De meldplicht datalekken

Wat is het en wat betekent het voor mijn organisatie?

Mw. mr. R.C.P. Marbus
werkt als adviseur voor KPMG IT Advisory. Zij houdt zich bezig met juridische vraagstukken op het gebied van privacy, compliance, information security en cybercrime. Zij studeerde Journalistiek aan de Academie voor Journalistiek te Tilburg en Nederlands Recht met een specialisatie in Recht en Informatisering aan de Universiteit van Tilburg.

marbus.rachel@kpmg.nl

Mr. Rachel Marbus

Een securitybedrijf wordt gehackt en beveiligde identiteitstokens lekken naar buiten, de gegevens van klanten van een fastfoodketen liggen voor het oprapen en de tapgegevens van het KLPD zijn ook al niet veilig... Datalekken komen helaas vaak voor. En ook steeds vaker komt dit publiekelijk naar buiten. Nog even en dan is het zelfs wettelijk verplicht dergelijke datalekken openbaar te maken; op 29 april 2011 maakten Teeven (ministerie V&J) en Donner (ministerie BZK) bekend dat een brede meldplicht voor alle aanbieders van informatiediensten opgenomen zal worden in de Wet bescherming persoonsgegevens. Op korte termijn zal een zogenaamde 'smalle meldplicht' gaan gelden voor alleen telecommunicatiebedrijven en internet-serviceproviders op grond van een wijziging van de Telecommunicatiewet.

Inleiding

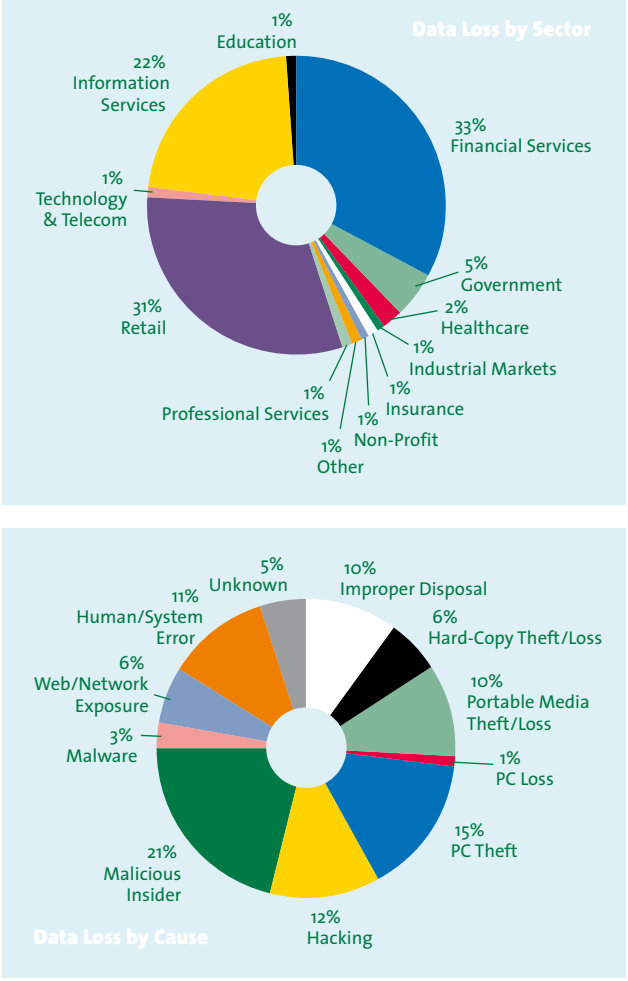
Datalekken zijn helaas bijna aan de orde van de dag. En het overkomt de besten onder ons. Niet lang geleden kampte zelfs een securitybedrijf met het uitlekken van informatie over beveiligde IDtokens. Soms had een lek makkelijk voorkomen kunnen worden, een andere keer is er sprake van domme pech of een geavanceerde aanval van buitenaf. Hoe het ook zij, het uitlekken van persoonlijke data van werknemers, klanten of anderszins is buitengewoon vervelend en ook problematisch in verband met allerlei juridische garanties die de 'eigenaars' van deze data verstrekt worden. 2011 wordt het jaar dat de (smalle) meldplicht datalekken in werking zal treden. Als alles volgens planning verloopt, moet dit voorjaar al de implementatie daarvan in de Telecommunicatiewet (Tw) gereed zijn. Vooralsnog geldt de meldplicht alleen voor telecommunicatiebedrijven (telco's) en Internet Service Providers (ISP's). Een bredere meldplicht die zal gelden voor *alle* aanbieders van informatiediensten (denk bijvoorbeeld aan banken, de Belastingdienst en verzekeringsmaatschappijen), is op 29 april aangekondigd door Teeven en Donner en zal een plaats krijgen in de Wet bescherming persoonsgegevens. Voorstanders van de meldplicht, zoals onder meer burgerrechtenorganisatie Bits of Freedom en de Consumentenbond, staan hier uitermate positief tegenover. Dit vanuit de wens tot meer transparantie en openheid daar waar het misgaat met de persoonlijke gegevens van burgers en klanten. Het bedrijfsleven weifelt. De gevolgen van een dergelijke meldplicht kunnen groot zijn, reputatieschade en praktische uitvoering lijken de meest voor de hand liggende factoren bij terughoudendheid. Dit artikel gaat nader in op de meldplicht datalekken: wat is het

en hoe zal die gaan werken? En hoe zit dat met een meldplicht voor alle organisaties die te maken (kunnen) krijgen met datalekken? Daarnaast worden enkele voor- en tegenargumenten op een rijtje gezet.

Een smalle meldplicht komt wettelijk vast te liggen

Data Loss Barometer

Hoewel uit onderzoek van KPMG blijkt dat er sprake is van een daling in de hoeveelheid incidenten waarbij persoonlijke data gelekt worden, is er desalniettemin nog steeds sprake van een enorme hoeveelheid gevallen waarbij data 'verloren' gaan ([KPMG10]). Meer dan 15 miljoen mensen worden hierdoor geraakt. Vooral binnen de financiële sector is het verlies van data ongemeen groot, zeker indien dit afgewogen wordt tegen de andere in de Data Loss Barometer onderzochte sectoren. Van de in totaal verloren 'records' is 33% afkomstig uit die financiële sector, maar ook retail (31%) en de informatiediensten (22%) scoren hoog. In 21% van de gevallen wordt het lek veroorzaakt door zogenaamde 'malicious insiders' (kwaadwillenden van binnen in de organisatie), 15% wordt veroorzaakt door de diefstal van pc's en 12% vindt zijn oorsprong in hacks.



Figuur 1. **Dataverlies naar sector (boven) en oorzaak (onder)** (bron: [KPMG10]).

De wordingsgeschiedenis van de meldplicht

Al sinds 2005 wordt er in politiek Nederland gestreden voor het invoeren van een wettelijke regeling rondom het verplicht melden van datalekken. Een motie van SP en PvdA uit 2005 met betrekking tot het invoeren van een meldplicht haalde het toentertijd niet. Toenmalig minister Donner oordeelde dat persoonsgegevens al afdoende beschermd werden onder het regime van de Wet bescherming persoonsgegevens. Eventuele door de markt zelf op te stellen regels zouden verdere bescherming moeten afdwingen. Indertijd is wel toegezegd dat onderzoek zou worden gedaan naar de vraag of een dergelijke meldplicht effect sorteert. Dit door te kijken naar de resultaten van de landen waar al wel een wettelijke plicht vastgelegd is. Het duurt daarna echter weer enkele jaren voor de discussie over de meldplicht opnieuw oplaait. In 2009 komen het Europees Parlement en de Raad met een aantal wijzigingen voor de zogenaamde ePrivacy-richtlijn, waarin onder meer een meldplicht is opgenomen voor de aanbieders van openbare telecommunicatiediensten (lees: telco's en internet-serviceproviders). Daarmee komt een smalle meldplicht wettelijk vast te liggen, alle EU-lidstaten verplichten zich dit in de nationale wetgeving op te nemen. Eerder zei Hirsch Ballin in antwoord op Kamervragen al dat de wijze waarop dit alles wordt vormgegeven, nog nader bepaald zal gaan worden. De zogenaamde 'smalle' meldplicht zou evenwel in mei 2011 geïmplementeerd dienen te zijn in de Nederlandse wet.[1] De Europese privacywaakhond, de artikel 29 werkgroep, had echter al in het advies op het voorstel tot wijziging van de ePrivacy-richtlijn aangegeven dat 'An extension of personal data breach notifications to Information Society Services is necessary given the ever increasing role these services play in the daily lives of European citizens…'.[2] Daarmee zouden alle dienstaanbieders van de informatiemaatschappij onder de plicht gaan vallen. Het advies werd niet overgenomen, maar is ook niet ongemerkt voorbijgegaan. Over de brede meldplicht volgt later in dit artikel meer.

1 Antwoord op Kamervragen van Gesthuizen, Aanhangsel van de handelingen 165, vergaderjaar 2010-2011.
2 Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive), p. 8.

Wat is dan die meldplicht datalekken?

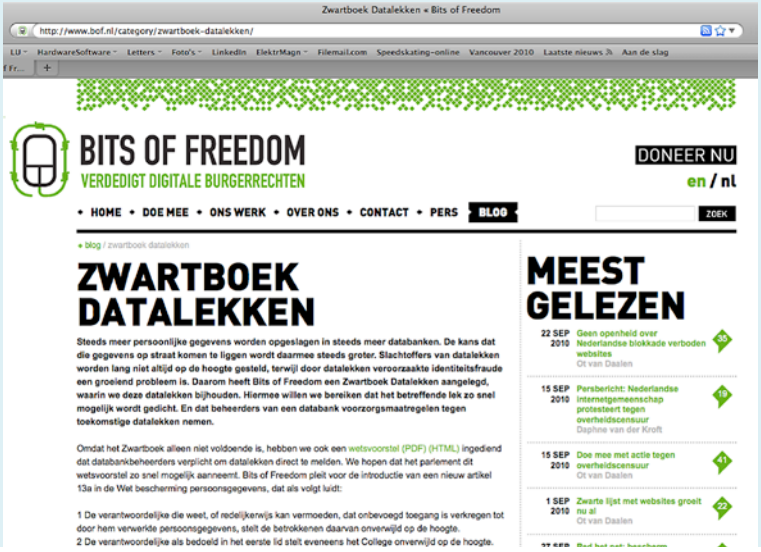
De meldplicht komt voort uit wijzigingen van de Europese privacy- en telecommunicatiewetgeving.[3] Deze 'smalle' meldplicht wordt opgenomen in de Telecommunicatiewet. In het voorstel van wet staat onder meer:

> Artikel 11.3b
> 1. De aanbieder van een openbare elektronische communicatiedienst stelt het college onverwijld in kennis van een inbreuk in verband met persoonsgegevens.
> 2. De aanbieder bedoeld in het eerste lid stelt degene wiens persoonsgegevens het betreft onverwijld in kennis van een inbreuk in verband met persoonsgegevens indien de inbreuk naar verwachting nadelige gevolgen heeft of kan hebben voor diens persoonlijke levenssfeer.

Als een inbreuk heeft plaatsgevonden waarbij persoonsgegevens in het geding zijn, dan moet de nationale bevoegde instantie in kennis gesteld worden van dit datalek – voor Nederland is dat het College bescherming persoonsgegevens. Dit moet zonder onnodige vertraging (lees eigenlijk 'vrijwel direct') gebeuren. Daarbovenop vereist de nieuwe regelgeving dat ook de personen om wier gegevens het gaat een bericht ontvangen, echter, dan moet er wel sprake zijn van waarschijnlijk nadelige gevolgen voor de persoonlijke levenssfeer van het individu. Er moeten dus mogelijk nadelige gevolgen voor de privacy van personen in het geding zijn. Zijn de gegevens bijvoorbeeld dermate versleuteld dat leesbaarheid daarvan niet erg aannemelijk is, dan mag die aanbieder ervan afzien om zijn klanten van het lek op de hoogte te brengen.

De nationaal bevoegde instantie (het Cbp) kan de aanbieders zelfs dwingen om het datalek in de openbaarheid te brengen als ze van oordeel is dat de inbreuk ongunstige gevolgen kan hebben. Als aanbieder moet je in het geval van de melding wel een aantal zaken op orde hebben. Zo moet gemeld worden:

- de aard van de inbreuk op de persoonsgegevens;
- de contactpunten voor meer informatie;
- aanbevolen maatregelen om de gevolgen van de inbreuk te verlichten (voor degene wiens gegevens betrokken zijn in het lek);
- een omschrijving van de gevolgen; en
- een omschrijving van de getroffen of voorgestelde maatregelen om de inbreuk daadwerkelijk aan te pakken.



Figuur 2. **Pagina van de website Zwartboek datalekken.**

De regeling kan zelfs zover strekken dat de nationaal bevoegde instantie specifieke aanwijzingen mag geven over hoe deze publieke kennisgeving gedaan moet worden; daarbij moet gedacht worden aan de manier waarop (online, via de eigen website, in de landelijke media, etc.) en het toepasselijke formaat daarvan. Overigens, als de aanbieder verzaakt het datalek te melden aan de bevoegde nationale instantie, kunnen sancties opgelegd worden. Wat betreft het College bescherming persoonsgegevens kan dan gedacht worden aan een last onder dwangsom of een bestuurlijke boete.[4] En daarbovenop kan dan dus nog eens die openbaarmaking van het lek komen.

Niet iedereen wacht op het verschijnen van de wetgeving. Bits of Freedom heeft al enige tijd een eigen *Zwartboek datalekken*, waarop verschillende forse lekken uitgebreid uit de doeken worden gedaan.[5] Dat het echt niet alleen maar gaat om uit burgerrechtelijke hoek gedane meldingen van datalekken, bewijst Gawker Media, dat in het openbaar te kennen gaf dat op de servers van het bedrijf een inbreuk had plaatsgevonden.[6] Bedrijven nemen dus ook zelf de verantwoordelijkheid op zich om lekken kenbaar te maken. Sterker nog, Gawker Media hield het niet alleen maar bij het melden dat er iets misgegaan was. Zo legde ze een uitgebreide FAQ aan waar gebruikers van hun websites onder meer kunnen lezen wat te doen als ze de account van Gawker-websites gelinkt hebben aan Facebook of Twitter, hoe de account van Gawker gedeletet kan worden en waarin ook uitgebreid aandacht is voor datgene wat het bedrijf zelf doet om het lek te dichten en de gevolgen zoveel mogelijk te beperken.

3 RICHTLIJN 2009/136/EG VAN HET EUROPEES PARLEMENT EN DE RAAD van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronische communicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming.

4 Artt. 65-75 Wbp.

5 Zie: www.bof.nl/category/zwartboek-datalekken/.

6 Zie: http://lifehacker.com/5712785/faq-compromised-commenting-accounts-on-gawker-media.

Een brede meldplicht datalekken

De meldplicht die dit jaar in werking moet gaan treden, treft slechts een gedeelte van de organisaties die te kampen (kunnen) hebben met het weglekken van data. Zoals eerder al aangegeven, is de roep om een bredere meldplicht al langere tijd sterker aan het worden. Zo geeft Eurocommissaris Kroes in de digitale agenda aan dat er op EU-niveau in ieder geval nagedacht wordt over een bredere meldplicht, alhoewel nog met een lichte slag om de arm: 'In het kader van de recent opgezette herziening van het algemene gegevensbeschermingskader zal de plicht om dergelijke inbreuken tegen de gegevensbeveiliging te melden, eventueel worden uitgebreid'.[7] En ook in Nederland zelf lijkt het erop dat een brede meldplicht, voor zowel de overheid als de private sector, inmiddels serieus dichtbij komt, daarmee dus wellicht zelfs vooruitlopend op regelgeving van Europese kant. In de evaluatie van de Wet bescherming persoonsgegevens in maart 2010 merkte Hirsch Ballin echter al op: 'De gedachte voor het invoeren van een meldplicht bij datalekken ondersteunen wij. Deze meldplicht zou een goede bijdrage zijn aan het bevorderen van de transparantie die een van de uitgangspunten moet blijven bij de bescherming van persoonsgegevens. Je moet kunnen weten wie jou registreert en op welke manier. De implementatie van het EU-brede traject *(de smalle meldplicht – RM)* verwachten wij dit kalenderjaar af te ronden'.[8] Hoe precies invulling gegeven kan worden aan die meer brede meldplicht wordt uit de evaluatie helaas nog niet duidelijk. Er is dus wel degelijk al langere tijd veel aandacht voor de realisering van de brede meldplicht en de discussie beperkt zich (gelukkig) niet alleen binnen de grenzen van het 'privacydebat'. Ook in de begin 2011 gepresenteerde Nationale Cyber Security Strategie (NCSS) wordt binnen de paragraaf rondom het vergroten van de weerbaarheid van de vitale infrastructuur gerefereerd aan een brede meldplicht datalekken.[9] De Memorie van Toelichting bij het wetsvoorstel rondom wijziging van de Telecommunicatiewet gaat expliciet in op de brede meldplicht. Daarin wordt nog eens benadrukt dat de minister van Justitie de Tweede Kamer de toezegging heeft gedaan dat er een concreet voorstel zal komen voor een brede meldplicht. Die brede meldplicht zal dan opgenomen gaan worden in de Wet bescherming persoonsgegevens. En ook wat dat aangaat, zal het College bescherming persoonsgegevens de instantie zijn die toezicht moet leveren op de naleving van de meldplicht.[10] Op 29 april maakten staatssecretaris Teeven en minister Donner officieel bekend dat de Wet bescherming persoonsgegevens aangepast zal worden en dat daarin een brede meldplicht opgenomen wordt voor alle aanbieders van informatiediensten.[11] Het kabinet heeft aangegeven dat het een wetsvoorstel daartoe dit jaar nog ter consultatie zal willen aanbieden.

Wat is er nu voor en wat is er nu tegen?

Overduidelijk pluspunt: meer privacybescherming voor individuen. Althans, meer wetenschap over het feit dat er een inbreuk heeft plaatsgevonden. Het kwaad is al wel geschied, maar dat is praktisch inherent aan een inbreuk op de privacy en wordt daarom door privacyspecialisten al geruime tijd één van de 'privacyparadoxen' genoemd.[12] Zijn de gegevens eenmaal overgegaan in andere handen, dan kan weliswaar actie ondernomen worden, maar de zaak kan nooit meer volledig ongedaan gemaakt worden. Wat een dergelijke meldplicht echter mogelijk wel kan bewerkstelligen, is dat bedrijven alerter zullen reageren indien er een inbreuk heeft plaatsgevonden en wellicht zullen zij ook meer toezien (voor zover mogelijk) op het voorkomen van dergelijke lekken. In zoverre zou de meldplicht dus ook een preventieve werking kunnen hebben. Daar staat echter wel tegenover dat een inbreuk dan ook daadwerkelijk opgemerkt moet kunnen worden. In het huidige voorstel van wet is een verplichting opgelegd om *iedere* inbreuk te melden. De onmogelijkheid van detectie van elke inbreuk en het feit dat ook geringe inbreuken gemeld zouden moeten worden, zijn dan ook van meet af aan kritiekpunten op de meldplicht geweest.[13] KPN geeft aan dat het 'lastig, zo niet onmogelijk' is om altijd te achterhalen of er een veiligheidsinbreuk heeft plaatsgevonden die mogelijke gevolgen heeft voor de privacy van een individu. Caiway, Tele2 en Vodafone lopen te hoop tegen de onmogelijkheid om elk lek te ontdekken. In hun reactie schrijven zij dan ook dat 'Indien een aanbieder veiligheidsmaatregelen heeft genomen die redelijkerwijs van hem kunnen worden verwacht, en hem een inbreuk op persoonsgegevens niet bekend is geworden, duidelijk zal moeten zijn dat hem niet kan worden verweten dat hij geen melding heeft gemaakt van de inbreuk.'[14] In haar samenvatting van de consultatie stelt het ministerie van Economische Zaken de betrokken partijen in zoverre gerust dat het

7 Een digitale agenda voor Europa, COM/2010/0245 f/2.
8 AO, TK 31051, 2009-2010, p. 20.
9 De Nationale Cyber Security Strategie, Slagkracht door samenwerking, 22 februari 2011.
10 Memorie van Toelichting wetsvoorstel wijziging Telecommunicatiewet, paragraaf 1.8 'Bescherming van persoonsgegevens en de persoonlijke levenssfeer', 15 april 2010.
11 Zie hiervoor onder meer het persbericht van 29 april 2011 op www.rijksoverheid.nl.
12 Een andere vaak gehoorde paradox is dat personen vaak zeggen veel waarde te hechten aan privacy en dus niet willen dat bijvoorbeeld de overheid veel gegevens verwerkt, maar tegelijkertijd wel zelf gemakkelijk (door middel van social media) allerlei persoonlijke informatie delen. Zie bijvoorbeeld: S. Barnes, A privacy paradox: social networking in the United States, *Firstmonday*, vol. 11, no. 9, 4 September 2006.
13 Zie hierover bijvoorbeeld de reactie van KPN in de consultatieronde van het ministerie van Economische Zaken over het voorontwerp van wet tot implementatie van Richtlijnen 2009/136/EG en 2009/140/EG (versie 15 april 2010), verkrijgbaar via: http://www.internetconsultatie.nl/nrfimplementatie/.
14 De reactie van Caiway, Tele2 en Vodafone in de consultatieronde van het ministerie van Economische Zaken over het voorontwerp van wet tot implementatie van Richtlijnen 2009/136/EG en 2009/140/EG (versie 15 april 2010), verkrijgbaar via: http://www.internetconsultatie.nl/nrfimplementatie/.

aangeeft dat er gevallen denkbaar zijn waarin het niet melden van een datalek de aanbieder niet verweten kan worden. 'Wat betreft mogelijke uitvoeringsproblemen wordt het volgende opgemerkt. Op grond van artikel 11.3 *(Telecommunicatiewet – RM)* dient de aanbieder van openbare elektronische communicatiediensten passende maatregelen te nemen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten. Indien die beveiliging op orde is en er vindt een veiligheidsinbreuk plaats die waarschijnlijk zal leiden tot een aantasting van persoonsgegevens, en die inbreuk wordt niet opgemerkt, dan kan de aanbieder niet verweten worden dat hij de melding ervan heeft nagelaten. Een aanbieder behoeft en kan ook niet altijd op de hoogte zijn van het feit of als gevolg van een veiligheidsinbreuk er waarschijnlijk persoonsgegevens worden aangetast. Maar in veel gevallen zal de aanbieder voldoende aanwijzingen hebben dat bij het transport persoonsgegevens betrokken zijn.[15]' De laatste zin laat raden dat men niet zo heel snel zal aannemen dat een aanbieder niets verweten kan worden. Overigens kent ook de Wet bescherming persoonsgegevens voor de verwerker van persoonsgegevens de plicht om 'passende technische en organisatorische maatregelen ten uitvoer [te leggen] om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking…'. Wel is deze eis strenger dan die welke is opgenomen in het wetsvoorstel van de wijziging Telecommunicatiewet, waar alleen gewezen wordt op 'gepaste technische maatregelen' en 'versleuteling'.

De meldplicht zou ook een preventieve werking kunnen hebben

Wat moeten organisaties regelen?

Elke organisatie – of het nu gaat om overheden of het bedrijfsleven – dient bij het verwerken van persoonsgegevens compliant te zijn met de Wet bescherming persoonsgegevens. Dit omvat onder meer het in kaart brengen van de informatiestromen binnen een organisatie (welke gegevens worden verwerkt en voor welke doeleinden), bezien of deze verwerkingen gemeld dienen te worden aan het College en indien er sprake is van zogenaamde Cross Border Data Transfer (gegevens worden buiten de EU/EER gebracht) moet rekening worden gehouden met een aantal specifieke vereisten, zoals bijvoorbeeld het verkrijgen van een vergunning daarvoor. Organisaties die deze zaken op orde hebben, zullen daardoor ook al een voorsprong hebben wat betreft de verplichtingen die voortvloeien uit de meldplicht. Door het op orde hebben van deze zaken zal een organisatie onder meer makkelijker kunnen aangeven wat de aard van de gegevens is en zal ze ook sneller een goed oordeel kunnen geven over de mogelijke impact van het datalek. Er dient immers een omschrijving van de gevolgen en de daarop genomen en nog te nemen maatregelen verstrekt te worden aan het College. In het verlengde daarvan is het noodzakelijk dat organisaties een zogenaamd 'actieplan' gereed hebben liggen voor het geval zich daadwerkelijk een datalek voordoet. Een dergelijk plan dient onder meer vast te leggen aan wie binnen de organisatie gemeld wordt dat er een onregelmatigheid heeft plaatsgevonden en welke maatregelen dientengevolge genomen moeten worden (denk daarbij aan het in kaart brengen van de gegevens die mogelijk bij het lek gecompromitteerd zijn geraakt, het gereed hebben van die concrete maatregelen en het uiteindelijke doen van de melding bij het College). Dit is te meer dringend daar een melding aan het College 'onverwijld' dient te geschieden.

Het adequaat beveiligen van persoonsgegevens die een organisatie verwerkt, is al onderdeel van de verplichtingen binnen de Wbp. Artikel 13 stelt dat een organisatie passende technische en organisatorische maatregelen ten uitvoer moet leggen tegen verlies of enige vorm van onrechtmatige verwerking. Daarbij moet rekening worden gehouden met de stand van de techniek (wat is feitelijk mogelijk?), de kosten (de kosten moeten proportioneel zijn), maar ook bijvoorbeeld de aard van de gegevens (zo geldt onder de Wbp een strenger regime voor het verwerken van gevoelige persoonsgegevens). Het begrip 'passende' maatregelen is niet nader ingevuld in de wet, alhoewel zoals vermeld wel enkele aanknopingspunten zijn gegeven waarmee rekening gehouden moet worden. Belangrijk in het licht van de meldplicht datalekken is het feit dat in het voorliggende voorstel voor de 'smalle' meldplicht opgenomen is dat, indien de gegevens cryptografisch versleuteld zijn, een lek weliswaar nog steeds gemeld dient te worden aan het College, maar dat daarbij niet tevens de personen om wier gegevens het gaat ingelicht hoeven te worden. Uit het oogpunt van bedrijfsrisico en dan met name wat betreft de publieke reputatie van een organisatie is het dus een groot pluspunt om de persoonlijke gegevens te versleutelen.

Een laatste belangrijk aspect wat betreft zaken rondom privacy en beveiliging van gegevens is dat het bij het puur technische op orde hebben van de beveiliging niet stopt. Zoals de Wet bescherming persoonsgegevens al aangeeft gaat het ook om het *organisatorisch* passend beveiligen van de gegevens die verwerkt worden. Privacy en beveiliging moeten dus ook ingebed raken in de organisatie zelf. Te denken valt dan aan het bevorderen van awareness onder werknemers (een e-learningcursus bij aanstelling of workshop voor huidige werknemers), het actief verspreiden en toetsen van het interne beleid (policies beschik-

15 Consultatieverslag wetsvoorstel implementatie gewijzigd Europees regelgevend kader (NRF) in de Telecommunicatiewet, verkrijgbaar via: http://www.internetconsultatie.nl/nrfimplementatie/.

baar stellen op intranet en deze regelmatig updaten) en het beschikbaar hebben van procedures voor het geval zich een datalek voordoet. Daarnaast dienen de verantwoordelijkheden op de juiste plaats belegd te worden en dient er een veiligheidsbeleid te zijn.

Concluderend: is het nu een zorg of een zegen?

Waarschijnlijk een beetje van beide. De angst voor de publieke schandpaal doet menig bedrijf beven. Reputatieschade wordt over het geheel genomen toch vaak zwaarder gewogen dan de (geringe) boete van het College bescherming persoonsgegevens. Waarbij overigens opgemerkt moet worden dat de boetecapaciteit van het College inmiddels ook serieus ter discussie staat en naar verwachting in de herziening van de privacywetgeving op EU-niveau zal worden uitgebreid. Hoe dat eruit komt te zien, is nog niet te zeggen, maar een uitbreiding naar hogere boetemogelijkheden lijkt wel voor de hand te liggen. Ook de praktische uitvoerbaarheid – het moeten melden van elk lek – zal vermoedelijk enige kopzorgen opleveren (om nog maar te zwijgen van de kosten, een aspect waar ook verschillende aanbieders op wezen binnen de consultatieronde op het wetsvoorstel). Maar toch ook een zegen. In ieder geval voor het individu wiens gegevens met enige regelmaat op straat lijken te liggen. Openbaarheid noopt wellicht tot meer voorzichtigheid. Hoe een en ander in de praktijk daadwerkelijk zal uitpakken is vooralsnog gissen. Maar dat erover gepraat zal worden in 2011 staat in ieder geval vast. En ... hopelijk zal ook serieus gewerkt worden aan die uitbreiding van de meldplicht. Datalekken komen namelijk echt niet alleen maar voor bij telco's en ISP's. Zo was recent ook de klant van McDonalds de klos ([Ring10a]), lekte het KLPD een fax met tapgegevens ([Zeng10a]), zagen miljoenen Amerikanen hun medische gegevens op straat liggen ([Ring10b]), lagen de medische gegevens van enkele Nederlanders bij de Kringloop ([Zeng10b]), en werd een Amerikaanse bank aangeklaagd omdat zij een datalek had geprobeerd te verdoezelen ([Brow10]).

Hoe kunnen organisaties zich nu voorbereiden op die aankomende meldplicht? Door er in ieder geval voor te zorgen dat:

- er alles aan gedaan is de beveiliging op orde te hebben (heeft u de kennis niet zelf in huis, dan loont het de moeite deze in te huren), daarnaast: versleutelde data hebben in beginsel het voordeel dat een mogelijk lek niet aan de personen (klanten vaak) om wier data het gaat, gemeld hoeft te worden;
- er besef is dat beveiliging niet alleen maar het technisch afdichten van de systemen is (denk aan de plicht binnen de Wet bescherming persoonsgegevens om ook organisatorisch de zaken op orde te hebben);
- er gewerkt wordt aan inrichting van processen en richtlijnen over hoe te handelen in geval zich een datalek voordoet, dit inclusief het op orde hebben van up-to-date informatie, zeker gezien het feit dat een lek 'onverwijld' gemeld moet worden en daarbij ook eisen gesteld zijn wat betreft welke informatie paraat moet liggen.

Referenties

[Brow10] D. Browning, *U.S. bank allegedly concealed data breach*, Star Tribune, 7 december 2010.

[KPMG10] *KPMG Data Loss Barometer*, november 2010, www.datalossbarometer.com.

[Ring10a] T. van Ringelestijn, *Hackers stelen data McDonalds-klanten*, Webwereld, 13 december 2010.

[Ring10b] T. van Ringelestijn, *Miljoenen medische gegevens Amerikanen gelekt*, Webwereld, 26 november 2010.

[Zeng10a] R. Zenger, Datalek: *KLPD lekt fax met tapgegevens*, 25 november 2010, *Zwartboek Datalekken*, BoF.

[Zeng10b] R. Zenger, Datalek: *Medische gegevens in Kringloopwinkel*, 13 december 2010, *Zwartboek Datalekken*, BoF.

Privacy en beveiliging moet ingebed raken in de organisatie zelf