Jan Baas, advocaat en partner bij BarentsKrans

(Cyber)security - een passend beveiligingsniveau

Organisaties zijn in toenemende mate afhankelijk van ICT. Beveiliging hiervan is inmiddels een groot punt van zorg. Dat heeft ook juridische implicaties. Dit artikel geeft een beknopt overzicht van de belangrijkste aandachtspunten. Rode draad daarbij is de norm 'een passend beveiligingsniveau' zoals die te vinden is in de Wbp en die ook bredere toepassing lijkt te krijgen.[1]

Beveiliging van persoonsgegevens

Op 28 januari 2015, de 'Internationale Dag van de Privacy' publiceerde het CBP haar toezichtagenda voor 2015. Beveiliging van persoonsgegevens is één van de vijf thema's waarop zij zich in 2015 zal richten.

Op grond van de Wet bescherming persoonsgegevens is een verantwoordelijke[2] gehouden persoonsgegevens te beveiligen. Hij dient met technische en organisatorische maatregelen een passend beveiligingsniveau te garanderen. Wat een passend beveiligingsniveau is, hangt af van de stand van de techniek, de kosten van de tenuitvoerlegging en de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

De maatregelen moeten er mede op zijn gericht om onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen. Hiermee wordt gedoeld op zg. *privacy enhancing technologies* of, in moderner jargon: *privacy by design* en *privacy by default*. Reeds bij het ontwerpen of inrichten van ICT-systemen moeten waarborgen meegenomen worden op het gebied van bescherming van persoonsgegevens. Gedurende de gehele 'levenscyclus' van de data moet zoveel mogelijk voorkomen worden dat privacy-inbreuken plaatsvinden.

De wet vult niet in welke concrete maatregelen genomen moeten worden. Het CBP heeft echter richtsnoeren gepubliceerd (te vinden op www.cbpweb.nl) waarin een methodiek staat volgens welke beveiliging moet plaatsvinden. Hoewel organisaties ook met andere standaarden, methoden en maatregelen het vereiste beveiligingsniveau kunnen bereiken, neemt het CBP de geschetste methodiek bij onderzoeken en beoordelingen van de beveiliging als uitgangspunt. Het CBP legt 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 en de schriftelijke vastlegging van dit alles.

Met de grote nadruk op schriftelijke verantwoording loopt het CBP vooruit op de in voorbereiding zijnde Verordening Gegevensbescherming ('de Ontwerpverordening').[3] De huidige wet stelt geen (expliciet) vereiste ten aanzien van schriftelijke vastlegging van het beleid van de verantwoordelijke. De Ontwerpverordening bevat op dit punt wel uitgebreide verplichtingen.

Gezien het voorgaande doen organisaties er goed aan om te voorzien in een deugdelijke risico-inventarisatie, maatregelen te nemen om de geïnventariseerde risico's het hoofd te bieden en dit alles te documenteren in een beveiligingsplan. Dat plan kan vervolgens niet in de kast verdwijnen. De verantwoordelijke zal naleving in bepaalde mate moeten controleren en de risico-inventarisatie en het plan van tijd tot tijd moeten evalueren en actualiseren. Voor zover deze documentatieverplichtingen nu al geen geldend recht zijn (hetgeen de richtsnoeren van

1 Een uitgebreide versie van dit artikel is verschenen in Tijdschrift voor Compliance 2014 (5), p. 292.

2 Termen als verantwoordelijke, betrokkene, bewerker en persoonsgegevens worden hier gebruikt in de betekenis van artikel 1 Wbp.

3 Het is op dit moment nog onzeker of en wanneer de Ontwerpverordening zal worden ingevoerd. Zie voor het commissieontwerp Com(2012)11 def. Zie voorts www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

het CBP suggereren) worden deze dat in ieder geval indien de Ontwerpverordening in werking treedt overeenkomstig het huidige ontwerp. Bij incidenten zal een organisatie daarnaast moeten kunnen aantonen dat het aan de op haar rustende verplichtingen heeft voldaan.

De verplichtingen ingevolge de Wbp en, na inwerkingtreding, de Ontwerpverordening, zullen in de ICT-omgeving geïmplementeerd moeten worden. Aanpassing van ICT-systemen is kostbaar en vergt een lange voorbereiding. Om vervroegde afschrijving van investeringen te voorkomen is het verstandig om bij invoering of aanpassing van systemen rekening te houden met huidige en toekomstige vereisten.

Persoonsgegevens: informatie- en meldplicht datalekken en beveiligingsinbreuken

Er is al geruime tijd een wetsvoorstel aanhangig tot invoering van een meldplicht en informatieplicht naar aanleiding van beveiligingsinbreuken (Kamerstukken 33 662). Op grond van het voorstel moet een beveiligingsinbreuk die 'ernstige nadelige gevolgen heeft voor de bescherming van de persoonsgegevens' worden gemeld aan het CBP. Indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van de betrokkene moet ook deze over de inbreuk geïnformeerd worden. De Ontwerpverordening bevat een vergelijkbare meld- en informatieplicht. Het wetsvoorstel en de Ontwerpverordening koppelen aanzienlijke sancties aan overtreding, variërend van (maximaal) 450.000 euro onder het wetsvoorstel tot (maximaal) 2% van de wereldwijde jaaromzet onder de Ontwerpverordening.

Op dit moment zijn alleen in sectorwetgeving (financiële ondernemingen, telecom) 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. Ook het informeren van betrokkenen is (buiten sectorwetgeving) op dit moment nog niet verplicht. Onder omstandigheden zou een verplichting echter kunnen volgen uit artikel 6 Wbp (rechtmatige verwerking/ *fair processing*), artikel 6:162 (onrechtmatige daad) of uit overeenkomst.

Netwerk- en informatiebeveiliging

De Europese Commissie heeft een voorstel gedaan voor een richtlijn betreffende de beveiliging van netwerken en informatiesystemen ('Ontwerp-NIB-richtlijn').[4] De beveiligingsverplichting die nu geldt voor persoonsgegevens, zou in de toekomst mogelijk een bredere strekking kunnen krijgen, zoals nu overigens bijvoorbeeld voor de telecomsector al het geval is.

Op grond van de Ontwerp-NIB-richtlijn moeten overheden en marktdeelnemers passende technische en organisatorische maatregelen 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 spelen. Tevens wordt voorzien in een meldplicht van incidenten met een aanzienlijke impact op de beveiliging van de kerndiensten aan de bevoegde autoriteit in de lidstaat. Op nationaal niveau is recent (3 februari 2015) de internetconsultatie Wet gegevensverwerking en meldplicht cybersecurity opengesteld, strekkende tot invoering van een vergelijkbare nationale meldplicht.[5]

Indirecte verplichtingen tot beveiliging

Recent deed zich een opvallende casus voor rond de beveiliging van de systemen van de Staatsloterij. Deze systemen zijn ingericht door een Grieks bedrijf. Medewerkers van dit bedrijf zouden toegang hebben tot de systemen en de uitslagen van trekkingen kunnen manipuleren. De Kansspelautoriteit heeft een inval gedaan bij de Staatsloterij en heeft inmiddels aanbevelingen gedaan rond het trekkingsproces, die door de Staatsloterij geïmplementeerd zullen worden.

Deze casus illustreert dat een 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. Beveiliging krijgt daarom steeds meer aandacht van toezichthouders en certificerende instanties tot wier aandachtsgebied bijvoorbeeld de betrouwbaarheid of continuïteit van die processen behoort, ook zonder dat er specifieke verplichtingen zijn opgelegd ten aanzien van beveiliging.

Civielrechtelijke aansprakelijkheid

Bij incidenten moet rekening gehouden worden met civielrechtelijke aansprakelijkheid. 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.

Het veroorzaken van schade door het niet nemen van passende maatregelen kan onder omstandigheden als onrechtmatig aangemerkt worden, ook waar een expliciete wettelijke beveiligingsverplichting ontbreekt. De publiekrechtelijke normering rond een passend beveiligingsniveau zal de civielrechtelijke aansprakelijkheid hieromtrent mede inkleuren.

In contracten is van belang dat wordt voorzien in waarborgen rond beveiliging, controleerbaarheid (via bijvoorbeeld een auditrecht), continuïteit van beschikbaarheid van systemen en een meldplicht bij datalekken en andere incidenten. Aanbieders van diensten zullen anderzijds 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.

4 Com(2013) 48 final.

5 http://www.internetconsultatie.nl/cybersecurity.