Datalekken en andere IT incidenten

Hoe bereidt u zich voor op de aankomende meldplichten?

Huub de Jong – advocaat bij Bird & Bird

De wetgever lijkt in de ban van de meldplicht als remedie tegen cybercrime en andere onfortuinlijke IT incidenten. Welke meldplichten zijn inmiddels ingevoerd en welke staan er op korte termijn nog op stapel? Wat wordt er van ondernemingen verwacht indien zich een incident voordoet en waarover maken bedrijven zich zorgen?

Het is nog maar de vraag in hoeverre meldplichten inderdaad bijdragen aan een veiligere ICT omgeving. Dit weerhoudt de wetgever er niet van om een serie van meldplichten te introduceren met ieder hun eigen toepassingsbereik en bijzonderheden.

Een nieuwe meldplicht voor iedere onderneming

Voor haast iedere onderneming relevant is het wetsvoorstel van 21 juni jl. ter invoering van een brede meldplicht. Dit wetsvoorstel introduceert artikel 34a in de Wet bescherming persoonsgegevens ('Wbp'). Het voorgestelde artikel verlangt van iedere onderneming die verantwoordelijk is voor de verwerking van persoonsgegevens dat deze het College bescherming persoonsgegevens ('Cbp') onverwijld in kennis stelt van inbreuken op de beveiliging van persoonsgegevens. Althans voor zover redelijkerwijs kan worden aangenomen dat die inbreuk een aanmerkelijke kans op nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Afgaand op de Memorie van Toelichting kunnen zeer uiteenlopende inbreuken tot melden verplichten, variërend van een hack van een ICT-systeem tot het per ongeluk bij het oud papier aanbieden van vertrouwelijke stukken. Indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor iemands persoonlijke levenssfeer, zal ook degene wiens persoonsgegevens het betreft in kennis gesteld dienen te worden. Het niet nakomen van de meldplicht kan door het Cbp worden gesanctioneerd met een boete van maximaal EUR 450.000.

“Door de stapeling aan meldplichten worden bedrijven opgezadeld met grote administratieve en juridische lasten als zij met een incident worden geconfronteerd. Het is essentieel dat de meldplichten tegen het licht worden gehouden en op zijn minst is zorgvuldige coördinatie tussen de nationale en Europese trajecten gewenst. Idealiter wordt gezorgd voor een naadloze aansluiting op de Brusselse trajecten.”
David de Nood (secretaris informatiebeleid bij VNO-NCW en MKB-Nederland)

Opvallend is dat de Nederlandse wetgever niet heeft willen wachten op de implementatie van de Algemene verordening gegevensbescherming die de Wbp moet gaan vervangen. Het voorstel voor de verordening bevat namelijk ook een algemene plicht tot het melden van datalekken aan de toezichthouder en betrokkene, met overigens een aanzienlijk forsere sanctionering. Zowel het Cbp, VNO/NCW als ICT~Office hebben aangedrongen op aansluiting bij de tekst van de verordening in het voorgestelde artikel 34a van de Wbp. Helaas vooralsnog zonder noemenswaardig resultaat. Wel heeft de wetgever in grote mate aansluiting gezocht bij de sinds juni 2012 in de Telecommunicatiewet (artikel 11.3a) opgenomen specifieke meldplicht voor aanbieders van openbare elektronische communicatiediensten. Dergelijke aanbieders dienen de Autoriteit Consument & Markt (‘ACM’) onverwijld in kennis te stellen van inbreuken op de beveiliging die nadelige gevolgen hebben voor de bescherming van persoonsgegevens. Indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor iemands persoonlijke levenssfeer dient de aanbieder ook deze persoon onverwijld in kennis te stellen.

Overlappende regelgeving
De verschillende meldplichten bij verscheidene (overheids)instanties zijn voor menig onderneming een zorg. Men vreest een forse toename in administratieve lasten. Ook bestaat de vrees dat de meldplichten mogelijk conflicteren. Dit geldt niet alleen voor de telecommunicatiesector, maar ook bijvoorbeeld voor beursgenoteerde instellingen, financiële ondernemingen en feitelijk ieder internationaal opererend bedrijf. Bovendien zijn er voor aanbieders van voor Nederland vitale infrastructuur en bijvoorbeeld aanbieders van gekwalificeerde certificaten (zoals in het verleden Diginotar) nog meer meldplichten in voorbereiding.

"De meeste multinationals werken met informatiesystemen en IT infrastructuur die grensoverschrijdend zijn. Stel dat er een incident is, moet je dan in alle Europese landen waar je opereert de daar van toepassing zijnde bevoegde toezichthouders gaan inlichten, ieder met hun eigen informatie vereisten? Daarnaast vallen veel bedrijven in een aantal landen waar ze opereren onder meerdere toezichthouders en je kunt je dan voorstellen dat bij een (grensoverschrijdend) incident een chaos kan ontstaan in communicatieverplichtingen en de reikwijdte daarvan."
Hendrik-Jan Buist en Kees Daniëls (Shell IT)

Vertrouwelijkheid
Een andere zorg die de meldplicht oplevert is de vertrouwelijkheid van een melding. Kunt u er gerust op zijn dat ten behoeve van de melding verstrekte gegevens niet bij (andere) toezichthouders terechtkomen of via bijvoorbeeld een Wob-verzoek in het publieke domein belanden? Bedrijven staan om deze reden terughoudend tegenover het delen van vertrouwelijke gegevens met het Nationaal Cyber Security Centre. Deze zorg lijkt terecht, want de concept Memorie van Toelichting bij de concept Wet melding inbreuken elektronische informatiesystemen doet wat betreft de vertrouwelijkheid geen harde toezeggingen.

Schematisch overzicht enkele meldplichten

Wie?	*Wanneer?*	*Waar?*
'iedere verwerker van persoonsgegevens'	inbreuken op de beveiliging van persoonsgegevens, indien redelijkerwijs kan worden aangenomen dat die inbreuk een aanmerkelijke kans op nadelige gevolgen heeft voor de bescherming van de persoonsgegevens	Cbp en afhankelijk van de gevolgen ook de betrokkene
aanbieders van openbare elektronische communicatiediensten	inbreuken op de beveiliging, die nadelige gevolgen heeft voor de bescherming van persoonsgegevens die zijn verwerkt in verband met de levering van een openbare elektronische communicatiedienst in de Europese Unie.	ACM en afhankelijk van de gevolgen ook de betrokkene
financiële onderneming	gedraging of gebeurtenis die een ernstig gevaar vormt voor de integere uitoefening van het bedrijf van de desbetreffende financiële onderneming.	AFM/DNB
beursgenoteerde ondernemingen	uitlekken informatie die invloed kan hebben op de koers, mits de informatie concreet is en gaat over de onderneming en de informatie nog niet algemeen verkrijgbaar is gesteld.	AFM / media
aangewezen aanbieders vitale infrastructuur	een inbreuk op de veiligheid of een verlies van integriteit van informatiesysteem waardoor de beschikbaarheid of betrouwbaarheid van een aangewezen product of dienst in belangrijke mate wordt of kan worden onderbroken.	NCSC en via NCSC eventueel andere aanbieders en het publiek

Grotere kans op claims
Een derde zorg die leeft bij ondernemingen is het toenemende risico aansprakelijk gesteld te worden in het geval zich een inbreuk of ander incident voordoet. Cybercrime en IT incidenten leveren immers forse schade op. De gedachte lijkt logisch: een publieke bekendmaking van incidenten vergroot de kans voor vermeende schade aansprakelijk gesteld te worden. Voor een deel zijn deze risico's te beperken door het afsluiten van de juiste verzekeringen. Allianz en enkele andere verzekeraars bieden sinds kort bijvoorbeeld een cybercrime verzekering aan die tot op bepaalde hoogte zowel eigen schade, aansprakelijkheid tegenover derden als schade voortvloeiend uit de meldplicht dekt.

Conclusie
De wetgever lijkt vastberaden de meldplichten uit te breiden. VNO-NCW, ICT~Office en anderen trachten de scherpe randjes er af te halen en vooral de administratieve lasten voor bedrijven te beperken. Als onderneming kunt u zich voorbereiden door enerzijds goed in kaart te brengen welke meldplichten voor uw onderneming van belang zijn en hoe deze in de praktijk ingevuld dienen te worden. Zodoende kunt u bij een eventueel incident snel genoeg handelen. Anderzijds dient u na te gaan in hoeverre de overeenkomsten die u sluit deugdelijke afspraken bevatten op dit punt. In een ICT omgeving bestaan immers veel afhankelijkheden. Zijn uw leveranciers contractueel verplicht eventuele incidenten direct aan u te melden? Als onderneming blijft u eindverantwoordelijk voor het voorkomen en eventueel melden van inbreuken. In het wetsvoorstel meldplicht datalekken is overigens ook bepaald dat verantwoordelijke en bewerker van persoonsgegevens verplicht worden op dit punt onderling afspraken te maken.

Huub de Jong is advocaat bij Bird & Bird. Hij heeft veel ervaring met adviseren over juridische aspecten van complexe technologievraagstukken, opstellen en beoordelen van contracten en oplossen van geschillen, inclusief het voeren van procedures. Hij heeft een talent voor het uitonderhandelen en juridisch begeleiden van complexe (internationale) ICT projecten. Hij combineert graag zijn juridische kennis met gevoel voor de technologie en de commerciële belangen van cliënten. Huub is lid van de Vereniging Informaticarecht Advocaten, de Nederlandse Vereniging voor Informatietechnologie en Recht, de Vereniging voor Media- en Communicatierecht, de Vereniging Privacy Recht en het internationale ITechLaw en de Association of Certified Fraud Examiners.