat het belang van de vertrouwelijkheid van details met betrekking tot de beveiliging van de gegevensverwerking daaraan in de weg zou staan.

(Opstellen van een 'datalek'-protocol

Aard en inhoud van de melding

Bij de melding moet in ieder geval het volgende worden aangegeven:

- de aard van de inbreuk;
- de instanties waar meer informatie kan worden verkregen over de inbreuk;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken (bijvoorbeeld: het veranderen van gebruikersnamen en wachtwoorden).

Dit laatste punt is iets waar organisaties ons inziens op zouden moeten anticiperen. Omdat de melding onverwijld moet plaatsvinden, is er op het moment dat zich een lek voordoet niet veel tijd om na te denken over eventuele schadebeperkende maatregelen. Wij menen dat organisaties een protocol zouden moeten opstellen met daarin een aantal actiepunten die moeten worden ondernomen op het moment dat er sprake is van een datalek. Daarin zouden ook alvast schadebeperkende maatregelen kunnen worden uitgewerkt voor een aantal mogelijke scenario's. Dit alles maakt dat organisaties sneller kunnen handelen op moment dat zich daadwerkelijk een datalek voordoet en hiermee eventuele schade zoveel mogelijk kunnen beperken. Vanuit het aansprakelijkheidsrecht hebben verantwoordelijken bovendien een schadebeperkingsplicht.

Kennisgeving aan betrokkenen

De aard van de inbreuk kan algemeen worden omschreven. Wanneer een betrokkene wil weten waar hij persoonlijk aan toe is, moet hij contact opnemen met de verantwoordelijke. Dit betekent dat in de kennisgeving contactgegevens moeten worden opgenomen.

Kennisgeving aan het CBP

De kennisgeving aan het CBP is meer omvattend dan de kennisgeving aan betrokkenen. Aan het CBP moeten ook gegevens van technische aard worden gemeld, opdat het CBP in staat is effectief toezicht uit te oefenen. Het kan zijn dat de verantwoordelijke en/of bewerker bij de kennisgeving melding moet maken van technische details die normaliter van vertrouwelijke aard zijn. Desgewenst kunnen bedrijven deze gegevens expliciet als bedrijfsvertrouwelijk in de zin van artikel 10, lid 1 onder c van de Wet openbaarheid van bestuur (WOB) aanmerken. Daarmee wordt voorkomen dat het CBP deze gegevens zal openbaren aan degene die op grond van de WOB daarin inzage zou willen verkrijgen.

> Bits of Freedom pleit om deze protocollen openbaar te maken

Wijze van melden

De wetgever heeft ervoor gekozen de meldingsplicht zo eenvoudig mogelijk te houden. Dit houdt in dat de verantwoordelijke zelf een afweging mag maken aan de hand van een aantal criteria:

- de aard van de inbreuk;
- de geconstateerde en de feitelijke gevolgen daarvan voor de verwerking van persoonsgegevens;
- de kring van betrokkenen;
- de kosten van tenuitvoerlegging.

Deze afweging past volgens de wetgever binnen het systeem van de Wbp. Indien de inbreuk een groot aantal betrokkenen betreft, zou de verantwoordelijke moeten kiezen voor een advertentie in de dagbladen, aldus de memorie van toelichting. Het kan zijn dat in een later stadium nog specifiekere regels aan de kennisgeving worden gesteld bij Algemene Maatregel van Bestuur [9].

Uitzondering meldplicht

Indien de persoonsgegevens zijn beveiligd door bijvoorbeeld encryptie, kan de melding aan betrokkenen wellicht achterwege blijven. Daarvoor is wel vereist dat het redelijkerwijs is uitgesloten dat een datalek kan leiden tot kennisname van persoonsgegevens door onbevoegden.

Aansprakelijkheid verantwoordelijke en/of bewerker?

De verantwoordelijke moet zich goed realiseren dat het voldoen aan de meldplicht nog niet betekent dat hij daarbij is ontheven van eventuele aansprakelijkheid voor schade die voortvloeit uit het toerekenbaar tekortschieten of niet voldoende naleven van de verplichting ex artikel 13 Wbp. Op grond van artikel 49 Wbp is de verantwoordelijke namelijk in beginsel aansprakelijk voor schade die voortvloeit uit het niet naleven van de voorschriften uit de Wbp. De bewerker kan daarnaast zelfstandig aansprakelijk zijn voor schade die voortvloeit uit zijn werkzaamheden. Dit geldt tenzij wordt bewezen dat deze schade niet aan de verantwoordelijke of bewerker kan worden toegewezen. Hieruit volgt het belang van het maken van goede afspraken tussen verantwoordelijke en bewerker.

Preventie: Monitoren werknemers

Hoe kunnen organisaties zich dan weren tegen datalekken? Bedrijven en organisaties zouden bijvoorbeeld kunnen overwegen de werkzaamheden van hun werknemers te monitoren om de kans op datalekken te minimaliseren. Dat zou in veel gevallen opportuun zijn. Recentelijk was te lezen dat werknemers in het Verenigd Koninkrijk steeds vaker worden aangeklaagd voor datadiefstal [10]. De vraag is echter of monitoren van werknemers zomaar mag. Immers, het bijhouden

van wat werknemers doen is een verwerking van persoonsgegevens. Persoonsgegevens mogen alleen worden verwerkt met een legitiem doel. Ook op de werkplek hebben werknemers recht op privacy [11]. Dat geldt in het bijzonder bij privégebruik van aan de werknemers ter beschikking gestelde bedrijfsmiddelen, zoals internettoegang, een e-mailbox of een I-pad. Bedrijfsmiddelen zijn eigendom van de werkgever en daarom mogen werkgevers wel eisen stellen aan het gebruik ervan. De regels omtrent het gebruik van bedrijfsmiddelen, zoals internet- en e-mailgebruik, moeten van tevoren worden vastgelegd in een reglement (ICT-protocol) dat aan de werknemer kenbaar wordt gemaakt. Ook moet in het reglement worden opgenomen wat de sancties zijn bij overtreding hiervan. In de regel gaat het recht op privacy van de werknemer voor op het bedrijfsbelang van de werkgever. De werkgever moet kunnen aantonen dat hij een redelijk vermoeden van wangedrag heeft, alvorens hij mag overgaan tot monitoren.

Aan de hand van een praktijkvoorbeeld zullen wij illustreren hoe de rechter met het monitorenvraagstuk pleegt om te gaan. In een recente rechtszaak deed zich het volgende voor. Een werknemer mailde naar een zakelijke klant de volgende teksten:

"(..) I can tell you it is impossible to work with pigs, and that is what I am facing now!"

en

"(..) Das wissen wir auch nicht was da los ist, es ist hier ein komplett chaos.(..)".

In een ICT-protocol zullen echter vooral verbodsbepalingen staan

De systeembeheerder van zijn werkgever kwam deze e-mails tegen bij een routinecontrole. De vraag die daarop volgde was destijds: "mag dat zomaar en wat kan het bedrijf tegen die werknemer doen?" Tegen de vader van de desbetreffende werknemer, die bij hetzelfde bedrijf werkzaam was, liep op dat moment een ontslagaanvraag. Wellicht is dat één van de redenen waarom de werknemer zich jegens klanten negatief uitliet over het bedrijf. Het bedrijf stelde zich op het standpunt dat zij de zakelijke e-mail zou mogen monitoren daar zij daartoe een gerechtvaardigd doel had en er in casu verdenkingen bestonden dat er meerdere werknemers bij betrokken waren. De werknemer daarentegen stelde zich op het standpunt dat het inkijken in de e-mail een inbreuk op zijn privacy vormde. Volgens hem dienden de e-mails dan ook niet mee te worden genomen in een ontslagprocedure. De kantonrechter was uiteindelijk van mening dat het monitoren van zakelijke e-mail gerechtvaardigd is [12]. Een werknemer mag en kan verwachten dat het bedrijf waarvoor hij werkt, eerder dan bij privé-berichten, de inhoud van de zakelijke e-mailberichten zal bekijken. In dit geval vond de rechter de inbreuk op de privacy van de werknemer dan ook gerechtvaardigd en proportioneel.

In een andere - vergelijkbare - zaak was er sprake van een werknemer die via zijn privé Gmail-account correspondentie voerde over het opzetten van een nieuw concurrerende vennootschap in China. Bovendien bleek uit het privé e-mailadres dat hij producttechnische tekeningen van het bedrijf kopieerde. In dit geval werd zijn privé e-mail soms ook zakelijk gebruikt. Uiteindelijk kreeg het bedrijf inzicht in die e-mails, waarna de werknemer op non-actief werd gezet. Het Gerechtshof stelde vast dat in casu het bedrijf geen toestemming had om de privé e-mail te bekijken [13]. Deze e-mailbox werd bovendien slechts sporadisch zakelijk gebruikt. Het Hof laat de werkgever toe om duidelijkheid te verschaffen hoe en wanneer zij toegang had tot het account en wat de status daarvan was.

Preventie: ICT Protocol

Bovenstaande voorbeelden betreffen het lekken van relatief onschuldige informatie, alhoewel het grote reputatieschade voor het bedrijf met

zich mee kan brengen. Maar stel dat werknemers, al dan niet bewust, veel belangrijkere bedrijfsinformatie lekken. Ze mailen het per ongeluk naar een klant, ze zetten het in de cloud zonder dat daarbij duidelijk is wie de eigendom van de informatie toekomt of ze downloaden software waarmee ze virussen binnenhalen die er uiteindelijk voor zorgen dat informatie beschikbaar wordt voor hackers.
Teneinde het lekken van informatie zoveel mogelijk te beperken, is het raadzaam een zogenaamd ICT-protocol te hanteren. In zo'n protocol kan de wijze waarop werknemers om dienen te gaan met informatie- en communicatietechnologie worden aangegeven. Zo'n protocol kan dan de gedragsregels en richtlijnen bevatten ten aanzien van het verantwoord en onverantwoord gebruik van de ICT-voorzieningen binnen en buiten de muren van het bedrijf.
Bovendien kunnen bedrijven met een ICT-protocol in de hand controles op het 'digitale' gedrag van hun werknemers legitimeren.

Organisaties zouden hun systemen en werkwijzen moeten aanpassen

Veel bedrijven, maar ook scholen, ziekenhuizen en andersoortige organisaties, hanteren al een soort reglement waarin het de gebruikers van hun ICT-voorzieningen verboden wordt bepaalde handelingen op het internet uit te voeren. Zo'n reglement zou echter veel breder moeten zijn. Gebruikers zouden idealiter moeten verklaren dat zij de ICT-voorzieningen en -diensten primair zullen gebruiken in het kader van de uitoefening van hun werkzaamheden en overeenkomstig hun functie. Daarbij zouden bedrijven kunnen overwegen een functionaris aan te stellen die verantwoordelijk is voor de correcte uitvoering en naleving van het bepaalde in het ICT-protocol. Overigens is het maar zeer de vraag of het gebruik van ICT-voorzieningen voor persoonlijke doeleinden volledig kan worden verboden. Dergelijk gebruik kan echter wel beperkt worden.

In een ICT-protocol zullen echter vooral verbodsbepalingen staan. Zo is het raadzaam werknemers te verbieden software te downloaden zonder toestemming van de functionaris. Tevens verdient het aanbeveling werknemers te wijzen op de risico's van het gebruik van sociale media, zowel binnen als buiten werktijd. Tot slot loont het bedrijven de moeite erover na te denken of zij wensen dat hun werknemers gebruik maken van cloudtoepassingen. Men vergeet nogal eens dat daaronder bijvoorbeeld ook Dropbox, Hotmail, Gmail en webmail van providers dienen te worden verstaan. De voorwaarden die die cloudaanbieders hanteren, kunnen in sommige gevallen ernstig nadelig zijn voor het bedrijf, de eigenaar van de gegevens die in die cloudtoepassing worden geüpload. In sommige gevallen is er op grond van die voorwaarden zelfs sprake van overdracht van het (intellectueel) eigendom van die data.

Uiteraard vallen dergelijke ge- en verboden slechts aan werknemers op te leggen indien zij daarmee in (moeten) stemmen en er adequate sanctioneringsmaatregelen zijn overeengekomen. Overigens dient daarbij opgemerkt te worden dat in veel gevallen de ondernemingsraad van het bedrijf toestemming moet verlenen voordat het ICT-protocol kan worden ingevoerd.

Of een ICT-protocol een adequaat middel is om datalekken door menselijke fouten zoveel mogelijk te voorkomen en aldus eventuele schade te beperken, zal de praktijk moeten uitwijzen.
Naast misstappen van personeel zijn er namelijk nog een aantal veel voorkomende oorzaken van dataverlies. Zo wordt er lang niet altijd een effectieve back-up gemaakt, worden data verwijderd die nog steeds in gebruik zijn, wordt het IT-beveiligingsbeleid niet getest of heeft men geen up-to-date antivirussoftware [14]. Een ICT-protocol is in ieder geval een belangrijke eerste stap om ondernemingen en hun werknemers bewust te maken van de gevaren van de omgang met de ICT-voorzieningen van hun bedrijf. Het is een onderdeel van de organisatorische aanpassingen van een onderneming teneinde datalekken te voorkomen. Voorbeelden van werknemers die kwaad willen en daarom doelbewust informatie lekken of zich doelbewust negatief uitlaten over hun werkgever zijn gemakkelijk te bedenken. In de praktijk komt het echter veel meer voor dat er onbewust informatie gelekt wordt. Door werknemers een ICT-protocol te laten tekenen en hen daarbij uitleg te verschaffen, worden zij bewust gemaakt van de risico's die zij,

en niet in de laatste plaats het bedrijf waarvoor zij werkzaam zijn, kunnen lopen. Een datalek ontstaat immers sneller dan men denkt. De eventueel negatieve gevolgen van een datalek kunnen middels een ICT-protocol wellicht (indirect) deels worden afgewenteld op de werknemer die het lek heeft veroorzaakt.

Aanbeveling: richt een adequaat informatiebeveiligingsbeleid in

Zoals besproken brengt het huidige wetsvoorstel een aantal wijzigingen met zich mee die gevolgen hebben voor organisaties. Hoewel de wet nog niet is aangenomen en er in het wetgevingsproces nog het nodige kan worden gewijzigd, is de algemene verwachting dat de meldplicht er komt. Om daarop te anticiperen signaleren wij dat er tenminste op een drietal terreinen het nodige moet veranderen. Ons inziens zouden organisaties hun systemen en werkwijzen moeten aanpassen op zowel technisch, organisatorisch als op juridisch vlak. Door deze driepoot op orde te brengen kunnen bedrijven voldoen aan de op hen rustende beveiligingsplicht op grond van de Wbp, waarmee ze de kans op datalekken en de daaruit voortvloeiende schade kunnen verkleinen.

In technisch opzicht moeten organisaties er voor zorgen dat de beveiliging van hun systemen voldoet aan het passende beveiligingsniveau als bedoeld in artikel 13 Wbp. Wat daaronder dient te worden verstaan verschilt per onderneming en per categorie data. Het is derhalve ondoenlijk om concreet een beveiligingsniveau aan te geven. Het is van bijzonder belang om de gegevens die men verwerkt goed in kaart te brengen en zo mogelijk te classificeren om het beveiligingsniveau in te kunnen schalen.

Op organisatorisch gebied kan worden gedacht aan het opstellen van protocollen waarin de gewenste werkwijzen en processen in een organisatie worden vastgelegd. Vooraf kan men zijn werknemers, al dan niet aan de hand van protocollen, bewust maken van de gevaren die het omgaan met de ICT-voorzieningen en (vertrouwelijke) data met zich mee kunnen brengen en waar men voorzichtigheid dient te betrachten. Dit kan bijvoorbeeld door het hanteren van een ICT-protocol. Indien zich een datalek heeft voorgedaan is het juist weer zaak dat men snel weet hoe te handelen. Dit kan door het hanteren van een 'datalek'-protocol waarin wordt vastgelegd wat er moet gebeuren om te voldoen aan de ophanden zijnde nieuwe verplichtingen uit de Wbp en hoe (verdere) schade zoveel mogelijk kan worden voorkomen of beperkt.

Ook juridisch kunnen organisaties de nodige maatregelen nemen. Voor verantwoordelijken of bewerkers die gehouden zijn een bewerkersovereenkomst te sluiten kan het verstandig zijn daarin al rekening te houden met de aankomende meldplicht. Eveneens kan men vooruitlopen op de eventuele boetes die opgelegd worden als gevolg van het niet naleven van de meldplicht en dan uiteraard met name ten aanzien van de vraag voor wiens rekening die dienen te komen. Contractueel gezien kunnen organisaties hun aansprakelijkheid voor schade uitsluiten en/of beperken.

> Verantwoordelijken of bewerkers kunnen al rekening houden met de aankomende meldplicht

Conclusie

Datalekken lijken, ondanks een ICT-protocol en adequate beveiligingsmaatregelen, niet geheel uit te sluiten. Organisaties kunnen echter veel ondervangen met goede contracten en het creëren van bewustzijn bij werknemers. Daarmee kan de schade die zal ontstaan als gevolg van het datalek zo veel mogelijk worden beperkt en tonen organisaties hun goede wil, wat eventueel bij een aansprakelijkheidstelling mee zal wegen. Wij raden bedrijven dan ook aan om hun processen en werkwijzen zoveel als mogelijk te protocolleren, zowel preventief als repressief, en in hun contracten goede aansprakelijkheids- en boetebepalingen op te nemen.

Links

[1] *Zie o.m. : 'VCD blundert met online verzuimregistratie', 20 april 2012, computable.nl, http://www.computable.nl/artikel/nieuws/security/4492289/1276896/vcd-blundert-met-onlineverzuimregistratie.html.*

[2] *'Twitter ontkent hack van gebruikersaccounts', 22 augustus 2013, informatiebeveiliging.nl, https://informatiebeveiliging.nl/nieuws/twitter-ontkent-hack-van-gebruikers/.*

[3] *'Groene Hart Ziekenhuis lekt medische dossiers', 7 oktober 2012, Nu.nl, http://www.nu.nl/binnenland/2927832/groene-hart-ziekenhuis-lekt-medische-dossiers.html.*

[4] *Kamerstukken II 2012/13, 33 662, nr. 1. Eerder werd al een internetconsultatie over dit onderwerp gehouden, zie: http://internetconsultatie.nl/camerabeelden. Het wetsvoorstel wordt momenteel behandeld door de Tweede Kamer.*

[5] *Zie voor een overzicht de memorie van toelichting bij het wetsvoorstel datalekken: Kamerstukken II 2012/13, 33 662, nr. 3 (MvT), p. 2-3 . Het voert te ver om in het bestek van dit artikel de diverse meldplichten uitvoerig te bespreken. Ik noem slechts de Cyber Security Richtlijn waarin een meldplicht voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen (hierna ook: ICT-inbreuken) wordt geïntroduceerd.*

[6] *COM (2012), 11 def.*

[7] *Kamerstukken II 2012/13, 33 662, nr. 3 (MvT), p. 2.*

[8] *CBP richtsnoeren: 'Beveiliging van persoonsgegevens', februari 2013,te raadplegen via: http://www.cbpweb.nl/downloads_rs/rs_2013_richtsnoeren-beveiliging-persoonsgegevens.pdf.*

[9] *Zie: artikel 34a lid 11 wetsvoorstel.*

[10] *'Werknemers vaker aangeklaagd voor datadiefstal', 4 september 2013, webwereld.nl, http://webwereld.nl/beveiliging/79140-werknemers-vaker-aangeklaagd-voor-datadiefstal.*

[11] *EHRM 3 april 2007, nr. 62617/00, NJ 2007, 617 (Copland / Verenigd Koninkrijk).*

[12] *Ktr. Rotterdam, 21 september 2011, ECLI:NL:RBROT:2011:BU4848.*

[13] *Hof 's-Hertogenbosch, 19 maart 2013, ECLI:NL:GHSHE:2013:BZ5206.*

[14] *'De 5 domste oorzaken van dataverlies', 9 augustus 2013, AutomatiseringGids.nl, http://www.automatiseringgids.nl/nieuws/2013/32/de-5-domste-oorzaken-van-dataverlies.*