Position paper Cybersecurity voor de logistieke sector

Datum 15 januari 2019
Versie 0.85

1 Inleiding

In juni 2017 werd de wereld opgeschud door een ernstige vorm van malware, de NotPetya worm. Een zogenaamde 'worm' schoot bliksemsnel door vele netwerken en waar het hoofddoel van deze malware waarschijnlijk de Oekraïne betrof, trok het wereldwijd een spoor van vernieling. In Nederland zien we ook ernstige gevolgen: in de Rotterdamse haven valt de APM containerterminal, onderdeel van Maersk, stil en een weeklang is er bij APM nauwelijks enig containertransport mogelijk, waarna het geleidelijk aan weer gaat functioneren. In de 10 dagen na de besmetting installeert Maersk zo'n 45.000 pc's opnieuw. Het duurt uiteindelijk enkele weken voordat alles weer naar behoren functioneert en schepen wijken in de tussentijd uit.
De problemen met de Nederlandse vestiging staan niet op zichzelf. De worm blijkt een boekhoudpakket uit de Oekraïne, M.E.Doc, besmet te hebben, dat APM ook gebruikt. Via een upgrade van deze software haalt men zelf de malware naar binnen. Het blijkt een voldoende bruggenhoofd voor de worm en een aanzienlijk deel van het wereldwijde netwerk van Maersk raakt geïnfecteerd. Andere delen worden bij wijze van voorzorg uitgeschakeld. De schade bij Maersk bedraagt enkele honderden miljoenen euro's, zo valt af te leiden uit de jaarcijfers van het bedrijf. Nog maar een bescheiden deel van de wereldwijde schade van enkele tientallen miljarden euro's ten gevolge van NotPetya.

De effecten op de logistieke sector zijn pijnlijk maar ook leerzaam:

- Zoals gezegd legde de infectie met NotPetya de APM-terminal aanvankelijk geheel plat. Deze uitval kon ook niet eenvoudig worden opgevangen. Een partij als ECT was ook niet in een positie om bijvoorbeeld het lossen van containers van binnenvaartschepen over te nemen. Hiervoor ontbraken de juridische en zakelijke voorwaarden, alsmede de benodigde informatie. In die zin staan partijen als APM en ECT op zichzelf en kunnen zij op niemand terugvallen bij dit soort ernstige incidenten.
- Ondanks de enorme gevolgen, zijn de effecten voor de Nederlandse maatschappij als geheel toch nog beperkt te noemen. De Rotterdamse haven ontving in 2017 toch aanzienlijk meer schepen dan in het jaar daarvoor en de burger heeft geen lege schappen in de winkel gezien.

In de nasleep van NotPetya is iedereen uiteraard weer alert en de beveiliging wordt op vele plaatsen aangetrokken. APM terminals is de lust tot de externe elektronische communicatie vergaan, zij kiezen ervoor om nog mondjesmaat met de buitenwereld te communiceren. In de Rotterdamse haven wordt de havenmeester René de Vries benoemd tot Port Cyber Resilience Officer en er wordt geregeld een Port Security Café georganiseerd, waar ervaringen worden uitgewisseld.

Iedereen is weer wakker en geschrokken van de grote gevolgen die cyberaanvallen kunnen hebben en het economisch belang van grote 'hubs' als de Rotterdamse haven is maar weer

eens onderschreven. Is daarmee de kous af, of blijft er toch een nut en noodzaak om meer te regelen? En zo ja, wat zou dat dan moeten zijn? En wat zijn dan de te onderscheiden rollen van de individuele bedrijven, de sector en de overheid? Vragen die we in de rest van dit paper beantwoorden.

2 Position paper

De Topsector Logistiek heeft de opdracht gegeven voor een position paper cybersecurity dat:

- duidelijk maakt wat het belang is van cybersecurity in de logistieke sector;
- beschrijft van de gewenste doelsituatie is, mede in het licht van de op komst zijnde Cybersecuritywet (inmiddels omgedoopt tot de Wet beveiliging netwerk- en informatiesystemen (Wbni)
- beschrijft wat er reeds geregeld is;
- analyseert wat daarvoor moet gebeuren op het niveau van individuele organisaties, samenwerkingsplatforms en de gehele sector,

waarbij het uiteraard van belang is dat wordt voortgebouwd op hetgeen reeds is gerealiseerd in de sector.

3 De uitgangssituatie

In dit position paper is de positie van de logistieke sector verwoord aangaande cybersecurity. Omdat cybersecurity een complex onderwerp is, dat nauwe samenwerking en coördinatie vergt, wordt nadrukkelijk samenloop gezocht met de Nationale Cybersecurity Agenda (NCSA). Ook wordt – waar relevant – aansluiting gezocht bij de Wet beveiliging netwerk- en informatiesystemen (Wbni, informeel ook bekend als de Cybersecuritywet).

Wet beveiliging netwerk- en informatiesystemen (Wbni)
Netwerken en Informatiesystemen zijn cruciaal voor de samenleving en moeten betrouwbaar zijn. Echter bedreigingen liggen op de loer, nemen ook steeds meer toe en de gevolgen zijn steeds groter op zowel nationaal als internationaal niveau, maar ook op economisch en maatschappelijk terrein.
Het juridisch kader waarbinnen de transportsector zich begeeft is zich mede vanwege die continue dreiging zich ten volle aan het ontwikkelen, zowel op nationaal als ook op Europees niveau. Overigens is de transportsector zeker niet uniek, de ontwikkeling van en bescherming tegen cyberdreigingen geldt immers breder in de maatschappij. De Europese Unie is ervan doordrongen dat cyberrisico's vragen om een Europees brede, strategische samenwerking en harmonisatie van de cybersecurity en de Unie vraagt daarom om een minimum beveiligingskader.
De voor de transportsector meest relevante wet is de Wet Beveiliging netwerk en informatiesystemen (verder: Wbni): een samensmelting van de NIB-Richtlijn (2016/1148 6 juli 2016) en de Wet gegevensverwerking en meldplicht cybersecurity (de WGMC). Laatstgenoemden zijn opgegaan in de Wbni (wet van 17 oktober 2018) omdat ze veel overlap vertoonden. Het streven van de Wbni is om meer *cyberweerbaar* te zijn. De Wbni is gepubliceerd in het Staatsblad op 8 november 2018 en inmiddels dus in werking.

De Wbni stelt eisen aan diverse sectoren om voldoende weerbaar te zijn tegen cyberrisico's. De wet bevat wettelijke bepalingen om te bevorderen dat netwerk- en informatiesystemen worden beveiligd. De wet is van toepassing op aanbieders van essentiële diensten en digitale dienstverleners, zoals online zoekmachines, clouddiensten en onlinemarktplaatsen. In het verband van de logistieke sector spreken we van aanbieders van essentiële diensten, niet zozeer over digitale dienstverleners.

De wet regelt onder andere:

- Dat er een Nationaal Cyber Security Incident Response Team aanwezig moet zijn.
  Zij moeten melding maken van een incident, bijstand leveren en opvolging geven om een incident af te kunnen doen. Nederland heeft het Nationaal Cyber Security Centre (NCSC) en draagt zorg voor de internationale samenwerking o.a. op het gebied van risico's.
- Definitie van essentiële dienstverleners en digitale dienstverleners.
  Gas, elektriciteit en zorg zijn bijvoorbeeld sectoren die essentieel zijn voor een samenleving. Immers, als dergelijke diensten niet beschikbaar zijn, ervoor kunnen zorgen dat een land of zo niet landen in verband met de afhankelijkheden van deze sectoren in diverse lidstaten, een samenleving kunnen stil leggen. De logistieke sector wordt ook benoemd. Het is aan de lidstaten zelf om te bepalen welke organisaties in een sector als essentieel worden bestempeld. Dit is dus nationale aangelegenheid.
- Minimumregels t.a.v. risicobeheersing (organisatorisch en technisch);
  Beveiliging geschiedt op basis van risicobeheersing: er is sprake van een gedegen analyse en passende maatregelen worden getroffen.
- Incidentbeheersing (voorkomen en gevolgen beperken);
  Onder andere door het uitwisselen van informatie.
- Omgang met gegevens door betrokken partijen;
- Verplichte en vrijwillige meldplicht.
  Vrijwillige melding beperkt zich tot effecten die mogelijk tot een incident kunnen leiden.
  Een incident voldoet aan norm "heeft substantiële gevolgen": en heeft een substantiële impact op de maatschappij, economie of (inter)nationale betrekkingen. Op basis van vermoedens en/of aanwijzingen mag de toezichthouder ook optreden. Een melding leidt niet tot verhoogde verwijtbaarheid. CSIRT en toezichthouder maken incidenten nooit zelf publiek (inhoudelijke informatie is en blijft vertrouwelijk).
- Bevoegdheden (toezicht, handhaving, sanctionering).
  De verschillende aangewezen sectoren hebben hun eigen toezichthouder waarbij bevoegdheden worden ingeregeld.

Voor de transportsector betekent dit dat het ministerie van IVW logistieke organisaties aan kan wijzen. Aangezien Agentschap Telecom belast is met het toezicht voor de Wbni, krijgt de sector met deze toezichthouder te maken, naast het gebruikelijke toezicht door de Inspectie Leefomgeving en Transport. In het Besluit beveiliging netwerk- en informatiesystemen (30 oktober 2018) is een eerste tranche dienstverleners aangewezen. Voor de logistieke sector betreft dit vooralsnog de 'usual suspects' die we ook uit de vitale infrastructuur kennen, zie de tabel hieronder.

Aangewezen dienstverlener	Essentiële dienst
De Divisie Havenmeester van het Havenbedrijf Rotterdam N.V.	Het afwikkelen van scheepvaartverkeer
Royal Schiphol Group N.V.	Een veilige en vlotte vlucht- en vliegtuigafhandeling voor wat betreft de luchthaven Schiphol
Luchtverkeersleiding Nederland	
Maastricht Upper Area Control Centre (MUAC)	
Aircraft Fuel Supply B.V.	
Koninklijke marechaussee	
elke luchtvaartmaatschappij met minimaal 25% van het totaal aantal vliegbewegingen op Schiphol in een kalenderjaar	

Het is aannemelijk dat in volgende tranches deze lijst nog wordt uitgebreid. Er zijn immers beduidend meer organisaties in de logistieke sector die een dusdanig belangrijke rol vervullen, dat we een goede cybersecurity bij die organisaties willen borgen.

Nationale Cybersecurity Agenda (NCSA)
Veiligheid in het digitale domein is voor het kabinet een topprioriteit. Daarom is in het regeerakkoord een structurele investering van 95 miljoen euro in cybersecurity vastgelegd. In dit jaar is door verschillende departementen, in nauwe samenwerking met partijen uit de publieke én private sector, de wetenschap en de samenleving, hard gewerkt aan een ambitieuze kabinetsbrede Nederlandse Cybersecurity Agenda (NCSA). Aansluiting bij de doelstellingen van deze agenda lijken voor de hand te liggen. Het ministerie van IenW is betrokken bij de NCSA. Het coördinerend ministerie is JenV.

De NCSA valt uiteen in zeven ambities die bijdragen aan de volgende doelstelling: Nederland is in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren en de nationale veiligheid in het digitale domein te beschermen.

1. Nederland heeft zijn digitale slagkracht op orde.
2. Nederland draagt bij aan internationale vrede en veiligheid in het digitale domein.
3. Nederland loopt voorop in het bevorderen van digitaal veilige hard- en software.
4. Nederland beschikt over weerbare digitale processen en een robuuste infrastructuur.
5. Nederland werpt door middel van cybersecurity succesvol barrières op tegen cybercrime.
6. Nederland is toonaangevend op het gebied van cybersecurity kennisontwikkeling.
7. Nederland beschikt over een integrale, publiek-private aanpak van cybersecurity.

Ambities 4 en 7 hiervan zijn met name relevant voor de logistieke sector.

Toenemende 'informatiegraad' in logistieke processen en dus afhankelijkheid van ICT
Al jarenlang is het een trend dat de informatisering in de logistieke processen toeneemt. Als partijen in een keten meer kennis hebben over de komst van een te vervoeren eenheid, maakt dit optimalisatie van logistieke processen mogelijk. Een voorbeeld is dat als een

containerterminal beter weet hoe de volgende vervoersstap van een container er uit ziet, is de ordening van de containerstacks te optimaliseren.
Een ontwikkeling die bij uitstek veel gegevens met een hoge actualiteit vraagt is *synchromodaal* transport. Een actueel beeld over ladingaanbod en vervoeraanbod is hiervoor essentieel.

Naast de logistieke besturing zelf, is er ook de geautomatiseerde afhandeling van vracht, met name containers. Hiermee wordt een grote efficiency behaald met behulp van de inzet van veel informatietechniek.

Het moge duidelijk zijn dat dit met soort ontwikkelingen de logistieke processen geoptimaliseerd kunnen worden. De keerzijde is echter dat de afhankelijkheid van een goed functionerende ICT groeit. Dit tot het punt dat de logistieke processen in hoge mate of geheel stagneren bij uitval van de ICT. Cyberaanvallen zijn daarin een serieus risico waarmee de individuele partijen in de sector maar ook de sector als zodanig, rekening moeten houden.

4 Het wenkend perspectief

Wat zou de sector moeten willen bereiken als het gaat om cybersecurity? Wat is het wenkend perspectief?

Een voorzet:

1. Logistieke dienstverleners kunnen de ‘bekende’ cyberdreigingen herkennen, detecteren en tegenhouden. Waar een cyberdreiging de preventieve beveiliging omzeild heeft, zijn er detectie- en herstelmaatregelen aanwezig, zodat de uiteindelijke schade wordt beperkt.
2. Logistieke dienstverleners maken gebruik van een sectoraal computersecurityteam om op de hoogte te zijn van actuele cyberdreigingen of -aanvallen en om slagvaardig te kunnen reageren als er actuele aanvallen zijn en er IT-systemen zijn gecompromitteerd.
3. Logistieke dienstverleners hebben voor hun eigen dienstverlening de business continuity geborgd. Daardoor weten ze, weliswaar met gereduceerde capaciteit, toch hun dienstverlening in stand te houden als er zich een cyberaanval voordoet. De gereduceerde capaciteit wordt daarbij aangewend voor die goederenstromen die slechts geringe vertraging kunnen verdragen en die maatschappelijk meer dan gemiddeld relevant zijn. Denk dan aan het in standhouden van het vervoer zelf, voedselvoorziening enzovoort.
4. De logistieke sector is in staat om de aanwezige redundantie en capaciteit in de sector flexibel aan te wenden. In het geval van een cyberaanval is het zodoende mogelijk om goederenstromen op alternatieve wijze af te handelen, mogelijk buiten de getroffen logistieke dienstverleners om.

5 De positie van de topsector logistiek over cybersecurity

De positie van de sector is hieronder puntsgewijs weergegeven. Per punt is een onderbouwing en toelichting toegevoegd.

1. Het belang van een goede cybersecurity in de logistieke sector is hoog. Verbetering van de cybersecurity is wenselijk.
Cybersecurity is een onderwerp, waar in de logistieke sector vrij weinig aandacht voor is geweest tot het genoemde incident bij APM. Het is geen geheim dat cybersecurity voor de meeste bedrijven in deze sector niet heel hoog op de agenda staat en dat het ook niet erg goed geregeld is. Transport en Logistiek Nederland (TLN) roept al jaren op tot verbeteringen. De recent benoemde Port Cyber Resilience Officer (Port CRO) van de Rotterdamse haven, René de Vries, beaamt dit beeld.

De sector kent wel enkele grotere logistieke partijen en op informatieuitwisseling gespecialiseerde partijen zoals Portbase. Deze partijen lijken hun zaken beter op orde te hebben. Ook zien we dat er rondom initiatieven als Single Maritime Window wel degelijk de nodige aandacht is voor informatiebeveliging en business continuity management, met name op het niveau van aanbeveling aan de individuele organisaties. Tevens is er een aantal verplichte technische maatregelen voor gemeenschappelijke ICT-voorzieningen. Denk aan de systemen van Portbase en de berichtenuitwisseling via DigiPoort. Als op eerdere rapportages en signalen kan worden afgegaan, is het sectorbreed echter minder goed gesteld met de 'cyber-readiness'.

Dit dient te verbeteren. Anders kan een grote cyberaanval tot gevolg hebben dat veel bedrijven in de sector tegelijkertijd worden geraakt, met mogelijk sectorbrede gevolgen, of grote gevolgen voor vitale knooppunten als de Rotterdamse haven of Schiphol. Dit omdat de keten uiteindelijk zo sterk is als de zwakste schakel. Een Portbase kan dan haar informatiebeveiliging wel goed geregeld hebben, als dat voor de aangesloten dienstverleners niet geldt, dan hebben we nog niets bereikt. We dienen ook te beseffen dat de tik die APM terminals kreeg van NotPetya eigenlijk in de categorie 'collateral damage' viel van een cyberwapen dat primair op de Oekraïne gericht was. Stel dat een cyberaanval direct gericht zou worden op Nederland of de logistieke sector in Nederland, dan zouden de effecten veel groter zijn.

Het economisch belang springt daarbij uiteraard onmiddellijk in het oog, maar ook het belang voor de voedselvoorziening maakt een bepaald minimumniveau van continuïteit van logistieke diensten dient te worden geborgd.[1] Bovendien is het – naast het objectieve belang van de sector - ook belangrijk voor het imago van de logistieke topsector om ook de cybersecurity goed geregeld te hebben. Samenvattend: *noblesse oblige*.

[1] Overigens lijkt de overheid tot op heden een halfslachtig standpunt te hebben ingenomen over de mate waarin logistieke dienstverlening een 'vitaal' karakter heeft. Enerzijds staat de logistieke sector niet op de A-lijst van vitaal, maar kennen de haven en luchthaven wel hun ISAC (zie https://www.ncsc.nl/samenwerking/isacs). Ook is de logistieke dienstverlening wel degelijk als 'essentieel' gekenmerkt in het wetsvoorstel voor de Wet beveiliging netwerk- en informatiesystemen (Wbni), de implementatie van EU Richtlijn 2016/1148 (de zogenaamde NIB-richtlijn). Het is dus wel veilig om te veronderstellen dat de overheid wel degelijk doordrongen is van het belang van een 'veilige logistieke sector'.

Verbetering is aan de orde op de volgende punten:

1. Bescherming (preventie/detectie/correctie) tegen cybersecurity incidenten van individuele logistieke dienstverleners, alsmede borging van business continuity van individuele logistieke dienstverleners.
2. Verhogen van de business continuity van de sector op een niveau, dat de individuele logistieke dienstverleners ontstijgt. Zo zagen we dat bij het in de inleiding genoemde incident met NotPetya dat de afhandeling van containervracht van APM niet eenvoudig was over te nemen door het naastgelegen ECT. De aanwezige redundantie in de sector kon dus niet worden benut!
3. Het ondervangen van sectorbrede afhankelijkheden van andere infrastructuur of diensten. Met name dient te worden gedacht aan de sectorbrede afhankelijkheid van de brandstofvoorziening.

Punt 3 van bovengenoemd lijstje valt buiten het handelingsperspectief van de logistieke sector zelf. Dit dient te worden geborgd in nationale overleggen voor de bescherming van vitale infrastructuur.
Op punten 1 en 2 zijn hieronder aanbevelingen in meer detail gedaan.

2. Individuele logistieke dienstverleners moeten zich aan gangbare standaarden voor informatiebeveiliging, cybersecurity en business continuity management conformeren. Dit is de 'basis'.

De primaire verantwoordelijkheid dat de ICT-systemen bestand zijn tegen cyberincidenten c.q. -aanvallen, ligt bij de individuele bedrijven in de logistieke sector.

Hiervoor zouden bedrijven zich aan gangbare standaarden en praktijken moeten gaan conformeren. Daarbij kan worden gedacht aan het hanteren van een managementsysteem voor informatiebeveiliging (ISMS) en eventueel het hanteren van sectorale standaarden. Tevens dient te worden gedacht aan standaarden voor business continuity management, zodat een organisatie – binnen de grenzen van haar eigen mogelijkheden – capabel is om zich voordoende crisissituaties het hoofd te bieden.

Gangbare standaarden zijn bijvoorbeeld de ISO 27001 (information security management system) en de ISO 22301 (business continuity management). Aanvullend kan worden gedacht aan elementen van het NIST Cyber Security Framework en/of de ISO 27032.

Daarnaast is er specifieke aandacht nodig voor het voorkomen en behandelen van specifiek cyberaanvallen (anders dan algemene informatiebeveiliging). In lijn met de bovengenoemde standaarden dienen de maatregelen gebaseerd te worden op een risicoanalyse. In deze analyse dient men zich vooral af te vragen hoe de informatievoorziening op een zodanig niveau gehouden kan worden, zodat de logistieke dienstverlening op de een of andere wijze in stand kan worden gehouden.

Bij het samenstellen van een pakket van maatregelen tegen cyberaanvallen dient men zich te realiseren dat het om verdediging in meerdere lagen gaat. Met alleen preventieve maatregelen komen we er nadrukkelijk niet. Er zijn bijvoorbeeld ook aanvallen die gebruik maken van nog niet bekende lekken in gebruikte systemen of protocollen (de zogenaamde

‘zero day’ aanvallen.) Het is dus van belang om een gebalanceerd pakket te hebben met maatregelen voor:

- Preventie.
- Beperking van effecten.
- Detectie van incidenten en tegenhouden of indammen.
- Opvangen van de resulterende verstoring.
- Terugkeer naar de normale situatie.
- Herstel van de schade (voor zover mogelijk).

Zonder volledig te willen zijn, kan dan concreet worden gedacht aan maatregelen als:

- Een adequate beveiliging van de grens van de ICT-infrastructuur van de individuele organisatie, de zogenaamde perimeterbeveiliging;
- Interne netwerksegmentering (microsegmentering) die eventuele cyberaanvallen tegenhouden of vertragen;
- Gebruik van bewakingsdiensten tegen cyberincidenten, eventueel aan te sluiten op bredere ‘waarschuwingsnetwerken’, die een tijdige reactie tegen cyberaanvallen mogelijk maken.
- Een tijdige en sluitende systematiek van updates / patches. Vaak blijkt dit lastig in verband met allerlei beperkende voorwaarden die verouderde software stelt. Dit leidt niet zelden tot minder goed patch-management. Hiervoor zijn compenserende maatregelen gewenst en tevens dient er alerter door betrokken management te worden opgetreden tegen dergelijke omstandigheden.
- Het ‘hardenen’ van de kritische computersystemen.
- Uitwijk en noodprocedures.

3. Het conformeren aan gangbare standaarden door individuele logistieke dienstverleners dient te worden bewaakt en gefaciliteerd.

Het voldoen aan bovenstaande standaarden en het zodoende borgen van een goede bescherming tegen cybersecurity-aanvallen is zeker nog niet eenvoudig. Veel vervoerders en logistieke dienstverleners zullen daarbij moeten worden geholpen. In de eerste plaats om hun eigen zaken op orde te brengen c.q. te houden. Hier ligt een nuttige taak voor een nader te bepalen koepelorganisatie. Mogelijke manieren waarop logistieke organisaties gefaciliteerd kunnen worden zijn:

1. Een eenduidige interpretatie en ‘meetlat’ voor de sector.
   Gangbare standaarden zijn bijvoorbeeld de ISO 27001 (information security management system) en de ISO 22301 (business continuity management). Aanvullend kan worden gedacht aan elementen van het NIST Cyber Security Framework. Het is allereerst nuttig en zinvol als hiervoor een eenduidige interpretatie en meetlat voor de sector beschikbaar komt. Daarbij is het van belang dat de sector een gedeelde perceptie heeft van de ‘kroonjuwelen’ die nodig zijn voor een goede logistieke dienstverlening en de dreigingen waartegen bescherming gewenst is.
   Bedrijven die audits of onafhankelijke beoordelingen op cybersecurity uitvoeren, dienen bekwaam te zijn het hanteren van deze interpretatie en meetlat.

Vervolgens laten organisaties zich ‘meten’ tegen de afgesproken meetlat en uitkomsten te delen.

2. Organiseren van kwaliteitskringen.
   Communities van (gelijksoortige) logistieke bedrijven bespreken hun scores tegenover de gemeenschappelijke meetlat, knelpunten en ‘best practices’ om op bepaalde aspecten van de meetlat beter te kunnen scoren.
3. Gemeenschappelijke diensten, om de operationele cybersecurity op een hoog niveau te handhaven. Gedacht kan worden aan:
   a. Implementatieondersteuning.
      Op zich is er voldoende commercieel aanbod aan implementatieondersteuning, om het security-management in een organisatie op voldoende niveau te krijgen. Er kunnen echter overwegingen zijn om op dit gebied toch specifiek iets voor de sector te organiseren. Dan kan bijvoorbeeld gedacht worden aan de bundeling van relevante sectorale kennis. Ook kan worden gedacht aan het bundelen van voldoende uitvoerende capaciteit, aangezien er op het uitvoerende niveau wel degelijk schaarste is.
   b. Een gemeenschappelijke sectorale CERT.
      Voor onder de Wbni aangewezen essentiële dienstverleners (AED’s) is het NCSC de wettelijk bepaalde CSIRT. Het staat sectoren uiteraard vrij om hun eigen sectorale computersecurityteams of CERT’s op te richten, die breder werken dan uitsluitend de aangewezen essentiële dienstverleners. Anders dan bij implementatieondersteuning gaat het hierbij om het informeren over dreigingen en het ondersteunen van aangesloten partijen in het afhandelen van security incidenten. Een CERT werkt dus voor een bepaalde doelgroep en in die zin is het oprichten van een sectorale CERT een logische stap. Andere sectoren als de zorg hebben ook gekozen voor een dergelijke stap.
   c. Operationele netwerk-/IT-infrabeveiliging.
      Denk hierbij aan diensten om de netwerkverbindingen goed te beveiligen (managed firewall diensten) en aan dienstverlening die beschermt tegen actuele cyberdreigingen zoals computersecurityteams. Ook veilige applicatiehosting kan een nuttige operationele dienst zijn.
      Ook hiervoor is het nodige aanbod aan commerciële dienstverlening. Dit is echter normaliter alleen haalbaar voor grotere bedrijven.

Het is goed om te starten met punten 1, 2 en van punt 3 de sectorale CERT. Als er tekenen zijn dat bedrijven daadwerkelijk ondersteuning wensen in de operationele IT, dan zou een behoeftepeiling nuttig zijn.

Hiernaast is het wenselijk om op sectoraal niveau inzicht te krijgen hoe het is gesteld met de ‘cyber-readiness’ van de sector. Hier is het aan te bevelen om een zogenaamde *monitor* in te richten om de naleving van genoemde gangbare standaarden in kaart te brengen en te kunnen volgen door de tijd heen.

4. Vrijwillig kan, vrijblijvend niet. Sectorale afspraken maken en bewaken. Wetgeving als stok achter de deur.

Het is eenvoudig om te stellen dat de logistieke sector haar cybersecurity dient te verbeteren en hiervoor zich aan gangbare standaarden dient te conformeren. Naast gebrek aan kennis en kunde in de sector, waarvoor een faciliterende insteek (aanbeveling 3) goed kan helpen, speelt echter ook dat de logistieke sector een zeer concurrerende sector is. Partijen staan klaar om elk kostenvoordeel uit te buiten. De notie dat cybersecurity iets is, waarop men niet zou moeten willen concurreren, is in de sector nog niet algemeen geaccepteerd.

Een vrijwillige implementatie van gangbare standaarden tegen cyberincidenten kan dus leiden tot eenzijdig kostennadeel bij die partijen die op dit gebied vooroplopen. Kosten voor state-of-the-art informatiebeveiliging lopen tegenwoordig op tot circa 10% van het ICT budget. Kostennadelen van deze ordegrootte kunnen weer een remmende factor vormen voor vorderingen in de cybersecurity. Het aansluiten van logistieke partijen bij vrijwillige afsprakenstelsels zou dan een factor kunnen zijn, die ervoor zorgt dat er een 'level playing field' blijft. Het delen van gegevens gaat dan samen met het verplicht goed regelen van de beveiliging tegen cyberincidenten. Het is te overwegen om het voldoen aan gangbare standaarden voor cybersecurity op te nemen in het iSHARE afsprakenstelsel.

Dit zou wel geborgd kunnen worden door de overheid, met name door mogelijke wettelijke aanwijzingen 'achter de hand' te houden en intussen marktpartijen te stimuleren om vrijwillige verbeteringen sectorbreed op te pakken. Hiertoe zouden de vorderingen in de sector inzichtelijk dienen te worden gemaakt, middels een 'monitor'.

De wetgeving waarbinnen de overheid eventueel een aanwijzing zou kunnen realiseren is de de nieuwe Cybersecurity wet, of exacter de Wet beveiliging netwerk- en informatiesystemen (Wbni). In eerste instantie zijn slechts enkele zeer grote logistieke knooppunten aangewezen, maar het staat de wetgever vrij om meer partijen aan een wettelijk kader te onderwerpen.

Overigens is het niet goed mogelijk dat ook de vele kleine logistieke dienstverleners onder dit wettelijk regime aangewezen worden. Immers, de gedachte achter deze wetgeving is dat verleners van essentiële diensten kunnen worden aangewezen en dat is voor de vele kleine partijen niet aan de orde. Daarmee zal er voor de kleinere logistieke partijen dus veeleer op basis van vrijwillige afspraken gewerkt moeten worden. Het verdient dus de voorkeur om sectorale afspraken te maken, waarbij de mogelijkheid van dwingende wetgeving als 'stok achter de deur' functioneert. Die 'stok achter de deur' kan nuttig zijn, om aarzelingen te overwinnen die er op grond van 'level playing field' overwegingen ongetwijfeld zullen zijn.

Bovenstaande definieert dus ook de gewenste opstelling van de overheid in deze. De overheid dient de logistieke sector aan te sporen en zij volgt de vorderingen van de sector op dit punt, mede op basis van eerdergenoemde monitor. De overheid houdt de mogelijkheid van dwingende wetgeving achter de hand, mocht dit niet leiden tot voldoende resultaat.
De overheid kan bovendien de sector stimuleren om op sectoraal niveau de verbetering te faciliteren, bijvoorbeeld door een gemeenschappelijk verbeterprogramma te financieren.

5. Aanvullende maatregelen zijn nodig op sectoraal niveau, zodat de logistieke sector blijft functioneren, ook als individuele partijen problemen hebben.
Waar het over het *belang* en het *vitale karakter* van de logistieke sector weinig discussie zal bestaan, zijn er wel wisselende beelden op te tekenen waar het gaat om de *kwetsbaarheid* van de sector.

Enerzijds is de logistieke sector daadwerkelijk zeer breed vertakt, met heel veel verschillende bedrijven. De ingebouwde redundantie is derhalve groot. Dat leidt al snel tot het beeld dat de kwetsbaarheid op het niveau van de sector beperkt is.
Daarmee is de eerste prioriteit om de continuïteit te borgen voor een aantal grote logistieke knooppunten. Naast de haven van Rotterdam en Schiphol komen wellicht ook andere logistieke centra in aanmerking.

Toch is het onze stelling dat dit een vertekend beeld geeft van de situatie om de volgende redenen:

- Logistieke diensten gaan steeds meer samen met geavanceerde informatiediensten. Elke logistieke verbetering - gericht op efficiency of kwaliteit - is tegenwoordig gebaseerd op het delen van data tussen en met ketenpartners. De afhankelijkheid van goed werkende IT is gegroeid en blijft groeien. Moderne logistieke concepten zoals synchromodaal transport zijn zelfs geheel ondenkbaar zonder snelle en accurate informatievoorziening.
- Omschakelen van goederenstromen naar andere – niet getroffen - logistieke dienstverleners is niet triviaal door het ontbreken van de juiste informatie en afspraken;
- Een grootschalige cybersecurity-aanval heeft het potentieel om een aanzienlijk aantal partijen in de sector te raken. Herstel van een dergelijke aanval kan tot enkele weken vergen, waarbij een relatief groot deel van de sector buiten bedrijf is.

In dit verband zou het raadzaam zijn als met name de grote logistieke spelers in de scope van hun maatregelen voor business continuity management ook samenwerkingen buiten hun eigen organisatie - mogelijk ook met hun concurrenten - in overweging zouden gaan nemen.
Gedacht zou bijvoorbeeld kunnen worden aan afspraken en informatie die het mogelijk maken voor andere logistieke dienstverleners om de meer essentiële logistieke diensten over te nemen bij grootschalige cyberincidenten. Denk bijvoorbeeld aan bevoorrading met brandstoffen en voedsel, en niet zozeer een aanzienlijke vertraging van duurzame gebruiksgoederen. Dergelijke afspraken hebben alleen kans van slagen als er daadwerkelijk een groter belang is dan het commercieel belang van de individuele logistieke organisaties!

Momenteel zijn zelfs verkenningen op sectoraal niveau ternauwernood mogelijk gegeven de concurrentieverhoudingen en gegeven het scherpe optreden van ACM c.q. angst voor dergelijk optreden. Het is wenselijk dat de overheid op dit punt helderheid verschaft, wat voor samenwerking op dit punt mogelijk is.

6. Sectorbrede voorzieningen zijn nodig. Verbeterprogramma. Publiek Private Samenwerking.

Het is gewenst om op sectorniveau een aantal voorzieningen te treffen, waarvoor een programmaorganisatie zou kunnen worden ingericht, welke publiek/privaat wordt gefinancierd en bemenst. In dit programma zouden tenminste de reeds geïdentificeerde sectorbrede zaken moeten worden opgepakt:

1. Een sectorale standaard c.q. implementatierichtlijn voor information security management, in aanvulling op algemene standaarden als ISO 27001 / 27002. Dit dient te worden geborgd in sectorale afspraken.
2. Een sectorale standaard voor de invulling van business continuity management, zulks waarschijnlijk te baseren op de gangbare standaard als ISO 22301. Dit dient te worden geborgd in sectorale afspraken.
3. Een sectorale standaard voor de invulling van specifieke maatregelen voor cybersecurity. Mogelijk te baseren op het NIST Cybersecurity Framework, ISO 27032 en/of specifieke NCSC richtlijnen. Dit dient te worden geborgd in sectorale afspraken.
4. Een monitor om de naleving van bovenstaande standaarden / afspraken te kunnen volgen.
5. De oprichting van een sectorale CERT, met de bredere doelgroep van logistieke dienstenverleners. Dit gaat dus om veel meer partijen dan alleen de onder de Wbni aangewezen logistieke partijen.

Daarnaast dient dit programma zich ook in te zetten om business continuity te verbeteren op het sectoraal niveau of tenminste een niveau dat de individuele logistieke dienstverlener overstijgt. Daarbij dient te worden onderzocht hoe de redundantie in de logistieke sector ook eenvoudig kan worden geoperationaliseerd, indien er zich een cyberincident voordoet:

- Welke logistieke diensten kunnen onder welke omstandigheden door andere partijen (normaliter concurrenten) worden overgenomen en voor welke logistieke diensten is dit ook belangrijk?
- Wat voor zakelijke afspraken zijn daarvoor nodig?
- Welke informatie dient hiervoor al aanwezig te zijn buiten de getroffen organisatie, opdat de diensten ook daadwerkelijk kunnen worden overgenomen?
- Wat voor soort informatiesysteem zou hiervoor dienen te worden ingericht en is hiervoor een (maatschappelijke) business case aanwezig?

Een tweede door het programma te onderzoeken punt is in welke mate de sector kwetsbaar is voor een grootschalige cybersecurity incident, dat een groot aantal partijen in de sector treft. Men kan daarbij denken aan incidenten als een ‘zero day’ aanval, waarbij een nog onbekende IT-kwetsbaarheid wordt uitgebuit. En wat in die situatie het handelingsperspectief is.

Ten slotte zou het programma ook de behoefte in kaart moeten brengen aan operationele ICT-diensten ter bevordering van de cybersecurity. Indien er voldoende animo bestaat voor dergelijke ICT-diensten, anders dan het reguliere marktaanbod, dan kan worden overwogen hiervoor sectorbrede ICT-dienstverlening te gaan organiseren of bepaald aanbod te certificeren.