Mr. M.A.M. Verveld-Suijkerbuijk en mr. A.J.P. Tillema[1]

Netwerk- en informatiebeveiliging: ontwikkelingen in het regelgevende kader

75

De auteurs beschrijven recente ontwikkelingen op het gebied van netwerk- en informatiebeveiliging (cybersecurity). Bijzondere aandacht gaat uit naar nationale en Europese wetsvoorstellen op het gebied van netwerk- en informatiebeveiliging, waaronder de meldplicht beveiligingsincidenten, de meldplicht datalekken en de verplichting beveiligingsmaatregelen te treffen en audits uit te voeren. Bekeken wordt of genoemde wetsvoorstellen gevolgen hebben voor ondernemingen, gezien de reeds bestaande wettelijke plichten op basis van onder meer de WBP, sectorale wetgeving en corporate governance-bepalingen. Ook worden in dit verband met een gebrekkige netwerk- en informatiebeveiliging samenhangende risico's op aansprakelijkheidstelling, reputatieschade en financiële schade besproken. Conclusie van het artikel is dat genoemde meldplichten voor bepaalde sectoren gevolgen hebben; datalekken en beveiligingsinbreuken moeten volgens in dit artikel beschreven voorstellen niet slechts intern worden opgelost maar ook verplicht extern worden gemeld. De voorstellen kunnen wat dat betreft toegevoegde waarde hebben op het gebied van publiek-private samenwerking. Het lijkt er verder op dat bestaande wettelijke plichten en risico's al voldoende noodzaak zijn voor ondernemingen tot een goed functionerende netwerk- en informatiebeveiliging te komen.

1. Inleiding

Deze inleiding zou kunnen bestaan uit een opsomming van actuele krantenkoppen over het onderwerp van dit artikel. Met die inleiding zouden wij de realiteit echter te kort doen; het is duidelijk dat slechts een handvol incidenten op het gebied van netwerk- en informatiebeveiliging (dikwijls afgekort als 'NIB' en ook wel minder specifiek geduid als *cybercrime* of *cybersecurity*) in de media verschijnt[2] en dat het fenomeen niet slechts iets van 2013 is. Wel kan worden gesteld dat recente incidenten maatschappelijk meer impact lijken te hebben dan eerder. Zo hebben de *Distributed denial of service* (Ddos)-aanvallen op Nederlandse banken bij ondernemers die betalingsproblemen ondervonden, tot de vraag geleid waar de schade kan worden verhaald en onder parlementariërs tot Kamervragen over de inzet en verantwoordelijkheden van banken om cybercrime te bestrijden en het toezicht daarop.[3] De aangifte tegen de vermeende cybercriminelen. De IT-wereld gooit olie op het vuur door in de media te benadrukken dat bestrijding van cybercrime toch vooral draait om techniek. Een gevoel van onveiligheid en wantrouwen in de digitale wereld van de burger gaat van mond tot mond. Eén op de acht van ons is in 2012 slachtoffer geweest van cybercrime.[4] NIB-inbreuken leveren daarnaast diverse nieuwe juridische vraagstukken op[5] en de behoefte om internationaal samen te werken. Wetgevers blijven net zo min buiten boord; de nationale, Europese en Amerikaanse tonen daadkracht met wetsvoorstellen.

In dit artikel bespreken wij recente wetsvoorstellen op het gebied van NIB met mogelijke consequenties voor het Nederlandse bedrijfsleven. Om te beoordelen in hoeverre deze voor-stellen de inrichting van ondernemingen op het gebied van NIB zullen veranderen, schetsen wij eerst het NIB-landschap zoals dat vandaag de dag in grote lijnen geldt.

2. Het NIB-landschap: wettelijke plichten, aansprakelijkheid en 'vrijwilligheid'

2.1 *Wettelijke plichten*

De actualiteit suggereert dat NIB in het bedrijfsleven onvoldoende attentie krijgt. Onderzoek bevestigt deze suggestie gedeeltelijk. Slechts 26% van Europese ondernemingen beschikte in 2012 over NIB-beleid.[6] In Nederland lijkt het bedrijfsleven beter voorbereid.[7] Dat het bedrijfsleven zich bezighoudt met NIB is terecht; Nederlandse onderneming-

1 M.A.M. Verveld-Suijkerbuijk en A.J.P. Tillema zijn beiden werkzaam als advocaat te Amsterdam.

2 Uit een besluit van 19 maart 2013 van de Minister van Veiligheid en Justitie op een verzoek op basis van de Wet Openbaarheid van Bestuur naar ICT-incidenten bij overheidsorganisaties (te raadplegen via www.rijksoverheid.nl/documenten-en-publicaties/wob-verzoeken/2013/03/19/besluit-wob-verzoek-ict-incidenten-bij-overheidsorganisaties.html) blijkt bijv. een groot aantal bij het Nationaal Cyber Security Centrum gemelde cyberincidenten dat niet in de media verscheen, zoals een mogelijke Ddos-aanval op de mailserver van de Autoriteit Financiële Markten en een mogelijk incident bij de Kamer van Koophandel.

3 *Kamerstukken II* 2012/13, 2113, vragen van de leden Dijkhoff en Aukje de Vries (beiden VVD) aan de Minis-ters van Veiligheid en Justitie en van Financiën over het bericht '*Banken te laks met de aanpak van cybercrime*', nr. 2013Z05566 (ingezonden 20 maart 2013).

4 Centraal Bureau voor de Statistiek, 28 februari 2013, PB13-016, p. 1.

5 Zie bijv. Afdeling Bestuursrechtspraak van de Raad van State 24 maart 2013, *LJN* BZ8406, waarin een op naam van appellant bij de Belastingdienst via DigiD ingediende aanvraag niet aan appellant mocht worden toegerekend, onder meer omdat niet kon worden uitgesloten dat een derde met een DigiD een aanvraag op naam van appellant had ingediend.

6 Commission staff working document, impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, SWD (2013), 32 final, 7 februari 2013, p. 21.

7 Commission staff working document, impact assessment accompanying the document Proposal for a Directive of the European Parliament and of the Council Concerning measures to ensure a high level of network and information security across the Union, SWD (2013), 32 final, 7 februari 2013, p. 23. Zie ook vragen van de leden Dijkhoff en Aukje de Vries (beiden VVD) aan de Ministers van Veiligheid en Justitie en van Financiën over het bericht '*Banken te laks met de aanpak van cybercrime*', nr. 2013Z05566 (ingezonden 20 maart 2013), waarin wordt bevestigd dat de Nederlandse banken voldoende zijn voorbereid op cybercrime.

gen zijn thans al op uiteenlopende wijzen verplicht hun NIB op orde te hebben. De maatschappij lijkt zicht daarvan niet altijd bewust. De wettelijke plichten vinden we met name in de Wet bescherming persoonsgegevens (WBP), in sectorspecifieke wetgeving en volgt verder uit diverse corporate governance-bepalingen.

Op basis van de WBP is een verantwoordelijke[8] verplicht persoonsgegevens conform de wet en op behoorlijke en zorgvuldige wijze te verwerken. Een belangrijk onderdeel van deze verplichting vormt het nemen van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking.[9] De Beveiligings-richtsnoeren van het College bescherming persoonsgegevens (CBP)[10] illustreren aan de hand van een '*Plan-do-check-act*-cyclus' dat en hoe beveiliging volgens het CBP een dagelijks en praktisch aandachtspunt moet zijn binnen ondernemingen. Beveiligingsmaatregelen moeten volgens de richtsnoeren worden ingericht, gecontroleerd en bijgesteld aan de hand van de voor een onderneming specifieke beveiligingsrisico's. Beveiligingsstandaarden kunnen daarbij nuttige handvatten bieden.[11] De verantwoordelijke dient ervoor te zorgen dat een bewerker[12] de beveiligingsmaatregelen naleeft.[13] Deze verplichting wordt neergelegd in de bewerkersovereenkomst.

Beveiliging van persoonsgegevens was één van de kernthema's van het CBP in 2012[14] en zal dat blijven in 2013.[15] Het CBP onderzoekt actief beveiligingsmaatregelen, op basis van door burgers afgegeven 'signalen' of op eigen initiatief en kan een last onder bestuursdwang opleggen tot handhaving van de beveiligingsverplichtingen uit de WBP. Mogelijk beschikt zij op termijn ook over een boetebevoegdheid bij niet-naleving van beveiligingsverplichtingen.[16] Het CBP publiceert verder haar onderzoeksbevindingen, handhavingsbesluiten en zienswijzen. Dit kan voor betrokken verantwoordelijken uiteraard bezwarend zijn en een reputatierisico inhouden. Verantwoordelijken kunnen zich tegen publicatie verzetten bij zwaarwichtige gronden of belangen.[17] De CBP-publicaties geven een inzicht in de wijze waarop het CBP naleving van de WBP toetst. Kern daarvan is dat actueel beleid én praktijk aan moeten sluiten bij algemeen geaccepteerde beveiligingsstandaarden. Zo leverde een actueel concept-beveiligingsbeleid samen met een beleidsdocument van ongeveer 10 jaar oud overtreding van norm 5.1.2. van de Code voor Informatiebeveiliging[18] en daarmee artikel 13 WBP op.[19] Bij haar onderzoeken is het CBP geneigd aan te sluiten bij conclusies in auditrapportages van externe auditbureaus.[20]

Zodra het onderwerp komt op beveiligingsstandaarden neemt de kennis, samen met de interesse, van juristen veelal af. Vaak zijn andere afdelingen dan de juridische (bijvoorbeeld IT-afdelingen in samenwerking met de Raad van Bestuur) binnen een onderneming op de hoogte van de toepasselijke en toegepaste beveiligingsstandaarden. Gezien de voortdurende focus van het CBP op beveiliging en de juridische aspecten van het onderwerp en onderzoek en handhaving daarvan, is het raadzaam dat jurist en IT'er elkaar op dit terrein ontmoeten. Concreet zou dit binnen ondernemingen kunnen worden vormgegeven in regelmatige overlegstructuren of een andere wijze van ondersteuning van de IT-afdeling met juridisch specialisten en het versterken van de rol van de vaak aanwezige security officer.

Naast de WBP bestaan voor een groot deel van de sectoren die van essentieel belang zijn voor de Nederlandse infrastructuur vergaande beveiligings- en meldplichten. Het gaat dan onder meer om de financiële sector, de accountantssector, de elektriciteitssector, de gassector, de drinkwatersector, de sector waterkering, de sector beheersing van waterkwantiteit, de telecomsector, de luchtvaartsector, de havensector en de spoorsector. Zo geldt voor financiële ondernemingen, zoals banken, dat zij over procedures en maatregelen beschikken om de integriteit, voortdurende beschikbaarheid en beveiliging van geautomatiseerde gegevens te waarborgen[21] en een verplichting incidenten die een ernstig gevaar vormen voor de integere bedrijfsvoering te melden aan de toezichthouder.[22] Hetzelfde geldt voor accountantsorganisaties.[23] In de luchtvaartsector geldt een meldplicht als sprake is van een operationele onderbreking, defect, fout of andere onregelmatigheid waardoor de vliegveiligheid wordt of kan worden beïnvloed.[24] Een ander voorbeeld is de plicht die geldt voor netbeheerders binnen de elektriciteitssector om de veiligheid en betrouwbaarheid van het net te waarborgen.[25] Niet-naleving van sectorale wet- en regelgeving is strafbaar gesteld in de Wet op de eceonomische delicten of beboetbaar op grond van die regelgeving.

8 Art. 1, onder d WBP. De gemiddelde onderneming zal in de regel als verantwoordelijke kwalificeren.
9 Art. 13 WBP.
10 CBP Richtsnoeren, Beveiliging van persoonsgegevens, februari 2013.
11 Bijv. Richtlijnen van het Nationaal Cyber Security Centrum, standaarden van het nationale normalisatie-instituut of standaarden van het Amerikaanse National Institute of Standards and Technology.
12 Art. 1, onder e WBP.
13 Art. 14 WBP.
14 Het CBP in 2012, april 2013, p. 5.
15 Agenda 2013, www.cbpweb.nl.
16 Art. 79, lid 6, onder e voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.
17 Beleidsregels actieve openbaarmaking door het CBP, 29 maart 2011.
18 NEN-ISO/IEC 27002:2007.
19 CBP, Rapport definitieve bevindingen, Stichting Hogeschool Utrecht, 17 januari 2013, p. 7.
20 CBP, Rapport definitieve bevindingen, Ruwaard van Putten Ziekenhuis, 31 augustus 2012.
21 Art. 20, lid 2 Besluit prudentiële regels Wet op het financieel toezicht. Een en ander is uitgewerkt in het Toet-singskader informatiebeveiliging, waaruit volgt dat instellingen aantonen dat het stelsel werkt. Blijkens haar toezicht acht De Nederlansche Bank daarbij in het bijzonder van belang dat de procedures een geïntegreerd onderdeel vormen van de organisatie als geheel.
22 Art. 12, lid 3 Besluit prudentiële regels Wet op het financieel toezicht en art. 19, lid 3, 24, lid 3 en 29, lid 3 Besluit gedragstoezicht financiële ondernemingen Wet op het financieel toezicht.
23 Art. 32, lid 4 Besluit toezicht accountantsorganisaties.
24 Art. 7.1. Wet luchtvaart.
25 Art. 16 Elektriciteitswet.

Beursgenoteerde ondernemingen in het bijzonder dienen zich er verder bewust van te zijn dat het de verantwoordelijkheid van het bestuur is om de naleving van toepasselijke wet- en regelgeving te garanderen en de risico's verbonden aan de ondernemingsactiviteiten te beheersen door middel van een intern risicobeheersings- en controlesysteem, dat is afgestemd op het aan de strategie van de onderneming verbonden risicoprofiel.[26] Beursgenoteerde ondernemingen die niet onder sectorale NIB-wet- en regelgeving vallen, dienen zich dus uit hoofde van corporate governance wel degelijk te vergewissen van NIB-risico's en maatregelen te treffen om die risico's af te wenden.

Ook uit het civiele recht kunnen verplichtingen voortvloeien op het gebied van NIB. Gezien de aanvullende werking van de redelijkheid en billijkheid[27] en de verplichting om als goed opdrachtnemer te handelen[28] is denkbaar dat in bepaalde situaties een beveiligingsverplichting of, bij incidenten, een meldplicht bestaat. Uiteraard kunnen dergelijke plichten ook voortvloeien uit door ondernemingen gesloten overeenkomsten.

Voorts zal in bepaalde situaties die de NIB raken een aangifteplicht kunnen gelden.[29]

2.2 *Aansprakelijkheid*

Ook los van de vraag of sprake is van een wettelijk plicht, verdient het aanbeveling aandacht te besteden aan NIB omdat een onderneming civiele en strafrechtelijke aansprakelijkheid riskeert bij een gebrekkige NIB. Civiele aansprakelijkheid in verband met een gebrekkige NIB kan mogelijk voortvloeien uit wanprestatie[30] of onrechtmatige daad[31], ook als geen sprake is van een wettelijke plicht, vanwege schending van zorgvuldigheidsnormen. Voorts is het verstandig beveiligingsmaatregelen te nemen om mogelijke strafrechtelijke aansprakelijkheid te voorkomen. Op grond van artikel 161septies Wetboek van Strafrecht is het veroorzaken van een stoornis in de gang of werking van een geautomatiseerd werk door verwijtbare onachtzaamheid strafbaar. Een dergelijke gedraging kan worden toegerekend aan een onderneming en ook een feitelijk leidinggever kan daarvoor mogelijk worden vervolgd. Voornoemde aansprakelijkheden zijn vooralsnog vrij theoretisch en worden in de praktijk zelden gezien, maar zouden krachtige instrumenten kunnen zijn tot versterking van NIB van ondernemingen.

2.3 *'Vrijwilligheid'*

Tot slot kan een onderneming overwegen op basis van vrijwilligheid – of gedreven door aansprakelijkheidsbeperkende motieven – beveiligingsmaatregelen te treffen. Drijfveren zijn dan simpelweg bedrijfszekerheid en – ook bepaald niet onbelangrijk – het voorkomen van reputatieschade. Dat ondernemingen op dit terrein in toenemende mate een eigen verantwoordelijkheid ervaren, volgt ook uit het gegeven dat ondernemingen vrijwillig contact zoeken met autoriteiten als sprake is van inbreuken op de NIB. In 2012 werden bijvoorbeeld 364 incidenten gemeld bij het Nationaal Cyber Security Centrum, terwijl dit in 2011 236 waren.[32] Ook het College bescherming persoonsgegevens wordt – zij het sporadisch – op de hoogte gesteld van lekken van persoonsgegevens.[33]

3. Het NIB-landschap: recente ontwikkelingen

Op het gebied van NIB volgen uiteenlopende ontwikkelingen zich in razend tempo op. Op de eerste plaats op wetgevingsterrein. Het 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 ('Conceptrichtlijn NIB'),[34] het voorstel voor een verordening van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens ('Conceptverordening')[35] en het Wetsvoorstel tot wijziging van de Wbp ('Wetsvoorstel Wijziging Wbp')[36] staan in het vervolg van dit artikel centraal, aangezien deze voorstellen vergaande verplichtingen bevatten waarop het Nederlands bedrijfsleven moet worden ingericht. Wetgeving die ondernemingen ook direct of indirect kan raken is opgenomen in het consultatiedocument Computercriminaliteit III. Dit consultatiedocument bevat voorstellen om het Wetboek van Strafrecht en het Wetboek van Strafvordering aan te passen aan de stand van de techniek. Het consultatiedocument bevat onder meer een bevoegdheid om een geautomatiseerd werk op afstand heimelijk binnen te dringen, een bevoegdheid tot het geven van een decryptiebevel en een strafbaarstelling van het wederrechtelijk overnemen van gegevens.[37]

26 Art. II.1. Corporate Governance Code.
27 Art. 6:248 Burgerlijk Wetboek.
28 Art. 7:401 Burgerlijk Wetboek.
29 Art. 160 Wetboek van Strafvordering, waaruit onder meer volgt dat een aangifteplicht bestaat indien sprake is van strafbare feiten met levensgevaar of waarbij mogelijk staatsgeheimen kunnen of worden geschonden.
30 C. Prins, 'Zorgplichten en cybercrime', *NJB* 2013/948, afl. 18.
31 Nationaal Cyber Security Centrum, 'Cybercrime. Van herkenning tot aangifte' januari 2012, p. 21.
32 *Kamerstukken II* 2012/13, 2092, Vragen van de leden Dijkhoff en De Liefde (beiden VVD) aan de Ministers van Veiligheid en Justitie en van Economische Zaken over het bericht dat de Verenigde Staten kiezen voor het vrijwillig melden van cybersecurity-incidenten (ingezonden 7 maart 2013), p. 3.
33 *Kamerstukken II* 2012/13, 2092, vragen van de leden Dijkhoff en De Liefde (beiden VVD) aan de Ministers van Veiligheid en Justitie en van Economische Zaken over het bericht dat de Verenigde Staten kiezen voor het vrijwillig melden van cybersecurity-incidenten (ingezonden 7 maart 2013), p. 3.
34 COM (2013) 48 definitief.
35 COM (2012) 11 final
36 Wijziging van de Wet bescherming persoonsgegevens en de Telecommunicatiewet in verband met de invoering van een meldplicht bij doorbreking van maatregelen voor de beveiliging van persoonsgegevens, 21 juni 2013 (ten tijde van het indienen van dit artikel was nog geen Kamernummer beschikbaar).
37 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (Computercriminaliteit III), www.internetconsultatie.nl/computercriminaliteit.

Op de tweede plaats is een groei aan instituties en overlegstructuren op het gebied van NIB waarneembaar en wordt de capaciteit van bestaande instituties uitgebreid. Ook wordt op het terrein van NIB zeer actief publiek-privaat samengewerkt. Het in januari 2012 gestarte Nationaal Cyber Security Centrum[38] ('NCSC') groeit in personele omvang, huist liaisons uit uiteenlopende sectoren[39] en zal in 2014 een publiekprivaat ICT Response Board voor alle vitale sectoren omsluiten ten behoeve van publiek-private samenwerking en intensivering van kennisuitwisseling.[40] Ook internationaal werkt het NCSC intensief samen met partners ten behoeve van NIB.[41] Vermeldenswaardig is verder dat EC3, het Europees Centrum voor de bestrijding van cybercriminaliteit en onderdeel van Europol, op 1 januari 2013 van start is gegaan in Den Haag. Tot slot is de capaciteit van de politie op het gebied van cybercrime in 2012 en 2013 aanzienlijk uitgebreid en wordt intensief gewerkt aan het kennisniveau.[42]

Op de derde plaats ontwikkelt de praktijk maatschappijbreed mee met de cybercrisis. Natio-naal en Europees worden ICT-crisisoefeningen uitgevoerd,[43] wordt geïnvesteerd in onderzoeksprogramma's op het terrein van NIB[44] en sectorale toezichthouders beschouwen NIB als een belangrijk toezichtthema[45].

4. Achtergrond Conceptrichtlijn NIB en Conceptverordening

Bestaande wet- en regelgeving blijft volgens de nationale en Europese wetgever achter bij de toename van beveiligingsincidenten en de groeiende omvang en complexiteit daarvan.[46] Beide wetgevers streven naar een meer doeltreffende NIB binnen sectoren die maatschappelijk een essentiële rol vervullen[47] en een betere equipering van toezichthouders om adequaat en efficiënt te reageren op incidenten.[48] Verder delen zij de mening dat consequenties van beveiligingsinbreuken voor burgers transparanter moeten zijn en dat persoonsgegevens op meer zorgvuldige en veilige wijze moeten worden behandeld.[49] De Europese wetgever is tot slot van mening dat het niveauverschil van NIB tussen lidstaten moet worden gedicht. Met name voornoemde overwegingen liggen ten grondslag aan hierna genoemde regelgeving en nationale en Europese (concept)wetgevingsvoorstellen.

5. Conceptrichtlijn NIB

5.1 *Samenwerking*

De Conceptrichtlijn NIB verplicht lidstaten een nationale NIB-strategie en een NIB-samenwerkingsplan op te stellen. Tevens verplicht de Conceptrichtlijn NIB-lidstaten een bevoegde autoriteit aan te wijzen met bevoegdheden voor de beveiliging van netwerk- en informatiesystemen en een computercrisisteam op te zetten dat verantwoordelijk is voor de behandeling van incidenten en risico's. Voorts voorziet de Conceptrichtlijn NIB in de oprichting van een Europees samenwerkingsnetwerk tussen de bevoegde nationale autoriteiten en de Europese Commissie om samen op te treden tegen risico's en incidenten met betrekking tot netwerk- en informatiesystemen en informatie uit te wisselen.

5.2 *Meldplicht beveiligingsincidenten*

Voornoemd samenwerkingsverband komt niet van de grond zonder hulp van private partijen. De Europese wetgever wenst daarom gebruik te maken van 'overheden' en 'marktdeelnemers' die diensten verlenen in de Europese Unie door hen te verplichten incidenten met een aanzienlijke impact op de beveiliging van de door hen verleende kerndiensten aan de nationale bevoegde autoriteiten te melden. Marktdeelnemers zijn platforms voor elektronische handel, gateways voor internetbetalingen, sociaalnetwerksites, zoekmachines, verleners van cloud computing-diensten, internetwinkels die applicaties aanbieden en partijen die werkzaam zijn in de energiesector, de vervoersector, het bankwezen, de infrastructuur voor de financiële markt en de gezondheidszorg.[50] De bevoegde autoriteit wordt volgens de Conceptrichtlijn NIB bevoegd het publiek te informeren over een aangemeld incident, of kan overheden en marktdeelnemers daartoe verplichten. Het is aan de Europese Commissie en de nationale bevoegde autoriteiten in te vullen onder welke omstandigheden een incident moet worden gemeld. De Conceptrichtlijn NIB streeft naar minimumharmonisatie.[51]

Ook de Nederlandse wetgever is voorstander van een meldplicht voor 'inbreuken op de veiligheid en/of integriteit van informatiesystemen die de continuïteit van de eigen of andermans dienstverlening in belangrijke mate kunnen verstoren en die leiden tot (potentieel) maatschappelijke ontwrichting'.[52] Een conceptwetsvoorstel is op dit moment

38 Het NCSC ondersteunt overheid, bedrijfsleven en burgers met het leveren van expertise, informatie, advies, response op dreigingen en het verstrekken van de crisisbeheersing en is het centrale meld- en informatiepunt voor ICT-dreigingen en ICT-veiligheidsincidenten.

39 Op 25 april 2013 werd bekendgemaakt dat ook vanuit de financiële sector een liaison wordt geplaatst bij het NCSC. *Kamerstukken II* 2012/13, 2113, vragen van de leden Dijkhoff en Aukje de Vries (beiden VVD) aan de Ministers van Veiligheid en Justitie en van Financiën over het bericht '*Banken te laks met de aanpak van cyber-crime*' nr. 2013Z05566 (ingezonden 20 maart 2013), p. 3.

40 *Kamerstukken II* 2012/13, 26 643, nr. 265, p. 19. Reeds aangesloten bij het NCSC is het Financial Information Sharing and Analysis Centre.

41 NCSC maakt deel uit van onder meer het Forum of Incident Response and Security Teams (FIRST), European Government CERTs (CERTs), European Network and Information Security Agency (ENISA) en onderhoudt banden met andere Computer Security en Incident Response Teams zoals CertCC en US-CERT in de V.S. en JPCert in Japan.

42 *Kamerstukken II* 2012/13, 26 643, nr. 265, p. 18.

43 *Kamerstukken II* 2012/13, 26 643, nr. 258, p. 3.

44 Het Europese Advanced Cyber Defence Center voert een driejarig onderzoek uit naar botnetproblematiek. In Nederland wordt onder meer in het kader van de Nationale Cyber Security Research Agenda onderzoek verricht op het gebied van cyberveiligheid.

45 Zie Thema's DNB Toezicht 2013, p. 21; het Toetsingskader Informatiebeveiliging DNB (www.toezicht.dnb.nl) en Speerpunten 2013 Autoriteit Consument & Markt, p. 4.

46 Conceptrichtlijn NIB, p. 2.

47 Conceptrichtlijn NIB, p. 2.

48 Conceptrichtlijn NIB, p. 4.

49 Consultatiedocument Wijziging Wbp, 20 december 2011, p. 1.

50 Art. 3, lid 8 jo. Bijlage II Conceptrichtlijn NIB.

51 Art. 2 Conceptrichtlijn NIB.

52 *Kamerstukken II* 2011/12, 26 643, nr. 247, p. 3.

in ontwikkeling.[53] Naast een afwijkende omschrijving van de meldplicht, wijkt de Nederlandse visie op de meldplicht op een aantal essentiële onderdelen af van de Europese. Zelf verwoordt de Minister van Buitenlandse Zaken subtiel dat *'Nederland het voorstel in grote lijnen kan ondersteunen'*.[54] Nederland is voorstander van een meldplicht, maar kant zich tegen een aantal essentiele onderdelen van de Conceptrichtlijn NIB. In algemene zin benadrukt Nederland dat de verantwoordelijkheid op het gebied van nationale veiligheid bij lidstaten rust. Zo moeten lidstaten grotendeels zelf kunnen bepalen wat voor hen vitale sectoren zijn waarop de meldplicht van toepassing is en moeten toezichthoudende bevoegdheden behouden kunnen blijven bij bestaande sectorale toezichthouders. Nederland beschouwt het onderwerp NIB verder mede als een verantwoordelijkheid van de private sector. De in de Conceptrichtlijn NIB voorgestelde *top-down*-benadering van gedetailleerde verplichtingen, moet om die reden worden verruild voor een systeem van verplichte zelfregulering en de ontwikkeling van eigen technische capaciteiten, opleidingen en *best practices* binnen bepaalde sectoren.[55] Een dergelijke benadering zou goed passen in het Nederlandse bedrijfsleven, waar verantwoordelijkheden ten aanzien van NIB thans al moeten worden genomen met het oog op eerdergenoemde wettelijke plichten, aansprakelijkheden en 'vrijwillige' drijfveren.

Discussiebevorderend is dat vitale sectoren in de V.S. onlangs zijn opgeroepen op vrijwillige basis informatie over incidenten te delen met de overheid.[56] De Europese Commissie wijkt bewust af van de in de V.S. gekozen strategie.[57] Nederland heeft toegezegd haar van het Europese voorstel afwijkende uitgangspunt te betrekken bij de besprekingen over de Concept-richtlijn NIB, met name met het oog op eventuele schending van belangen van Nederlandse bedrijven als gevolg van deze afwijking.[58]

5.3 *Beveiligingsmaatregelen en verplichte audit*

Een ander voor ondernemingen relevant voorstel uit de Conceptrichtlijn NIB is de verplichting voor overheden en marktdeelnemers passende technische en organisatorische beveiligingsmaatregelen te treffen. Deze maatregelen moeten zijn afgestemd op de voor een onderneming specifieke risico's en rekening houden met actuele technische mogelijkheden.[59] Deze verplichting is interessant in combinatie met de voorgestelde bevoegdheid van de nationale bevoegde autoriteit een onderneming te verplichten een beveiligingsaudit te ondergaan en de resultaten daarvan te delen.[60] Het is voorstelbaar dat Nederland ook dit voorstel niet vindt stroken met de eigen verantwoordelijkheid van de private sector op NIB-terrein. Om dergelijke audits van waarde te laten zien dient ons inziens de kwaliteit daarvan te worden gegarandeerd, mede gezien de met de dag evoluerende techniek, en dienen maatregelen te worden getroffen op basis van de uitkomsten van de audits.

6. Conceptverordening

6.1 *Meldplicht inbreuk in verband met persoonsgegevens/meldplicht datalekken*

De Conceptverordening bevat een meldplicht van inbreuken in verband met persoongegevens. Inbreuken moeten binnen 24 uur na kennisname worden gemeld aan de toezichthouder. De inbreuken moet worden gedocumenteerd en betrokkenen geïnformeerd voor zover het datalek een negatief gevolg heeft voor de verwerking van hun persoonsgegevens.

Ook de Nederlandse wetgever heeft een meldplicht datalekken geïntroduceerd. De meldplicht datalekken zoals opgenomen in het Wetsvoorstel Wijziging Wbp wijkt af van de meldplicht uit het Europese voorstel. Het Nederlandse voorstel bevat een meldplicht aan het CBP indien redelijkerwijs kan worden aangenomen dat een inbreuk op beveiligingsmaatregelen leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van persoonsgegevens die worden verwerkt.[61] Volgens het Nederlandse voorstel zal dus minder snel sprake zijn van een meldplicht. Idee daarachter is het bedrijfsleven niet nodeloos te belasten en de instandhouding van de effectiviteit van de meldplicht.[62] Verder onderscheidt de voorgestelde 'Nederlandse' meldplicht zich van de 'Europese' doordat 'onverwijld' aan de toezichthouder moet worden gemeld. Het Wetsvoorstel Wijziging Wbp bevat ook een meldplicht aan betrokkenen, indien een inbreuk op de beveiligingsmaatregelen waarschijnlijk ongunstige gevolgen zal hebben voor de persoonlijke levenssfeer van betrokkenen.[63] Het informeren van betrokkenen kan achterwege blijven als de gelekte persoonsgegevens versleuteld zijn of onbegrijpelijk zijn gemaakt voor eenieder die geen recht heeft op kennisname van de gegevens.[64] Een uitzondering op de meldplicht aan betrokkenen geldt onder meer voor financiële ondernemingen.[65] Achtergrond van deze uitzondering is de overtuiging dat de zorgplicht die rust op een financiële onderneming zal waarborgen dat zij, ook zonder dat dit dwingend wordt voorgeschreven, haar verantwoordelijkheid jegens haar cliënten in rechtstreeks contact met die cliënten zal nemen.[66]

De Conceptverordening blijft naar verwachting niet in stand zoals voorgesteld. Eerder zijn amendementen ingediend ten

53 Een consultatiewetsvoorstel met een voorstel voor een meldplicht voor certificaatdienstverleners ten aanzien van gekwalificeerde certificaten is naar aanleiding van het Diginotar incident op 20 februari 2013 in consultatie gegaan. Zie www.internetconsultatie.nl/meldplicht_certificaten.
54 *Kamerstukken II* 2012/13, 22 112, nr. 1587, p. 19.
55 *Kamerstukken II* 2012/13, 22 112, nr. 1587, p. 20.
56 *Executive Order – Improving Critical Infrastructure Cybersecurity*, 12 februari 2013.
57 Europese Commissie Memo/13/71, 7 februari 2013.
58 Kamerbrief 24 april 2013, nr. 376504, p. 5.
59 Art. 14, lid 1 Conceptrichtlijn NIB.
60 Art. 15, lid 2, onder b Conceptrichtlijn NIB.
61 Art. 34a, lid 1 Wetsvoorstel Wijziging Wbp.
62 MvT bij Wetsvoorstel Wijziging Wbp, p. 4.
63 Art. 34a, lid 2 Wetsvoorstel Wijziging Wbp.
64 Art. 34a, lid 6 Wetsvoorstel Wijziging Wbp.
65 Art. 34a, lid 10 Wetsvoorstel Wijziging Wbp
66 MvT bij Wetsvoorstel Wijziging Wbp, p. 8.

aanzien van de 24-uurstermijn[67] en is discussie gevoerd over de vraag of een verordening het juiste instrument is.[68] Op dit moment past de Raad van de Europese Unie de Conceptverordening aan. Zij wenst te komen tot een meer risicogeoriënteerde benadering van de meld- en andere verplichtingen voor de verantwoordelijke.[69] Dit is in lijn met de wens van de Eerste Kamer.[70] Op dit moment wordt door het Ministerie van Justitie en Veiligheid geïnvesteerd in de onderhandelingen over de Conceptverordening; de verordening zal immers ook bindend zijn voor Nederland.[71]

7. Tot slot

Uit het geschetste NIB-landschap blijkt dat een goed functionerende NIB voor ondernemingen op dit moment al noodzakelijk is. Niet alleen om te voldoen aan genoemde wettelijke plichten. Risico's op aansprakelijkheidstelling, reputatieschade en financiële schade zijn voor ondernemingen minstens evenzeer van belang. Wat dat betreft zullen genoemde wetgevende initiatieven niet direct consequenties hebben voor de inrichting van de meeste ondernemingen. Men kan zich afvragen of de bestaande plichten en risico's niet reeds voldoende aanleiding zijn voor het bedrijfsleven om tot een goed functionerende NIB te komen. De voorgestelde meldplichten, echter, zullen voor betrokken sectoren wel gevolgen hebben; datalekken en beveiligingsinbreuken moeten niet slechts intern worden opgelost, maar ook extern bekend worden gemaakt. Deze privaat-publieke samenwerking levert de overheid veel kennis op en kan ook het bedrijfsleven sterker maken. Voorwaarde daarbij is wel dat de overheid de door haar vergaarde kennis deelt met het bedrijfsleven en ook overigens doelmatig capaciteit ter beschikking stelt om schendingen van NIB te helpen te bestrijden.[72] Alleen dan zal niet alleen de publieke sector, maar ook de private sector kunnen profiteren van de meldplichten.

67 European Parliament, 2011/011 COD, Amendments (6), 6 maart2013, 1829-2090, amendementen 1949-1959.

68 European Council, 2012/0011 COD, 25 oktober 2012, Debate in Council, www.europarl.europa.eu/oeil/popups/summary.do?id=123225&t=&l=en.

69 Interinstitutional File 2012/011 (COD), 6607/1/13, Council of the European Union, 1 maart 2013, p. 3.

70 *Kamerstukken I* 2012/13, 33 169, p. 16.

71 *Kamerstukken II* 2012/13, 33 605 VI, nr. 1, p. 29.

72 Zie in dat verband bijv. Forum, nr. 8, april 2013, p. 5 onder 'Opinie VNO-NCW "Overheid kan meer doen tegen cybercrime"': "Het is voor bedrijven en burgers belangrijk dat de overheid met menskracht en techniek meer aandacht schenkt aan de opsporing en vervolging van internetcriminaliteit, niet alleen aan de ingewikkelde zaken, ook aan de kleine die makkelijk op te lossen zijn."