Aandacht voor cyberrisico’s bij risico-relevante bedrijven

Een verkenning van de cyberrisico’s binnen mechanismen voor de signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven

landelijk expertise centrum
industriële veiligheid

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Het aantal cyberaanvallen in de industriële sector neemt de afgelopen jaren toe. Dit blijkt uit verschillende berichtgevingen, statistieken en onderzoeken. Tegelijkertijd lijkt er nog weinig aandacht te zijn voor cyberrisico's vanuit dergelijke industriële bedrijven en vanuit inspectie-instanties, mogelijk door een gebrek aan kennis.

Het toezicht en de handhaving van de cyberbeveiliging van de industriële sector werd tot voor kort niet geregeld in nationale wetgeving. Een kleine uitzondering is het toezicht en de handhaving op de cyberbeveiliging van de energiesector, waar mogelijk een aantal industriële bedrijven onder vallen, op basis van de Wet beveiliging netwerk- en informatiesystemen (hierna Wbni). Met de komst van de Cyberbeveiligingswet (gebaseerd op de NIS2-richtlijn) in 2025, wordt de Wbni vervangen en komt hier verandering in. Onder deze wet vallen dadelijk ook de sectoren *chemische stoffen*, *afvalstoffenbeheer* en *afvalwater.* Met deze wijziging zal de industriële sector in zijn geheel onder de nieuwe wetgeving vallen.

Er komt daarmee binnen de industriële sector meer aandacht voor de cyberbeveiliging. De inspectie vanuit de Inspectie Leefomgeving en Transport (hierna ILT) en Rijksinspectie Digitale Infrastructuur (hierna RDI) zal zich voornamelijk richten op cyberrisico's die de bedrijfscontinuïteit van (zeer) kritieke sectoren voor de maatschappij en economie in gevaar kunnen brengen. Het Landelijk Expertisecentrum Industriële Veiligheid (hierna LEC-IV) is voornamelijk benieuwd naar het afdekken van de cyberrisico's die de continuïteit van mechanismen voor de signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven in gevaar kunnen brengen.

Risico-relevante bedrijven
Veiligheidsregio's verzorgen, samen met de omgevingsdiensten en de Nederlandse Arbeidsinspectie, de toezicht en handhaving bij Seveso-bedrijven. Er zijn echter ook bedrijven die net niet boven de drempelwaarden van de Seveso-richtlijn uitkomen en daardoor niet worden geïnspecteerd. Steeds meer veiligheidsregio's breiden hun focus uit naar deze bedrijven, omdat ongevallen bij deze bedrijven wel degelijk kunnen zorgen voor een substantiële impact op de omgeving. Uit verkenning van het Nederlands Instituut Publieke Veiligheid (hierna NIPV) uit 2019 blijkt dat veiligheidsregio's andere definities hanteren voor deze net-niet Seveso-bedrijven. Op basis van deze verkenning hanteert het NIPV de volgende definitie: 'een bedrijf die net onder de Seveso-drempelwaarden blijft, maar dermate veel gevaarlijke stoffen heeft dat dit tot een fors incident kan leiden met impact op de omgeving, buiten de terreingrens van het bedrijf'. Deze net-niet Seveso-bedrijven vormen samen met de Seveso-bedrijven de groep 'risico-relevante bedrijven'.

Het LEC-IV ondersteunt de veiligheidsregio's bij het uitvoeren van taken, zoals de inspectie bij Seveso-bedrijven, op het gebied van industriële veiligheid. Het gaat bij de inspectie vanuit de veiligheidsregio vooral om risico's die de bestrijding van incidenten en de beheersing van de bijhorende effecten in gevaar kunnen brengen. De vraag is of deze invalshoek specifiek aan bod zal komen tijdens de inspectie vanuit de ILT en RDI.

Omdat de veiligheidsregio's al inspecties uitvoeren bij Seveso-bedrijven, die onder de sectoren van de NIS2-richtlijn vallen, kunnen zij mogelijk een rol spelen bij de signalering

van cyberrisico's en de bewustwording daarvan bij deze bedrijven. Dit zal voornamelijk interessant zijn voor de veiligheidsregio's wanneer blijkt dat de mechanismen voor de signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven doelwit kunnen zijn van toekomstige cyberaanvallen.

Dit alles aanleiding voor het LEC-IV om een onderzoek te starten naar de cyberrisico's binnen mechanismen voor de signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven.

1.1.1 Achtergrond wetgeving

Onder de huidige Wbni is enkel de cyberbeveiliging geregeld voor vitale aanbieders en digitale dienstverleners. Onder vitale aanbieders vallen onder andere de energiesector, de transportsector en drinkwaterbedrijven. De RDI verzorgd de toezicht en handhaving van de energiesector en de ILT verzorgd de toezicht en handhaving van de transportsector en drinkwaterbedrijven. Onder deze sectoren vallen mogelijk een aantal bedrijven uit de industriële sector, maar het overgrote deel van deze sector valt niet onder de Wbni.

In 2025 wordt de Wbni vervangen door de Cyberbeveiligingswet, welke is gebaseerd op de Europese NIS2-richtlijn. Onder deze nieuwe wet vallen meer sectoren dan voorheen, zoals *chemische stoffen*, *afvalstoffenbeheer* en *afvalwater*. De ILT zal de toezicht en handhaving van deze sectoren verzorgen, op basis van de NIS2-richtlijn. Met deze wijziging zal de industriële sector in zijn geheel onder de nieuwe wetgeving vallen. Dit maakt dat deze sector moet voldoen aan de zorgplicht en dus de digitale risico's moet beoordelen en passende maatregelen moet nemen. Daarnaast moet deze sector incidenten melden bij de toezichthouder en het Computer Security Incident Response Team (hierna CSIRT).

Binnen de NIS2-richtlijn wordt onderscheid gemaakt tussen zeer kritieke sectoren en andere kritieke sectoren. Vervolgens kan een sector, afhankelijk van het aantal werknemers en de jaaromzet, een essentiële of belangrijke entiteit zijn. Essentiële entiteiten vallen onder een intensiever regime van toezicht, waarin zowel voor- als achteraf toezicht wordt gehouden op de naleving van de verplichtingen. Voor belangrijke entiteiten geldt een lichtere vorm van toezicht, die alleen achteraf plaatsvindt (zie bijlage 8.1 voor meer informatie).

1.2 Doelstelling

Het LEC-IV is voornamelijk benieuwd naar de cyberrisico's die de signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven in gevaar kunnen brengen. Het doel van deze verkenning is daarom om inzichtelijk te krijgen of deze repressieve mechanismen een mogelijk doelwit, al dan niet indirect, en een aantrekkelijk doelwit kunnen zijn van een cyberaanval. Daarnaast is het doel om een aantal scenario's te schetsen en een globaal overzicht te geven van de mogelijke maatregelen waarmee deze scenario's beheerst kunnen worden. Tot slot is het doel om inzichtelijk te krijgen of het van toegevoegde waarde is dat de inspectie vanuit de veiligheidsregio's aandacht besteed aan eventuele cyberrisico's.

1.3 Onderzoeksvragen

Uit de doelstelling komen de volgende onderzoeksvragen naar voren:

1. In hoeverre is er een mogelijkheid voor een, al dan niet indirecte, cyberaanval op een mechanisme voor signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven (H2)?

2. In hoeverre is een mechanisme voor signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven een aantrekkelijk doelwit (H3)?
3. Welke scenario's zijn denkbaar als het gaat om een cyberaanval op een risico-relevant bedrijf, met directe of indirecte betrokkenheid van een dergelijk repressief mechanisme (H4)?
4. In hoeverre is er aandacht voor dergelijke cyberrisico's binnen inspectie-instanties en is het noodzakelijk dat cyberveiligheid aandacht krijgt binnen de inspectie vanuit de veiligheidsregio (H5)?
5. Welke maatregelen zijn mogelijk om de mechanismen voor signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven te beschermen tegen een cyberaanval (H6)?

1.4 Afbakening

Deze verkenning richt zich op mechanismen die **tijdens en/of na** een incident bij een risico-relevant bedrijf worden ingezet. Dit zijn **repressieve** mechanismen en staan aan de rechterkant van het vlinderdasmodel (zie figuur 1-1). Repressieve maatregelen worden genomen om, in het geval dat er toch een incident plaatsvindt, het incident te kunnen signaleren en om de effecten te kunnen beheersen en te bestrijden. Aan de linkerkant van het vlinderdasmodel staan preventieve maatregelen. Preventieve maatregelen worden genomen om de kans op het incident en de bijhorende effecten aan de voorkant te beperken. Ook richt deze verkenning zich op de mechanismen die bij het bedrijf zelf aanwezig zijn en niet op de mechanismen die de hulpdiensten inzetten tijdens een incident.

Figuur 1-1 Vlinderdasmodel (Adlig Safety Consultants, z.d.)

Een risico-relevant bedrijf kan een groot aantal repressieve mechanismen hebben en niet elk bedrijf zal dezelfde mechanismen hebben. Er zullen mechanismen zijn die exclusief ontworpen zijn voor incidenten die alleen kunnen plaatsvinden door de aanwezigheid van specifieke stoffen, installaties en omstandigheden in een bedrijf. Op basis van de afbakening zijn er voor deze verkenning een aantal repressieve mechanismen geselecteerd (zie tabel 1-1) die bij de meeste bedrijven zullen voorkomen en waar eenieder zich een beeld van kan vormen.

Tabel 1-1 Voorbeelden van mechanismen voor de signalering, bestrijding en beheersing van incidenten

Voorbeelden repressieve mechanismen bij een risico-relevant bedrijf		
Signalering	Bestrijding	Beheersing
Brandmelders	Blusinstallatie	Vloeistofkerende deuren
Brandmeldinstallatie		Brandwerende deuren
Doormelding meldkamer		Nooddeuren
Ontruimingsinstallatie		

1.5 Aanpak

Om antwoord te krijgen op de onderzoeksvragen is er een grondige documentenstudie uitgevoerd en een achttal online interviews uitgevoerd met een:

1. Leverancier van brandmeldinstallaties; Bosch B.V.
2. Leverancier van blusschuiminstallaties; InnoVfoam B.V.
3. Risico-relevant bedrijf en ervaringsdeskundige cyberaanval; Tanatex Chemicals B.V.
4. Inspectie-instantie; Inspectie Leefomgeving en Transport (ILT)
5. Inspectie-instantie; Veiligheidsregio IJsselland (VRIJ), samen met het Nederlands Instituut Publieke Veiligheid (NIPV)
6. Inspectie-instantie; Milieudienst Rijnmond (DCMR), samen met de Omgevingsdienst Noordzeekanaalgebied (ODNKG), die een onderzoek heeft gedaan naar cybervolwassenheid van Seveso-bedrijven
7. Hoogleraar Handel en Logistiek van de Erasmus Universiteit, die onderzoek heeft gedaan naar de cyberkwetsbaarheid van de Rotterdamse maritieme sector
8. Ferm-Rotterdam, onderdeel van het Port Cyber Resilience Programma.

2. De mogelijkheid van een cyberaanval op repressieve mechanismen

Een cyberaanval wordt ingezet voor het ongeautoriseerd binnendringen in een computersysteem of netwerk met als doel informatie te stelen, schade toe te brengen, de werking ervan te verstoren of controle te verkrijgen over het systeem. Het kan worden uitgevoerd door individuen, groepen of georganiseerde criminele hackers. Er zijn verschillende soorten cyberaanvallen; phishing, malware (waaronder ransomware), DDoS-aanval, SQL-injecties, cross-site scripting, botnets, et cetera. Deze cyberaanvallen zijn afhankelijk van de aanwezigheid van een internetverbinding.

Echter beginnen niet alle cyberaanvallen daar waar een internetverbinding is. Een cybercrimineel kan proberen fysiek toegang te krijgen tot het bedrijf en een USB-stick met schadelijke software op een systeem aansluiten of hardware (keylogger) aansluiten op een computer die de toetsaanslagen vastlegt om gevoelige informatie te stelen. In plaats van fysiek toegang proberen te krijgen, kan de cybercrimineel een medewerker van het bedrijf manipuleren om dergelijke acties uit te voeren (social engineering) of het via een leverancier te proberen (supply chain aanvallen) door de hardware die zij leveren aan het bedrijf te infecteren. Een andere optie via de supply chain is om systemen aan te vallen via software-updates die vanaf externe schrijven worden geïnstalleerd. Tot slot is er de mogelijkheid om de communicatie te verstoren tussen systemen die gebruik maken van radiosignalen (radio jamming).

De vraag is of de mechanismen voor de signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven doelwit kunnen zijn van dergelijke cyberaanvallen, of indirect betrokken kunnen raken.

2.1 Beschrijving van de repressieve mechanismen

Zoals in paragraaf 1.4 beschreven, beperkt deze verkenning zich tot de mechanismen uit tabel 2-1. Deze mechanismen kunnen onderdeel zijn van een algeheel brandbeveiligingssysteem (zie figuur 2-1).

Tabel 2-1 Voorbeelden repressieve mechanismen bij een risico-relevant bedrijf

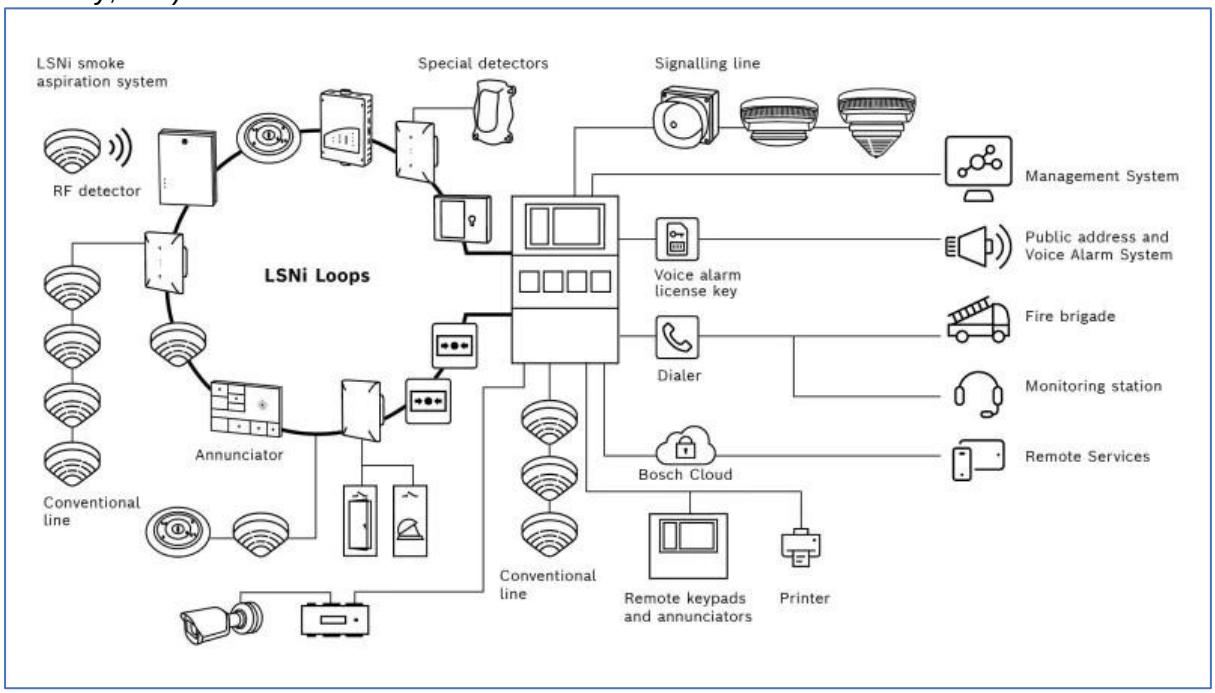
Voorbeelden repressieve mechanismen bij een risico-relevant bedrijf		
Signalering	Bestrijding	Beheersing
Brandmelders	Blusinstallatie	Vloeistofkerende deuren
Brandmeldinstallatie		Brandwerende deuren
Doormelding meldkamer		Nooddeuren
Ontruimingsinstallatie		

Er zijn verschillende brandmelders die een brand kunnen signaleren; rookmelders, hittemelders en vlamdetectoren. De meeste rookmelders zijn optische puntrookmelders die bestaan uit een fotodiode en een lichtbron. Wanneer hier rook bij komt, zal het licht verstrooid worden en door de diode worden gedetecteerd, waarna de melder alarm zal slaan (ELRO, z.d.). De meeste hittemelders zijn uitgevoerd met een gekoppeld paar thermistors om de temperatuur te detecteren. Eén thermistor wordt blootgesteld aan de omgevingstemperatuur, terwijl de andere thermistor geïsoleerd is. Onder normale omstandigheden registreren beide thermistors dezelfde temperatuur. Wanneer er echter een brand ontstaat, zal de temperatuur die door de blootgestelde thermistor wordt geregistreerd snel stijgen. Dit verstoort het evenwicht tussen de thermistors en brengt de detector in de alarmtoestand (rookmelderwereld, z.d.). Een vlamdetector bestaat uit een

besturingssysteem dat bewegend licht detecteert. Het alarm treedt in werking als er in dit licht sporen van infrarood- of ultravioletstraling worden gedetecteerd (Somati Systems, z.d.). Dergelijke melders kunnen ook onderling met elkaar communiceren. Wanneer de ene detector rook, hitte of straling detecteert, kan deze via een bekabelde of draadloze (voornamelijk via radiosignalen) verbinding communiceren met een detector in een andere ruimte, om ook daar het alarm te activeren.

Een brandmelder is vaak verbonden met een brandmeldinstallatie (hierna BMI). De communicatie tussen de brandmelders en de BMI verloopt meestal via een bekabelde verbinding, genaamd de melderslus (EPM, z.d.). De BMI kan weer in verbinding staan met andere brandbeveiligingssystemen; een ontruimingsinstallatie, een blusinstallatie, brandwerende en vloeistofkerende deuren, nooddeuren, een ventilatiesysteem en liften. Wanneer de BMI een signaal krijgt van een brandmelder, zal de BMI deze componenten inschakelen. Als er een ontruimingsinstallatie is gekoppeld aan de BMI zal er een optisch of akoestisch alarm afgaan om aan te geven dat de ontruiming moet worden gestart. Ook een blusinstallatie kan worden gekoppeld aan de BMI, maar deze treden toch veelal zelfstandig in werking. In dat geval faalt een hittegevoelig element van de installatie en komt het ontsluitingsmechanisme in beweging. Het in werking treden van een blusinstallatie zal in veel gevallen leiden tot automatische alarmering in het gebouw en doormelding naar de meldkamer. Verder kunnen ook brandwerende (en/of vloeistofkerende) deuren en nooddeuren worden gekoppeld aan de BMI. De BMI schakelt de elektriciteitsvoorziening uit van de kleefmagneten die op deze deuren zitten. Brandwerende deuren vallen daardoor dicht en nooddeuren kunnen op dat moment geopend worden.

Een BMI zal in sommige gevallen ook een signaal doorgeven, dan wel indirect via een particuliere meldkamer, aan de meldkamer van de brandweer. Om de werking van deze doormelding te garanderen, is het verboden om voor de alarmtransmissie gebruik te maken van het open internet en moet de transmissie via twee gescheiden methoden worden uitgevoerd. Dit is de zogenaamde redundantie van verbindingen en kan gebeuren via een besloten Alarm over IP-verbinding (AoIP) en een besloten draadloos verbinding, met GPRS en/of RAM Mobile (Mobitex). Beide transmissiemethoden worden continu getest en gecontroleerd. Als één van de verbindingen niet werkt, schakelt het systeem automatisch over naar de tweede verbinding en ontvangt de meldkamer hierover een melding (ASB Security, z.d.).



Figuur 2-1 Voorbeeld van een brandbeveiligingssysteem

Een brandbeveiligingssysteem (zie 2-1) is voornamelijk een bekabeld systeem met een eigen besloten netwerk (*standalone systeem*) zonder internetverbinding. Dit wordt bevestigd door Marc Rijs van de Brand Preventie Academy en Ruud Frissen van Strukton in een interview met Brandveilig.com. Draadloze verbindingen moeten volgens Rijs en Frissen niet de standaard worden, maar alleen overwogen worden in geval van noodzaak, bijvoorbeeld in geval van monumentale panden of tijdelijke opstellingen. Wanneer er sprake is van een draadloze verbinding, zal voornamelijk gebruikt worden gemaakt van radiofrequenties. Volgens Rijs is het wettelijke gezien uit den boze om een brandbeveiligingssysteem aan te sluiten op het internet of met andere, met internet verbonden, systemen (Kort, A. de, 2020). Het interview met InnoVfoam B.V. (hierna InnoVfoam), een leverancier van blusschuiminstallaties, bevestigd dat hun installaties *standalone* systemen zijn:

‘’Onze installaties worden automatisch geactiveerd door de brandmeldinstallatie via een analoge of digitale verbinding. Een handmatige activering is ook altijd mogelijk. Verder zijn onze installaties in de meeste gevallen standalone systemen die niet verbonden zijn met andere, eventueel met internet verbonden, systemen of netwerken. Daardoor kan een kwaadwillig persoon de installatie alleen bedienen als hij toegang tot de locatie waar de installatie zich bevindt. Naast de levering van blusschuiminstallatie, verzorgen we ook het jaarlijkse onderhoud en testen. De monteur die hiervoor langskomt, kan indien nodig een dongle op de besturingsapparatuur aansluiten om een beveiligde internetverbinding tot stand te brengen. Met deze geëncrypteerde verbinding kunnen onze ingenieurs, indien wenselijk, op afstand meekijken en veranderingen aanbrengen. Dit zijn geen geplande acties, dus voor een kwaadwillig persoon is het bijna onmogelijk om dit als ingang te gebruiken.’’

Het is daarmee minder voor de hand liggend dat repressieve mechanismen betrokken raken bij een cyberaanval via phishing, malware (waaronder ransomware), DDoS-aanval, SQL-injecties, cross-site scripting of botnets. Echter is er veel mogelijk als een kwaadwillig persoon het lukt om fysiek toegang te krijgen tot het bedrijf of een medewerker weet te manipuleren. Een rookmelder, ontruimingsinstallatie of blusinstallatie kan dan worden geactiveerd als er een handmatige optie is. Of er kan een USB-stick met schadelijke software in een brandmeldinstallatie, ontruimingsinstallatie of blusinstallatie worden gestoken wanneer deze beschikt over een USB-poort. Tot slot kan de communicatie tussen de verschillende onderdelen van een brandbeveiligingssysteem, in geval van draadloze verbindingen, worden onderbroken via *radio jamming*.

2.2 De trend van ‘slimme’ repressieve mechanismen

InnoVfoam geeft wel aan dat ze gaan verkennen welke voordelen het heeft om hun installaties te verbinden met andere systemen en netwerken (met eventueel een internetverbinding), zodat deze op afstand gereguleerd kunnen worden. Daarbij geven ze aan terughoudend te zijn in verband met cyberrisico’s. Deze verkenning die InnoVfoam mogelijk gaat uitvoeren, lijkt niet een opzichzelfstaande ontwikkeling te zijn. De ‘slimme’ brandbeveiliging is in opkomst door ontwikkelingen zoals het Internet of Things (IoT) en kunstmatige intelligentie (AI).

Het **Internet of Things** (IoT) verwijst naar een netwerk van fysieke objecten (zoals apparaten, sensoren, voertuigen, apparaten in woningen en fabrieken) die met elkaar communiceren via het internet. **Kunstmatige intelligentie** (AI) is het vermogen van een machine of computer om taken uit te voeren die normaal gesproken menselijke intelligentie vereisen, zoals leren, redeneren, probleemoplossing en patroonherkenning.

Dankzij AI en IoT zijn slimme brandbeveiligingssystemen sneller in staat om een brand te detecteren en te communiceren met de verschillende onderdelen van het systeem. Daarnaast zijn de Cloud-gebaseerde brandbeveiligingssystemen ook in opkomst. Daarbij is er sprake van een centrale online omgeving voor het bewaken en beheren van brandbeveiligingssystemen. Dit maakt het gemakkelijker voor beheerders om de brandbeveiliging in real-time te monitoren en te beheren, waardoor de respons op brandgevaar snel en effectief is. Er zijn ook steeds meer oplossingen beschikbaar die brandbeveiliging integreren met andere gebouwbeheerssystemen zoals energiebeheer, HVAC (verwarming, ventilatie en airconditioning), verlichting, beveiliging en toegangscontrole (Masset, 2023).

Dit lijken trends te zijn die tot zorgen baren. Ook volgens de Amerikaanse Fire Protection Research Foundation (FPRF) waren brandbeveiligingssystemen eerder vooral *standalone* systemen, maar worden deze steeds vaker gekoppeld aan het *Internet of Things*, gebouwbeheerssystemen en andere systemen of netwerken die zijn verbonden met het internet. In het onderzoeksrapport dat zij hierover hebben opgeleverd, wordt het volgende geschreven: '*A quick search for two popular internet protocols on the most popular ports uncovered over 43,000 building control systems (BCS) exposed to the open internet, leaving the BCS and connected fire systems vulnerable to cyber-attacks*'. Deze ontwikkeling kan leiden tot ongekende cyberkwetsbaarheden met aanzienlijke gevolgen. Tegelijkertijd is er nog onvoldoende bewustzijn van de omvang van deze kwetsbaarheden en de ernst van de gevolgen (FPRF, 2021).

Het interview met Bosch, leverancier van onder andere brandmeldinstallaties, bevestigd deze tendens:

'Een brandmeldinstallaties (BMI) is überhaupt vaak slecht beveiligd met zwakke toegangscodes. Als er dongles worden gebruikt om een tijdelijke internetverbinding op te zetten, zijn deze vaak niet goed versleuteld. Daarnaast zien we dat brandmeldinstallaties steeds vaker gekoppeld worden aan andere gebouwbeheerssystemen, zoals cybersecuritysystemen. Dit maakt het mogelijk om gekoppelde systemen adequaat op afstand te reguleren. Op dat moment is een BMI een redelijk makkelijk doelwit voor een cybercrimineel, want het verkrijgen van toegang vraagt om weinig kennis.'

De mogelijkheid wordt daarmee groter dat repressieve mechanismen betrokken raken bij een cyberaanval via phishing, malware (waaronder ransomware), DDoS-aanval, SQL-injecties, cross-site scripting of botnets.

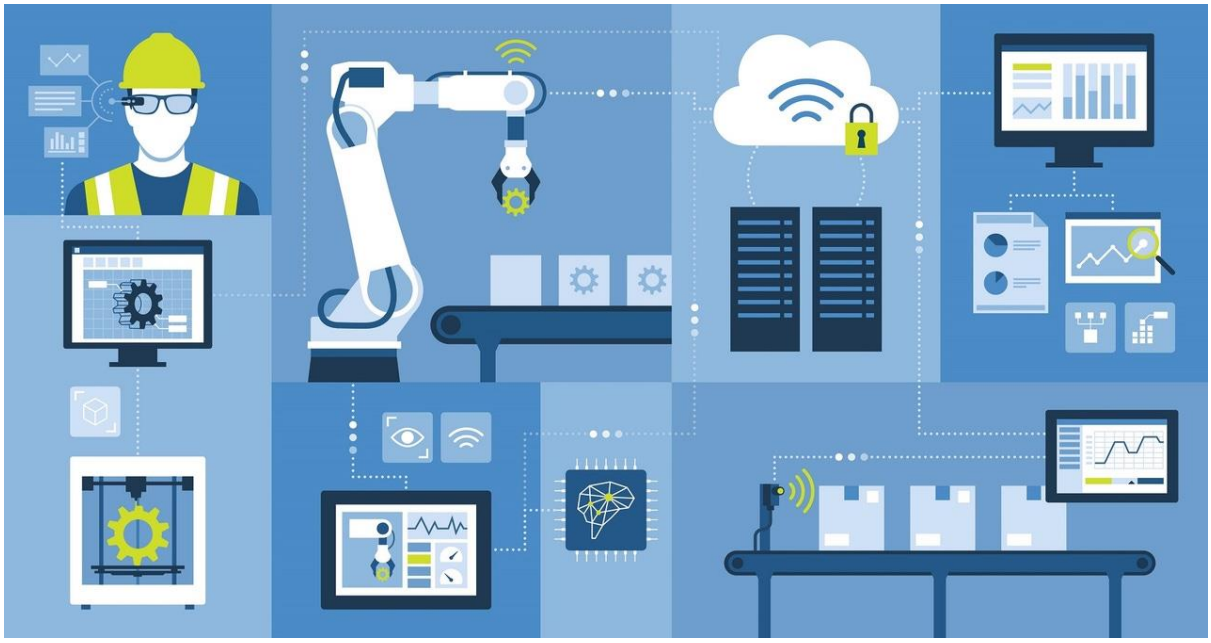
Tyler Robinson, een ethische hacker, vertelt in een interview met de Amerikaanse National Fire Protection Association (NFPA) dat niet elke cyberaanval momenteel bij een gebouwbeheersysteem begint, maar dit wel een steeds aantrekkelijker doelwit wordt voor cybercriminelen die kiezen voor de minste weerstand. Al die systemen en hun onderlinge verbondenheid op eenzelfde netwerk laten, volgens Robinson, een behoorlijk grote voetafdruk achter. Veel van die systemen zijn verouderd of draaien op verouderde besturingssystemen (Roman, J., 2023). Dit wordt bevestigd in het interview met het NIPV en Veiligheidsregio IJsselland:

''Wat we veel zien bij de bedrijven waar we inspecteren is dat (de aansturing van) systemen zijn verouderd, de beveiliging niet op orde is, maar er al wel een digitale verbinding is. Dit maakt het voor cybercriminelen natuurlijk heel makkelijk om binnen te komen.''

2.2.1 De trend van IT en OT-convergentie in de industrie

De trend van ‘slimme’ brandbeveiligingssystemen past binnen de algehele automatisering en digitalisering die binnen de industriële sector plaatsvindt. Binnen de industrie (waar risico-relevante bedrijven onder vallen) worden OT-systemen daarvoor steeds meer gekoppeld aan IT-systemen (convergentie). Daarmee is een bedrijf continu in staat om (op afstand) prestatiegegevens over haar processen te verzamelen en te analyseren, en waar nodig (op afstand) bij te sturen (zie figuur 2-2).

IT staat voor informatietechnologie. Het verwijst naar het gebruik van servers, netwerkapparatuur en *endpoint devices* (desktopcomputers, laptops, smartphones, POS systemen, printers, scanners en tablets) voor de uitwisseling en verwerking van informatie. **OT** staat voor operationele technologie. OT slaat doorgaans op de machines en hardware die worden gebruikt om de productie in een productieomgeving te bewaken en te besturen. In tegenstelling tot IT, die zich voornamelijk bezighoudt met internet, speelt OT een belangrijke rol in de omgang met de fysieke wereld.



Figuur 2-2 Convergentie van IT- en OT-systemen (Industrial Automation, 2024)

Dat cybercriminelen makkelijker toegang krijgen tot OT-systemen door de convergentie met IT-systemen, wil nog niet zeggen dat de cybercrimineel ook daadwerkelijk in staat is om een succesvolle aanval hierop uit te voeren. Door de verschillen in technologie, vraagt een cyberaanval op een OT-systeem veel meer specialistische kennis van de aanvaller (Afdeling van het toezicht op de chemische risico's, 2024). Dat zegt ook Jason Larsen, onderzoeker bij een Amerikaans cyberbeveiligingsbedrijf, die in opdracht van vele industriële bedrijven heeft geëxperimenteerd met cyberaanvallen om erachter te komen hoe een cybercrimineel fysieke schade aan zou kunnen brengen. Om met een cyberaanval toegang te krijgen tot een industrieel proces is een lange periode van onderzoek en experimenteel sleutelen aan de pompen en kleppen nodig om te begrijpen hoe ‘unexpected physics’ in gang gezet kunnen worden, aldus Larsen (Technology Review, 2015). Dit wordt bevestigd in het interview met de Hoogleraar Handel en Logistiek van de Erasmus Universiteit:

‘’Het is erg lastig om met een cyberaanval een zwaar ongeval met gevaarlijke stoffen te bewerkstelligen. Je hebt daarvoor enorm veel informatie nodig over het proces en de stoffen. Een hacker moet bijvoorbeeld weten welke stoffen niet in aanraking mogen komen met elkaar, bij welke temperatuur of dichtheid een gevaarlijke situatie kan ontstaan, en waar in het proces en op wat voor manier hij een gevaarlijke situatie kan creëren.’’

2.3 Cybervolwassenheid van de industrie

Ondanks alle ontwikkelingen op het gebied van cyberrisico’s, blijft de cyberveiligheid achter. Bedrijven hebben nog lang niet altijd kennis in huis van cyberveiligheid. Als dat wel het geval is, dan is het nog maar de vraag of IT-specialisten voldoende verstand hebben van gebouwbeheerssystemen, brandbeveiligingssystemen en OT-systemen om de cyberveiligheid daarvan te kunnen regelen. Een nauwe samenwerking tussen IT- en OT-teams is dan wenselijk. Jessica Chevreaux, een cyberveiligheidsprogramma-manager, geeft in een interview met NFPA aan dat deze teams vaak niet dezelfde taal spreken door een gebrek aan gedeelde beveiligingsstandaarden en beslissingsprotocollen (Roman, J., 2023). Palo Alto Networks, een globale dienstverlener in cyberbeveiliging, heeft in december 2023 een wereldwijde vragenlijst uitgezet bij bedrijven met een OT-omgeving. Bijna 1.980 respondenten hebben de vragenlijst ingevuld. Een van de vragen was hoe ze de relatie tussen IT- en OT-teams zouden omschrijven. Maar liefst 57% geeft aan dat er geen contact is tussen de twee teams of dat er sprake is van veel frictie (Palo Alto Netwerks & ABI Research, 2023).

In een onderzoek van de Universiteit Twente, waarvoor voornamelijk brancheorganisaties voor Seveso-bedrijven zijn geïnterviewd, wordt de conclusie getrokken dat de chemische industrie op dit moment onvoldoende voorbereid is op cyberincidenten die impact kunnen hebben op de procesveiligheid. Dit gebrek aan voorbereiding blijkt al uit het bewustzijn van de risico’s op bedrijfsniveau, dat in veel bedrijven, voornamelijk de kleinere, onvoldoende aanwezig is. Dit bewustzijn is noodzakelijk om ervoor te zorgen dat er voldoende tijd, geld en personeel gestoken wordt in cybersecurity. Dat laatste is uit zichzelf ook al een bottleneck, aangezien er maar weinig mensen te vinden zijn met voldoende kennis van zowel cybersecurity als de OT-omgeving (Universiteit Twente, 2023).

In hetzelfde onderzoek van Palo Alto Networks is aan de respondenten gevraagd in hoeverre ze de beveiliging van hun OT-omgevingen tegen cyberaanvallen als prioriteit zien. Daarbij geeft 64% aan dat dergelijke cyberbeveiliging vaak of altijd prioriteit heeft boven andere activiteiten. De rest van de respondenten geeft aan dat cyberbeveiliging even of minder belangrijk is. Hierbij is er een sterke correlatie tussen ervaringen hebben met cyberaanvallen en het beschouwen van cyberbeveiliging als prioriteit (Palo Alto Netwerks & ABI Research, 2023). Deze tendens wordt ook bevestigd in het interview met Tanatex:

‘’Leren doe je door fouten te maken. Nadat wij een cyberaanval hebben meegemaakt, hebben we goed gekeken naar de cyberveiligheid van onze systemen en processen. En dat doen we ook bij de inkoop van systemen. Maar we hebben bijvoorbeeld ook beter nagedacht over de toegangsmogelijkheden van bezoekers en bijhorende registratie.’’

Voor een cybervolwassenheidsonderzoek van Fox-IT, in opdracht van de DCMR, zijn 13 Seveso-bedrijven geïnterviewd en hebben 26 Seveso-bedrijven een self-assessment ingevuld. Op basis van de uitkomsten is geconstateerd in hoeverre, op een schaal van 0 (niet geïmplementeerd) tot en met 5 (volledig geïmplementeerd), Seveso-bedrijven zich bezighouden met cybermaatregelen op vijf verschillende gebieden, waar de IT-omgeving en de OT-omgeving er twee van zijn. Hieruit blijkt dat Seveso-bedrijven gemiddeld een 2,2 van

de 5 scoren op alle gebieden. Dat betekent dat maatregelen over het algemeen consistent wordt geïmplementeerd, maar dat dit vaak afhankelijk is van de kennis en toewijding van een specifieke groep medewerkers. Er is vaak wel beleid voor de cyberbeveiliging en documentatie over de ingevoerde maatregelen (zoals werkinstructies), maar het uitvoeren van compliance-checks en audits wordt beperkt gedaan. Als we kijken naar de cybervolwassenheid per gebied, ligt de score van de cybervolwassenheid van OT-systemen onder het gemiddelde (een 2 of lager). Er kan zelfs geconcludeerd worden dat 4 op 10 Seveso-bedrijven geen of beperkt maatregelen heeft geïmplementeerd op dit gebied. Daarbij lijkt er een positieve correlatie te zijn tussen cybervolwassenheid en de omvang van een bedrijf (Fox-IT, 2021).

Deze tendens wordt ook bevestigd in het interview met Bosch:

‘’Grote internationale ondernemingen hebben vaak wel een IT-afdeling. Maar onder de Seveso-regeling vallen ook kleinere ondernemingen die geen dergelijke afdeling hebben en waar IT dus weinig aandacht krijgt. Het is goed om daar bewust van te zijn en de inspectie daarop in te richten.’’

2.4 Conclusies

De volgende conclusies kunnen getrokken worden:

- Voorheen waren brandbeveiligingssystemen, waaronder repressieve mechanismen, bekabelde systemen met een eigen besloten netwerk. De betrokkenheid bij een cyberaanval is daarmee minder voor de hand liggend. Echter begint niet elke cyberaanval daar waar een internetverbinding is. Wanneer een kwaadwillend persoon fysiek toegang kan krijgen tot het bedrijf of een medewerker kan manipuleren, is een cyberaanval alsnog mogelijk.
- De ‘slimme’ brandbeveiliging is steeds meer in opkomst. Dat wil zeggen dat brandbeveiligingssystemen, waaronder repressieve mechanismen, steeds meer gebruik maken van het IoT, AI en de Cloud. Ook worden deze systemen steeds vaker geïntegreerd met andere gebouwbeheerssystemen die vaak ook verbonden zijn met het internet. Als deze trend doorzet in de brandbeveiliging wordt de betrokkenheid van repressieve mechanismen bij een cyberaanval meer voor de hand liggend.
- Tegelijkertijd blijft de cybervolwassenheid van de industrie, en dus risico-relevante bedrijven, achter. De kleinere bedrijven zonder ervaring met een cyberaanval, hebben vaak nog geen IT-specialisten in huis. Als dit wel het geval is, dan hebben deze IT-specialisten niet altijd voldoende kennis van gebouwbeheerssystemen, brandbeveiligingssystemen en OT-systemen om deze te beschermen tegen een cyberaanval. Een goede samenwerking tussen IT- en OT-teams is ook niet altijd gegarandeerd door een gebrek aan gedeelde beveiligingsstandaarden en beslissingsprotocollen.

3. De aantrekkelijkheid van een cyberaanval op repressieve mechanismen

De aantrekkelijkheid van een brandbeveiligingssysteem als doelwit van een cyberaanval wordt vergroot door de trend dat deze steeds vaker verbonden is met het internet (zie paragraaf 2.2) en tegelijkertijd door het achterblijven van het bewustzijn over de cyberrisico's en het niet nemen van veiligheidsmaatregelen (zie paragraaf 2.4). De vraag is of een risico-relevant bedrijf, de industrie, specifieke kenmerken heeft die de aantrekkelijkheid van een cyberaanval op een brandbeveiligingssysteem vergroten.

3.1 Recente cyberaanvallen binnen de industrie

De maakindustrie lijkt (waaronder risico-relevante bedrijven) in het bijzonder een aantrekkelijk doelwit voor cyberaanvallen door de complexe en onderling verbonden aard. De sector is afhankelijk van talrijke factoren zoals technologie, grondstoffen en transport. Het stilleggen van processen in één deel van de keten kan leiden tot tekorten die zich mogelijk over de hele wereld kunnen verspreiden. Daarmee is de procesindustrie een aantrekkelijk doelwit voor cybercriminelen die uit zijn op maatschappelijke ontwrichting. Daarnaast is er een lagere tolerantie voor een leveringsstop, omdat dit direct leidt tot grote verstoringen van de bedrijfsvoering van afnemers. Door een cyberaanval kunnen producttekorten ontstaan die ertoe kunnen leiden dat afnemers van leverancier wisselen. Door imagoschade is de kans klein dat deze afnemers in de toekomst weer terug zullen komen. Het verlies van klanten zal, samen met de onderzoeks- en herstelkosten van een cyberaanval, vaak leiden tot faillissement. Dit geeft de concurrentie een betere marktpositie. Ook beschikt de procesindustrie vaak over waardevolle intellectuele eigendommen, die opgeslagen zijn in kwetsbare verouderde databases. Het kan de concurrentie veel tijd en geld besparen als ze deze eigendommen in handen krijgen (KnowBe4, 2024).

Schneider Electric (2024)
In november 2024 werd Schneider Electric, een bedrijf dat machines en systemen maakt voor fabrieken, slachtoffer van een cyberaanval. De aanval richtte zich op een systeem voor projectmanagement. De hacker stal 40 gigabyte aan bedrijfsgegevens. De hacker probeerde Schneider Electric onder druk te zetten om $125.000 te betalen. Bij ontvangst van dit bedrag zou de hacker de gegevens niet delen. Het bedrijf ontdekte de aanval toen de hacker aankondigde dat hij toegang had tot hun data.

De recente berichtgevingen over en onderzoeken naar cyberaanvallen in de industrie geven dan ook een gezamenlijk beeld; het aantal aanvallen neemt toe. Kaspersky, een internationale dienstverlener op het gebied van cyberbeveiliging, heeft in augustus 2024 een uitgebreide enquête gehouden onder 203 industriële organisaties in sectoren als energie, productie en olie en gas in Nederland, België en het Verenigd Koninkrijk. Uit onderzoek van Kaspersky blijkt dat bijna 95% van de industriële organisaties een cybersecurity-incident heeft gehad in de afgelopen twaalf maanden. Maar liefst 29% van de organisaties heeft in het afgelopen jaar één keer te maken gehad met een cyberaanval dat resulteerde in operationele downtime. Bijna twee derde (59%) heeft twee of drie keer hier mee te maken gehad en 12% vier of vijf keer (Maakindustrie Nieuws, 2024). De IBM Corporation heeft in 2024 een 'Threat Intelligence Index' gepubliceerd met 2023 als analysejaar. Daarin is de lezen dat de maakindustrie in de top 10 (25,7% van alle cyberaanvallen) staat van sectoren die het vaakst een cyberaanval hebben meegemaakt (IBM, 2024).

LitePuter (2025)
In januari 2025 werd Liteputer, een maakindustrie-fabrikant van verlichtingstechnologie in Taiwan, slachtoffer van een cyberaanval. De hackersgroep Ransomhub pleegde een ransomware-aanval op LitePuter.
De hackers versleutelden bedrijfsgegevens en eisten losgeld. Het doel van de aanval was hiermee dus financiële winst. De aanval richtte zich op de computernetwerken van het bedrijf. LitePuter ontdekte het probleem toen systemen niet meer werkten en schakelde direct IT-specialisten in. Ze besloten het losgeld niet te betalen en herstelden hun gegevens via back-ups. Vervolgens verbeterden ze hun beveiliging om toekomstige aanvallen te voorkomen.

Waterfall Security Solutions, een globale dienstverlener op het gebied van industriële cyberveiligheid, publiceert elk jaar een ‘dreigingsrapport’ met een wereldwijde analyse van cyberaanvallen in de industrie. Daarbij kijken ze voornamelijk naar cyberaanvallen waarbij OT-systemen betrokken waren en leidde tot fysieke gevolgen zoals productiestoringen, schade aan apparatuur, milieurampen of slachtoffers (dus niet alleen diefstal van gevoelige informatie of het buiten gebruik stellen van IT-systemen). Het rapport van 2024 (met 2023 als analysejaar) laat zien dat sinds 2020 het aantal cyberaanvallen op OT-omgeving per jaar hard stijgt. In 2023 zijn er 68 cyberaanvallen bekend die de OT-omgeving van meer dan 500 fysieke locaties hebben getroffen. Dit is een stijging van 19% ten opzichte van het voorgaande jaar. Op basis van dit verloop voorspellen ze dat in 2024 maar liefst 100 dergelijke cyberaanvallen zullen plaatsvinden (Waterfall Security Solutions, 2024).

Voorbeeld Colonial Pipeline (2024)
In mei 2021 werd Colonial Pipeline, een van de grootste brandstofpijpleidingen in de Verenigde Staten, getroffen door een ransomware-aanval uitgevoerd door de hackersgroep DarkSide. De aanval leidde tot een tijdelijke stillegging van de pijpleiding, wat resulteerde in brandstoftekorten en prijsstijgingen aan de oostkust van de VS. De aanvallers infiltreerden de IT-systemen van Colonial Pipeline en versleutelden kritieke gegevens, waardoor het bedrijf gedwongen werd de operaties stop te zetten om verdere schade te voorkomen. De hackers eisten losgeld in ruil voor het ontsleutelen van de gegevens. Hiermee was het directe doel dus financieel gewin. Ze richtten zich op de IT-infrastructuur van het bedrijf om maximale impact te bereiken. Colonial Pipeline ontdekte de aanval toen hun systemen werden versleuteld en onbruikbaar werden, wat leidde tot de beslissing om de pijpleiding stil te leggen. Als reactie op de aanval schakelde Colonial Pipeline cybersecurity-experts en autoriteiten in om de situatie te beoordelen en te beheren. Het bedrijf betaalde uiteindelijk het geëiste losgeld om de systemen te herstellen en nam aanvullende maatregelen om de beveiliging te verbeteren en toekomstige aanvallen te voorkomen.

Palo Alto Networks, een globale dienstverlener in cyberbeveiliging, heeft in december 2023 een wereldwijde vragenlijst uitgezet bij bedrijven met een OT-omgeving. Bijna 1.980 respondenten hebben de vragenlijst ingevuld. Daaruit blijkt dat 76% van de respondenten een cyberaanval heeft meegemaakt op hun OT-omgeving. Daarvan zegt 65% dat ze vierjaarlijks of maandelijks een cyberaanval op hun OT-systemen meemaken. Dus 35% maakt cyberaanvallen mee met nog een hogere frequentie (Palo Alto Netwerks & ABI Research, 2023).

3.2 Type cyberaanvallen binnen de industrie

In het ‘dreigingsrapport’ van Waterfall Security Solutions is verder te lezen dat 25% van de cyberaanvallen, waarvan het aanvalsplan bekend is, als direct doel had om impact te maken op een OT-systeem. Het overige aantal cyberaanvallen veroorzaakte een, bedoeld of onbedoeld, indirect gevolg op een OT-systeem. Bijvoorbeeld omdat het bedrijf in geval van een cyberaanval op een IT-systeem voor de zekerheid OT-systemen stillegt. Een andere reden kan zijn dat de continuïteit van de OT-systemen van het bedrijf afhankelijk is van de IT-systemen die slachtoffer zijn geworden van een cyberaanval. Tot slot kan het zijn dat een leverancier van het bedrijf slachtoffer is geworden van een cyberaanval waardoor de productie van het bedrijf staakt (Waterfall Security Solutions, 2024). Het onderzoek van Palo Alto Networks laat eenzelfde tendens zien. Daaruit kwam naar boven dat 28% van de cyberaanvallen direct gericht was op de OT-omgeving en in 72% van de gevallen, waar de OT-omgeving werd geraakt, was dit het gevolg van een cyberaanval op de IT-omgeving (Palo Alto Netwerks & ABI Research, 2023).

Ransomware-aanvallen blijken elk jaar weer het grootste aandeel te hebben. In 80% van de aanvallen in 2023, waarvan bekend is wat de oorzaak is, ging het om een ransomware-aanval en in 10% van de gevallen ging het om hacktivisme. Het aantal cyberaanvallen door hacktivisten lijkt jaar in jaar uit stabiel te blijven. Hacktivisme is alsnog noemenswaardig, omdat het doel over het algemeen is om opzettelijk fysieke gevolgen teweeg te brengen om een politiek statement te maken. Bij een ransomware-aanval wordt nog vaak geclaimd dat dit niet het doel is, en dat het vooral draait om financieel gewin. In de dataset van 2023 is ook voor het eerst sinds jaren een cyberaanval naar boven gekomen die door een statelijke actor is geïnitieerd (Waterfall Security Solutions, 2024). Uit het onderzoek van de IBM Corporation komt naar voren dat bij 43% van alle cyberaanvallen sprake was van malware, waarvan 20% ransomware betrof en daarmee ook in dit onderzoek het grootste aandeel blijkt te hebben (IBM, 2024).

Malware is een overkoepelende term voor inbraaksoftware die apparaten uitbuit ten koste van de gebruiker en ten behoeve van de aanvaller. Er zijn verschillende soorten malware, maar ze gebruiken allemaal technieken die niet alleen ontworpen zijn om gebruikers te misleiden, maar ook om beveiligingsmaatregelen te omzeilen om zichzelf heimelijk en zonder toestemming op een systeem of apparaat te installeren. Ransomware is een vorm van malware. Ransomware is afpersingssoftware die apparaten of bestanden kan vergrendelen om vervolgens losgeld te eisen voor het vrijgeven ervan.

3.3 Conclusies

De volgende conclusies kunnen getrokken worden:

- De industriële sector is een aantrekkelijk doelwit, cyberaanvallen nemen toe en zijn niet alleen meer gericht op IT-systemen maar ook steeds vaker op OT-systemen. De geraadpleegde onderzoeken zeggen weinig over de betrokkenheid van brandbeveiligingssystemen bij cyberaanvallen.
- Het motief bij het overgrote deel van de cyberaanvallen is momenteel financieel gewin, waarvoor gebruik wordt gemaakt van ransomware. Voor cybercriminelen worden OT-systemen (machines, computersystemen, hardware) steeds aantrekkelijker, om de grote impact die ze met het stilleggen ervan kunnen creëren. De bereidheid om losgeld te betalen is daarom waarschijnlijk groter. Een brandbeveiligingssystemen is daarmee geen voor de hand liggend doelwit, want het saboteren van een

brandbeveiligingssysteem heeft in de eerste instantie geen grote gevolgen voor de bedrijfscontinuïteit.

- Andere motieven van een cyberaanval kunnen zijn het versterken van de concurrentiepositie of het creëren van maatschappelijke ontwrichting (eventueel met slachtoffers) vanuit een bepaalde ideologie (politiek, sociaal, milieu, religieus). Hierbij lijkt een brandveiligheidssysteem ook niet het meest voor de hand liggende doelwit. Met een cyberaanval op andere systemen (IT-systemen, OT-systemen, stroomvoorzieningen, etc.) kan een veel groter effect worden bewerkstelligd.
- Het is niet uit te sluiten dat brandbeveiligingssystemen indirect betrokken raken bij cyberaanvallen met een ander doelwit, ook gezien de trend dat brandbeveiligingssystemen steeds vaker gebruik maken van IoT, AI en de Cloud en geïntegreerd zijn met andere gebouwbeheerssystemen met een internetverbinding.

4. Denkbare scenario's met betrokkenheid van repressieve mechanismen

4.1 Scenario's vanuit de literatuur en interviews

In de literatuur en de interviews komen een paar motieven naar voren waarbij brandbeveiligingssystemen wel als direct doelwit gebruikt kunnen worden:

Als digitale toegangsdeur
Cybercriminelen kunnen brandbeveiligingssystemen gebruiken als achterdeur naar grotere bedrijfsnetwerken. Als de hacker eenmaal binnen is, hoeft hij alleen maar de digitale paden te volgen die systemen met elkaar verbinden om de cruciale databases te bereiken. Als hij de verdediging van de databases kan doorbreken, kan hij waardevolle informatie stelen of versleutelen om vervolgens losgeld te eisen (Roman, J., 2023). Dit hoeft echter verder geen effect op het functioneren van het brandbeveiligingssysteem te hebben.

Als fysieke toegangsdeur
Cybercriminelen kunnen brandbeveiligingssystemen ook vergrendelen of manipuleren. Het activeren van een brandalarm kan, via de brandmeldinstallatie, onbewaakte nooddeuren openen om kwaadwillige personen toegang te verlenen (Roman, J., 2023). Het openen van nooddeuren is onwenselijk als het geen crisissituatie is, maar het heeft geen effect op het functioneren van het brandbeveiligingssysteem.

Als afleidingsstrategie
Cybercriminelen kunnen ook het brandalarm activeren om personen van een bepaalde plek weg te lokken, zodat onbevoegden daarmee ongezien het gebouw kunnen binnengaan (SFPE, 2021). In het interview met Bosch wordt nog een ander motief genoemd:

''Cybercriminelen zouden op vijf verschillende plekken het brandalarm kunnen activeren, om hulpdiensten weg te lokken en bezig te houden. Op een zesde plek kunnen ze vervolgens een gevaarlijke situatie creëren, terwijl de inzet van hulpdiensten enorm vertraagd zal zijn''.

Als concurrentiestrategie
In het interview met InnoVfoam wordt het volgende motief genoemd om een brandbeveiligingssysteem te saboteren:

''Cybercriminelen zouden een blusinstallatie kunnen activeren om de bedrijfscontinuïteit te saboteren. Het blusschuim zal productieprocessen stil kunnen leggen en goederen kunnen beschadigen. Dit verbetert de concurrentiepositie van andere bedrijven''.

Als maximalisatiestrategie
Cybercriminelen zouden ook brandalarmen buiten werken kunnen zetten, om te voorkomen dat een brand wordt gedetecteerd en gealarmeerd (FPRF, 2021).

4.2 Scenario's op basis van logische redenering

De onderstaande scenario's zijn opgesteld op basis van de documentenstudie en interviews, en dus op basis van de conclusies uit hoofdstuk 2 en 3. Deze scenario's zijn voornamelijk opgesteld met bewustwording als doel, en niet om een kwantitatieve inschatting van de kans van een cyberaanval of de waarschijnlijkheid van het effect te geven.

4.2.1 Scenario Concurrentie

Scenario: Concurrentie	
Het productiebedrijf BioChemTech, gespecialiseerd in de vervaardiging van biochemische stoffen, heeft recent zijn veiligheidsmechanismen geïntegreerd met slimme technologieën zoals IoT-apparaten en AI-gestuurde controlesystemen. Het bedrijf maakt gebruik van een geavanceerd gebouwbeheersysteem (GBS) dat branddetectie, toegangscontrole en productieoverzicht combineert.	
Hoe is de cyberaanval verlopen?	
Voorbereiding	De cyberaanval begon met een uitgebreide voorbereidende fase waarin de aanvallers verschillende methoden toepasten om toegang te verkrijgen tot het GBS van BioChemTech. Ze voerden geautomatiseerde scans uit om kwetsbare IoT-apparaten te identificeren die verbonden waren met het internet. Parallel hieraan stuurden ze phishingmails naar systeembeheerders, vermomd als betrouwbare communicatie van leveranciers. Dit resulteerde in het verkrijgen van inloggegevens voor het beheerplatform van het GBS. Bovendien infiltreerden ze de toeleveringsketen door malafide software te introduceren in een update van een externe leverancier van de blusinstallatie. Deze gecombineerde aanpak zorgde voor een solide basis voor de geplande sabotage.
Uitvoering	De uitvoering van de aanval verliep snel en effectief. De aanvallers manipuleerden meldingen binnen de brandmeldinstallatie, waardoor essentiële brandblusmechanismen werden gedeactiveerd. Tegelijkertijd activeerden ze meerdere alarmsystemen tegelijkertijd, wat leidde tot een stroomstoring en een verstoring van de normale werking van alle mechanische systemen in het gebouw. Een ander cruciaal onderdeel van de aanval was de sabotage van vloeistofkerende deuren via het GBS, waardoor chemische lekkages zich ongecontroleerd konden verspreiden in het gebouw. Deze acties veroorzaakten een ernstige crisis en maakten directe interventie noodzakelijk.
Herstel	Na de aanval begon BioChemTech aan een intensief herstelproces. IT-teams en externe experts voerden een forensisch onderzoek uit, waarbij werd vastgesteld dat meerdere IoT-apparaten waren gehackt via onveilige software-updates. Dit onderzoek leidde tot een grondige her-configuratie van het GBS en het herstellen van fysieke controlesystemen. Het herstelproces vereiste aanzienlijke investeringen in tijd en middelen, met als doel de operationele capaciteit en de beveiliging van het bedrijf volledig te herstellen.
Wat waren de gevolgen?	
Financieel	• Kosten voor herstel en beveiligingsverbeteringen • Contractuele boetes door vertraagde leveringen en schadeclaims van klanten
Operationeel	• Stillegging van de productie gedurende zes weken • Vertragingen in de levering van biochemische producten
Reputatie	• Aanzienlijke schade aan het vertrouwen van klanten en investeerders • Negatieve media-aandacht
Waardoor was de cyberaanval mogelijk?	
1	Kwetsbare IoT-apparaten: Onveilige configuratie en gebruik van standaard wachtwoorden.

2	Gebrekkige segmentatie: Het GBS was niet gescheiden van andere bedrijfsnetwerken.
3	Social engineering: Onvoldoende bewustzijn bij medewerkers.
Welke repressieve mechanismen hebben bij kunnen dragen?	
1	Brandmeldinstallatie: Valse signalen geïnitieerd door de aanvallers
2	Blusinstallatie: Sabotage via een gecompromitteerde update
3	Vloeistofkerende deuren: Manipulatie van de open/dicht-functionaliteit

4.2.2 Scenario Losgeld

Scenario: Losgeld	
Het internationale productiebedrijf Metalworks Inc. produceert hoogwaardige componenten voor de auto-industrie. Het bedrijf maakt gebruik van een hybride infrastructuur van IT- en OT-systemen om zowel administratieve als productieprocessen te beheren. Deze systemen zijn fysiek gescheiden, maar data afhankelijkheden zoals ERP(Enterprise Resource Planning) integraties maken het bedrijf kwetsbaar voor cyberaanvallen.	
Hoe is de cyberaanval verlopen?	
Voorbereiding	Een medewerker van de financiële afdeling ontvangt een phishingmail, schijnbaar afkomstig van een vertrouwde leverancier, met de vraag een bijlage te openen. De bijlage bevat een schadelijke macro die een backdoor installeert. Hiermee verkrijgen de aanvallers beperkte toegang tot het IT-netwerk. Met de toegang identificeren en stelen ze inloggegevens. Met de gegevens en kennis van het systeem breiden ze hun controle uit naar het ERP-systeem. Met de toegang tot het ERP-systeem detecteren ze de zwakke punten in het systeem waardoor het mogelijk is om belangrijke bedrijfsgegevens, zoals order- en klantinformatie, met ransomware te versleutelen. Nu begint op de achtergrond het versleutelingsproces op de back-up.
Uitvoering	Op een vrijdag op het einde van de werkdag worden de verschillende actieve databronnen versleuteld. Op maandag treffen de eerste medewerkers een pop-up op hun scherm met de boodschap dat de data versleuteld is en dat er losgeld wordt geëist. De aanvallers eisen $1,5 miljoen losgeld. Meteen wordt er een escalatie uitgevoerd richting de directie en de IT-afdeling. De standaardmethodes om een back-up terug te zetten worden geprobeerd, maar de data is ook versleuteld. Een groot voordeel van het IT-landschap van MetalWorks is dat door de strikte segmentatie tussen OT en IT, het OT-landschap ongeschonden blijft. Dit betekent dat het productieproces door kan gaan. De aansturing en verwerking van de productie ligt wel plat omdat dit normaal via het ERP-systeem loopt. Dit leidt tot vertragingen in leveringen, contractbreuken en stilstaande productie bij enkele klanten die afhankelijk zijn van MetalWorks.
Herstel	Na intensief overleg besluit MetalWorks geen losgeld te betalen. Het herstelproces begint met het opnieuw op bouwen van de data inclusief het ERP-systeem en de herstructurering van de IT-systemen. Dit proces is zeer uitgebreid en tijdrovend, met wekenlange verstoringen in de administratieve en logistieke processen. Gedurende deze periode verliest het bedrijf opdrachten en wordt het geconfronteerd met boetes van klanten. Na drie weken worden de kritieke IT-systemen hersteld, maar het duurt maanden voordat de bedrijfsefficiëntie terug op het oude niveau is. Ondertussen blijft MetalWorks kampen met aanzienlijke reputatieschade: belangrijke klanten hebben langdurige contracten beëindigd en het vertrouwen in de betrouwbaarheid van het bedrijf is geschaad.
Wat waren de gevolgen?	
Financieel	• Directe kosten van IT-herstel en veiligheidsaudits • Verlies van inkomsten door productieverlies

	• Klantenclaims
Operationeel	• Vertragingen in de leveringen • Werkonderbrekingen • Herstructurering ICT en organisatie
Reputatie	• Het vertrouwen van klanten • Het vertrouwen van mogelijke aandeelhouders
Waardoor was de cyberaanval mogelijk?	
1	IT-aanval via phishing: Een enkele menselijke fout leidde tot grootschalige toegang voor de aanvallers.
2	Gebrek aan snelle detectie: De aanval werd pas opgemerkt nadat systemen al waren versleuteld.
3	Afhankelijkheid van IT binnen bedrijfsprocessen: Hoewel de OT-systemen operationeel bleven, was de afhankelijkheid van IT voor logistiek en administratie een kritieke zwakte binnen het ICT-landschap.

4.2.2 Scenario Milieu-extremisten

Scenario: Milieu-extremisme	
Een Seveso-olieraffinaderij genaamd OilTech, bekend om haar grootschalige opslag en verwerking van gevaarlijke stoffen, wordt het doelwit van een langdurige geplande cyberaanval door milieu-extremisten. Het doel is niet alleen verstoring van productieprocessen, maar ook het veroorzaken van wantrouwen in de betrouwbaarheid van het bedrijf.	
Hoe is de cyberaanval verlopen?	
Voorbereiding	De aanvallers starten met een uitgebreide fase van verkenning en initiële toegang (+/- 6 maanden): • Phishing en social engineering: Medewerkers, voornamelijk uit administratieve en IT-afdelingen, ontvangen overtuigende phishing-e-mails, zogenaamd afkomstig van interne afdelingen of vertrouwde leveranciers. Dit leidt tot een handvol compromitteringen, waarbij inloggegevens voor systemen zoals mailservers en HR-portals worden buitgemaakt. • Reconnaissance: Met beperkte toegang beginnen de aanvallers aan het verkennen van de netwerkstructuur. Ze identificeren zwakheden in informatiestromen tussen IT en OT, waaronder zwak beveiligde API's en monitoringtools. • Infiltratie van leverancierssketens: De aanvallers richten zich op derden die diensten leveren, zoals onderhoudssoftware of logistieke systemen. Ze plaatsen malware in updates, waardoor indirecte toegang tot de OT-systemen van de raffinaderij wordt verkregen. • Manipulatie van informatiestromen: Geleidelijk beginnen de aanvallers valse gegevens in rapportagesystemen in te voegen. Productiecijfers, voorraadstatus en operationele waarschuwingen worden subtiel gewijzigd, zonder directe schade aan apparatuur te veroorzaken.
Uitvoering	Met hun bestaande toegang starten de aanvallers met een meer agressieve verstoringscampagne (+/- 1 maand): • Verstoring van IT-systemen: De aanvallers blokkeren essentiële bedrijfsprocessen door middel van DDoS-aanvallen gericht op externe portals, zoals leveranciersportals en transportbeheerplatforms. Dit vertraagt de logistiek en veroorzaakt chaos in de planning. • Kantoorpersoneel kan niet meer werken omdat de systemen traag of helemaal niet meer werken. • Manipulatie van OT-monitoring: Door toegang te benutten tot systemen die IT- en OT-gegevens synchroniseren, veranderen de aanvallers parameters in procesrapportages. Operators zien bijvoorbeeld schijnbaar normale waarden terwijl kritieke alarmen onopgemerkt blijven. Dit verstoort de productie en de logistieke data waardoor laad en los systemen ervoor zorgen dat er te veel of juist te weinig geladen of gelost wordt. • Desinformatiecampagne: Door valse waarschuwingen in en extern te creëren, dwingen de aanvallers het management om delen van de raffinaderij proactief stil te leggen vanwege vermeende

	veiligheidsproblemen. De waarschuwingen komen ook in de systemen van de veiligheidsregio's en toezichthoudende instanties naar voren.
Herstel	De raffinaderij besluit productieprocessen stil te leggen nadat meerdere kritieke incidenten en tegenstrijdige meldingen van systemen tot onzekerheid leiden over de veiligheid. In deze fase (+/- 2 maanden): • Forensisch onderzoek: Interne teams en externe cybersecurity-experts analyseren de omvang van de inbreuk. Ze ontdekken dat de aanvallers geen volledige toegang tot OT hebben gehad, maar wel de betrouwbaarheid van kritieke rapportages hebben ondermijnd. • Incidentbeheersing: Alle systemen worden opnieuw opgebouwd vanuit schone back-ups, wat weken in beslag neemt.
Wat waren de gevolgen?	
Financieel	• Directe kosten van IT-herstel en veiligheidsaudits. • Verlies van inkomsten door productieonderbrekingen. • Mogelijke boetes vanwege niet-naleving van de Seveso-richtlijn.
Operationeel	• Vertragingen in de levering van olieproducten. • Stillegging van enkele faciliteiten als voorzorgsmaatregel.
Reputatie	• Het vertrouwen van klanten en regelgevende instanties wordt geschaad. • De raffinaderij moet aanzienlijke investeringen doen om het vertrouwen te herstellen.
Waardoor was de cyberaanval mogelijk?	
1	Onvoldoende segmentatie: Hoewel OT gescheiden was van IT, waren bepaalde interfaces onvoldoende beveiligd.
2	Beperkte monitoring: Afwijkend gedrag in informatiestromen werd niet tijdig gedetecteerd.
3	Menselijke factor: Succesvolle phishing-campagnes benadrukken het belang van training en bewustwording.

4.2.3 Scenario Maatschappelijke ontwrichting

<table>
<tr><th colspan="2">Scenario: Maatschappelijke ontwrichting</th></tr>
<tr><td colspan="2">Het jaar is 2025. Nederland functioneert als een belangrijk logistiek en economisch knooppunt in Europa, met de Rotterdamse haven als het kloppende hart. Een vijandige staatsactor, opererend via een schaduworganisatie, heeft als doel de Nederlandse samenleving te ontwrichten. De operatie combineert geavanceerde cyberaanvallen met strategische fysieke infiltratie, gericht op maximale chaos en economische schade.</td></tr>
<tr><th colspan="2">Hoe is de cyberaanval verlopen?</th></tr>
<tr><td rowspan="4">Voorbereiding +/- 5 maanden</td><td>Cyber</td></tr>
<tr><td>• Spear-phishingcampagnes: Medewerkers van havenbedrijven ontvangen gerichte e-mails met onderwerpen zoals douanedocumentatie en HR-updates. Via nepportals worden inloggegevens buitgemaakt.
• Supply-chain-aanvallen: De aanvallers infiltreren kleinere, minder beveiligde leveranciers van IT-diensten in de haven. Via deze kanalen krijgen ze toegang tot kernsystemen.
• Infiltreren van OT-netwerken: Hackers installeren backdoors in systemen die essentiële havenprocessen aansturen, zoals containerverplaatsing en scheepvaartcommunicatie.
• Digitale desinformatie: De aanvallers maken nepaccounts aan op sociale media om paniek en verwarring te kunnen zaaien op het moment van de aanval.</td></tr>
<tr><td>Fysiek</td></tr>
<tr><td>• Strategische plaatsing: Geïnfiltreerde agenten worden geplaatst als tijdelijke werknemers via uitzendbureaus die de haven van arbeidskrachten voorzien. Geïnfiltreerde agenten nemen posities in bij cruciale logistieke knooppunten, zoals terminals en distributiecentra. Ze verzamelen informatie over fysieke veiligheidsprotocollen en kritieke locaties.
• Monitoring met drones: Onopvallende drones worden gebruikt om de bewegingen van beveiligingspersoneel en de fysieke infrastructuur in kaart te brengen. Resultaat: De aanvallers verkrijgen toegang tot IT-systemen én gedetailleerde kennis van fysieke operaties. Kleine storingen worden veroorzaakt om de reacties van beveiligingsteams te testen en veiligheidslekken te identificeren.</td></tr>
<tr><td rowspan="2">Uitvoering +/- 3 dagen</td><td>Dag 1</td></tr>
<tr><td>• IT-systemen voor vrachtbeheer en scheepsbewegingen worden vergrendeld met ransomware. Geen enkel schip kan aanmeren of lossen, en alle logistiek stopt abrupt
• Administratieve systemen van de douane worden stilgelegd met ransomware, wat internationale handel stilzet
• Websites en communicatiesystemen van de haven worden overspoeld met verkeer middels DDoS-aanvallen, waardoor bedrijven en autoriteiten geen informatie kunnen uitwisselen.</td></tr>
</table>

	• Controle over containerkranen wordt tijdelijk overgenomen, waardoor containers op de verkeerde plekken worden verplaatst. • Tankopslagsystemen geven foutieve temperatuur- en drukwaarden weer, wat operators dwingt om processen stil te leggen.
	Dag 2
	• Explosies op terminals: Infiltranten plaatsen kleine explosieve ladingen op terminals. Hoewel de schade beperkt is, veroorzaken de explosies paniek en evacuaties. • Blokkeren van toegangswegen: Vrachtwagens met opzettelijk defecte voertuigen blokkeren belangrijke toevoerwegen naar de haven.
	Dag 3
	• Sociale media worden overspoeld met valse berichten over chemische lekken en explosies in de haven, wat de chaos vergroot. • Lokale en internationale media verspreiden onjuiste informatie, waardoor de indruk ontstaat dat de situatie oncontroleerbaar is.
Herstel	Het Nationaal Cyber Security Centrum (NCSC) en internationale partners worden gemobiliseerd om ransomware te decoderen en geïnfecteerde systemen te isoleren. Dit proces duurt dagen: • Back-ups worden hersteld, maar veel systemen draaien wekenlang op beperkte capaciteit. • De haven schakelt over op handmatige operaties, wat de efficiëntie drastisch verlaagt.
Wat waren de gevolgen?	
Maatschappelijk	• Containers met essentiële goederen blijven wekenlang vastzitten, wat leidt tot tekorten aan voedsel, medicijnen en andere producten. • Door de tijdelijke stillegging van tankopslag en raffinaderijen stijgen brandstofprijzen met tientallen procenten. • Het vertrouwen in de veiligheid en stabiliteit van de haven en de Nederlandse infrastructuur is ernstig beschadigd.
Waardoor was de cyberaanval mogelijk?	
1	Kwetsbaarheden in de supply chain
2	Onbekende EDI's (electronic data interchange) in de keten
3	Ongelimiteerde resources en uitgebreide voorbereiding

5. Aandacht voor cyberrisico's binnen de inspectie

Omdat de veiligheidsregio's al inspecties uitvoeren bij Seveso-bedrijven, die onder de sectoren van de NIS2-richtlijn vallen, kunnen zij mogelijk een rol spelen bij de signalering van cyberrisico's en de bewustwording daarvan bij deze bedrijven. De vraag is in hoeverre er aandacht is voor dergelijke cyberrisico's binnen inspectie-instanties en of het noodzakelijk is dat cyberveiligheid aandacht krijgt binnen de inspectie vanuit de veiligheidsregio. Daarvoor wordt in paragraaf 5.1 gekeken naar de inspectie vanuit de veiligheidsregio en wordt in 5.2 een vergelijking gemaakt met de inspectie vanuit de ILT en RDI.

5.1 Huidige inspectie vanuit de veiligheidsregio

Wetgeving
De inspectie van de veiligheidsregio is gebaseerd op de Seveso-richtlijn en de Wet Veiligheidsregio's.

Inspectie-object
Alle bedrijven die met hun opslag van gevaarlijke stoffen boven de drempelwaarden uit bijlage I van de Seveso-richtlijn komen, worden geïnspecteerd. In Nederland gaat het om zo'n 400 bedrijven. Daarbij wordt onderscheid gemaakt tussen lage en hoge drempelinrichtingen, met elk hun eigen drempelwaarden. Van de 400 Seveso-bedrijven behoren er ongeveer 250 tot de lage drempelinrichtingen en ongeveer 150 tot de hoge drempelinrichtingen. Bedrijven die net onder deze drempelwaarden vallen hoeven dus niet geïnspecteerd te worden. Deze risico-relevante bedrijven krijgen echter wel steeds meer aandacht vanuit verschillende veiligheidsregio's, omdat ongevallen bij deze bedrijven wel degelijk kunnen zorgen voor een substantiële impact op de omgeving.

Inspectie-organisatie
De inspectie van Seveso-bedrijven wordt uitgevoerd door een inspectieteam, samengesteld vanuit verschillende organisaties. Dit team bestaat uit de omgevingsdienst, veiligheidsregio's, de Nederlandse Arbeidsinspectie en soms aanvullende inspecteurs (zoals het waterschap, Rijkswaterstaat en ILT). In een inspectieplan wordt beschreven welke organisatie verantwoordelijk is voor welke specifieke taken en hoe de samenwerking tussen de verschillende organisaties wordt gecoördineerd.

Inspectie-focus
Het doel van de inspectie is om inzichtelijk te krijgen of de effecten van eventuele zware ongevallen zoveel mogelijk beheerst worden met de aanwezigheid van kwalitatieve voorzieningen, zowel preventief als preparatief en zowel technisch als organisatorisch. Tijdens de inspectie wordt er onder andere gekeken naar de opslaglocaties, technische installaties, risicoanalyses, veiligheidsbeheerssystemen- en rapporten, bedrijfsnoodplannen en opleidingen van personeel. In een inspectieprogramma wordt beschreven dat het doel en de scope is van een inspectie.

Inspectie-frequentie
Een hoge drempelinrichting dient minimaal 1 keer per jaar te worden geïnspecteerd en een lage drempelinrichting minimaal 1 keer in de 3 jaar. In de praktijk worden de meeste lage drempelinrichtingen ook 1 keer per jaar geïnspecteerd.

5.2 Toekomstige inspectie vanuit ILT en RDI

Wetgeving
De ILT en RDI zijn bestaande inspectie-instanties die vanuit de huidige Wet beveiliging netwerk- en informatiesystemen (de Nederlandse uitwerking van de Europese NIS1-richtlijn)

bepaalde sectoren al inspecteren op het gebied van cyberbeveiliging. Deze Europese richtlijn is in 2023 vervangen door de NIS2-richtlijn die, ten opzichte van zijn voorganger, een bredere scope heeft. Dit betekent dat hier meer sectoren dan voorheen onder vallen. Dit betekent dit dat hier meer sectoren dan voorheen onder vallen. De NIS2-richtlijn wordt uitgewerkt in de Cyberbeveiligingswet, die in 2025 de huidige Wbni zal vervangen.

Inspectie-object (zie flowchart in bijlage 8.1)
Binnen de NIS2-richtlijn wordt onderscheid gemaakt tussen zeer kritieke sectoren en andere kritieke sectoren. Zeer kritieke sectoren zijn *energie, transport, infrastructuur financiële markt, gezondheidszorg, drinkwater, digitale infrastructuur, afvalwater, overheidsdiensten, ruimtevaart, beheerders van ICT-diensten en het bankwezen.* Andere kritieke sectoren zijn *digitale aanbieders, post- en koeriersdienst, afvalstoffenbeheer, levensmiddelen, chemische stoffen, onderzoek en vervaardiging.* Vervolgens wordt er binnen een sector onderscheid gemaakt tussen kleine (<50 medewerker en <10 miljoen jaaromzet), middelgrote (50-249 medewerker en >10 miljoen jaaromzet) en grote organisaties (>250 medewerker en >50 miljoen jaaromzet en >43 miljoen balanstotaal). Bij een middelgroot bedrijf is er sprake van een zogenaamde belangrijke entiteit. Bij een groot bedrijf is er sprake van een zogenaamde essentiële entiteit als deze in een zeer kritieke sector valt en is er sprake van een belangrijke entiteit indien deze in een andere kritieke sector val. Bij een kleine organisatie is er enkel sprake van een belangrijke of essentiële entiteit indien dit een aanwijzing van het ministerie is.

De Seveso-bedrijven vallen voornamelijk onder de sectoren *energie, transport, drinkwater, afvalwater, afvalstoffenbeheer* en *chemische stoffen.*

Inspectie-organisatie
De sectoren onder de NIS2-richtlijn worden verdeeld onder verschillende inspectie-instanties, waaronder de ILT en RDI. De ILT is in ieder geval verantwoordelijk voor de inspectie van de sectoren *transport, drinkwater, afvalwater, afvalstoffenbeheer* en *chemische stoffen.* Volgens een eerste inschatting van het ILT zal het gaan om ongeveer 1.850 bedrijven. De RDI is in ieder geval verantwoordelijk voor de inspectie van de sector *energie*. Volgens een eerste inschatting van het RDI zal het gaan om ongeveer 6.000 bedrijven. Er zullen bedrijven zijn die onder meerdere sectoren vallen, waardoor afstemming tussen de verschillende inspectie-instanties belangrijk is. De ILT geeft bijvoorbeeld aan dat ongeveer 150 bedrijven uit de sector *chemische stoffen* ook in de sector *energie* vallen.

Inspectie-focus
Het doel van de inspectie is om de digitale veiligheid van netwerk- en informatiesystemen te waarborgen, vooral in de sectoren die van cruciaal belang zijn voor de maatschappij en de economie. Tijdens de inspectie wordt er onder andere gekeken naar risicomanagement van het bedrijf en de beveiligingsmaatregelen op het gebied van cyber.

Inspectie-frequentie
Het voornemen is om een essentiële entiteit minimaal 1 keer per 3 jaar te inspecteren (proactief) en een belangrijke entiteit wordt enkel naar aanleiding van een melding geïnspecteerd (reactief). Bedrijven die onder de NIS2-richtlijn en dus de Cyberbeveiligingswet vallen, hebben een meldplicht in geval van een significant cyberincident boven een nog vast te stellen drempelwaarde.

5.3 Conclusies

Op basis van de vergelijking tussen de huidige inspectie vanuit de veiligheidsregio en de toekomstige inspecties vanuit de ILT en RDI, kunnen de volgende conclusies worden getrokken:

- Voor de veiligheidsregio is het van belang dat zware ongevallen worden voorkomen en daarom de eventuele cyberrisico's binnen de mechanismen voor de signalering, bestrijding en beheersing van incidenten bij risico-relevante bedrijven tijdig worden gesignaleerd. De inspectie vanuit de ILT en RDI zal een bredere focus hebben en kijken naar de cyberbeveiliging in zijn geheel ten behoeve van de continuïteit van de aangeboden dienst. Het is aan de onderneming om de belangrijke IT en OT te identificeren en te beschermen waarvan de aangeboden dienst afhankelijk is. Het toezicht zal zich vervolgens daarop richten. Het is daarom de vraag of de mechanismen voor de signalering, bestrijding en beheersing van incidenten specifieke aandacht zullen krijgen tijdens de inspectie.
- Er zijn mogelijk een aantal (net-niet) Seveso-bedrijven die als 'klein' worden ingeschaald door de NIS2-richtlijn. Deze bedrijven worden niet geïnspecteerd op het gebied van cyberbeveiliging. Er zijn mogelijk ook een aantal (net-niet) Seveso-bedrijven die als 'belangrijke entiteit' worden ingeschaald door de NIS2-richtlijn. Deze bedrijven worden enkel geïnspecteerd naar aanleiding van een melding van een cyberincident. Eventuele cyberrisico's bij deze (net-niet) Seveso-bedrijven zijn daarmee nauwelijks in beeld.
- De veiligheidsregio inspecteert bedrijven met een hogere frequentie dan de ILT en RDI. De veiligheidsregio inspecteert Seveso-bedrijven 1 keer in het jaar en ILT en RDI inspecteert essentiële entiteiten 1 keer per 3 jaar en belangrijke entiteiten alleen naar aanleiding van een melding. De veiligheidsregio kan eventuele cyberrisico's bij Seveso-bedrijven dus eerder signaleren.
- Met de invoering van de Cyberbeveiligingswet neemt het aantal bedrijven dat door ILT en RDI geïnspecteerd moeten worden substantieel toe. Dit vraagt om een serieuze capaciteitssprong in 2025.

6. Een inspectie-checklist voor veiligheidsregio's

Dit hoofdstuk bevat een tweetal checklists die door de veiligheidsregio gebruikt kan worden bij de inspectie van Seveso-bedrijven, als een veiligheidsregio ervoor kiest om ook aandacht te gaan schenken aan cyberrisico's bij repressieve mechanismen. De checklist onder paragraaf 6.1 kan worden gebruikt om het bewustzijn bij het Seveso-bedrijf in beeld te brengen als het gaat om de risico's en bijhorende wet- en regelgeving. De checklist onder paragraaf 6.1 kan worden gebruikt om de cyberveiligheid (de genomen maatregelen) van de repressieve mechanismen binnen het Seveso-bedrijf inzichtelijk te maken.

6.1 Checklist bewustzijn cyberrisico's

Vraag		Antwoord	Actie inspecteur
1	Is uw organisatie bekend met cyberveiligheid?	Ja/Nee: Ga door naar vraag 2	
2	Valt uw organisatie binnen een (zeer) kritieke sector volgens de NIS2-richtlijn (zie flowchart)?	Ja: Ga door naar vraag 3 Nee: Ga door naar vraag 6	
3	Is uw organisatie een essentiële of belangrijke entiteit volgens de NIS2-richtlijn (zie flowchart)?	Ja: Ga door naar vraag 4 Nee: Ga door naar vraag 6	
4	Heeft uw organisatie zich geregistreerd als NIS2-entiteit bij het NCSC?	Ja: Ga door naar vraag 5 Nee: Instrueer om dit te doen en ga door naar vraag 5	Maak een melding bij ILT / RDI
5	Heeft uw organisatie de zorgplicht (zie infosheet) vanuit de Cyberbeveiligingswet ingevuld?	Ja: Ga door naar vraag 6 Nee: Instrueer om dit te doen en ga door naar vraag 6	Maak een melding bij ILT / RDI
6	Zijn de kansen en motieven voor een cyberaanval binnen uw organisatie in beeld gebracht? Zijn er bijvoorbeeld OT-systemen aan IT-systemen gekoppeld?	Ja: Ga door naar vraag 7 Nee: Instrueer om dit te doen en ga door naar vraag 7	Maak eventueel een melding bij ILT / RDI als het gaat om een belangrijk of essentiële entiteit
7	Zijn er in uw organisatie maatregelen genomen ter beveiliging van deze cyberrisico's (zie checklist onder paragraaf 6.2)?	Ja: Ga door naar vraag 8 Nee: Instrueer om dit te doen en ga door naar vraag 8	Maak eventueel een melding bij ILT / RDI als het gaat om een belangrijk of essentiële entiteit
8	Heeft uw organisatie haar supply-chain goed in beeld en de eventuele bijhorende cyberrisico's?	Ja: Ga door naar vraag 9 Nee: Instrueer om dit te doen en ga door naar vraag 9	Maak eventueel een melding bij ILT / RDI als het gaat om een belangrijk of essentiële entiteit
9	Heeft uw organisatie de bedrijven in deze supply-chain benaderd voor afstemming over de cyberbeveiliging?	Ja: Ga door naar vraag 10 Nee: Instrueer om dit te doen en ga door naar vraag 10	Maak eventueel een melding bij ILT / RDI als het gaat om een belangrijk of essentiële entiteit
10	Heeft uw organisatie eerder een cyberaanval meegemaakt?	Ja: Ga door naar vraag 11 Nee: Einde checklist	

11	Heeft uw organisatie dit gemeld[1] bij uw toezichthouder en het Computer Security Incident Response Team (zie infosheet)?	Ja: Ga door naar vraag 12 Nee: Instrueer om dit te doen en ga door naar vraag 12	Maak een melding bij ILT / RDI als het gaat om een belangrijk of essentiële entiteit
12	Heeft uw organisatie na deze cyberaanval passende maatregelen genomen?	Ja: Einde checklist Nee: Instrueer om dit te doen en dan einde checklist	Maak een melding bij ILT / RDI als het gaat om een belangrijk of essentiële entiteit.

6.2 Checklist cyberveiligheid repressieve mechanismen

	Vraag	Antwoord	Uitleg
1	Zijn er 'slimme' brandmelders die gebruik maken van Wi-Fi of Bluetooth?	Ja / Nee	Dit heeft niet de voorkeur, want het maakt een cyberaanval op de brandmelder mogelijk.
2	Is er een brandmeldinstallatie (BMI) die, al dan niet via een gebouwbeheerssysteem, is verbonden met het internet of een ander netwerk?	Ja / Nee	Dit heeft niet de voorkeur, want het maakt een cyberaanval op de brandmeldinstallatie mogelijk.
3	Wordt er gebruikgemaakt van netwerksegmentatie?	Ja / Nee	Netwerksegmentatie verdeelt het netwerk in kleinere delen, waardoor de kans op verspreiding van een aanval wordt verkleind.
4	Zijn de BMI, de ontruimingsinstallatie en de blusinstallatie voorzien van up-to-date firmware en beveiligingspatches?	Ja / Nee	Houd de firmware up-to-date om beveiligingslekken te dichten. Schakel automatische updates uit als deze het risico vergroten, en plan handmatige updates zorgvuldig.
5	Is er een firewall actief tussen de BMI en het internet of andere netwerken?	Ja / Nee	Maak gebruik van specialistische en updated firewalls om ongeoorloofde toegang te detecteren, registreren en te blokkeren.
6	Is er sprake van Endpoint-beveiliging van apparaten die in verbinding staan met de BMI?	Ja / Nee	Maak gebruik van Endpoint Detection and Response (EDR) en adequate antivirussoftware om computers, servers, IoT apparaten, printers en scanners en netwerkapparatuur te beschermen.
7	Wordt de toegang tot de BMI, de ontruimingsinstallatie en de blusinstallatie gecontroleerd met sterke wachtwoorden en multi-factor authenticatie (MFA)?	Ja / Nee	Volg het principe van "least privilege" en geef niet alle werknemers toegang tot het besturingssysteem van de BMI en blusinstallatie. Dwing het gebruik van complexe wachtwoorden af en

[1] Alleen significante incidenten moeten gemeld worden. De drempelwaarde die een incident significant maakt, moet nog worden bepaald.

			maak gebruik van een door de organisatie beheerde wachtwoordmanager. Vereis MFA voor toegang tot kritieke systemen. Minimaliseer of controleer de toegang van externe partijen, zoals onderhoudsbedrijven. Gebruik encrypted VPN met strikte toegangsregels. Gebruik een bastion host of een jump server als toegangspunt voor onderhoud. Volg het principe van ‘’zero trust’’ en beoordeel elke gebruiker en elk apparaat voordat toegang wordt verleend.
8	Zijn er maatregelen genomen om ongeautoriseerde toegang tot de BMI, de ontruimingsinstallatie en de blusinstallatie via fysieke interfaces te voorkomen?	Ja / Nee	Beperk de fysieke toegang tot de onderdelen van de BMI en ontruimingsinstallatie (bedieningspanelen) en blusinstallatie (opslagsysteem, pompsysteem, verdeelstations, et cetera) door deze te plaatsen in een afgesloten ruimte met toegangscontrole. Zorg voor een algemene en locatie specifieke toegangscontrole van het gehele terrein en gebouwen (waaronder nooddeuren).
9	Wordt gebruik gemaakt van anomaliedetectie bij de BMI, de ontruimingsinstallatie en blusinstallatie?	Ja / Nee	Gebruik Security Information and Event Management (SIEM) voor realtime analyse van verdachte activiteiten (bijv. plotselinge uitschakeling van sensoren).
10	Wordt gebruikt gemaakt van een fail-safe mechanisme voor de BMI, de ontruimingsinstallatie en de blusinstallatie?	Ja / Nee	Zorg dat de BMI en blusinstallatie een "fail-safe" modus heeft, waarbij het systeem in geval van een mankement overgaat naar een veilige staat (bijvoorbeeld automatisch een alarm activeren).
11	Wordt de beveiliging van de BMI, de ontruimingsinstallatie en de blusinstallatie regelmatig getest via penetratietests of kwetsbaarheidsanalyses?	Ja / Nee	Regelmatige tests helpen om kwetsbaarheden op te sporen en te verhelpen voordat ze kunnen worden misbruikt.
12	Zijn de BMI, de ontruimingsinstallatie en de blusinstallatie onderdeel van de reguliere ICT-audit?	Ja / Nee	Tijdens een ICT-audit wordt gecontroleerd of systemen goed beveiligd zijn tegen risico's.
13	Is er een incident response-plan aanwezig voor cyberaanvallen die de BMI, de ontruimingsinstallatie en de blusinstallatie kunnen beïnvloeden?	Ja / Nee	Zorg voor een team dat klaarstaat om te reageren op aanvallen (bijv. een Computer Security Incident Response Team, CSIRT).

			Test dit plan regelmatig door middel van table-top oefeningen of simulaties
14	Wordt het doormeldsysteem naar de meldkamer van de brandweer of particuliere meldkamer beschermd tegen netwerkindringers en is sprake van een back-up?	Ja / Nee	Zorg voor een redundante communicatieverbinding (bijvoorbeeld een secundaire lijn via een andere provider) die automatisch wordt geactiveerd bij een mankement. Test deze back-up verbinding regelmatig.
15	Zijn de betrokken medewerkers getraind in het herkennen en melden van cyberdreigingen?	Ja / Nee	Train personeel in het herkennen van phishing en social engineering-aanvallen. Stel duidelijke protocollen op voor het detecteren en melden van cyberincidenten.
16	Worden ontwikkelingen op het gebied van cyberveiligheid actief gevolgd?	Ja / Nee	Werk samen met leveranciers van systemen als de BMI om op de hoogte te blijven van kwetsbaarheden en beveiligingsupdates. Deel kennis en ervaringen met andere industriële bedrijven en brancheorganisaties. Initieer communicatielijnen met verschillende brancheorganisaties en cybersecurity-organisaties.
17	Is er een proces om nieuwe medewerkers, leveranciers van brandmeldinstallaties en blusinstallatie, en onderhoudsbedrijven te screenen?	Ja / Nee	Screen medewerkers voordat ze in dienst treden, leveranciers voordat er wordt afgenomen en onderhoudsbedrijven (van bijvoorbeeld de blusinstallatie) voordat er contracten worden afgesloten.

7. Verwijzingen

Adlig Safety Consultants. (z.d.). *BowTie*. Opgehaald van adlig.nl: https://www.adlig.nl/bowtie/

Afdeling van het toezicht op de chemische risico's. (2024). *De impact van cyberaanvallen op de preventie van zware ongevallen.* Brussel: Algemene Directie Toezicht op het Welzijn op het Werk.

ASB Security. (z.d.). *Openbaar MeldSysteem (OMS dienstverlening)*. Opgehaald van abs.nl: https://asb.nl/diensten/openbaar-meldsysteem-doormelding/

Brady. (z.d.). *Inleiding over IT/OT-convergentie 101*. Opgehaald van brasy.nl: https://www.brady.nl/intelligente-productie/traceren-van-assets-met-rfid#:~:text=Eenvoudig%20gezegd%20is%20IT%2FOT,van%20elk%20systeem%20te%20begrijpen.

Brandpreventiewinkel. (z.d.). *Wifi rookmelder, Smart rookmelder, RF rookmelder of koppelbare rookmelder?* Opgehaald van brandpreventiewinkel.nl: https://www.brandpreventiewinkel.nl/blog/wifi-rookmelder-smart-rookmelder-rf-rookmelder-of-koppelbare-rookmelder/

ELRO. (z.d.). *Hoe werkt een rookmelder?* Opgehaald van elro.eu: https://www.elro.eu/nl/advies/brandbeveiliging-advies/alles-over-rookmelders/werking-rookmelder

EPM. (z.d.). *Brandmeldinstallatie (BMI) uitgelegd*. Opgehaald van epm.nl: https://epm.nl/brandmeldinstallatie-bmi-uitgelegd/

Fox-IT. (2021). *Eindrapportage Cybervolwassenheidsonderzoek.* Schiedam: DCMR.

FPRF. (2021). *Cybersecurity for Fire Protection Systems.* Virginia: National Fire Protection Association.

IBM. (2024). *X-Force Threat Intelligence Index .* New York: IBM Corporation.

Industrial Automation. (2024). *Cybersecurity in de industrie: Wat betekent de NIS2-richtlijn voor jouw bedrijf?* Opgehaald van industrialautomation.nl: https://www.industrialautomation.nl/control-network/cybersecurity-in-de-industrie-wat-betekent-de-nis2-richtlijn-voor-jouw-bedrijf/

Kiwa. (2021). *Cyberveiligheid brandbeveiligingssystemen vraagt om compliance- en risicogebaseerde aanpak*. Opgehaald van kiwa.com: https://www.kiwa.com/nl/nl/themas/cyber-security/nieuws/cyberveiligheid-brandbeveiligingssystemen-vraagt-om-compliance-en-risicogebaseerde-aanpak/

KnowBe4. (2024). *Manufacturing: Maintaining Stability as Cyber Threats Explode in Volume and Sophistication.* Clearwater: KnowBe4.

Kort, A. de. (2020, november 3). Draadloze brandmeld- en ontruimingsalarminstallaties: meer noodzaak dan oplossing. *Brandveilig.com magazine*, p. 52.

Larsen & Krotofil. (2015). *Rocking the pocket book: Hacking chemical plants for competition and extortion.* Hamburg: Hamburg University of Technology.

Maakindustrie Nieuws. (2024). *Bijna 95% van de organisaties in de industriële sector is het afgelopen jaar getroffen door cyberaanvallen*. Opgehaald van maakindustrie.nl: https://www.maakindustrie.nl/nieuws/algemeen/bijna-95-van-de-organisaties-in-de-industriele-sector-is-het-afgelopen-jaar-getroffen-door-cyberaanvallen/

Masset. (2023). *De laatste ontwikkelingen in de brandbeveiliging*. Opgehaald van masset.nl: https://www.masset.nl/kennisbank/brandbeveiliging/de-laatste-ontwikkelingen-in-de-brandbeveiliging/

Palo Alto Netwerks & ABI Research. (2023). *The state of OT security: A comprehensive guide to trends, risks & cyber resilience.* New York: ABI Research.

Roman, J. (2023). *Weak Spots: High-tech building and fire systems offer a wealth of benefits, but they are also becoming targets for cybercriminals. What can we do to harden these vulnerable systems?* Opgehaald van nfpa.org: https://www.nfpa.org/news-blogs-and-articles/nfpa-journal/2023/03/09/cybersecurity

rookmelderwereld. (z.d.). *Beschrijving hittemelder*. Opgehaald van rookmelderwereld.nl: https://www.rookmelderwereld.nl/product/aritech-dt654-hittemelder/?srsltid=AfmBOoqIhZpXJT9Jg296NK99rXO8XETGauBN14AjJsJblBWC3pBU9bsC

SFPE. (2021). *Cybersecurity for Fire Protection Systems*. Opgehaald van sfpe.org: https://www.sfpe.org/publications/periodicals/sfpeeuropedigital/sfpeeurope22/europeissue22feature5?_zs=P3a2k1&_zl=178n7

Somati Systems. (z.d.). *Vlamdetectie*. Opgehaald van somatisystems.com: https://www.somatisystems.com/systemen/vlamdetectie/#:~:text=Een%20vlamdetectiesysteem%20of%20vlammenmelder%20bestaat,treedt%20het%20alarm%20in%20werking.

Technology Review. (2015). *How to Damage a Chemical Plant over the Internet*. Opgehaald van technologyreview.com: https://www.technologyreview.com/2015/08/07/166807/how-to-damage-a-chemical-plant-over-the-internet/

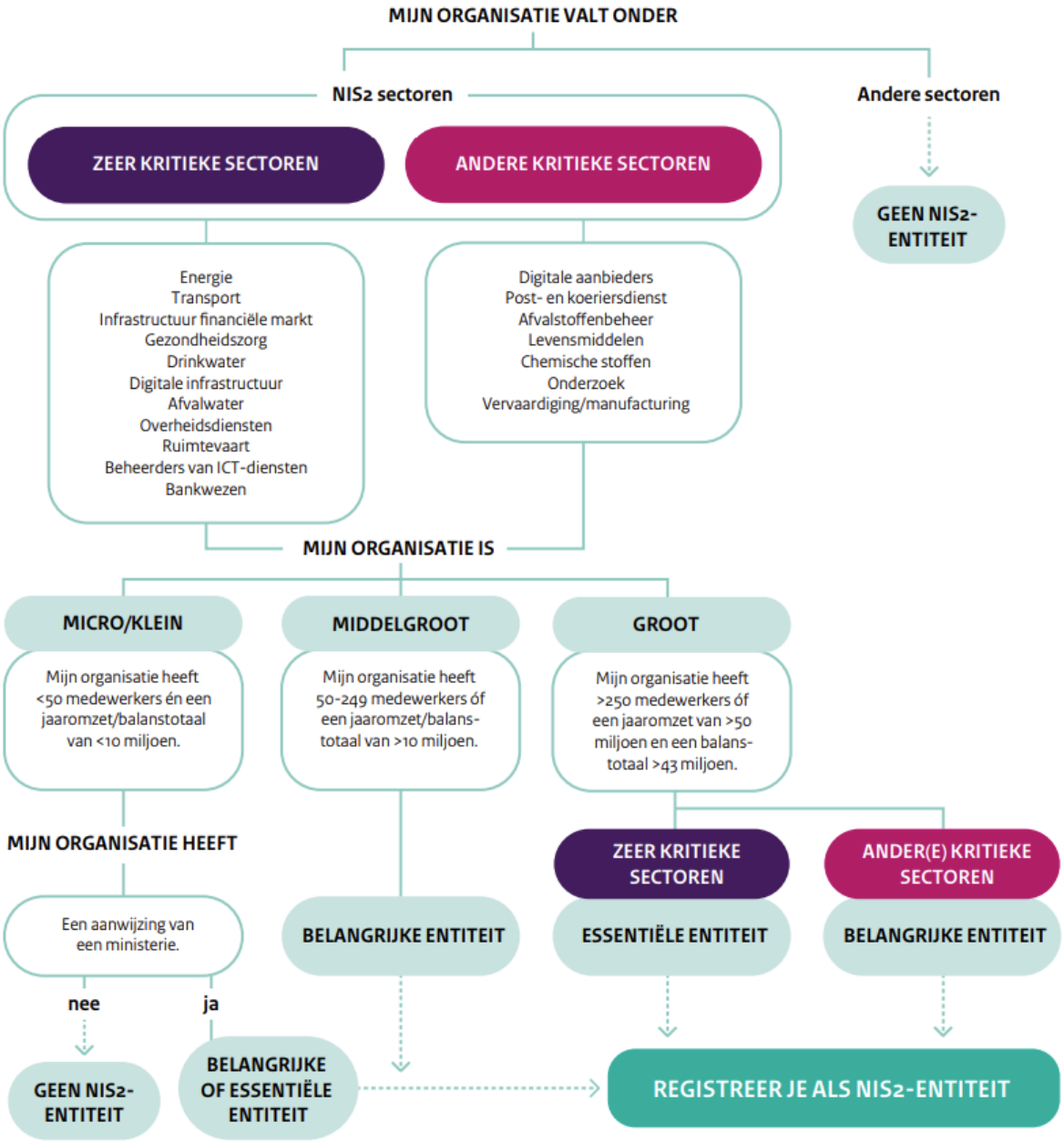
Universiteit Twente. (2023). *De impact van cybersecurity op de procesveiligheid van gevaarlijke stoffen in de Nederlandse chemische industrie.* Terschuur: Safety Delta Nederland.

Waterfall Security Solutions. (2024). *Threat Report: OT cyberattacks with physical consequences.* Waterfall Security Solutions.

8. Bijlagen

8.1 Indeling van sectoren en organisaties onder de NIS2-richtlijn

Infosheet NIS2 (verplichtingen)



8.2 Interviewvragen leveranciers

Met welk doel zou een risico-relevant bedrijf een direct doelwit kunnen zijn van een cyberaanval?

- Hoe zou een dergelijk doel met een cyberaanval bij een risico relevant bedrijf bereikt kunnen worden, met welk type cyberaanval?
- Zou bij een dergelijke cyberaanval een mechanisme voor de signalering, beheersing en bestrijding van een incident betrokken kunnen raken?
- Zou bij een dergelijke cyberaanval een van jullie installaties betrokken kunnen raken? Wat zijn de verschillende manieren van betrokkenheid? Welke repressieve mechanismen die aan een installatie gekoppeld zijn, zouden hierbij indirect betrokken kunnen raken?

Met welk doel zou een mechanisme voor de signalering, beheersing en bestrijding van een incident een direct doelwit kunnen zijn van een cyberaanval?

- Hoe zou een dergelijk doel met een cyberaanval op een repressief mechanisme bereikt kunnen worden, met welk type cyberaanval?
- Welke repressieve mechanismen die momenteel in de markt zijn, kunnen doelwit worden van een dergelijke cyberaanval?
- Zou bij een dergelijke cyberaanval een van jullie installaties een doelwit kunnen zijn? Zit daar nog verschil in per bedrijf?

Houden jullie rekening met cyberrisico's in het ontwerp/installatie/verkoop van jullie installatie?

- Met welke scenario's houden jullie rekening en waarom?
- Welke maatregelen nemen jullie om een cyberaanval te signalering, beheersing en bestrijden?
- Tonen jullie op een of andere manier aan dat jullie installaties cyberproof zijn?
- Zijn jullie klanten bekend met de cyberrisico's en de maatregelen die jullie eventueel nemen?
- Is jullie installatie al een keer (indirect) doelwit geweest van een van cyberaanval bij een van jullie klanten?

- Hoe blijven jullie op de hoogte van de cyberontwikkelingen in de maatschappij?
- Zijn er nog documenten die voor ons interessant zijn om te raadplegen?
- Welke vragen zou de inspectie kunnen stellen bij controle van het bedrijf/systeem?

8.2 Interviewvragen inspectie-instanties

Met welk doel zou een risico-relevant bedrijf een doelwit kunnen zijn van een cyberaanval?

- Hoe zou een dergelijk doel met een cyberaanval bij een risico relevant bedrijf bereikt kunnen worden, met welk type cyberaanval?
- Zou bij een dergelijke cyberaanval een mechanisme voor de signalering, beheersing en bestrijding van een incident betrokken kunnen raken?
- Met welk doel zou een mechanisme voor de signalering, beheersing en bestrijding van een incident een **direct doelwit** kunnen zijn van een cyberaanval?
- Hoe zou een dergelijk doel met een cyberaanval op een repressief mechanisme bereikt kunnen worden, met welk type cyberaanval?
- Welke mechanismen **die momenteel in de markt** zijn voor de signalering, beheersing en bestrijding van een incident, kunnen (indirect) doelwit worden van een dergelijke cyberaanval?
- Kortom: Wat zijn de scenario's die kunnen plaatsvinden?
- Kennen jullie specifieke casussen van een cyberaanval bij een risico-relevant bedrijf? Waren daarbij dergelijke mechanismen voor de signalering, beheersing en bestrijding van een incident betrokken?

Hoeveel inspecties verwachten jullie uit te voeren in een jaar? Hoe vaak verwachten jullie bij een risico-relevant bedrijf te komen? Hoe bepalen jullie een eventuele prioritering?

- Hoe bereiden jullie je voor op de komende inspecties? Hoe gaat zo'n inspectie eruitzien?
    - Hoelang duurt zo'n inspectie en met hoeveel collega's?
    - Worden de systemen fysiek langsgegaan of bekijken jullie voornamelijk de bijhorende documentatie?
    - Welke functies van een dergelijk bedrijf zullen betrokken worden bij de inspectie? Welke vragen stellen jullie en aan wie?
- Welke systemen gaan jullie voornamelijk controleren? Bij welke systemen verwachten jullie het grootste cyberrisico? Richten jullie je ook specifiek op mechanismen voor de signalering, beheersing en bestrijding van incidenten?
- Wat zijn de consequenties als jullie misstanden constateren? Welke stappen worden dan ondernomen met het bedrijf? Wat zijn jullie handhavingsmogelijkheden?
- Hoe ziet de samenwerking tussen RDI en ILT eruit? Wat is de rolverdeling?
- Hoe zien jullie de samenwerking met de inspecteurs van de veiligheidsregio's voor jullie? Heeft cyberinspectie vanuit de VR toegevoegde waarde volgens jullie?
- Welke vragen zou de inspectie van de veiligheidsregio kunnen stellen bij controle van het bedrijf/systeem?
- Hebben jullie tips en tricks voor de inspecteurs van de veiligheidsregio's wat betrecht cyberrisico's?
- Hoe kunnen deze inspecteurs hun bevindingen met jullie delen, als dit überhaupt uitgewisseld mag worden?
- Wat zijn de consequenties als jullie misstanden constateren? Welke stappen worden dan ondernomen met het bedrijf? Wat zijn jullie handhavingsmogelijkheden?
- Hoe blijven jullie op de hoogte van de cyberontwikkelingen in de maatschappij?
- Zijn er nog documenten die voor ons interessant zijn om te raadplegen?

8.3 Interviewvragen risico-relevant bedrijf

- Welke mechanismen voor de signalering, beheersing en bestrijding van een incident hebben jullie?
- Welk van deze repressieve mechanismen zijn losstaande systemen en welke zijn gekoppeld aan online apparaten en systemen?
- Welk repressief mechanisme zou betrokken kunnen raken bij een cyberaanval, met welk type cyberaanval?
- Met welk doel zou jullie bedrijf een doelwit kunnen zijn van een cyberaanval?
    - Zijn jullie al eens doelwit geweest van een cyberaanval? Kunnen jullie daar iets meer over vertellen?
- Houden jullie binnen de bedrijfsvoering rekening met cyberrisico's?
    - Welke maatregelen nemen jullie om een cyberaanval te signaleren, beheersen en bestrijden?
    - Tonen jullie op een of andere manier aan dat jullie cyberproof zijn?
    - Hoe blijven jullie op de hoogte van de cyberontwikkelingen in de maatschappij?
- Zijn er nog documenten die voor ons interessant zijn om te raadplegen?
- Welke vragen zou de inspectie kunnen stellen bij controle van een bedrijf/systeem?

Dit is een uitgave van: Landelijk expertisecentrum industriële veiligheid (LEC IV)

Projectleider: Jan Meinster (Landelijk Expertisecentrum Industriële Veiligheid)
Auteurs: Sebastiaan Bruggink (OK10)
Ben Jonker (OK10)
Nandi van Voorst (OK10)

Stuurgroep: Patrick van de Heisteeg (Inspectie Leefomgeving en Transport)
Johan Kloppenburg (Veiligheidsregio IJsselland)
Jan Meinster (LEC IV)

Contact
Postbus 9154, 3007 AD Rotterdam
https://leciv.nl
088 - 8779 556

Uitgave: Maart 2025
Versie: 1.0 (definitief)