CYBERVEILIGHEID IN DE CHEMISCHE LOGISTIEK:

ONDERNEEM NU ACTIE

Uit onderzoek blijkt dat één op de vijf Nederlandse bedrijven in 2024 schade ondervond als gevolg van een cyberaanval. De totale schade in Nederland betrof 10 miljard euro. Omgerekend komt dit neer op 300k per incident. De sector transport en logistiek blijkt hierbij een verhoogd risico te hebben. Met name kleinere bedrijven lopen een risico, omdat veel van hen hun cybersecurity nog niet op orde hebben. Toch lijken veel bedrijven nog niet (genoeg) voorbereid te zijn op een mogelijke aanval. Tijdens de Chemie on Tour op 26 september - georganiseerd door branchevereniging voor de chemische logistiek VNCW - werd stilgestaan bij de cyberdreigingen binnen de chemische logistiek en wat je als bedrijf kunt doen om een hack voor te zijn.

TEKST *Bernadine Kok-Snijder (CLM)*

Stefan Brandt (IenW)

De cyberbeveiligingswet voor de chemische sector

Eén van de onderwerpen die de agenda van de eerste spreker van de Chemie on Tour al geruime tijd vult is de Network and Information Security Directive, ofwel NIS2-richtlijn. Deze richtlijn is eind 2022 vastgesteld door de Europese Unie en is erop gericht de digitale en economische weerbaarheid van Europese lidstaten te versterken. Op dit moment wordt de richtlijn omgezet naar de Nederlandse Cyberbeveiligingswet (Cbw). Organisaties vallen automatisch onder de Cbw als zij actief zijn in aangewezen sectoren en volgens bepaalde criteria gekenmerkt worden als 'essentiële' of 'belangrijke' entiteit. De vervaardiging, productie en distributie van chemische stoffen is één van de aangewezen sectoren die automatisch onder de Cbw valt. Automatisch wil zeggen dat de verplichtingen van de Cyberbeveiligingswet voor deze organisaties direct gaan gelden zodra de wet in werking treedt.

De spreker is Stefan Brandt: beleidsmedewerker milieu bij het ministerie van Infrastructuur en Waterstaat en bij de wetgeving betrokken vanuit de verantwoordelijkheid voor de chemie. Brandt: "Ik ga m'n best doen jullie zoveel mogelijk de gedachtenspinsels en overwegingen bij de totstandkoming van de Cyberbeveiligingswet mee te geven. Geef hier vooral je input, mening of kritiek op." Dit was niet tegen dovemansoren gezegd: menig aanwezige stelde een kritische vraag over de praktische gevolgen van de wet. Zo verplicht de NIS2 bedrijven tot risicobeheersing, het melden van incidenten en ketenverantwoordelijkheid. Maar wat valt er exact onder de term 'incident'? En hoe zit het met de aansprakelijkheid binnen het bedrijf? Met name de zogenoemde 'zorgplicht' van bedrijven, de drempelwaarden van de NIS2 en de manier van inspecteren leveren vragen vanuit het publiek op.

Val ik onder de Cyberbeveiligingswet?

Voordat we verder in het onderwerp duiken: als bedrijf wil je uiteraard eerst weten of je überhaupt onder de Cbw gaat vallen. Brandt raadt aan om hiervoor de NIS2 Zelfevaluatie NL in te vullen: een door de Rijksinspectie Digitale Infrastructuur gemaakte zelfhulp-tool.

Mocht je onder de wet vallen dan ben je verplicht om de cyberweerbaarheid van je bedrijf te verhogen. De plichten die de Cbw voorschrijft zijn:

• *Registratieplicht*

Organisaties die vallen onder de Cyberbeveiligingswet zijn wettelijk verplicht zich te registreren in het entiteitenregister. De registratie vindt plaats via E-herkenning bij het Nationaal Cyber Security Centrum (NCSC) via mijn.nscs.nl.

• *Zorgplicht*

Het wetsvoorstel bevat een zorgplicht die organisaties verplicht zelf een risicoanalyse uit te voeren, op basis waarvan zij passende en evenredige maatregelen nemen voor de beveiliging van hun netwerk- en informatiesystemen die worden gebruikt voor de verlening van hun diensten. De Cbw omvat tien maatregelen die organisaties minimaal moeten nemen (zie kader).

De leden van het bestuur van entiteiten moeten de maatregelen goedkeuren en toezicht houden op de uitvoering ervan. Om dit goed te kunnen doen, dienen zij ook een opleiding te volgen.

Het bestuur moet nadenken over de verdeling van verantwoordelijkheden binnen de organisatie. Aandachtspunt hierbij is dat het bestuur altijd eindverantwoordelijkheid blijft voor cyberbeveiliging. Ook als taken gedelegeerd zijn aan bijvoorbeeld een CISO (Chief Information Security Officer) of een externe partij. In dit geval moet het bestuur zich actief laten informeren en betrokken zijn bij de belangrijkste vraagstukken en risico's. Dit vraagt om onderlinge afstemming: samen binnen het bestuur bepalen hoe men op de hoogte blijft en welke rapportages en/of signalen men wil ontvangen.

De Cyber Security Raad (CSR) heeft een handreiking Cybersecurity voor Bestuurders en Bedrijfseigenaren opgesteld. Deze handreiking is bedoeld om besturen te helpen bij het beheer van cyberrisico's als integraal onderdeel van hun taak.

De 10 maatregelen uit de Cyberbeveiligingswet

De nieuwe Cyberbeveiligingswet schrijft tien maatregelen voor waar organisaties in onder meer de chemische sector minimaal aan moeten voldoen:
- Maak een risicoanalyse.
- Versterk de beveiliging op het gebied van personeel, toegang en assetbeheer.
- Maak een Bedrijfscontinuïteitsplan (BCP).
- Richt 'Incident Response' in.
- Zorg dat cyberhygiëne op orde is.
- Schrijf beleid op de beveiliging van netwerk- en informatiesystemen.
- Maak de toeleveringsketen veilig.
- Maak beleid op cryptografie en encryptie.
- Gebruik beveiligde authenticatieoplossingen.
- Hanteer processen om de effectiviteit van maatregelen te beoordelen.

Op de website van het NCSC worden deze maatregelen uitgebreid toegelicht: Zorgplicht | Over het NCSC | Nationaal Cyber Security Centrum.

• *Meldplicht*
Het wetsvoorstel schrijft voor dat entiteiten significante incidenten zo snel mogelijk, maar in ieder geval binnen 24 uur moeten melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Het gaat om incidenten die de verlening van de diensten van de organisatie aanzienlijk (kunnen) verstoren. Een melding van een incident kan gemaakt worden op mijn.ncsc.nl , een centraal meldpunt geschikt voor significante meldingen en vrijwillige meldingen. Na een melding zal het CSIRT hulp en bijstand verlenen. Voorbeelden van factoren die incidenten tot een significant incident kunnen maken zijn de omvang van de financiële verliezen voor betrokkenen en het veroorzaken van (operationele) schade aan andere entiteiten dan de getroffen entiteit

De drempelwaarden voor significante incidenten worden nader uitgewerkt in de Ministeriële Regelingen. Deze Regelingen worden ter consultatie aangeboden zodat iedereen de kans heeft te reageren. Via de website Internetconsultatie kan tot 22 december op de Cyberbeveiligingsregeling IenW en de Regeling weerbaarheid kritieke entiteiten IenW. Brandt roept bedrijven op vooral van zich te laten horen tijdens deze internetconsultaties om zoveel mogelijk geluiden uit de praktijk te kunnen verzamelen.

• *Toezicht*
Organisaties die onder de Cyberbeveiligingswet vallen zijn onderworpen aan toezicht. Hierbij wordt gekeken naar de naleving van de verplichtingen uit de Cyberbeveiligingswet, zoals de zorg- en meldplicht. Toezichtsmaatregelen richten zich tot de entiteit maar kunnen in een uiterst geval ook de individuele bestuurders raken. De toezichthouder voor de chemische sector zal de Inspectie Leefomgeving en Transport (ILT) zijn. Zij zullen reactief toezicht houden, wat betekent dat zij achteraf langs komen na incidenten of signalen van tekortkomingen. De ILT zal dan nagaan of een bedrijf wel heeft voldaan aan de zorgplicht om het incident te voorkomen.

Acties IenW
Om bedrijven te ondersteunen bij het vergroten van hun cyberweerbaarheid is het ministerie van Infrastructuur en Waterstaat (IenW) gestart met het programma 'Versterken cyberweerbaarheid milieu en internationaal'. Dit is het overkoepelende cyberweerbaarheidsprogramma voor onder andere de sector chemie. Door samen te werken tussen sectoren, kan men ervoor zorgen dat Nederland meer cyberweerbaar wordt. Hier draagt IenW aan bij door allerlei activiteiten te organiseren. Denk aan overleggen waarin bedrijven uit de chemische sector bespreken hoe ze de cyberweerbaarheid kunnen versterken. Of aan trainingen en webinars, zoals die over de nieuwe Cbw wetgeving. Ook maakt IenW handreikingen, bijvoorbeeld voor de beveiliging van operationele technologie (OT). Daarnaast organiseert IenW sessies om kwetsbaarheden in de ketens van sectoren in kaart te brengen. Zo helpt men elkaar om bedrijven, sectoren en daarmee Nederland cyberweerbaar te maken. Op de website van IenW is meer informatie over het programma en

de projecten die worden aangeboden terug te vinden. Voor vragen en opmerkingen kan er contact opgenomen worden via de e-mail. Het is ook mogelijk via dit mailadres je aan te melden voor de nieuwsbrief.

Brandt: “Wacht als organisatie niet tot de Cbw inwerking treedt, maar kom vroeg genoeg in actie. Het versterken van de cyberweerbaarheid is in het eigen bedrijfsbelang. Vanuit IenW ondersteunen we graag, dus zorg dat u op de hoogte blijft van alle activiteiten en klop bij ons aan als we kunnen helpen.”

Digitale dreigingen raken ook de logistiek

Ron Vermeulen, partnermanager bij Samen Digitaal Veilig, presenteerde tijdens de Chemie on Tour actuele cijfers uit de sector. Uit onderzoek van het ABN AMRO blijkt dat 47% van de transportbedrijven cybercriminaliteit als een groot risico beschouwt, terwijl 56% nog niet bekend is met de NIS2-verplichtingen. De financiële schade is aanzienlijk: gemiddeld €300.000 per incident, met een totale schade van €10 miljard per jaar in Nederland. Er zijn veel voorbeelden van internetcriminaliteit in de sector die veel impact en schade hebben opgeleverd. Vermeulen: “Neem niet alleen maatregelen omdat het moet, maar ook om je bedrijf, je reputatie en je klantportefeuille te beschermen. Los van wetgeving en verplichting is het verstandig je bedrijf te beschermen tegen cybercriminaliteit.”

Waarom NIS2 ook relevant is voor toeleveranciers

Hoewel niet alle bedrijven in de chemische logistiek direct onder de NIS2 vallen, krijgen ze er indirect vaak wel mee te maken als toeleverancier van NIS2-plichtige organisaties. Denk aan bedrijven die betrokken zijn bij het transport, de opslag en distributie van olie, chemicaliën, afvalstoffen of

Ron Vermeulen (Samen Digitaal Weerbaar)

levensmiddelen. Een voorbeeld: als bedrijf met 49 medewerkers val je nét niet direct onder de NIS-2. Wegens de zorgplicht van het bedrijf waaraan je levert krijg je echter alsnog indirect met de regelgeving te maken. Vermeulen: “Naar verwachting zullen er zo’n 8.000 bedrijven direct onder de NIS2 vallen en tussen de 50.000 tot 100.000 toeleveranciers indirect. De NIS2 verplicht organisaties om hun digitale ketenrisico’s in kaart te brengen en te beheersen. Je kunt in de toekomst dus vragen verwachten van je klanten of je kunt aantonen dat je de cyberveiligheid om orde hebt.”

De zorgplicht die als verplichting in de NIS2-richtlijn is opgenomen verplicht bedrijven om:

- Strategische leveranciers te identificeren en hun cyberrisico’s te analyseren.
- Leveranciers te toetsen op naleving van NIS2-verplichtingen.
- Beveiligingsmaatregelen contractueel vast te leggen.
- Periodiek te evalueren of de digitale weerbaarheid van leveranciers op peil is.

Marktontwikkelingen en internationale voorbeelden

Vermeulen: “In de praktijk zien we al dat bedrijven zoals KPN, Tata Steel en ASML cybersecurity-eisen stellen aan hun leveranciers. Gemeenten en ziekenhuizen nemen digitale veiligheid op in aanbestedingen. In België is de wetgeving al van kracht en kunnen leidinggevenden persoonlijk aansprakelijk worden gesteld bij ernstige nalatigheid. Met de komst van de nieuwe Cyberbeveiligingswet (CBW) die naar verwachting in Q2 van 2026 van kracht gaat, zullen deze eisen alleen maar gaan toenemen. Het nemen van cybersecurity maatregelen kost tijd en geld, dus begin op tijd en verspreid je middelen!”

NIS2 Quality Mark

Het initiatief Samen Digitaal Veilig van MKB-Nederland en VNO-NCW, waar ook de VNCW als branchepartner bij is aangesloten, biedt mkb-bedrijven praktische ondersteuning bij het verbeteren van hun digitale veiligheid. Organisaties krijgen een tool in handen met praktische hulpmiddelen om de maatregelen te kunnen nemen en te kunnen aantonen dat deze maatregelen genomen zijn. Hiervoor gebruikt Samen Digitaal Veilig het normenkader van het NIS2

Quality Mark.

Het NIS2 Quality Mark is een normeringskader dat bedrijven helpt aantoonbaar te voldoen aan de NIS2-eisen. Het kent drie niveaus (Basic, Substantial, High) en is speciaal ontwikkeld voor mkb-bedrijven die toeleverancier zijn van een NIS2 entiteit of zelf direct aan de nieuwe richtlijn en toekomstige Cyberbeveiligingswet moeten voldoen.

Ketenverantwoordelijkheid is nú

Branchevereniging VNCW roept haar leden op om tijdig werk te maken van digitale veiligheid. De NIS2-wetgeving legt nadruk op aantoonbaarheid en ketenverantwoordelijkheid. Door nu te investeren in risicobeoordeling, contractuele borging en certificering, kunnen bedrijven hun positie in de keten versterken en voldoen aan de eisen van hun opdrachtgevers. En het belangrijkste… het bedrijf tijdig beschermen tegen internetcriminaliteit.

"Gekeken naar de toekomst van de

"HET KUNNEN AANTONEN VAN JE CYBERSECURITY-NIVEAU WORDT EEN LICENSE TO OPERATE"

chemische keten: digitale veiligheid zal een kernonderdeel van de risicobeoordeling worden, waarbij je als bedrijf aan moet kunnen tonen dat je je digitale veiligheid geborgd is. Het kunnen aantonen van je cybersecurity-niveau wordt een license to operate. Denk hierbij aan certificeringen als de ISO 27001 of het NIS2 Quality Mark. Daarnaast worden cyberverzekeringen strenger en legt de NIS2-wetgeving ketenverplichtingen op. Houd er rekening mee dat het voorbereiden op dit alles tijd gaat kosten", aldus Vermeulen.

De wereld van cybercrime

"Die NIS-wetgeving is allemaal mooi bedacht en vervelend tegelijkertijd, maar het is ook echt wel nodig. Ik was dan ook heel erg blij toen mijn aanbevelingen door Bart Groothuis van het Europees Parlement overgenomen werden. Eindelijk. Bedrijven komen namelijk niet in beweging totdat het misgaat." Aan het woord is ethisch hacker Peter Lahousse (CCInfo). In het dagelijks leven monitort hij continu wat er zich afspeelt in de digitale wereld en geeft hij op basis van zijn inzichten dreigingsrapportages af aan diverse diensten in binnen- en buitenland. Samen met zijn collega Jonathan van Eerd (Digiweerbaar) gaat hij in op de wereld van cybercrime, toegespitst op de chemische logistiek.

Lahousse: "Veiligheid zit in het DNA van de chemische logistiek. Al decennialang worden protocollen en procedures aangescherpt om ervoor te zorgen dat gevaarlijke stoffen veilig worden vervoerd en opgeslagen. De aandacht ging daarbij traditioneel vooral uit naar fysieke veiligheid: installaties, transportmiddelen en menselijk handelen. Maar de realiteit van vandaag vraagt om een bredere blik. Digitale veiligheid is in korte tijd net zo onmisbaar geworden als fysieke beveiliging."

Dat klinkt logisch, maar de praktijk laat zien dat veel bedrijven nog zoekende zijn. Systemen zijn steeds meer met elkaar verbonden, van logistieke planning tot temperatuurregeling in opslag. Daarmee groeit ook de afhankelijkheid van digitale technologie. Waar een storing vroeger hooguit vertraging opleverde, kan een cyberincident tegenwoordig leiden tot stilstand, datalekken of zelfs risico's voor de fysieke veiligheid.

De Europese wetgeving onderstreept dit. Met de komst van de NIS2-richtlijn wordt van bedrijven in en rond de chemische sector verwacht dat ze hun digitale weerbaarheid aantoonbaar op orde hebben. Voor veel organisaties, zeker in het mkb, roept dat vragen op: wat betekent dit concreet en waar begin je?

Om die vragen te beantwoorden, liet de International Foundation for Chemical Logistics (IFCL) door Digiweerbaar een praktijkonderzoek uitvoeren. Drie bedrijven uit de sector werden onder de loep genomen. Niet met de bedoeling om met de vinger te wijzen, maar om een eerlijk beeld te schetsen: waar staan we nu, wat gaat goed en waar liggen de kansen om sterker te worden?

Een kwetsbare sector met een hoge urgentie

"De chemische logistiek is aantrekkelijk én kwetsbaar tegelijk. Het gaat om complexe ketens waarin veel partijen samenwerken, vaak internationaal. Bedrijven werken onder hoge druk: leveringen moeten doorgaan, processen mogen niet stilvallen. Dat maakt de sector interessant voor criminelen. Bij een aanval is de kans groot dat er snel gereageerd wordt, al dan niet door het betalen van losgeld", aldus Lahousse.

De risico's zijn breed. Denk aan ransomware, waarbij systemen of data worden versleuteld en bedrijfsprocessen stilvallen. Of aan doxware: aanvallen waarbij niet alleen bestanden worden gegijzeld, maar ook wordt gedreigd met het openbaar maken van gevoelige informatie. Daarnaast zijn er gevaren voor operationele technologie, zoals koelinstallaties, pompen of blussystemen die via netwerken worden aangestuurd. En natuurlijk is er altijd de dreiging van phishing en social engineering, gericht op medewerkers die dagelijks toegang hebben tot gevoelige systemen.

"DE CHEMISCHE LOGISTIEK IS AANTREKKELIJK ÉN KWETSBAAR TEGELIJK."

Kortom, het speelveld is veranderd. Digitale veiligheid is niet langer een luxe of iets voor alleen de grootste

Peter Lahousse (CyberCrimeInfo)

spelers, maar een randvoorwaarde om überhaupt betrouwbaar te kunnen opereren.

Wat het onderzoek liet zien

Digiweerbaar sprak met drie representatieve bedrijven. De gesprekken gaven een genuanceerd beeld: er gebeurt al veel, maar er zijn ook duidelijke hiaten.

Beleid en organisatie

Cyberveiligheid staat vaak wel op de radar, maar is zelden verankerd in formeel beleid. Bij veel bedrijven ontbreekt een draaiboek voor incidenten. Dat betekent dat er bij een aanval of datalek ad hoc moet worden gehandeld. Niet per se uit onwil, maar simpelweg omdat capaciteit en kennis in het mkb vaak beperkt zijn.

Technische basis

De technische basis is doorgaans aanwezig. Firewalls, antivirus en back-ups zijn bij vrijwel alle bedrijven geregeld. Maar die basis zegt niet alles: controle of maatregelen écht werken, vindt niet altijd plaats. Een back-up is waardevol, maar alleen als zeker is dat het terugzetten ook daadwerkelijk lukt.

Toegangsbeheer

Hier liggen duidelijke verbeterpunten. Multifactor-authenticatie is nog niet overal standaard, terwijl het een eenvoudige en effectieve maatregel is. Ook het onderscheid tussen gewone gebruikers en beheerders is niet altijd scherp. In de praktijk betekent dit dat een medewerker soms meer rechten heeft dan strikt noodzakelijk is.

Menselijke factor

De grootste kans om beter te worden zit misschien wel bij de mens. Medewerkers zijn vaak de eerste die een verdachte mail openen of een fout kunnen maken. Toch blijkt structurele bewustwordingstraining nog zeldzaam. Phishingtests, korte e-learnings of toolboxen zijn eenvoudig in te voeren, maar worden nog nauwelijks toegepast.

Ketenafhankelijkheid

Vrijwel alle bedrijven vertrouwen op externe ICT-dienstverleners. Dat is logisch en vaak praktisch. Maar opvallend genoeg ontbreken er regelmatig duidelijke afspraken over verantwoordelijkheden, beveiliging of incidentafhandeling. Ook richting ketenpartners in transport en opslag is er weinig transparantie. Terwijl digitale veiligheid niet ophoudt bij de voordeur, maar de hele keten raakt.

De boodschap is helder: er is werk aan de winkel

De gesprekken bevestigen een beeld dat breder in het mkb speelt. Bedrijven willen wel degelijk investeren in digitale veiligheid, maar zoeken naar houvast. Wat is genoeg? Waar begin je? En hoe voorkom je dat het een papieren exercitie wordt?

Het goede nieuws is dat er veel te winnen valt met relatief eenvoudige maatregelen. Cyberveiligheid hoeft geen ingewikkeld technisch verhaal te zijn. Het gaat vaak om structuur, bewustwording en samenwerking.

Aanbevelingen voor de sector

Uit het onderzoek kwamen vijf duidelijke adviezen naar voren die de sector verder kunnen brengen.

1. Zet in op bewustwording

Cyberveiligheid is geen kwestie voor de IT-afdeling alleen. Medewerkers in magazijnen, chauffeurs en

kantoorpersoneel komen dagelijks in aanraking met digitale systemen. Juist daar is bewustzijn cruciaal. Korte, praktische trainingen en periodieke phishingtests maken medewerkers alerter.

2. Versterk toegangsbeheer
Met een paar basale maatregelen zijn grote stappen te zetten. Zorg dat multifactor-authenticatie overal wordt toegepast waar het kan, scheid gebruikers- en beheerdersrechten, en ondersteun medewerkers met gebruiksvriendelijke tools voor wachtwoordbeheer. Zo wordt het risico op misbruik kleiner, zonder dat het ingewikkelder wordt voor de gebruiker.

3. Werk samen in de keten
Omdat bedrijven steeds nauwer met elkaar verbonden zijn, is het essentieel om gezamenlijke afspraken te maken. Een branchebreed keurmerk, zoals het NIS2 Quality Mark, kan helpen om vertrouwen en transparantie te vergroten. Zo kunnen partners elkaar beoordelen op basis van duidelijke standaarden.

4. Bied kant-en-klare hulpmiddelen
Veel bedrijven willen wel, maar weten niet hoe te beginnen. Brancheorganisaties kunnen hier helpen met voorbeeldbeleid, checklists en zelfscans. Daarmee kunnen organisaties laagdrempelig hun huidige situatie toetsen en concrete stappen zetten.

5. Neem een verbindende rol als branche
Cyberveiligheid vraagt om samenwerking. Een brancheverenigingkan de rol van verbinder op zich nemen: kennis bundelen, ervaringen delen en bedrijven begeleiden. Zo hoeft niemand het wiel zelf uit te vinden.

Samen digitaal veilig
De rode draad is duidelijk: digitale veiligheid hoeft niet ingewikkeld te zijn, maar vraagt wel om aandacht en samenwerking. De chemische logistiek is een sector waarin veiligheid rondom het werken met gevaarlijke stoffen altijd centraal heeft gestaan. Nu is het moment om diezelfde mentaliteit door te trekken naar de digitale wereld.

Jonathan van Eerd (Digiweerbaar)

Wie nu stappen zet, bouwt vertrouwen en continuïteit in de keten. Wie achterblijft, loopt het risico op verstoringen, reputatieschade en gemiste opdrachten.

Het onderzoek van Digiweerbaar laat zien dat bedrijven bereid zijn om te leren en te investeren, maar dat ze praktische handvatten nodig hebben. Door samen te werken en ervaringen uit te wisselen, kan de sector op een haalbare manier de stap zetten naar een veilige digitale toekomst. Maak gebruik van de hulpmiddelen die door IenW en CSR aangereikt worden en bescherm je bedrijf tijdig tegen cyberdreigingen door gebruik te maken van het NIS2 Quality Mark normeringskader.

Om zoveel mogelijk professionals die met gevaarlijke stoffen werken van hulp te zijn, zal het door brancheverenigingVNCW geïnitieerde onderzoek omgezet worden in een Best practice. Deze zal voor eenieder gratis online beschikbaar gesteld worden, samen met een gratis E-learning aangaande cyberveiligheid in de chemische logistiek.

Houdt de website van Chemische Logistiek Magazine in de gaten om hierover op de hoogte de blijven of stuur een e-mail naar onze redactie. Je krijgt dan een seintje wanneer het één en ander beschikbaar is.