Mr. ir. B. Nieuwesteeg[1]

Van Silicon Valley via Den Haag naar Brussel: de invoering van de meldplicht datalekken

AV&S 2016/24

Het internet is een ongekende katalysator voor economische groei. Aan het eind van het jaar 2000 gebruikten zo'n 360 miljoen mensen het internet. Volgens de website liveinternetstats.com waren dit op 24 maart 3334 miljoen mensen. Het internet heeft ons veel gebracht. Bijvoorbeeld 21% van de economische groei in ontwikkelde landen tussen 2006 en 2011 aldus het adviesbureau McKinsey. Helaas brengt het gebruik van het internet ook risico's voor bedrijven en personen met zich mee, zoals het lekken van persoonsgegevens van individuen. De meldplicht datalekken is een wet(sonderdeel) waarmee, in theorie, op verschillende manieren de impact van datalekken verminderd kan worden. Een meldplicht datalekken is kortgezegd een wettelijke verplichting voor organisaties om datalekken te melden naar de persoon wiens data gelekt is en/of een overkoepelende autoriteit persoonsgegevens. Als een organisatie een datalek niet meldt, kan er een boete opgelegd worden. Dit artikel geeft kort de belangrijkste stand van zaken weer over de meldplicht datalekken. Ik zal eerst de rationale achter de wet toelichten. Vervolgens zal ik kort ingaan op de bakermat van de meldplicht: de Amerikaanse *data breach notification law* die in verschillende staten verschillende vormen aangenomen heeft. Hierna zal ik respectievelijk het Europese en Nederlandse wetgevingsproces toelichten, dat recentelijk tot een afronding is gekomen. Vanaf 1 januari is namelijk de relatief stringente Nederlandse meldplicht datalekken in werking getreden, die gehandhaafd wordt door de Autoriteit Persoonsgegevens. Bovendien is eind 2015 besloten dat er een nieuwe Europese meldplicht datalekken gaat gelden vanaf 2018 die de Nederlandse wet vervangt.

De primaire reden waarom landen meldplichten invoeren is de privacy van het individu. Door het melden van datalekken, althans dat is de gedachte, kunnen consumenten wiens data gelekt is snel op de hoogte gesteld worden en stappen zetten om de gevolgen van het lek te verminderen. Het delen van kennis over datalekken en de oorzaak ervan kan ook zorgen voor kennisdeling tussen bedrijven over dreigingen van persoonsgegevensinbreuk. Een ander effect van de meldplicht is dat de beschikbare gegevens in de markt kunnen helpen bij het ontwerpen van andere cyberveiligheidsproducten zoals bijvoorbeeld cyberverzekeringen. Bovendien wordt in de literatuur nog het *sunlight als disinfectant* effect genoemd. Doordat organisaties met de billen bloot moeten zullen andere organisaties de gegevens van hun klanten beter beveiligen en zullen consumenten ook beter op hun persoonsgegevens passen, zo is de gedachte. Maar, er is ook een keerzijde van de meldplichtmedaille. Zo zijn er, afhankelijk van de gekozen drempel van melden, grotere of kleinere administratieve lasten en nakomingskosten van de organisatie die moet melden. Er zijn ook kosten voor de overheid, die een instantie in het leven moet roepen om naar te melden en ook de wet in enige mate moet handhaven. Een overactieve meldplicht kan tevens zorgen voor een overmaat aan informatie bij consumenten en organisaties. Als er elke dag meerdere meldingen zijn, zal de aandacht wellicht verslappen. Ten slotte kan voor de meldende organisatie een melding reputatieschade met zich meebrengen.

Zoals bij veel technologische innovaties is ook de door digitale technologie gedreven meldplicht datalekken om en nabij *Silicon Valley* ontstaan in 2004. Californië was namelijk de eerste staat om de meldplicht in te voeren. Andere staten volgden snel. In 2006 hadden reeds 26 Amerikaanse staten een meldplicht ingevoerd en 16 staten hadden het wetgevingsproces opgestart. In 2016 hebben slechts Alabama, New Mexico, en Zuid Dakota geen meldplicht voor datalekken. Opvallend aan deze ontwikkeling is dat de juridische inhoud van de meldplicht zich niet uniform heeft verspreid. Zo verschillen boetes voor niet melden significant. Een voorbeeld: in 2012 kon de staat Michigan een boete opleggen voor het niet nakomen van de wet van 750.000 dollar terwijl Wyoming slechts een boete van 1000 dollar kon opleggen. Ook verschilt de ontvanger van de meldplicht, soms is dat de Federal Trade Commission, soms de Attorney General en soms hoeft alleen aan de *data subject* gemeld te worden. Dit alles heeft geleid tot vrij veel wrevel en rechtsonzekerheid bij bedrijven en daarom is de roep om een overkoepelende meldplicht steeds groter geworden. President Obama heeft daarom in de state of the Union van 2015 een voorstel gedaan voor één federale meldplicht die de meldplichten op staatsniveau vervangt.

We zien een parallelle ontwikkeling aan onze kant van de Atlantische oceaan. In 2009 voerde de Europese Unie de telecommunicatierichtlijn 2009/136/EC in, ook wel bekend als de E-Privacy richtlijn, die een meldplicht datalekken voor de telecommunicatiesector bevat. Simultaan aan deze ontwikkeling bestond al reeds lang in de Europese Unie de wens om de verouderde databeschermingsrichtlijn 95/46/EC (uit 1995) te vervangen door een striktere verordening. In 2012 kwam het dan ook tot een voorstel voor een zogenaamde algemene databeschermingsverordening (de *General Data Protection Regulation*). Eind 2015 is er overeenstemming bereikt over dit voorstel, weliswaar in gewijzigde vorm, in de zogenaamde trialoog van raad, commissie en parlement. Onderdeel van dit voorstel is tevens een meldplicht datalekken voor alle bedrijven (dus niet alleen de telecommuni-

1 Bernold Nieuwesteeg is promovendus in de rechtseconomie van de cybersecurity aan de Erasmus Universiteit Rotterdam. Hij heeft een achtergrond in Europees Recht (Universiteit Utrecht) en Technische Bestuurskunde (TU-Delft). Citeerwijze: Bernold Nieuwesteeg, 'Van Silicon Valley via Den Haag naar Brussel: de invoering van de meldplicht datalekken', *AV&S* 2016/x, afl. 3.

catiesector), die in 2018 zonder tussenkomst van nationale wetgeving van de lidstaten van kracht zal worden. Opvallend is dat er, zeker in vergelijking met de Amerikaanse wetgeving, *de jure* zware middelen worden ingezet om te zorgen dat organisaties hun datalekken ook daadwerkelijk melden. Zo is er een boete op niet melden die kan oplopen tot 4% van wereldwijde jaaromzet van bedrijven, een systematiek die doet denken aan de Europese mededingingswetgeving. De nationale autoriteiten zullen samen werken met de European Data Protection Authority om de wet te handhaven.

In Nederland besloot men in 2012 niet te wachten op het relatief trage wetgevingsproces van de Europese Unie, maar alvast zelf een eigen nationale meldplicht datalekken op te stellen. Aanvankelijk was de verwachting dat de Nederlandse meldplicht midden 2014 ingevoerd zou worden. Uitgebreide discussies omtrent de exacte juridische formulering in tweede en met name eerste kamer hebben erin geresulteerd dat de inwerkingtreding van de Nederlandse meldplicht meerdere malen is uitgesteld. Uiteindelijk is deze 1 januari 2016 van kracht geworden. De Nederlandse meldplicht datalekken maakt deel uit van de algemene wet bescherming persoonsgegevens. Praktisch gezien kan een organisatie (een overheidsinstantie of een bedrijf) een datalek online melden via de website van de Autoriteit Persoonsgegevens. In de eerste maand waren er enkele honderden meldingen binnengekomen aldus de autoriteit. De boete op niet melden kan oplopen tot 830.000 euro.

Er zijn bestaan echter, nu de Nederlandse meldplicht is ingevoerd, vanuit juridisch oogpunt nog een flink aantal onduidelijkheden. Ik zal er drie uitlichten: de drempel om te melden, de snelheid waarmee gemeld wordt en de striktheid van de handhaving. Ten eerste, het gemodificeerde artikel 14 van de WBP stelt in lid vijf de drempel waarin gemeld wordt als volgt: 'de verplichting tot melding van een inbreuk op de beveiliging die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens die door hem worden verwerkt.' De vraag is natuurlijk, hoe individuele organisaties beoordelen wat een 'aanzienlijke kans' is en wat 'ernstige gevolgen' zijn. Ten tweede, de termijn waarop gemeld moet worden is niet geheel duidelijk. Het nieuwe artikel 34a stelt de termijnen waarbinnen gemeld dient te worden. Er moet (lid 1) 'onverwijld gemeld worden aan de autoriteit persoonsgegevens' en (lid 2) ook onverwijld aan de betrokkene (de eigenaar van de data), maar alleen als dit 'waarschijnlijk' ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Het blijft echter nog onduidelijk wat 'onverwijld' en 'waarschijnlijk' precies betekent in de context van deze wetgeving. Veel Amerikaanse *data breach notification laws* hebben een exacte termijn om te melden in de wet vastgelegd zoals bijvoorbeeld 24 uur na de ontdekking van het lek. Dit principe, hoewel het meer duidelijkheid zou verschaffen, is niet overgenomen door de Nederlandse wetgever. Ten derde, het is nog zeer onduidelijk hoe strikt de meldplicht gehandhaafd gaat worden. De Autoriteit Persoonsgegevens heeft naar eigen zeggen aangegeven dat er minimale capaciteit voor handhaving beschikbaar is en dat derhalve de pijlen alleen gericht worden op grote lekken die bekendgemaakt worden in de media maar niet gemeld zijn. Dit roept vraagtekens op met betrekking tot de uiteindelijke *de facto* effectiviteit van de wet.

Samenvattend, de Nederlandse wetgever heeft na veel debat sinds 1 januari een meldplicht datalekken ingevoerd, ruim een decennium nadat de Verenigde Staten deze introduceerde. Er zijn een aantal onduidelijkheden, onder andere met betrekking tot de drempel van melden, de snelheid waarmee gemeld dient te worden en de handhaving van de wet. De Nederlandse meldplicht is meer een tussenpaus omdat de Europese verordening deze uiteindelijk gaat vervangen in 2018.