(Cyber)security en compliance – een *passend* beveiligingsniveau

mr. J.A.N. Baas*

Trefwoorden: beveiliging van persoonsgegevens, meldplicht bij beveiligingsinbreuken en datalekken, netwerk- en informatiebeveiliging

Inleiding

In een relatief korte periode is de door organisaties beheerde informatie verplaatst van papieren dossiers, kaartenbakken, papieren agenda's en kladblaadjes naar digitale opslagmedia. Waar nog met papier wordt gewerkt is er vaak een digitale schaduw, omdat het papieren document digitaal is aangemaakt of omdat het is gescand en opgenomen in een *document management system.*

De gebruikte digitale opslagmedia zijn veelal verbonden met het internet. In veel gevallen bevinden de media zich niet meer fysiek in het gebouw van de organisatie – door alomtegenwoordige mobiele apparaten zoals *notebooks*, *tablets* en *smartphones* en doordat opslag en back-up in toenemende mate in *'the cloud'* plaatsvindt.

Niet alleen de verwerking van (persoons)gegevens, maar bijna ieder proces dat voor de organisatie van belang is wordt gedigitaliseerd. Van banktransacties en de analyse van bloed- en urinemonsters in medische laboratoria tot het beheer van waterstanden door het hoogheemraadschap en de snelheden van centrifugemotoren in een nucleaire opwerkingsfabriek.[1]

Er wordt al langer gewaarschuwd voor de beveiligingsrisico's die dit met zich meebrengt. Dat deze risico's zich ook daadwerkelijk verwezenlijken is vooral de laatste jaren steeds zichtbaarder geworden door een groot aantal gevallen waarbij beveiligingsinbreuken en datalekken hebben plaatsgevonden, bijvoorbeeld door achtergelaten usb-sticks, cyberinbraken en het kopiëren van vertrouwelijke bestanden door personeelsleden. Dat heeft geleid tot onbevoegde kennisneming en verspreiding van persoonsgegevens en vertrouwelijke bedrijfsgegevens maar ook tot het platleggen van websites (bijvoorbeeld door DDoS-aanvallen) en fraude. De gevolgen variëren van ongemak tot ernstige vermogens- en reputatieschade en potentieel tot ontwrichting van het maatschappelijk leven.

Als dit soort incidenten in de krant komt leidt dit doorgaans tot politiek activisme en wetgevingsinitiatieven. Deze bijdrage geeft een overzicht van een aantal bestaande en toekomstige verplichtingen waar uw organisatie rekening mee dient te houden.

Persoonsgegevens: beveiliging

Het nemen van adequate beveiligingsmaatregelen is altijd een integraal onderdeel geweest van *compliance* op het gebied van bescherming van persoonsgegevens.[2] Al in de eerste *Code of Fair Information Practices* uit 1973 vindt men het voorschrift '*Any organization maintaining an administrative automated personal data system shall (...) take reasonable precautions to protect data in the system from any anticipated threats or hazards to the security of the system.*'[3]

De huidige uitwerking van deze verplichting is te vinden in art. 13 Wet bescherming persoonsgegevens ('Wbp'), gebaseerd op art. 17 Richtlijn Bescherming Persoonsgegevens.[4] Ingevolge art. 13 Wbp legt de verantwoordelijke[5] 'passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtma-

* Jan Baas is advocaat bij BarentsKrans te Den Haag.

1 Dit laatste voorbeeld is niet toevallig. In 2010 hebben Amerikaanse en Israëlische geheime diensten een Iraanse nucleaire opwerkingsfabriek onklaar gemaakt middels een computervirus, Stuxnet. Dit virus zou de centrifuges onklaar hebben gemaakt door de snelheden van de centrifugemotoren te manipuleren. Zie o.a. Y. Visser, Oorlog zonder slachtoffers is stap vooruit, *Volkskant* 26 november 2010.

2 Chr. Kuner, *European Data Protection Law*, New York: OUP 2007, p. 288.

3 *Records, Computers and the Rights of Citizens* (US Dep. Health, Education and Welfare 1973); Code of Fair Information Practices.

4 Richtlijn 95/46/EG.

5 Termen als verantwoordelijke, betrokkene, bewerker en persoonsgegeven worden in dit artikel gebruikt in de betekenis die hieraan wordt gegeven in art. 1 Wbp.

tige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.'[6]

De kern van de verplichting is gelegen in het vereiste van een 'passend beveiligingsniveau'. Bepalend bij de vraag wanneer sprake is van een passend beveiligingsniveau zijn de stand van de techniek en de kosten van de tenuitvoerlegging, afgezet tegen de risico's die de verwerking en de aard van de te verwerken gegevens met zich meebrengen.[7] De wet geeft geen details over de specifieke beveiligingsmaatregelen die genomen dienen te worden. Uiteindelijk is het, zo wordt gesteld in de parlementaire geschiedenis bij het artikel, aan de professionele ethiek van personen belast met de informatiebeveiliging, overgelaten welke maatregelen in het licht van de stand van de techniek een passend beveiligingsniveau vormen.[8] Wel zal de verantwoordelijke moeten kunnen verantwoorden dat de door hem genomen maatregelen een passend beveiligingsregime vormen.

Het verantwoordingselement dat van de verplichting deel uitmaakt wordt in de komende Verordening Gegevensbescherming ('Ontwerpverordening')[9] aanzienlijk verder benadrukt nu o.a.:

- in de artikelen 11 en 22 een verplichting is opgenomen dat naleving van de verordening aantoonbaar wordt vastgelegd in beleid;
- artikel 30 een verplichting om een beveiligingsbeleid te voeren, te testen, te beoordelen en te evalueren;
- in artikel 32a een verplichting om risico analyses te maken;
- in artikel 33 een verplichting om in bepaalde gevallen *data protection impact assessments* uit te voeren met daarin o.a. een overzicht van de beveiligingsmaatregelen en waarborgen;
- en in artikel 33a een verplichting om periodieke *data compliance reviews* uit te voeren.

Het criterium 'passend beveiligingsniveau' blijft in de Ontwerpverordening gehandhaafd, zij het dat art. 30 Ontwerpverordening gedetailleerder weergeeft aan welke vereisten de beveiliging dient te voldoen, zonder overigens specifieke maatregelen te noemen die genomen moeten worden. Net als de Wbp en de Richtlijn Bescherming Persoonsgegevens is de Ontwerpverordening techniekneutraal opgesteld.
Als kompas bij de invulling kunnen diverse beschikbare richtsnoeren en normen worden gehanteerd.[10] Het College Bescherming Persoonsgegevens ('CBP') heeft zelf ook een document met richtsnoeren uitgebracht ('Richtsnoeren'),[11] waarin het een methodiek beschrijft volgens welke beveiliging dient plaats te vinden. Ofschoon het CBP aangeeft dat organisaties in specifieke situaties ook met andere standaarden, methoden en maatregelen het vereiste beveiligingsniveau kunnen bereiken, neemt het de geschetste methodiek bij onderzoeken en beoordelingen van de beveiliging als uitgangspunt.[12] In de richtsnoeren legt het CBP sterk de nadruk op het beoordelen van de risico's (risicoanalyse, al dan niet in het kader van een *data protection impact assessment*), het nemen van maatregelen, het periodiek controleren van de naleving ervan, het periodiek evalueren ('*plan - do - check - act* cyclus') en de schriftelijke vastlegging van dit alles.[13] In die zin loopt het CBP vooruit op de invoering van de Ontwerpverordening. Daarnaast benadrukt het CBP de toepassing van bestaande beveiligingsstandaarden. Het volgen van beveiligingsstandaarden is niet in alle gevallen voldoende om een passend beveiligingsniveau te bewerkstelligen, zeker niet indien dat wordt gedaan door het slaafs

[6] Op grond van art. 11:3 Tw geldt een vergelijkbare verplichting, strekkende tot bescherming van persoonsgegevens.

[7] Zie over deze risico-gebaseerde benadering tevens *Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218, 30 mei 2014 ('Statement Risk-based approach').

[8] *Kamerstukken II* 1997/98, 25 892 nr. 3, p. 98-99.

[9] Zie voor het commissieontwerp Com(2012)11 def. Bij het opstellen van dit artikel is uitgegaan van de inofficiële geconsolideerde versie van 22 oktober 2013 met de amendementen die zijn voorgesteld door de LIBE parlementscommissie zoals te vinden via www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

[10] Zoals de Code voor Informatiebeveiliging, NEN-ISO/IEC 27002:2013 nl of voor de medische sector NEN 7510.

[11] Richtsnoeren Beveiliging van Persoonsgegevens, CBP februari 2013, te vinden op www.cpbweb.nl.

[12] Richtsnoeren, p. 17.

[13] Vgl. in verband met deze schriftelijke vastlegging ook het Statement on Risk Based Approach, p. 3: '*All data controllers should at least to some extent document their processing activities in order to further transparency and accountability. Documentation is an indispensable tool for controllers to manage accountability effectively and for ex-post control by DPAs as well for the exercise of rights by data subjects. It goes beyond the information to be given to the data subjects*'.

zetten van 'vinkjes'.[14] Het niet volgen ervan kan in de ogen van het CBP onder omstandigheden echter als een overtreding van art. 13 Wbp gelden, bijvoorbeeld indien de betreffende norm gebruikelijk is in een branche of sector.[15] Waar in het hierboven aangehaalde citaat uit de parlementaire geschiedenis nog de ethiek van de informatieprofessional bepalend is, zoekt het CBP duidelijk naar objectivering van de norm.
Art. 30 lid 3 Ontwerpverordening voorziet in door het op te richten Europees Comité voor gegevensbescherming op te stellen richtlijnen, aanbevelingen en *best practices* waarin o.a. kan worden vastgesteld wat de stand van de techniek is voor in bepaalde sectoren en voor bepaalde verwerkingen te hanteren beveiligingsmaatregelen.
Uit de Richtsnoeren blijkt dat het CBP van een hoog niveau van bescherming uitgaat. Mede afhankelijk van de aard van de gegevens en de risico's zijn investeringen in geavanceerde beveiligingsoplossingen benodigd.[16] Ook indien de aard van de gegevens of de risico's niet tot het allerhoogste niveau van beveiliging nopen mag echter een adequate beveiliging worden verwacht overeenkomstig de stand van de techniek. Men kan zich bijvoorbeeld voorstellen dat niet aan het minimumniveau wordt voldaan indien voor apparatuur die is verbonden met internet onbeveiligde of verouderde software wordt gebruikt (software die door de leverancier niet meer wordt ondersteund en van beveiligingsupdates wordt voorzien), beveiligingsupdates niet worden geïnstalleerd, of indien de in de software aanwezige beveiligingsmogelijkheden (zoals *firewalls*, veilige wachtwoordinstellingen etc.) niet worden benut.

Privacy Enhancing Technologies; Data Protection by Design en by Default

De verplichting tot beveiliging van persoonsgegevens kan niet los worden gezien van de overige verplichtingen ingevolge de Wbp, in het bijzonder doelbinding, bewaartermijn en het verbod op bovenmatige verwerking.[17] Het gaat ook om keuzen als wie toegang heeft tot welke gegevens, welke gegevens op het netwerk blijven staan en welke gegevens worden gewist of gearchiveerd. De slotzin van art. 13 Wbp, 'de maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen', ziet op technische maatregelen die dit waarborgen, zg. '*Privacy Enhancing Technologies*.'[18]
In moderner jargon wordt in verband met het voorgaande ook wel gesproken van '*data protection (of privacy) by design*' en van '*data protection (of privacy) by default*'. Bij *data protection by design* worden reeds bij het het ontwerpen of inrichten van ICT-systemen de benodigde waarborgen meegenomen op het gebied van bescherming van persoonsgegevens. Gedurende de gehele 'levenscyclus' van de data wordt zoveel mogelijk voorkomen dat privacy-inbreuken kunnen plaatsvinden. Bij '*data protection by default*' is de standaardinstelling in het systeem dat gegevens niet verder worden verwerkt dan minimaal benodigd voor de doeleinden van de verwerking. De betrokkene dient zelf te kunnen kiezen of de gegevens verder worden verwerkt of gedeeld. Art. 23 Ontwerpverordening bevat verplichtingen tot het toepassen van *data protection by design* en *by default*. O.a. in de hierboven besproken *data protection impact assesments* zal mede aandacht besteed moeten worden aan de toegepaste *data protection by design* en *by default* maatregelen.

Bewerker; derden

Indien de verantwoordelijke zich van bewerkers bedient om de persoonsgegevens te verwerken dient hij ervoor zorg te dragen dat deze voldoende waarborgen bieden ten aanzien van de technische en organisatorische beveiligingsmaatregelen met betrekking tot de te verrichten verwerkingen. De verantwoordelijke dient toe te zien op de naleving van die maatregelen. De verplichting tot naleving van de beveiligingsverplichtingen die op de verantwoordelijke rusten dient voorts schriftelijk vastgelegd te worden.[19] Dat is ook een verstandige beleidslijn in verhouding met andere derden aan wie gegevens worden toevertrouwd. Contracten met bewerkers of andere dienstverleners die gegevens

[14] Vgl. Recital 65 van de Ontwerpverordening, 'However, equal emphasis and significance should be placed on good practice and compliance and not just the completion of documentation.'
[15] Vgl. Onderzoek naar het gebruik van waarneemdossiers bij Centrale Huisartsenpost Nightcare BV te Heerlen, CBP 21 augustus 2013, z2012-00624.
[16] C.M.M. Zwinkels, 'Artikel 13 Wbp: de zorgplicht en informatiebeveiliging', *P&I* 2014, afl. 3, p. 123 leidt uit 'Toegang tot digitale patientendossiers binnen zorginstellingen', *CBP*, juni 2013, p. 9 en 14 af dat 'het CBP niet snel het hoofd zal buigen voor argumentaties van directies dat de 'kosten van de uitvoering' in art. 13 Wbp voorlopig te hoog zijn voor hun organisatie.' Ik merk op dat het aangehaalde rapport ziet op de medische sector, waar de aard van de verwerkte (medische) gegevens de lat hoger legt dan in andere sectoren. Uit de wettekst en parlementaire geschiedenis blijkt dat de kosten wel degelijk een overweging kunnen zijn om van (aanvullende) maatregelen af te zien, in het bijzonder indien de meeropbrengst aan veiligheid gering is ten opzichte van de investering. Zie *Kamerstukken I* 1997/98, 25 892 nr. 92c, p. 15-16. Een adequaat beveiligingsniveau zal uiteraard wel verzekerd moeten zijn.
[17] Art. 7-11 Wbp.
[18] *Kamerstukken II* 1997/98, 25 892 nr. 22.
[19] Art. 14 Wbp.

ontvangen dienen goed te worden gecontroleerd op naleving van de verplichtingen ingevolge de Wbp, waarbij mede aandacht besteed dient te worden aan beveiliging van de gegevens, controleerbaarheid (bijvoorbeeld door opname van een auditrecht) en een meldplicht bij datalekken en andere incidenten.

Persoonsgegevens: informatie- en meldplicht datalekken en beveiligingsinbreuken

Indien zich ondanks de toegepaste beveiligingsmaatregelen onverhoopt een incident heeft voorgedaan zal afgewogen moeten worden of dit incident wordt gemeld – aan het bevoegd gezag of aan betrokken derden. Met mijn kantoorgenoot mr. M.H.J. van Rest schreef ik al eens een artikel over dit onderwerp.[20] Inmiddels is op dit gebied alweer behoorlijk wat gebeurd, zodat een actualisatie op haar plaats is.
Ter recapitulatie: op dit moment zijn alleen in sectorwetgeving (financiële ondernemingen,[21] telecom[22]) concrete verplichtingen opgenomen tot het melden van beveiligingsinbreuken aan het bevoegd gezag. Daarnaast kan in zeer specifieke gevallen een verplichting bestaan om strafrechtelijke aangifte te doen.[23]
Een concrete verplichting tot het informeren van betrokkenen is opgenomen in art. 11.3a lid 2 Telecommunicatiewet ('Tw'). Een dergelijke verplichting kan daarnaast onder omstandigheden volgen uit art. 6 Wbp (rechtmatige verwerking/ *fair processing*)[24] en bijvoorbeeld art. 6:162 (onrechtmatige daad), art. 6:248, art. 7:401, art. 7:403 en art. 7:611 BW (overeenkomst; opdracht; arbeidsovereenkomst).
Ten aanzien van art. 6 Wbp merkten wij ter relativering op dat wij in de internationale literatuur weinig bevestiging hadden gevonden voor het in Nederland breder gedragen standpunt, dat een informatieplicht in geval van datalekken volgt uit art. 6 (althans 33 of 34) Wbp en art. 6, art. 10 en art. 11 Richtlijn Bescherming Persoonsgegevens waarop de artikelen uit de Wbp zijn gebaseerd. Inmiddels heeft de artikel 29-werkgroep, het overlegorgaan van toezichthouders op het gebied van persoonsgegevens in de Europese Unie, een opinie uitgebracht over meld- en informatieplichten bij beveiligingsinbreuken ('Opinion 03/2014').[25] Uit Opinion 03/2014 lijkt afgeleid te moeten worden dat in de ogen van de artikel 29-werkgroep geen verplichting voortvloeit uit de Richtlijn Bescherming Persoonsgegevens nu Opinion 03/2014 uitgaat van verplichtingen voortvloeiend uit de Telecommunicatierichtlijn[26] en verder alleen verwijst naar de Ontwerpverordening en naar nationale wetgeving. Desondanks zal, in ieder geval naar Nederlands recht, voorlopig rekening gehouden moeten worden met de mogelijkheid dat een verantwoordelijke is gehouden om de betrokkene te informeren als diens persoonsgegevens zijn gelekt, zeker indien nadelige gevolgen voor de betrokkene kunnen ontstaan.
Bij de Tweede Kamer is een wetsvoorstel aanhangig[27] dat strekt tot de invoering van een meldplicht en informatieplicht naar aanleiding van beveiligingsinbreuken. Ten tijde van het verschijnen van ons eerdere artikel was hiervan slechts het consultatievoorstel beschikbaar. Onze kritiek was destijds dat er zeer forse boetes werden gekoppeld aan onduidelijke open normen. Inmiddels is het voorstel aanzienlijk afgezwakt omdat de meld- en informatieplicht nog slechts aan de orde is in geval van een beveiligingsinbreuk die 'ernstige nadelige gevolgen heeft voor de bescherming van de persoonsgegevens.'[28]
Voor de informatieplicht aan de betrokkene geldt als aanvullend vereiste dat de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer.
In de Ontwerpverordening is een meld- en informatieplicht opgenomen in art. 31 en 32 in geval van een 'inbreuk in verband met persoonsgegevens'. De Ontwerpverordening verstaat daaronder een onopzettelijke of

[20] J.A.N. Baas & M.H.J. van Rest, 'Informatie- en meldplichten bij datalekken en beveiligingsinbreuken', *P&I* 2012, afl. 6, p. 260.
[21] Art. 3:17 en art. 4:15 Wft jo. art. 3:10 lid 3 en 4:11 lid 4 Wft.
[22] Art. 11.3a Tw.
[23] Ingevolge art. 160 Sv o.a. in relatie tot misdrijven tegen de veiligheid van de staat, misdrijven tegen de koninklijke waardigheid en misdrijven waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht voor zover daardoor levensgevaar is veroorzaakt.
[24] Deze verplichting wordt ook wel geconstrueerd aan de hand van art. 33 en art. 34 Wbp. In het aangehaalde artikel, noot 20, *supra*, wordt onzerzijds betoogd dat deze artikelen geen verplichting tot het melden van een datalek met zich meebrengen.
[25] 'Article 29 Data Protection Working Party, Opinion 03/2014 on Personal Data Breach Notification', *WP* 213, 25 maart 2014.
[26] Zie in het bijzonder noot 6 op de (ongenummerde) vierde pagina van de Opinion 03/2014.
[27] Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij de doorbreking van maatregelen voor de beveiliging van persoonsgegevens (meldplicht datalekken), *Kamerstukken II* 2013/14, 33 662, nr. 2.
[28] *Kamerstukken II* 2013/14, 33 662, nr. 7, p. 1. Eerder ging het om een meldplicht bij een beveiligingsinbreuk 'waarvan redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de persoonsgegevens' terwijl de betrokkene geïnformeerd diende te worden 'indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer'.

onrechtmatige vernietiging, verlies, wijziging, ongeautoriseerde openbaarmaking of toegang tot verzonden, opgeslagen of anderszins verwerkte persoonsgegevens.
Op grond van art. 31 is de verantwoordelijke verplicht een inbreuk in verband met persoonsgegevens te melden aan de toezichthoudende autoriteit. Wanneer de inbreuk waarschijnlijk negatieve gevolgen voor de bescherming van de persoonsgegevens of de privacy van de betrokkene heeft, moet de inbreuk ingevolge art. 32 na de melding aan de toezichthoudende autoriteit ook gemeld worden aan de betrokkene zelf. Gezien in het bijzonder de ruime definitie van het begrip inbreuk in verband met persoonsgegevens is nadere afbakening benodigd van de verplichtingen. De Ontwerpverordening draagt het Europees Comité voor gegevensbescherming op ook hierover richtlijnen, aanbevelingen en *best practices* op te stellen.
Zowel voor het wetsvoorstel als voor de Ontwerpverordening geldt dat aan overtreding aanzienlijk zwaardere sancties worden gekoppeld dan die gelden onder de huidige wetgeving, variërend van (maximaal) 450.000 euro onder het wetsvoorstel tot (maximaal) 2% van de wereldwijde jaaromzet onder de Ontwerpverordening.

Netwerk- en informatiebeveiliging

De Europese commissie heeft een voorstel gedaan voor een richtlijn betreffende de beveiliging van netwerken en informatiesystemen ('Ontwerp-NIB-richtlijn').[29] Uit dit voorstel blijkt dat te verwachten valt dat de beveiligingsverplichting die nu geldt voor persoonsgegevens, in de toekomst een bredere strekking zal krijgen, zoals nu overigens bijvoorbeeld voor de telecomsector al het geval is.[30]
Allereerst dienen ingevolge art. 14 Ontwerp-NIB-richtlijn overheden en marktdeelnemers passende technische en organisatorische maatregelen te nemen ter beheersing van de risico's voor de beveiliging van de netwerken en informatiesystemen die zij controleren en bij hun activiteiten gebruiken, in het bijzonder ter voorkoming of minimalisering van impact op hun kerndiensten. Deze maatregelen zorgen, rekening houdend met de meest recente technische mogelijkheden, voor een beveiligingsniveau dat is afgestemd op de risico's die zich voordoen. Het zal de zorgvuldige lezer opvallen dat het criterium dat is verwoord in belangrijke opzichten lijkt op dat uit art. 13 Wbp.[31]
Bij de bedoelde marktdeelnemers gaat het om aanbieders van diensten van de informatiemaatschappij en exploitanten van kritische infrastructuur, zoals genoemd op een niet-limitatieve bijlage bij het ontwerp. Op die lijst komen partijen voor zoals handelsplatforms, betaaldiensten, sociaalnetwerksites, zoekmachines, *cloud computing-diensten, app stores*, energiebedrijven, vervoersbedrijven, bankwezen, beurzen en gezondheidszorginstellingen.
Het eerder genoemde art. 14 Ontwerp-NIB-richtlijn voorziet voorts in een meldplicht van incidenten met een aanzienlijke impact op de beveiliging van de kerndiensten aan de bevoegde autoriteit in de lidstaat.[32] De bevoegde autoriteit kan in het algemeen belang het publiek informeren over het incident, of de betrokken overheid of marktdeelnemer daartoe verplichten.
Ingevolge art. 15 Ontwerp-NIB-richtlijn kan de autoriteit in de lidstaat marktdeelnemers en overheden verplichten om alle informatie te verschaffen die nodig is om de beveiliging van hun netwerken te beoordelen. Onderdeel van die informatie kan een beveiligingsplan zijn (dat de betreffende marktdeelnemers en overheden dus verplicht zouden moeten opstellen). Daarnaast kan de nationale autoriteit audits (doen) verrichten.

Indirecte verplichtingen tot beveiliging

Een opvallende casus die zich recent heeft voorgedaan is het rumoer rond de beveiliging van de systemen van de Staatsloterij. De systemen van de Staatsloterij zijn ingericht door een Grieks bedrijf. Medewerkers van dit bedrijf zouden toegang hebben tot de systemen van de Staatsloterij en de uitslagen van trekkingen kunnen manipuleren. De toegang door deze medewerkers werd niet gelogd. De Kansspelautoriteit heeft een inval gedaan bij de Staatsloterij. De exacte grondslag daarvoor is nog niet bekend, noch is bekend of overtredingen zijn geconstateerd.
Wat de Staatsloterij-casus duidelijk illustreert is dat de verplichting tot beveiliging niet beperkt is tot persoonsgegevens, de telecomsector of het beperkte aantal bedrijven dat in de Ontwerp-NIB-richtlijn wordt geïdentificeerd. ICT raakt dermate nauw aan bedrijfsprocessen dat de beveiliging ervan een kernvoorwaarde is geworden voor de betrouwbaarheid en continuïteit van deze processen. Dat betekent dat deze beveiliging steeds meer aandacht krijgt van toezichthouders en certificerende

[29] Voorstel voor een richtlijn van het Europees Parlement en de Raad houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, Com(2013) 48 final.
[30] Zie Hoofdstuk 11a Tw.
[31] Vgl. in dit verband tevens art. 11a.1 Tw.
[32] Vgl. tevens art. 11a.2 lid 1 Tw.

instanties tot wiens aandachtsgebied bijvoorbeeld de betrouwbaarheid of continuïteit van die processen behoort, ook zonder dat er specifieke verplichtingen zijn opgelegd ten aanzien van beveiliging. Vergelijk in dit verband ook de voor financiële ondernemingen geldende verplichtingen voor een integere bedrijfsvoering zoals opgenomen in de Wet op het financieel toezicht ('Wft').[33]

Civielrechtelijke aansprakelijkheid

In geval van incidenten dient rekening gehouden te worden met civielrechtelijke aansprakelijkheid. Deze aansprakelijkheid kan voortvloeien uit contractuele regelingen (zoals *service level agreements*) waarin bijvoorbeeld een bepaald niveau van beveiliging, integriteit van data of continuïteit van beschikbaarheid van systemen is gegarandeerd. Ook kunnen incidenten ertoe leiden dat bijvoorbeeld verplichtingen tot levering of tot het verrichten van diensten niet kunnen worden nagekomen.
Daarnaast mogen de risico's en potentiële schade inmiddels zodanig bekend worden geacht en de maatregelen om deze tegen te gaan dermate algemeen, dat het veroorzaken van schade door het niet nemen van passende maatregelen onder omstandigheden als onrechtmatig aangemerkt dient te worden, ook waar een expliciete wettelijke beveiligingsverplichting zoals die bestaat ten aanzien van persoonsgegevens vooralsnog ontbreekt.
Verwacht mag worden dat de publiekrechtelijke normering rond een passend beveiligingsniveau mede de civielrechtelijke aansprakelijkheid zal inkleuren, zowel in een contractuele als in een buitencontractuele context (onrechtmatige daad). Bij het sluiten van overeenkomsten tussen ondernemingen kunnen partijen hierin over het algemeen hun eigen keuzes maken (zie voor een uitzondering het hiervoor aangehaalde art. 14 Wbp, dat voor de bewerkersovereenkomst een verplicht kader schept). Het is van belang om te voorzien in de nodige waarborgen op vlakken als beveiliging, controleerbaarheid (bijvoorbeeld door opname van een auditrecht), continuïteit van beschikbaarheid van systemen en een meldplicht bij datalekken en andere incidenten. De keerzijde hiervan is uiteraard dat bijvoorbeeld aanbieders van diensten goed moeten opletten dat zij op dit vlak geen verplichtingen op zich nemen die zij niet, of slechts tegen hoge kosten, kunnen naleven en dat wordt voorzien in eventuele beperkingen van aansprakelijkheid.
In de Verenigde Staten is reeds een markt ontstaan voor *class actions* naar aanleiding van datalekken. In een recent onderzoek bestond 76% van de onderzochte aansprakelijkheidsprocedures naar aanleiding van datalekken uit collectieve procedures.[34] In Nederland loopt dit nog niet op een vergelijkbare wijze vaart, mogelijk ook omdat de Nederlandse wet niet voorziet in *punitive damages* terwijl het bij inbreuken op de Wbp vaak moeilijk zal blijken om vermogensschade aan te tonen. Art. 49 Wbp voorziet overigens wel in een naar billijkheid vast te stellen vergoeding voor niet-vermogensschade.
Gezien de toenemende betrokkenheid van ICT bij veelsoortige bedrijfsprocessen zijn situaties waarbij zich in de toekomst door beveiligingsinbreuken grote vermogensschade zal voordoen niet denkbeeldig.

Aanbevelingen

Uit het voorgaande moge volgen dat beveiliging van de ICT-omgeving een belangrijk aandachtspunt is in het kader van *compliance*.
De Wbp voorziet in de verplichting om te voorzien in een passend beveiligingsniveau. Dat aan dit vereiste wordt voldaan zal in toenemende mate gedocumenteerd moeten worden. Indien wordt gekeken naar het soort invulling dat het CBP in zijn richtsnoeren geeft aan het vereiste ligt het voor de hand om in ieder geval te voorzien in een deugdelijke risico-inventarisatie (al dan niet als onderdeel van een *data protection impact assessment*), te voorzien in de passende maatregelen die nodig zijn om de geïnventariseerde risico's het hoofd te bieden en deze ook te documenteren in een beveiligingsplan. Dat plan kan vervolgens niet in de kast verdwijnen. Naleving zal in een bepaalde mate gecontroleerd dienen te worden en de risico-inventarisatie en het plan zullen ook van tijd tot tijd geëvalueerd en geactualiseerd moeten worden. Waar van toepassing (zoals bijvoorbeeld in de medische sector) zullen mede bestaande beveiligingsstandaarden zoals NEN 7510 in aanmerking genomen dienen te worden om min of meer geobjectiveerd aan te kunnen tonen dat aan de eisen wordt voldaan.
Voor zover deze documentatieverplichtingen nu al geen geldend recht zijn (hetgeen de Richtsnoeren van het CBP suggereren) worden deze dat in ieder geval met de inwerkingtreding van de Ontwerpverordening. Ook bij incidenten zal een organisatie

[33] Vide art. 3:17 en art. 4:15 Wft.

[34] S. Romanosky, D. Hoffman & A. Acquisti, Emperical Analysis of Data Breach Litigation, *Journal of Empirical Legal Studies*, Volume 11, Issue 1, pages 74–104, March 2014.

moeten kunnen aantonen dat het aan de eisen heeft voldaan. Organisaties doen er verstandig aan hierop te anticiperen.
Aanpassingen aan het ICT-systeem brengen hoge kosten met zich mee en vergen een lange voorbereiding. De verplichtingen ingevolge de Wbp en, na inwerkingtreding, de Ontwerpverordening zullen in de ICT-omgeving geïmplementeerd moeten worden middels *privacy enhancing technologies* althans *data protection by design* en *by default*. Om vervroegde afschrijving van investeringen te voorkomen is het verstandig om bij de invoering van nieuwe systemen direct rekening te houden met alle huidige en, voor zover mogelijk, toekomstige vereisten.
Ook buiten het gegevensbeschermingsrecht behoort ICT-beveiliging vanuit *compliance*-oogpunt een aandachtspunt te zijn. Vanwege (toekomstige) wettelijke verplichtingen maar ook vanwege het belang voor de continuïteit en betrouwbaarheid van essentiële bedrijfsprocessen. Verstoring van de processen, of, zoals de Staatsloterij-casus aantoont, zelfs twijfel over de betrouwbaarheid ervan, kan grote gevolgen hebben voor de reputatie van een bedrijf, raken aan de naleving van wettelijke plichten en aansprakelijkheid veroorzaken.
Bij het sluiten van overeenkomsten zijn beveiliging en continuïteit van ICT-systemen en beveiliging van (persoons)gegevens belangrijke aandachtspunten. Het is van belang om de nodige regelingen op te nemen op vlakken als beveiliging, controleerbaarheid (bijvoorbeeld door opname van een auditrecht), continuïteit van beschikbaarheid van systemen, een meldplicht bij datalekken en andere incidenten en aansprakelijkheid. ■