Internetconsultatie ProRail B.V. op wetsvoorstel en memorie van toelichting Cyberbeveiligingswet

Algemeen	ProRail constateert dat de wettekst nauwelijks echt concreet is voor essentiële entiteiten en dat het vooral de rol van de overheid beschrijft. Hoe essentiële entiteiten concreet invulling aan de wet moeten gaan geven, moet uit de lagere regelgeving, de te ontwikkelen richtsnoeren, drempelwaarden etc volgen. Maar die zijn er (nog) niet, niet duidelijk is wat er moet komen en wanneer die er zullen komen. Zonder die nadere regelgeving, richtsnoeren e.d. is niet duidelijk wanneer invulling aan de wet wordt gegegeven.

Wetsvoorstel

Artikel	Bladzijde	Commentaar
1	1 en 2	Nationale cyberbeveiligingsstrategie' is niet gedefinieerd terwijl dit wel is gedaan in artikel 6 sub 4 van de NIS 2-richtlijn. 'Grootschalig beveiligingsincident' is niet gedefinieerd terwijl dit wel is gedaan in artikel 6 sub 7 NIS 2-richtlijn. ProRail meent dat het ook goed zou zijn dit begrip te definieren omdat nu niet duidelijk is wanneer er sprake is van een 'grootschalig' beveiligingsincident, zie ook de opmerking bij artikel 19 en 21.
4 lid 4 regel 2	3	Het woord 'beheer' moet vervangen worden door 'beheersen'
17	8 en 9	In artikel 11 van de NIS 2-richtlijn worden de eisen die aan een CSIRT gesteld uitgebreid uiteengezet. ProRail merkt op dat er nergens in de Cyberbeveiligingswet (hierna: Cbw) eisen worden gesteld aan CSIRT's. ProRail meent dat het goed zou zijn als er ook in de Cbw eisen worden gesteld aan CSIRT's.
19 en 21	9 en 10	Wanneer is er precies sprake van een 'grootschalig' cyberbeveiligingsincident? Dit staat voor zover ProRail kan zien nergens uitgewerkt in de Cbw.
23 lid 1	10	Essentiële en belangrijke entiteiten moeten zelf beoordelen wat passende en evenredige maatregelen zijn. ProRail meent dat dit voor deze entiteiten nog best lastig kan zijn wat in welke situatie passend en evenredig is. Uit de memorie van toelichting blijkt dat zij dit kunnen doen op basis van een eigen risicobeoordeling (zie MvT paragraaf 5.3.1), maar er is nergens in de Cbw iets opgenomen over het doen van een risicobeoordeling en hoe dit zou moeten. Uit artikel 16 Wet Weerbaarheid Kritieke entiteiten (hierna: Wwke) volgt dat entiteiten passende en evenredige maatregelen nemen, mede op basis van de door de bevoegde autoriteit verstrekte relevante informatie over de door haar uitgevoerde risicobeoordeling (artikel 9 Wwke) en op basis van de resultaten van de risicobeoordeling van de kritieke entiteit (artikel 14 Wwke). In artikel 9 en 14 Wwke staat ook wat zo'n risicobeoordeling precies is en wat daarin moet worden meegenomen. ProRail meent dat het goed zou zijn om in de Cbw ook artikelen als artikel 9 en 14 Wwke op te nemen en in artikel 23 op te nemen dat de door de essentiële en belangrijke entiteiten te nemen maatregelen genomen kunnen op basis van deze risicobeoordelingen.
23 lid 1 en lid 2	10	ProRail vraagt zich af wie naast reizigers- en goederenvervoerders hier als 'afnemers van haar diensten' kunnen worden gekwalificeerd? Hoewel de Memorie van Toelichten op blz. 21 daar wel iets over zegt, lijkt dat nog ruimte te laten.
23 lid 2	10	Belangrijke en essentiële entiteiten moeten rekening houden met de maatschappelijke gevolgen. Soms is dat gemakkelijk vast te stellen maar met name de cascade-effecten die kunnen optreden vanuit een geraakte belangrijke of essentiële entiteit op een andere belangrijke of essentiële entiteit kunnen binnen een sector niet altijd overzien worden. Daarvoor zijn intersectorale ketenanalyses nodig die alleen door de bovenliggende landelijke autoriteit opgesteld kunnen worden.
23 lid 2	10	In het verlengde van het voorgaande merkt ProRail op dat belangrijke en essentiële entiteiten vaak afhankelijk zijn van contractpartijen die zelf niet onder een vitale sector hangen. Op welke wijze worden de belangrijke en essentiële entiteiten ondersteund in het doorvertalen van hun benodigde weerbaarheidsmaatregelen naar hun contractanten (dit is in feite supplychain continuity)?
23 lid 3	10	"..gebaseerd op een benadering die alle gevaren omvat...". Wat wordt daar precies mee bedoeld? Wat zijn 'alle gevaren'?
23 lid 4	10	Het artikel gebruikt de term 'type entiteiten' terwijl het in de bijlagen gaat over 'soort entiteit', waarschijnlijk wordt hetzelfde bedoeld? Vanuit oogpunt van eenduidigheid meent ProRail dat het beter zou zijn om dezelfde term te gebruiken ter voorkoming van verwarring.

24 en 33	11 en 13-14	Op basis van artikel 4 van de NIS2-richtlijn kan het toepassingsgebied worden beperkt in geval van sectorspecifieke rechtshandelingen van de EU wanneer de voorschriften daarin tenminste gelijkwaardig worden geacht aan de in de NIS2-richtlijn genoemde verplichtingen. Wie bepaalt die gelijkwaardigheid en wat betekent dat met betrekking tot bijvoorbeeld de Spoorwegveiligheidsrichtijn, de TSI's en andere spoorse richtlijnen en verordeningen en wat betekent dat dan specifiek voor ProRail in relatie tot het wetsvoorstel? In bijvoorbeeld de TSI CCS (spoorse EU verordening) zijn met betrekking tot ERTMS enkele eisen opgenomen voor cyberbeveiliging waardoor, wanneer die maatregelene gelijkwaardig zijn, de verplichting genoemd in artikel 23 (zorgplicht) niet van toepassing zou zijn. ProRail begrijpt dat nadat het EU legal cybersecurity framework gereed komt/is dat daarna de TSI CCS zal worden aangepast, maar vraag blijft wie en waar wordt bepaald en geregeld dat spoorse EU cybermaatregelen gelijkwaardig zijn met als gevolg dat artikel 23 voor ProRail niet van toepassing? Datzelfde geldt voor artikel 33 (meldpicht) bij meldinge van significante incidenten op basis van (sectorspecifieke rechtshandelingen) spoorse EU regelgeving. Hoe zit het dan?
26 lid 2	11	ProRail vraagt zich af of het realistisch is om van het bestuur te verlangen dat het dergelijke detaillistische kennis bezit over ICT-systemen en cyberbeveiligingsmaatregelen. Zou het niet effectiever zijn wanneer het bestuur de mogelijkheid krijgt om deze verplichtingen op een lager uitvoerend niveau in de organisatie te beleggen?
26 lid 4	11	Moet ProRail onder "aantoonbaar actueel" houden lezen dat er een voortdurende scholingsverplichting bestaat? Wat houdt 'aantoonbaar actueel' houden in? In de MvT (blz. 23) staat dat cyberweerbaarheid is een continue en cyclisch proces is. Een bestuurslid moet haar kennis en kunde verversen en indien nodig aanvullen door bijvoorbeeld een opfriscursus. Alsnog is het dan de vraag wanneer de kennis en kunde dient te worden 'ververst'. Is dit wanneer er grote nieuwe ontwikkelingen zijn op het gebied van cyberbeveiliging of moet dit eens in de zoveel tijd sowieso?
27	12	ProRail meent dat hier een meldplicht wordt ingesteld zonder aan te geven wat het doel van de meldingen is. Dient dit een administratief doel? Is de melding bedoeld om hulp van het CSIRT te krijgen? Of is de meldplicht bedoeld om andere kritieke entiteiten zo snel mogelijk te waarschuwen voor een toename van cyberaanvallen zodat deze in verhoogde staat van paraatheid kunnen komen?
27	12	Zou de veiligheidsimpact niet ook terug moeten komen als maatstaf voor de significantie van incidenten?
28 lid 1	12	Dubbele meldplicht: entiteiten moeten melden aan CSIRT en de bevoegde autoriteit. In de MvT (zie paragraaf 5.5.1) staat dat er een dubbele meldplicht bestaat, maar dat er naar gestreefd wordt *'deze dubbele meldplicht technisch zo in te richten dat het verspreiden van de benodigde informatie maar één handeling voor de entiteit vergt.'* Dit ziet ProRail nu nog niet terug in de Cbw. Graag benadrukt ProRail dat dit streven moet resulteren in één loket. Sectoraal is al besproken dat twee loketten absoluut niet werkbaar zijn.
29 lid 1 sub d	12	Betekent dit dat ProRail eventueel ook vertrouwelijke informatie moet verschaffen? En zouden er dan niet ook afspraken moeten worden gemaakt hoe die gegevens worden uitgewisseld (in verband met cyberdiefstal) en het (beperken van het) gebruik van die gegevens?
30	13	ProRail vraagt zich af of er eisen worden gesteld aan de tussentijdse verslaglegging of dat dit volledig free format blijft. Ook hier zou ProRail een minimale eis neerleggen voor duidelijkheid voor belangrijke en essentiële entiteiten en voor uniformiteit.
30	13	Er staat 'eem' in plaats van 'een'.
39	15	Dit artikel gaat over verplichtingen op het gebied van openbaarmakingen. De gedachte en het belang van transparantie en openbaarheid is voor ProRail te volgen, maar er zijn ook situaties denkbaar dat openbaarmaking juist niet gewenst is. Mogen op basis van dit artikel slechts bepaalde aspecten aan het publiek openbaar worden gemaakt? ProRail vraagt zich daarnaast af hoe hierin wordt voorzien en hoe wordt omgegaan met 'de wens/stem' van de betreffende entiteit in deze? Gelet ook op het aspect van schade van openbaarmaking dat hierbij een (belangrijke) rol kan spelen en waarop hier nu niet wordt ingegaan. Er zal iets van een belangenafweging gemaakt moet worden tussen het belang van het publiek bij openbaarmaking enerzijds en het belang van de entiteit om het niet openbaar te maken (schade die het voor haar kan opleveren) anderzijds.
50 lid 5	19	Er staat 'verlemem' en dient 'verlenen' te zijn.

50 lid 6	19	Er is aangegeven 'inzage vorderen'. In de toelichting staat sec vorderen. Indien ze de gegevens wenst te ontvangen dan is het voorstel van ProRail om de woorden 'vorderen deze gegevens te verstrekken' te gebruiken. 'inzage' impliceert dat ze de gegevens mogen inzien maar niet ontvangen. Of is dit de bedoeling? Daarnaast vraagt ProRail zich af binnen welke termijn hieraan dient te worden meegewerkt?
52 lid 1 tot en met 55	19-20	Betreffende het uitwisselen/verstrekken van data meent ProRail dat er een koppeling gelegd zou moeten worden met 'het oog op een zwaarwegend algemeen belang ten behoeve van .....' verstrekking noodzakelijk is.
54	20	In dit artikel wordt niet vermeld dat er bij de informatie-uitwisseling ook sprake kan zijn van persoonsgegevens (aangezien dit bij andere artikelen wel specifiek benoemd staat). ProRail neemt aan dat hier wellicht ook persoonsgegevens onder kunnen vallen en dat dan artikel 64/64a Cbw van toepassing is.
55 lid 1	20	ProRail meent dat er een doel aangegeven zou moeten worden waarvoor de informatie mag worden gebruikt.
56	20	ProRail stelt voor om 'benodigde gegevens' te vervangen door 'noodzakelijke gegevens'.
59	21	De definitie van 'inbreuken in verband met persoonsgegevens' is opgenomen in lid 2 en dient te worden opgenomen in lid 1 omdat dit begrip daar als eerste wordt gebruikt. Het begrip kan ook eventueel worden opgenomen in artikel 1 en in artikel 59 lid 2 worden verwijderd.
61 lid 3	22	ProRail vraagt zich af of er niet wordt getoetst op noodzakelijkheid?
62	22-23	Als een bevoegde autoriteit een dergelijk bijstandsverzoek ontvangt, mag zij dan zelf beslissen of zij er wel of niet aan meewerkt? In artikl 61 zijn namelijk wel specifieke redenen aangegeven op grond waarvan een bijstandsverzoek afgewezen mag worden.
62 lid 3	23	In geval van de uitwisseling van persoonsgegevens, neemt ProRail aan dat artikel 64/64a Cbw van toepassing is.
63	/	Dit nummer is overgeslagen.
64	23	Zijn zij alleen verwerkingsverantwoordelijken voor zover er persoonsgegevens worden verwerkt? Mocht dit gelden voor alle gegevens dan meent ProRail dat het wellicht beter zou zijn om een andere term gebruiken omdat dit verwarring kan brengen (bijvoorbeeld 'zelf verantwoordelijk voor'). Deze term wordt namelijk ook in de AVG gebruikt.
65 lid 1 sub d	23	ProRail vraagt zich af hoe wordt bepaald dat de commerciële en veiligheidsbelangen van de entiteit worden beschermd? Worden de entitieit nog betrokken bij deze afweging?
27 e.v. en 65	12 e.v. en 23	Begrijpt ProRail het goed dat haar meldingen, verslagen, rapporten etc. met bedrijfsvertrouwelijke informatie, buiten de reikwijdte van de Wet Open Overheid (WOO) vallen?
68	24	ProRail vraagt zich af in hoeverre zij betrokken wordt bij de aanwijzing van een dergelijke controlfunctionaris door de bevoegde autoriteit.
68	24	ProRail vraagt zich af wat deze controlefunctionaris toevoegt ten aanzien van de aan te stellen toezichthouders?
69	24-25	ProRail vraagt zich af wanneer dit middel precies kan worden ingezet? Worden de objectieve, niet-discriminerende, eerlijke en transparante risicobeoordelingscriteria verder uiteengezet in een AMvB? En wat houdt een veiligheidscan precies in? Dit artikel (en de MvT) geeft hier maar weinig informatie over.
71	25	ProRail meent dat dit een erg vergaande verplichting is. Een entiteit doet dan als het ware aan 'self-incrimination'. Is deze maatregel wel doeltreffend en evenredig? Wat zijn grondslagen om over te gaan tot openbaarmakening? ProRail meent dat artikel 71 maar weinig informatie geeft terwijl deze handhavingsmaatregel erg vergaand is.
75	26	ProRail vraagt zich af welke certificering of vergunning hier wordt bedoeld?
75-77	26-27	Op basis van artikel 36 van de NIS2-richtlijn kunnen lidstaten regels vaststellen met betrekking tot op te leggen sancties op inbreuken. Deze moeten doeltreffend, evenredig en afschrikkend zijn. ProRail is van mening dat de sancties genoemd in de artikelen 75-77 die opgelegd kunnen worden aan (het bestuur van) een essentiële entiteit niet-proportioneel zijn. In het bijzonder met betrekking tot het bestuur van een essentiële entiteit acht ProRail de sancties te vergaand aangezien het bestuur reeds op basis van meerdere wettelijke regelingen verantwoordelijk is voor het reilen en zeilen van een essentiële entiteit.
76	26	ProRail meent dat een erg zwaar middel is. Een autoriteit kan interveniëren in de samenstelling van een directie of bestuur op basis van een heel specifiek aspect t.w. de cybersecurity. Zijn de overige toezichts- en controlemechanismen niet toereikend? Zijn de potentiële neveneffecten voldoende in beschouwing genomen?
90	31	Begrijpt ProRail het goed dat haar meldingen, verslagen, rapporten etc. met bedrijfsvertrouwelijke informatie, ook buiten de reikwijdte van de Wet Open Overheid (WOO) vallen?

Memorie van Toelichting			
	Paragraaf	Bladzijde	Commentaar
	2.2 onder d	5	ProRail merkt op dat het woord 'beheer' beter vervangen zou kunnen worden door het woord 'beheersen'
	2.2 onder h	6	In de NIS 2-richtlijn zijn artikelen 14-16 gewijd aan de samenwerkingsgroep, CSIRT-netwerk en EU-CyCLONe. In de Cbw wordt het CSIRT-netwerk een paar keer genoemd. Artikel 15 van de NIS 2-richtlijn is een erg uitgebreid artikel, waarin veel meer informatie staat over een dergelijk CSIRT-netwerk. De samenwerkingsgroep en EU-CyCLONe ziet ProRail nergens terugkomen in de Cbw. ProRail vraagt zich af of er in de Cbw niet ook artikelen moeten worden opgenomen over deze instanties? Het zijn namelijk wel belangrijke instanties en ProRail meent dat het daarom goed zou zijn om de taken van deze instanties ook vast te leggen in de Cbw.
	2.3	6	Wat zijn 'ernstige cyberincidenten'. Dit is een ruim begrip en dient specifieker te worden gemaakt. Gaat het hier om 'significante incidenten'?
	3	9	Er staat hier dat er ruimte is voor een specifieke invulling door sectorale beleidskaders. Naast de minimumharmonisatie en het recht om aanvullende eisen te stellen kunnen er ook nog sectoraal eisen worden opgelegd. ProRail vraagt zich af of dit niet een niet-werkbaar geheel wordt?
	3	9	De NIS 2- en de CER-richtlijn zijn wettelijk kaders voor het versterken van de vitale infrastructuur. Wordt daarmee de Aanpak Vitaal (Spoor) ook opnieuw vormgegeven?
	4	11	Punt 8 en 9 lijken in tegenspraak. Significante incidenten moeten gemeld worden volgens 8 (meldplicht) en er is de mogelijkheid tot vrijwillige melding van significante incidenten in 9. ProRail meent dat bij punt 9 het woord 'significant' dus weggehaald zou moeten worden. Nu wordt er namelijk eigenlijk geïmpliceerd dat significante incidenten ook vrijwillig gemeld kunnen worden terwijl er een verplichting bestaat om significante incidenten te melden (zie artikel 27 lid 1 Cbw).
	5.2.3	18	Betreffende de 2e paragraaf, 4e regel vraagt ProRail zich af wanneer een risico onaanvaardbaar is?
	5.3.2	20	In de laatste alinea staat dat het ook gaat om gebeurtenissen zonder kwade wil met een hele opsomming daarnaast. Het gaat dan ook over menselijke fouten etc. Dit betekent nog al wat voor de te hanteren scope. Hoe moet deze afgebakend worden?
	5.3.3	20	"Wat ook een rol kan spelen bij de evenredigheid van maatregelen, zijn de nadelige effecten of risico's van die maatregelen, zoals de verstoring van de continuïteit van de kritieke processen van een entiteit." Kan ProRail dit opvatten als de vrijheid om de Cbw te scopen tot kritieke processen? Geldt dit ook voor het scopen van de meldplicht?
	5.3.4 (onder g)	21	Wat zijn 'basispraktijken op het gebied van cyberhygiëne'? Gaat dat over awareness? Dat kan, zo meent ProRail, wat specifieker. Daarnaast mist ProRail de classificatie van je assets in de lijst en het hebben van een CMDB (Configuration management database).
	5.3.5	22	Wordt de AMvB onder meer gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO)?
	5.4	23	Er wordt gesproken over 'een training'. Wordt de organisatie helemaal vrijgelaten of worden er iets meer eisen aan een training voor het bestuur gesteld? Komen er nog richtlijnen voor de inhoud van zo'n training? Daarnaast vraagt ProRail zich af of er nog een termijn wordt gegeven voor de aantoonbare 'verversing' van kennis?
	5.5.1	24	Het Ministerie van IenW is de laatste 2 jaar bezig geweest om voor de spoorsector te definieren wat significant is en welke drempelwaarden gehanteerd moeten worden. Hier is nog geen uitsluitsel uitgekomen. ProRail vraagt zich af of deze beoordeling, totdat er uitsluitsel is, voorlopig zal worden overgelaten aan de essentiële en belangrijke entiteiten zelf?
	5.7.8	34	ProRail vraagt zich af op basis van welke grondslag essentiële en belangrijke entiteiten kunnen worden verplicht een door de entiteit begane overtreding openbaar te maken? En wat zijn criteria waaraan moet worden voldaan om iets openbaar te maken?
	5.7.11.2	36	Hier wordt gesproken over het "activeren" van bevoegdheden voor de toezichthoudende instantie. ProRail ziet graag dat gespecificeerd wordt wat voor bevoegdheden dat zijn. Daarnaast wordt gesproken over een "lichte" verplichting. Wanneer is er sprake van een "lichte" verplichting?
	5.7.12	39	ProRail merkt allereerst op dat er hoge boetes opgelegd kunnen worden en vraagt zich daarom ook af aan wie de toezichthoudende instantie de motivering voor een bestuurlijke boete dient te overhandigen en of deze ook wordt getoetst?
	6.2.2.1 (onder CSIRT)	45	Hier staat "betrokkenheid" terwijl waarschijnlijk "betrokkenen" is bedoeld.
	6.2.2.2	45 en 46	De Minister van Justitie en Veiligheid maakt een afweging of het nodig is om persoonsgegevens te bewaren en voor hoelang. ProRail vraagt zich af of deze afwegingen worden geborgd in een verwerkingsregister en of daar ook op wordt toegezien? Het CSIRT staat duidelijk onder toezicht. Dat ziet ProRail niet bij de Minister staan.
	7.2	51	ProRail meent dat er "Kosmisch" zou moeten staan i.p.v. "kosmetisch".

8.1.2	54	De zorgplicht beschrijft dat de risico's voor de beveiliging van de netwerk- en informatiesystemen beheerst moeten worden. ProRail merkt op dat er niets wordt gezegd over tot welk niveau. Is dat een voor de organisatie acceptabel niveau of is daar een standaard voor? Het creëren van volledige bescherming is niet mogelijk (zie laatste alinea 5.3.3) dus bepaalde risico's (restrisico's) zijn dus 'acceptabel'.

Artikelsgewijze toelichting		
Artikel	**Bladzijde**	**Commentaar**
50 en verder	80 en verder	Er wordt gesproken over noodzakelijkheid maar niet over subsidiariteit en proportionaliteit in geval van persoonsgegevens. De AVG geeft aan dat dit in de afweging wel dient te worden meegenomen. Of wordt in deze wet hiervan expliciet afgeweken?
51	81	ProRail vraagt zich af wat een grondslag zou kunnen zijn voor een natuurlijk persoon om de betreffende informatie te mogen opvragen? ProRail stelt voor om hier een voorbeeld van in MvT op te nemen.