Verslag Security Seminar

Datum: dinsdag 23 september 2014

Op 23 september is bij NEN het Security Seminar gehouden als onderdeel van de stakeholderanalyse voor een op te richten Normcommissie Security. Deze commissie zal het werk van ISO/TC 292 en CEN/TC 391 volgen en mogelijk op een van de volgende domeinen ook eigen initiatieven ontwikkelen:

- Security management
- Security diensten
- Bedrijf continuïteit management
- Crisis management
- Bescherming vitale infrastructuren
- Supply chain security en supply chain continuïteit management
- Bestrijding van fraude en vervalsingen
- Preparatie op industriële incidenten / CBRNe-veiligheid

Allereerst werd door Jolien van Zetten namens NEN een introductie gegeven in het werk van ISO/TC 292 en CEN/TC 391, de mogelijke inbreng daarbij vanuit Nederland en de rol van NEN en in de organisatie en financiering van normalisatie (zie de bijgevoegde presentatie). Vervolgens zijn door aanwezigen een aantal vragen gesteld en opmerkingen gemaakt.
Zie hiervoor de bijlage onder Plenaire discussie.

Daarna volgde een bevlogen presentatie van Eduard Emde namens ASIS International. Zijn persoonlijk betoog gaf antwoord op de vraag: “Waarom doen we het?”
Met sprekende voorbeelden uit de praktijk illustreerde Eduard hoe normen bijdragen aan efficiënte, beheersbare, veilige en verantwoorde ‘security diensten’. Hiermee gaf hij een stimulerend en motiverend pleidooi voor normalisatie in het domein van Security, Business Continuity en Veiligheid.

In drie Break-out sessies hebben de deelnemers zich over verschillende kansen voor normalisatie uitgesproken. Hieronder volgt de korte terugkoppeling van de moderatoren van die sessies. Zie de bijlage onder Break-out sessies voor meer details.

Break-out sessie Security

Ronald Boon, NEN geeft een korte terugkoppeling van de sessie over Security:

- veel draagvlak voor een norm voor het Security Management proces, waarin o.a. de aanpak van een dreigingsanalyse, risicoanalyse, fysieke aspecten, cyber aspecten en de mens centraal staan;
- ook belangstelling voor een norm voor kwaliteit van Security Professionals (met name het hogere kader);
- belangstelling voor een norm voor schaalbaarheid van security (ook voor MKB).

Break-out sessie BCM, Vitaal en Supply Chain Security

Dick Hortensius, NEN geeft een korte terugkoppeling over de sessie BCM, Vitaal en Supply Chain Security. Er is geconstateerd dat er al veel gebeurt en beschikbaar is. De volgende aandachtsgebieden en – punten worden belangrijk gevonden:

- de samenhang tussen preventie beschermingsmaatregelen en de CM en BCM maatregelen;
- overzicht van de vele normen (en hun onderlinge relatie en samenhang) die in dit veld een rol kunnen spelen;
- de samenhang tussen BCM en Cyber Security en informatiebeveiliging;
- de beveiliging en beschikbaarheid/continuïteit van dataverkeer;
- management van supply chain security en de integriteit van containers.

Break-out sessie CBRNe en CM

Marc Ritter, NEN geeft een terugkoppeling van de sessie over CBRNe en CM:

- men heeft behoefte aan overzicht van beschikbare normen over de hele keten heen;
- er is draagvlak voor het opstellen van een norm voor CM en CBRNe voor bedrijven die niet aan BRZO eisen hoeven te voldoen;
- men vraagt aandacht voor nationale, Europese en internationale normen;
- het voorstel wordt gedaan voor een NC met onderliggende werkgroepen.

Daarna geeft Jolien van Zetten aan hoe nu verder:
- belangstellingsformulier invullen,
- oprichtingsbijeenkomst NC Security donderdag 27 november in de middag.

Het Security Seminar werd door Jeannette Hoffman als dagvoorzitter, begeleid en onder dankzegging voor de komst van bijna 80 deelnemers memoreerde zij nog kort, dat:

- het seminar onderstreepte dat Security mogelijkheden biedt voor nieuwe norminitiatieven;
- deze middag vele suggesties en haalbare mogelijkheden voor nieuwe normen zijn geïnventariseerd;
- het een levendige en enthousiasmerende bijeenkomst was geweest met veel mogelijkheden tot netwerken.

Oprichtingsbijeenkomst Normcommissie Security

Het Security Seminar heeft aangetoond dat er veel belangstelling bestaat voor het deelnemen aan, volgen van en bijdragen aan Europese en internationale normalisatiewerk en voor nieuwe initiatieven voor veiligheidsvraagstukken.

Afgesproken is dat op donderdag 27 november om 13.00 uur bij NEN de oprichting van de Normcommissie Security zal plaatsvinden. Een uitnodiging en agenda zullen worden toegestuurd.

hierna worden enkele kansrijke norminitiatieven beschreven die het Security Seminar (inclusief de gesprekken voor tijdens en na het seminar en de ingevulde belangstellingsformulieren) heeft opgeleverd.

1. Organisatie van beveiliging

Probleem: Voor veel organisaties is het onduidelijk hoe je de security functie in de organisatie het best kunt organiseren. Welke processen komen daarbij kijken, welke afdelingen en functionarissen zijn daarbij betrokken en hoe pak je het allemaal aan. Ook zijn er spraak verschillen, jargon en uiteenlopende beveiligingsconcepten.

Voorstel: Een norm met (Nederlandse) termen en definities, een schets van het werkveld (security, BCM, CM, de veiligheidsketen etc.), en een beschrijving van het 'security proces' op hoofdlijnen (belangen analyse, dreigingsanalyse, kwetsbaarheidsanalyse, risicoweging, maatregelen selectie, kosten-baten afweging, total cost of ownership e.d.). Deze norm moet voor iedereen te begrijpen zijn en van toepassing zijn op kleine en grote organisaties.

Motivatie: Dit moet als eerste worden opgepakt omdat dit helderheid schept en kaders geeft voor vervolg trajecten. Ook is een groot aantal partijen hierin geïnteresseerd.

Belanghebbenden: Alle bedrijven, NGO's, overheden etc.

2. Beveiliging als onderdeel van aanbestedingen

Aanbestedingen gaan vaak om grote investeringen en zetten het fundament voor toekomstige bedrijvigheid en ontwikkelingen. Het is belangrijk om aanbestedingen zo 'slim' mogelijk te doen. Opgeleverde diensten en producten laten zich doorgaans slechts tegen hoge kosten later aan veranderende wensen of nieuwe inzichten aanpassen. Ook security wensen zijn later slechts tegen hoge kosten te realiseren. Het is dus belangrijk dat ook in aanbestedingsprocedures het aspect security (beveiliging: fysiek, organisatorisch, elektrisch, cyber, personeel etc.) eenduidig, transparant en liefst meetbaar wordt uitgevraagd.

Voorstel: Een norm voor het inpassen van security-aspecten in bestande aanbestedings-procedures. De norm moet de aanbestedende organisatie ondersteunen in het formuleren van de eisen die voor verschillende security-aspecten relevant zijn. Bovendien moet de norm handvatten bieden voor het beoordelen en vergelijken van opgestelde offertes. De aanbiedende partijen vinden in de norm dus ook houvast voor het opstellen van concurrerende offertes. De norm kan eisen stellen aan het op te leveren product en dienst, aan het wordingsproces, aan de betrokken partijen/functionarissen en aan het offerte proces.

Motivatie: Bij de aanbesteding van producten en diensten laat security zich nog tegen relatief lage kosten 'inbakken'. Bovendien zou deze norm werkgelegenheid voor de security-sector kunnen bevorderen. Ook kan de kwaliteit van producten en diensten hiermee aanzienlijk worden verbeterd. Het is een gemiste kans als we dit niet snel zouden oppakken.

Belanghebbenden: Rijksvastgoedbedrijf, ingenieursbureaus, architecten, security branche

3. Operationele Cyber Security:

Cyber dreigingen en incidenten zijn dagelijks in het nieuws. Steeds meer organisaties maken werk van cyber security. Het aantal cyber-experts neemt gestaag toe. Voor functionarissen in andere disciplines (anders dan IT/Cyber) is het ingewikkeld om te doorgronden wat van hen of hun organisatieonderdeel hierin wordt verwacht. Welke impact kan cyber crime op hun bedrijfsprocessen hebben. Wat zijn mogelijke te nemen maatregelen? Deze materie wordt extra complex door het eigen jargon en zware technische component waarmee de cyber-experts dagelijks werken. Daarbij worden steeds meer processen en diensten in organisaties door cyber systemen ondersteund. Ook de 'security' sector is niet meer vrij van cyber dreigingen.

Voorstel: Een norm met relevante termen en definities over cyber security, een schets van het cyber security werkveld, een beschrijving van het 'cyber security proces' op hoofdlijnen (daar waar die afwijkt van de eerdergenoemde Security Management norm). Deze norm moet voor iedereen te begrijpen zijn en van toepassing zijn op kleine en grote organisaties.

Motivatie: Deze norm kan alle functionarissen in een organisatie helpen cyber security in relatie tot het eigen functioneren en het eigen bedrijfsonderdeel te begrijpen. De norm zal handvatten bieden om de eigen cyber security wensen onder woorden te brengen. Deze norm zal de brug slaan tussen ons allen en de cyber-experts.

Belanghebbenden: Alle bedrijven, NGO's, overheden etc.

4. Antecedentenonderzoek

Veel organisaties hebben geïnfesteerd in kwalitatief hoogwaardig personeel, in veilige en beveiligde werkomgeving of in het verantwoord omgaan met kwetsbare informatie, materiaal of cliënten. Bij het aannemen van nieuw personeel ontstaat het risico dat een 'rotte appel' deze gekoesterde belangen zal schaden. Hoe kan een organisatie nu voorkomen dat een charlatan, bedrieger, crimineel, fraudeur of pedoseksueel in die veilige en wellicht kwetsbare omgeving wordt toegelaten? Hoe weet je wat voor vlees je in de kuip hebt.

Voorstel: Een norm die aangeeft hoe een antecedentenonderzoek of 'pre-employment screening' moet worden uitgevoerd, welke opties mogelijk zijn (binnen de Nederlandse wet- en regelgeving) en hoe de kwaliteit van dat onderzoek kan worden geborgd.

Motivatie: Deze norm kan bijdragen aan een afname van het aantal incidenten met 'insiders'. Bovendien zal de acceptatie van antecedentenonderzoek kunnen worden vergroot en de kwaliteit van dergelijke onderzoeken worden verbeterd.

Belanghebbenden: Alle bedrijven, NGO's, verenigingen, overheden etc.

5. Beveiliging van de cash in retail

Geld en waardepapieren zijn aantrekkelijke doelen voor criminelen. Maar ook eigen medewerkers kunnen soms de verleiding niet weerstaan als deze niet goed beveiligd zijn. Vanaf kassa tot aan de waarde transporteur zijn verschillende situaties die kwetsbaar zijn voor verduistering, diefstal en beroving. Wat zijn in de retail goede werkwijzen om deze cash te beveiligen en wat voor eisen moet aan het waardetransport gesteld worden.

Voorstel: Een norm die aangeeft hoe in de retail de cash beveiligd kan worden. Op basis van welke risico's en omstandigheden worden maatregelen overwogen. Wat zijn verantwoordelijkheden, processtappen en afspraken voor de verschillende momenten van waardeoverdracht en waardeberging.

Motivatie: Deze norm draagt bij aan het beperken van financiële schade en letsel schade door verduistering, diefstal en roof van geld en waardepapieren in de retail. De afspraken met waarde transporteurs worden eenduidiger vastgelegd en uitgevoerd.

Belanghebbenden: Retail, horeca, waarde transport bedrijven, verzekeraars. In tweede instantie mogelijk ook leveranciers van techniek (kluis, cashmanagement) en overval-preventie trainingen.

6. Beveiliging van containers

Verzegeling van containers en goede controle hierop is een essentieel onderdeel van supply chain security en van internationale regelgeving. In de praktijk conflicteert de controle in havens op verzegelde containers met een snelle afhandeling. Daardoor is smokkel mogelijk en zijn containerbedrijven kwetsbaar voor criminele infiltratie met alle bijeffecten van dien.
De zwakke controle wordt veroorzaakt door concurrentie tussen havens en door een gebrek aan praktische normen.

Voorstel: Een internationale/Europese norm voor de beveiliging van containers en verwijzen vanuit internationale regelgeving naar deze norm.

Motivatie: Met een internationale norm voor de beveiliging van containers ontstaat een gelijk speelveld hoe havens en zeevracht georiënteerde bedrijven met containerbeveiliging omgaan. De smokkel via containers wordt lastiger en de criminele infiltratie in havens en containerterminal bedrijven neemt af.

Belanghebbenden: Havenbedrijf, Zeehavenpolitie, Douane, containeroverslagbedrijven, reders

7. Food defense en supply chain security

Vanuit voedselveiligheid worden nieuwe security eisen gesteld. Voor de levensmiddelenhandel en supermarkten is het van belang om die in supply chain security onder te brengen.

Voorstel: Norm waarin de eisen van food defense in bestaand supply chain security framework worden geplaatst.

Motivatie: Vanuit een aangepast supply chain security framework wordt tevens aan de eisen van fooddefense voldaan.

Belanghebbenden: Supermarkten, voedsel gerelateerde transportbedrijven, voedsel gerelateerde distributiecentra

8. Retail security

Binnen de retail branche is behoefte aan een brede retail security norm. In deze norm kunnen ook verwijzingen zijn naar cash flow security, supply chain security, food defense en antecedentenonderzoek.

9. Command and Control

Bij grote industriële incidenten is efficiënte communicatie en samenwerking tussen de betrokken partijen essentieel. Een voortvarende afwikkeling van het incident, het organiseren van de hulpverlening en het informeren van direct betrokkenen, omwonenden en het publiek vragen om effectieve coördinatie.

Voorstel: Een norm waarin helder is vastgelegd hoe in Nederland de taken, hiërarchie, verantwoordelijkheden en bevoegdheden zijn belegd.

Motivatie: Deze norm kan de afhandeling en communicatie van grootschalige industriële incidenten verbeteren en gevolgschade daarvan verminderen.

Belanghebbenden: Veiligheidsregio, omgevingsdiensten, brandweer, ambulance, politie, bedrijven, particuliere brandweer, burgers etc.

Bijlage bij verslag van het Security Seminar

Plenaire discussie

Tijdens de eerste plenaire sessie zijn door aanwezigen de volgende opmerkingen gemaakt.

1) Vraag van Glenn Schoen van G4S: is NEN de host, die internationale experts naar NL uitnodigt en experts samenbrengt? Antwoord: Ja, ook in het buitenland komen experts aan tafel en die komen in contact met NL deelnemers bij internationale vergaderingen. Experts ontmoeten elkaar in ISO en CEN en werken nauw samen.
2) Vraag van Rob Kistjes van Deerns: hoe passen technische normen in nieuw te ontwikkelen systemen en procedures? Antwoord: als er relaties zijn tussen nieuwe normontwikkelingen en bestaande normen, zal NEN met desbetreffende andere NC een link leggen en werk afstemmen.
3) Opmerking van Piet Bel van Philips: Ik heb nog niets over cyber security gehoord. Antwoord: Cyber security is ondergebracht bij andere TC's. Die link moet wel worden gelegd. Het zelfde geldt voor Privacy Management.
4) Opmerking van Eelco Dykstra van Diem: in de Roadmap voor normalisatie van CBRNe en CM die door een CEN/TC 391 werkgroep is geschreven wordt het inrichten van Communities of Interest (COI) voorgesteld om 'fragmentation and lack of impact' te adresseren. Vanuit internationale optiek is COI iets anders dan normalisatie. Deze gaan van 1 -1 -2014 van start. Antwoord: in die roadmap wordt normalisatie als instrument geponeerd en de COI ondersteunend daaraan.
5) Vraag van Collectief Gezin en Jeugd: huishoudens en de jeugd zijn steeds meer aangesloten op internet. Cyber crime is daarin een belangrijk aandachtspunt, wat gaat NEN daaraan doen? Antwoord: Dat wordt in een andere NC's opgepakt.
6) Vraag van Gijs Spiele van TÜV: is NEN betrokken bij Horizon 2020? Antwoord: ja NEN vindt dat normalisatie zo snel mogelijk bij nieuwe initiatieven en innovatie betrokken moet worden. De EC heeft ook onderkend dat normalisatie bijdraagt aan research en dat tijdige normalisatie de EU markt een voordeel kan opleveren t.o.v. andere regio's.

Break-out sessie Security

Rene Visser van het Rijksvastgoedbedrijf vraagt zich in zijn presentatie af: "Doen we de dingen die we doen wel goed?" Hij vraagt zich af of het RVB de uitvragen t.a.v. security van Rijksgebouwen wel goed doet. Hoe kunnen we de inschrijvingen die vaak sterk van elkaar verschillen goed beoordelen? Soms is het moeilijk uit te leggen hoe en waarom oplossingen zijn gekozen, of risico's wel juist zijn geschat en afgedekt. Nu worden in aanbestedingstrajecten (noodgedwongen) vaak appels met peren te vergeleken. Kan dat met nieuwe normen anders en beter? Idealiter zouden bestaande normen daarin een plek moeten krijgen.

Een retailer vraagt zich af hoe fraude en winkelcriminaliteit beter kunnen worden bestreden. En hoe manage je dat efficiënt in een grote winkelketen? Hoe kun je in een semi-openbare omgeving security organiseren? Wat zijn de mogelijkheden en wat kun je nog waarborgen?

Daarna volgt een ronde waarin de 20 aanwezigen hun kansen voor normalisatie toelichten. Het volgende is geopperd:

- Norm voor het inrichten van het security proces in een organisatie,
- Norm voor het objectief meten van de perceptie van veiligheid/security,
- Norm voor het omgaan met Internet of Things, device management, cyber security,
- Security in huishoudens en bij jongeren t.a.v. dreigingen via het Internet, speelgoed-winkels die video's voor 18 en ouder aan jonger verkoopt, energiedrankjes die vol gif aan de jeugd worden verkocht,
- Overzicht voor de Gouden driehoek (kennisinstellingen, bedrijfsleven en overheid) van het woud van normering, certificerende instelling
- Norm voor opschaling van maatregelen op praktisch niveau (er zijn nu veel verschillende systemen in de EU),
- Norm voor security van grote evenementen, verbetering van huidige richtlijnen,
- Norm voor security voor transportmodaliteiten ferry's, zeehavens, stations,
- Norm voor Hoger Security Management opleidingen,
- Hoe kun je bestaande security normen beter vindbaar en toegankelijk maken,
- Norm voor security voor planontwikkeling beter geformuleerd kan worden, zodat eerder in de planontwikkeling de marges voor security worden aangegeven,
- Norm voor een risicoanalyse voor security problemen,
- Norm voor cyclisch proces waarin security management is ingericht voor organisaties om tot juiste maatregelen te komen,
- Integraliteit van beveiligingsdomein in norm vastleggen,
- Cyber security norm voor MKB,
- NEN normen upgraden naar EU eisen voor beveiligingssystemen,
- Norm voor beveiliging tegen Brandoverslag,
- Eenduidige begrippen en methoden definiëren voor security,
- Norm waaraan een Security Manager of Adviseur zou moeten voldoen,
- Norm voor security risico analyse en maatregelen selectie,
- Norm voor cyber security voor intelligent gebouw security,
- Normen voor security producten en systeem,
- Norm om security bewustzijn te beïnvloeden en te meten,
- Norm voor managen van interne dreigingen,
- Norm voor schaalbaarheid van security ook voor MKB,
- Norm voor Security Risk Assessment, consultant,
- Norm voor Security Management Systeem in een multi-user omgeving,
- Norm voor Retail Cash Management Systemen, componenten en afstemming,
- Norm voor cash devalidation systems,
- Norm voor cyber security diensten zoals penetratie testen,
- Norm voor fysieke penetratietesten,
- Norm voor het proces om security van gebouwen te ontwerpen,
- Norm voor kwaliteit van security dienstverlening en de leidinggevende,
- Keurmerk Particuliere Beveiligingsorganisaties tot landelijke NEN norm verheffen.
- Norm voor betere uitvoering van onderzoekwerkzaamheden,
- Procesmatige aanpak om tot security maatregelen te komen,
- Norm om weerstand van security maatregelen te beoordelen,
- Norm voor cyber security voor gebouwen (beheerssystemen, security systemen),
- NL norm voor antecedentenonderzoek / pre-employment screening.

Break-out sessie BCM, Vitaal en Supply Chain Security

De sessie voor Business Continuity Management (BCM), Vitale Infrastructuur en Supply Chain Security wordt door 35 personen bezocht.

NEN heeft al een BCM-commissie. De heer Kogenhop (BCM+) geeft als voorzitter van deze BCM-commissie aan, waaraan gewerkt wordt:

- Guideline voor resilience,
- Guideline voor business impact asessement,
- Guideline voor supply chain resilience,
- Idee voor het ontwikkelen van een instapversie BCM voor kleinere bedrijven.

Liesbeth Segers (Wil Research) geeft dat binnen haar internationale organisatie de BCP's (bedrijf continuïteit plannen) via ISO goed zijn vastgelegd, maar dat de emergencyplannen, BHV-plannen en dergelijke per land en locatie verschillen. Emergency zit niet in BCM-normen. Zij heeft behoefte aan samenhang van Emergency met BCM.

Piet Bel (Philips) vraagt aandacht voor de samenhang van BCM met cyber-incidenten. Over de hele wereld werkt de bedrijfsbrandweer uitstekend. In relatie daarmee is de cyberbrandweer onderontwikkeld en spreekt verschillende talen. Dick Hortensius (NEN) geeft aan dat er een norm bestaat als 'IT-readiness for business continuity management'. Kogenhop geeft aan dat de BCM-commissie hier aandacht aan gaat geven.

Tom Brabers (Geodis Wilson) geeft aan dat er binnen NEN/CEN/ISO heel veel kennis is vastgelegd, maar dat hij het overzicht hierop mist. Dat wordt breed gevoeld. Hortensius geeft aan dit juist een belangrijke reden is voor een 292 supercommissie op security. De opgave voor de Nederlandse commissie zou moeten zijn om de samenhang van kennis en normen over het voetlicht te brengen.

Ferry Plug (Mitigate) geeft aan dat de normgeving op security en beschikbaarheid van datatransport rommelig is. Er is een toename van high impact dataprocessen die gebruik maken van het internet (bv IDEAL). Datacom-leveranciers, installatiebedrijven en mogelijk ook verzekeraars zijn belanghebbenden bij goede normgeving op datatransport in relatie tot security en beschikbaarheid.

De heer Drost (AON) geeft het belang aan van de samenhang tussen BCM, IT en crisismanagement. Dat wordt breed onderschreven.

Jaap van Wissen (Rijkswaterstaat) geeft aan hoe de Rijksoverheid de basisvraag op BCM in campagnes naar voren heeft gebracht: wat te doen met 1 week zonder stroom of 1 week zonder IT?

Reinout Gunst (Havenbedrijf) geeft aan dat vanuit internationale regelgeving containers op een gecontroleerde wijze tot terreinen moeten worden toegelaten. Een integere verzegeling van containers en controle hierop blijkt in de praktijk lastig te zijn en te botsen met commerciële belangen. Containerbedrijven zijn kwetsbaar voor smokkel en criminele infiltratie.

Dubois (Zeehavenpolitie) geeft aan dat er veel (gefragmenteerde) regelgeving is en dat normen deze kunnen concretiseren. De belanghebbenden bij containerbeveiliging zijn reders, terminal

operators en havenbedrijven. Vanwege concurrentie tussen havensteden zou dit Europees opgepakt moeten worden.

Tom Brabers (Geodis Wilson) vindt het belangrijk dat er een goede link komt tussen het normenkader van ISO 28000 en het normenkader van TAPA.

In de voorbereiding op het seminar is het onderwerp 'Food defense in relatie tot Supply Chain Security' naar voren gebracht. Vanuit voedselveiligheid worden security eisen gesteld. Voor levensmiddelenhandel/supermarkten is het van belang om die in supply chain security onder te brengen.

De volgende thema's zijn benoemd (met het aantal belangstellenden van deze sessie):
- Samenhang BCM met cyber/ISO27000 (11 personen)
- Samenhang BCM met emergency planning en crisismanagement (13 personen)
- Security en beschikbaarheid van datatransport (3 personen)
- Schets van de samenhang van normen (5 personen)
- Supply chain security, integriteit van containers, samenhang met TAPA (13 personen)

Break-out sessie CBRNe en CM

De sessie start met een introductie door Marc Ritter over het doel en de werkwijze. Het doel is enerzijds het brengen van informatie over lopende normalisatietrajecten en –mogelijkheden en anderzijds het verkrijgen van informatie over normalisatiebehoeften.
De introductie-case wordt gepresenteerd door een vertegenwoordiger van de omgevingsdienst Midden- en West Brabant en heeft betrekking op de rol van de omgevingsdienst bij grote industriële incidenten zoals zij de afgelopen jaren onder andere hebben meegemaakt op het industrieterrein Moerdijk (brand Chemiepack en recenter brand Shell). Op basis van deze case ontstaat een discussie over welke afspraken gemaakt moeten worden tussen de betrokken partijen.
Betrokken partijen bij dergelijke incidenten zijn:
- Veiligheidsregio
- Omgevingsdienst
- First responders (brandweer, ambulance, politie)
- Brandweer industrieterrein
- Bedrijven
- Burgers
- Etc.

Het is van groot belang vast te leggen wie welke verantwoordelijkheden en rollen heft en hoe de hiërarchie is in geval van incidenten. Hierover kunnen en moeten afspraken worden gemaakt.
Vragen die middels normalisatie kunnen worden beantwoord zijn:
- Wie heeft welke verantwoordelijkheid?
- Welke functies kunnen eenduidig worden benoemd en omschreven (ook binnen bedrijven!)?
- Welke functie hoort bij welke partij?
- Welke functies binnen de veiligheidsdiensten moeten in geval van een incident altijd bereikbaar zijn voor bedrijven?

- Welke functies binnen bedrijven moeten in geval van een incident altijd bereikbaar zijn voor de hulpdiensten?
- Welke competenties horen bij welke functies, wat moet men kunnen en weten?
- Wie heeft beslissingsbevoegdheid over wat?
- Hoe en door wie wordt wat gecommuniceerd?
- Hoe kan je bij een incident de gevolgen voor het milieu beperken?
- Wat is het minimumniveau van operationaliteit/bereikbaarheid/infrastructuur dat beschikbaar moet zijn na een incident om de maatschappij draaiend te houden?

De bedrijven die betrokken moeten worden in de dialoog zijn niet alleen de topbedrijven (omgevingsdienst heeft een lijst met 200 topbedrijven qua risico), maar ook de kleinere, minder risicovolle bedrijven. Ook als daar iets gebeurt, moeten er afspraken zijn.
Voor wat betreft de link met het milieu geldt dat de dagelijkse grenzen voor bodemverontreiniging niet altijd toepasbaar zijn bij incidenten.
De gezamenlijke brandweer werkt aan scenario's voor incidenten, waarbij wordt gekeken naar de situatie voor, tijdens en na een incident. Belangrijk deze te benaderen voor betrokkenheid.
De veiligheidsregio is een platform om afspraken te maken, maar daar zitten de omgevingsdiensten en bedrijven niet aan tafel.

Deelnemerslijst Security Seminar 23 september 2014

naam	*ini*	*vv*	*geslacht*	*bedrijf*
Barendse	L.M.P.		mevrouw	APM Terminals Rotterdam
Bel	P.S.A.		de heer	Philips
Bosman	M.O.		de heer	Ziggo
Brabers	T.		de heer	Geodis Wilson
Broek	P.J.	van den	de heer	SAVR Consultancy
Bruyn Kops	G.F.	de	de heer	Mininsterie BZK
Cortenraad	S.P.W.		de heer	AES Security Management
Crooymans	M.G.M.		de heer	Sogeti
Dersjant	P.		de heer	Rijkswaterstaat
Deursen	E.	van	de heer	SYSQA
Dondorp	S.S.C.		de heer	Northwave BV
Drost	I.C.A.		de heer	Aon
Dubois	N.L.		de heer	Zeehavenpolitie
Dwars	H.		de heer	DEKRA Certification BV
Dykstra	E.H.		de heer	Diem - Dykstra Int l Emergency Management
Emde	E.		de heer	ASIS International
Etten	N.	van	de heer	G4S
Fazzi	E.A.		de heer	Veiligheidsregio Utrecht
Grumner	J.C.M.		de heer	SVPB/ECABO
Gunst	R.J.M.		de heer	Havenbedrijf Rotterdam
Hendriks	G.		de heer	ASIS International
Heuvel	J.W.	van den	de heer	Fire defender systems BV
Hoogteijling	P.A.		de heer	Hoogteijling
Hutter	J.		de heer	Adviescentrum BVI
Ivanovic	A.		de heer	Advies- Onderzoekbureau Forta Nova
Jansen	F.A.		de heer	KPN
Kampschoer	R.F.H.M.		de heer	Ahold
Kisjes	R.		de heer	Deerns Nederland BV
Kogenhop	G.		de heer	BCM+
Leurs	C.M.R.		de heer	KPN
Lierop	P.A.M.	van	de heer	van Lierop Security Awareness
Migchelsen	M.		de heer	Ministerie BZK
Minderman RSE	Mr. H.		mevrouw	Transport en Logistiek Nederland
Nieuwenhuis	R.L.		de heer	Ahold
Nieuwkoop-Buchner	J.M.	van	mevrouw	Vegro Verpleegartikelen
Noordegraaf	D.P.L.		de heer	Octant Veiligheids- & Risicomanagement B.V
Nuland Msec	R.M.		de heer	NU Security Consultancy/Saxion

				Security Managen
Nunes	E.S.		de heer	Van Gogh Museum Amsterdam
Oey	K.H.		de heer	innoSECURE
Oey	K.H.		de heer	innoSECURE
Olivari	S.		de heer	Vandenberg-ID
Plug	F.		de heer	Mitigate
Rademaker	J.G.M.		de heer	Den Haag Centrum voor Strategische Studies
Rijen	F.	van	de heer	CVO
Rijsewijk	J.	van	de heer	Cofely
Rijthoven	F.		de heer	IBM
Robrechts	P.		de heer	Robrechts & Thienpont
Royen	L.J.H.		de heer	ELROY Consultancy & Projectmanagement
Ruijten	M.		de heer	CrisisTox COnsult
Scheers	P.G.		de heer	KPN
Schoen	G.		de heer	G4S
Schreuder	P.		de heer	Rijksvastgoedbedrijf
Segers	E.J.		mevrouw	WIL Research
Spiele	G.		de heer	TÜV Nederland
Spit	M.J.W.		de heer	Adviescentrum BVI
Steenbakkers	J.		de heer	Ordina
Top	E.		de heer	TOP Security Advies Bureau
Troost	T.		de heer	TOTAL Nederland BV
Veen	R.L.M.	van	de heer	
Veenstra	M.J.W.		de heer	Gezamenlijke Brandweer
Visser	W.		de heer	Northrop Grumman Sperry Marine
Weijers	J.W.		de heer	Sitech Services
Winden	R.A.C.	van	de heer	De Nederlandse Veiligheidsbranche
Wissen	J.H.M.	van	de heer	Rijkswaterstaat
Wit	J.J.	de	de heer	Siemens Nederland NV
sprekers				
Maas	P.			NEN
Zetten	J.	van		NEN
Emde	E.			ASIS International