Dreigingsprofielen, noodplannen en trainingen

Integratie als

De afgelopen tijd zijn meerdere grote, internationale bedrijven getroffen door cyberaanvallen. Wat begon als security-incidenten met op zichzelf al grote impact, veroorzaakte zeer ernstige safety-risico's. Die met gemak grotere gevolgen hadden kunnen hebben.

tekst Kees Kappetijn en Fred Byrman

Onlangs werden diverse bedrijven getroffen door cyberaanvallen: containeroverslagbedrijf APM, post- en logistiekbedrijf TNT, farmaciebedrijf MSD, voedingsgigant Mondelez, International en reinigingsproductenfabrikant Reckitt Benckiser. Het gevolg: hectische situaties, dagenlange stilstand en grote veiligheids- en beveiligingsdilemma's. Naast het stilvallen van de productie en quality-control konden safety- en securityafdelingen niet meer bij noodzakelijke documenten. Security-instructies waren bijvoorbeeld alleen digitaal beschikbaar en daardoor dus niet beschikbaar. Overzichten van gevaarlijke stoffen op het terrein konden niet meer worden uitgedraaid, net zomin als de evacuatielijst voor de bezoekers, piketlijsten voor bezetting van crisisteams en telefoon- en bereikbaarheidslijsten. Wat begon als security-incidenten, met op zichzelf al een grote impact, veroorzaakte ernstige safety-risico's die met gemak nog veel grotere gevolgen hadden kunnen hebben. Voldoende motivatie om de voorbereiding en response op zulk een breed dreigingsscala integraal vorm te geven en ook onderlinge afhankelijkheden te borgen, zou je zeggen. Vooral nu systemen steeds meer onderling verweven raken en dreigingen steeds minder eenduidig worden.

Regels

Bedrijven moeten zich voorbereiden op calamiteiten en verstoringen van de bedrijfsvoering en productie, om de omvang en periode van discontinuïteit zo beperkt mogelijk te houden. Naast een mooie bedrijfsvisie en een serie stevige ambities, hoort dit sub-doelstelling nummer één van elk bedrijf te zijn. Voor bedrijven die zich niet realiseren dat een ongeval, een hack, een brand of een criminele actie geen 'of-' maar een 'wanneer'-vraagstuk is, helpt de regelgever een handje. Ter borging van de werknemersveiligheid dwingt de Arbowet tot een noodplan, het Brzo wil een noodplan om grote brand- en milieuincidenten te kunnen managen, terwijl ISPS (International Ship and Port facility Security) vraagt om een securitymanagementplan inclusief ontruimingsprocedure ter voorbereiding op security- en terreurdreigingen. Onderdeel van deze noodplannen is een noodorganisatie die tijdens een incident de operationele taakuitoefening borgt. De Wet veiligheidsregio's en de Kernenergiewet kunnen zelfs plannen met een hele bedrijfsbrandweer voorschrijven.

Meer regelgevingskaders

Organisaties die binnen verschillende regelgevingskaders vallen, hebben het zwaar: chemische bedrijven in een open havengebied tikken zo maar drie of vier van de genoemde kaders af en hebben veel te organiseren. De uitdaging is dat het bedrijf al die normen met elkaar in verband moet zien te brengen. Voordeel

voor ISPS-bedrijven?

toverwoord

is dat er dan echt goed moet worden nagedacht over de inrichting van een bedrijfsnoodorganisatie. Het is als in een kinderkamer: het is eenvoudig om vier verschillende gebouwen te maken van respectievelijk Knex, Lego, Mecano en houten blokken. Maar probeer maar eens om één gebouw te maken met een mix van deze elementen.
Hoe moeilijk is het nu voor bijvoorbeeld ISPS-plichtige bedrijven om de relatieve last van een (aparte) securityorganisatie het hoofd te bieden, naast verplichtingen vanuit andere wettelijke drivers? Niet zo moeilijk, als je één element – Lego, Knex, Mecano of houten blokken – kiest als *backbone* van de bedrijfsorganisatie en daarin de andere bouwmiddelen naadloos opneemt. Dus de ISPS securityorganisatie integraal opgenomen in één noodorganisatie met plannen, procedures, faciliteiten, piketten en vooral opgeleide mensen die bij alle incidenttypen kunnen ingrijpen. Integratie van systemen en methoden is het toverwoord.

Verantwoordelijkheden

Bedrijven hebben te maken met een scala aan richtlijnen bedoeld om de veiligheid te borgen, deels wettelijk en deels zelfopgelegd, zoals ISO9001:2015. Bedrijven die zeegaande schepen ontvangen, zoals het containeroverslagbedrijf APM, zijn bijvoorbeeld onderworpen aan de internationaal geldende ISPS-code, in Europa beter bekend als EU Verordening 725/2004. Dit is een aanvulling op hoofdstuk XI-2 van het internationale SOLAS-verdrag (Safety of Life at Sea), in 2004 in werking getreden. Deze code richt zich op de verbetering van de beveiliging van schepen en havenfaciliteiten en stelt veiligheid- en beveiligingsmaatregelen verplicht. Denk hierbij aan:

- het aanstellen van een beveiligingsverantwoordelijke, de PFSO (Port Facility Security Officer) met afdoende kennis en kunde;
- het inrichten van een beveiligingsorganisatie;
- het beschikken over veiligheidscommunicatiemiddelen;
- het controleren van personen en goederen bij toegang;
- het toezicht houden op de havenfaciliteit;

»

» het zo nodig aanwijzen van beperkt toegankelijke gebieden: gebieden waarvoor aanvullende beveiligingsmaatregelen worden genomen wegens een verhoogd risico, zoals bij de opslag van gevaarlijke stoffen;
» de behandeling van lading en scheepsvoorraden;
» de omgang met onverzegelde bagage.

Ook eist de ISPS maatregelen ten aanzien van de ICT (informatie- en communicatietechnologie). De gedachte hierachter is tweeledig. Ten eerste is communicatie essentieel voor het behoud van veiligheid. Ten tweede kan verstoring van het computersysteem processen verstoren, in het bijzonder daar waar men gebruik maakt van Scada -systemen, met alle risico's van dien. Verder moet het bedrijf minimaal beschikken over een dreigingsevaluatie/ RI&E en een ontruimingsplan, gelden er opleidings- en trainingseisen voor het bij ISPS betrokken personeel en moeten er met een vaste frequentie trainingen en oefeningen plaatsvinden met aandacht voor de diverse onderwerpen die ISPS adresseert. Hoe de beveiliging is vormgegeven en hoe blijvend aan de eisen wordt voldaan, moet beschreven staan in een door de overheid te toetsen beveiligingsplan, het Port Facility Security Plan (PFSP). Bij de overheid op lokaal niveau is de Port Security Manager (PSO) verantwoordelijk voor toetsing van deze plannen. De havenmeester vervult deze rol, ondersteund door een team van deskundigen. Evaluatie van het PFSP en zijn toepassing moet eens per jaar plaatsvinden middels een audit. Ten minste eens per 5 jaar moet het PFSP naar de PSO voor hertoetsing. Het schema op pagina 15 toont de procedure om tot een dergelijk plan te komen.

Combinaties maken

Voor veiligheidskundigen klinkt het ISPS-stramien – het planmatig moeten voorbereiden op (dreigende) incidenten – niet vreemd. De Arbowet vraagt namelijk hetzelfde en verwacht een noodplan, een BHV-organisatie en opgeleide en getrainde mensen voor kleine en beginnende incidenten, branden en onwelwordingen. Het Brzo verwacht een intern noodplan met bijpassende noodorganisatie voor het optreden bij zware ongevallen, vaak met een specialistische brandweer- of gevaarlijkestoffenorganisatie. In eigen huis verwacht de verzekeraar een continuïteitsplan dat is gericht op bijzondere scenariotypes die tot grote schades en langdurige procesverstoringen kunnen leiden, met mensen die daarop zijn getraind. En de ISPS-code schrijft zoals gezegd voor dat bedrijven die zeeschepen ontvangen, beschikken over een beveiligingsplan, een ontruimingsplan en opgeleide en getrainde mensen. Dit alles om voorbereid te zijn op incidenten die de veiligheid van de haven, het havenbedrijf of de daar afgemeerde schepen in gevaar kunnen brengen, met onderliggend een dekkende RI&E voor security-dreigingen. Voor de nodige bedrijven in Nederland gelden meerdere van bovengenoemde wettelijke *drivers*. Het gevolg: vijf drivers leiden tot vijf dreigingsinventarisaties, vijf noodplannen met structuren en rollen en procedures, vijf piketsystemen en vooral 5 'hoeders' in de organisaties die onafhankelijk van elkaar de veiligheid van de mensen en de continuïteit van het bedrijf bewaken. De arbocoördinator op het bedrijfsnoodplan, de milieu-adviseur op het Brzo, de brandweercommandant op de artikel 31-brandweeraanwijzing, de Port Facility Security Officer op ISPS en de verzekeringstussenpersoon op het continuïteitsplan. Veel losse stukjes Knex, Lego en Mecano die uiteindelijk hetzelfde doel beogen: het voorkomen en/of beperken van de gevolgen die zowel safety- als security-incidenten uiteindelijk kunnen hebben – verwonding van mensen, schade aan assets en bedreiging van de bedrijfscontinuïteit. Reden genoeg om te kijken waar combinaties te maken zijn om tot een efficiëntere inrichting en een brede inzetbaarheid van de bedrijfsnoodorganisatie te komen. Helaas, niet iedereen denkt zo.
De PFSO's, zo leert de ervaring, hebben veelal geen of een beperkte security- of safety-achtergrond en -ervaring. Vaak is de functie verbonden aan hoofdfuncties als facility manager, KAM/QHSE functionaris, hoofd transport of hoofd technische dienst. Na een cursus van twee dagen zijn deze mensen PFSO en die functie vervullen ze vervolgens 'ernaast'. Andere bedrijven beleggen de

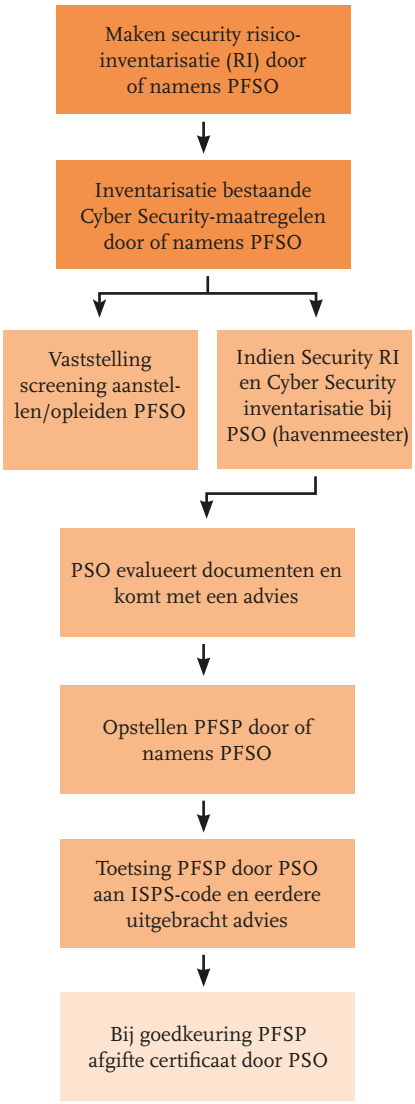
verplichte functie van PFSO bij een externe partij. De havenautoriteiten verzetten zich hier – terecht – tegen. Want een externe partij heeft vrijwel altijd (te) weinig kennis van het bedrijf, is op het moment van een calamiteit niet aanwezig en mist het gezag om een noodorganisatie op een doortastende en effectieve manier de sturing te geven die tijdens een crisis nodig is. Ook laten veel bedrijven de verplichte kwartaaloefeningen door externen uitvoeren. Vaak met het gevolg dat het enige dat de opdrachtgever ervan merkt een kort verslag is waarmee hij kan aantonen aan de oefenverplichting te hebben voldaan. Beide oplossingen zijn niet strijdig met de regelingen. En het kan op grond van specifieke expertise te rechtvaardigen zijn om bepaalde taken extern te beleggen. Daarom geldt sinds kort de eis dat de ISPS-plichtige bedrijven die het PFSO-schap uitbesteden, toch minimaal één intern contactpersoon aanwijzen en daarnaast duidelijk uitschrijven en aangeven welke verantwoordelijkheden bij wie zijn belegd.

Integratie: alles naar Lego

Om tot één breed inzetbare bedrijfsnoodorganisatie te komen die ook compliant is aan ISPS-criteria, zijn twee zaken nodig:

1. Security- en safety-verantwoordelijken dienen een brede kennis van calamiteiten en business impact te hebben. Want dreigingen zijn niet meer eenduidig en systemen zijn gekoppeld, waardoor security-incidenten sneller ook tot safety-incidenten leiden.
2. De opzet, structuur, gelaagdheid en rolverdeling van de bedrijfsnoodorganisatie dient zodanig te zijn dat ze op alle incidenttypen kan ontvouwen. Een bedrijf dat de noodorganisatie invult op vier niveaus (uitvoerend, leidinggevend, coördinerend en regisserend), ritsbaar maakt met de capaciteiten van de overheidshulpdiensten, voorziet van de juiste middelen, procedures maakt voor zaken die maar op één manier mogen worden aangepakt en de bezetting van sleutelfuncties borgt middels piketten, kan voorzien in incident- en crisismanagement op welhaast alle incidenttypen. Dit is precies de kern die in alle wettelijke drivers terugkomt.

Een bedrijf is gebaat bij een sterke, zelfbewuste en vooral ook simpele en eenduidige bedrijfsnoodorganisatie. Met mensen die bij alle dreigingstypen en op alle niveaus kunnen optreden. Aangejaagd door een functionaris die een relatief autonome positie heeft. En die op MT-niveau is betrokken bij het bepalen van zowel preventieve als preparatieve maatregelen op gebieden die kunnen leiden tot een bedreiging van de continuïteit. Mede door de snel veranderende wereld leiden versnippering en verzuiling makkelijk tot verzwakking en gebrek aan slagkracht. Wie denkt vanuit een geïntegreerd beeld van een enkelvoudige noodorganisatie met bijbehorende faciliteiten, zal snel de kracht ervan ervaren. Eén integraal dreigingsprofiel, één simpel maar compleet plan voor zowel incident- als continuïteitsmanagement en sleutelrollen die geborgd zijn middels piket en een goede crisisruimte. Met daarnaast een uitdagend opleidings- en trainingsprogramma. Maar dat is een cadeautje dat arbo-, Brzo-, Wvr- en ISPS-bedrijven automatisch gegeven is! «



Schema: procedure Port Facility Security Plan

Kees Kappetijn is safety-adviseur deskundige inrichting bedrijfsnood- en crisismanagementorganisaties. Was interim Bedrijfsbrandweercommandant en Port Facility Security Officer bij Lanxess Rubber in Zwijndrecht, België. **Fred Byrman** is security-adviseur, deskundige ISPS-vraagstukken en auteur van de Nederlandse opleiding tot PFSO/Havenbeveiliger, docent havenbeveiliging en lid van de Examencommissie havenbeveiliging van de SVPB.