Eindrapportage Cybervolwassenheidsonderzoek

DCMR Milieudienst Rijnmond

Fox-IT Risk Management & Governance
Juli 2021

Introductie

In oktober 2020 is Fox-IT door DCMR gevraagd een onderzoek uit te voeren naar de cybervolwassenheid die vallen onder Besluit risico's zware ongevallen 2015 (verder Brzo-bedrijven). Het onderzoek is erop gericht om een zo representatief mogelijk beeld te krijgen van de cyberrisico's en digitale weerbaarheid van de Brzo-bedrijven in de provincies Zuid-Holland en Zeeland. Hierbij gaat het om een selectie van zeventig Brzo-bedrijven.

Om de cybervolwassenheid van de bovengenoemde Brzo-bedrijven inzichtelijk te maken is gebruik gemaakt van hetzelfde toetsingskader als dat er is gebruikt bij het onderzoek voor het Ministerie van Infrastructuur en Waterstaat. Als Brzo-bedrijf is het belangrijk om inzicht te hebben in het eigen ICS-landschap (Industrial Control System), ook wel het OT-landschap (Operational Technology) genoemd. De beveiliging ervan en de mitigatie van de kwetsbaarheden zijn zeer belangrijk voor veilige operationele processen binnen een organisatie. Binnen het toetsingskader zijn er in het onderzoek verdiepingsvragen gesteld over OT.

Inhoudsopgave

1. Managementsamenvatting

Opdracht

- Het doel van het onderzoek is om een representatief beeld te krijgen van de cyberrisico's en de digitale weerbaarheid van de Brzo-bedrijven waar de DCMR namens de provincies Zuid-Holland en Zeeland de vergunningverlenende- en toezichtstaken uitvoert.

- Het onderzoek is erop gericht om een zo representatief mogelijk beeld te krijgen van de cyberrisico's en digitale weerbaarheid van een selectie van 70 Brzo-bedrijven.

- In deze rapportage wordt inzichtelijk gemaakt wat de cybervolwassenheid is van de Brzo-bedrijven in de provincies Zuid-Holland en Zeeland. Hiervoor wordt het toetsingskader 'risico's cyber versie 2.2' van het ministerie van Infrastructuur en Waterstaat gebruikt.

- Als Brzo-bedrijf is het belangrijk om inzicht te hebben in het eigen ICS-landschap (OT), de beveiliging ervan en de kwetsbaarheden daarbinnen. Binnen het toetsingskader zijn er in het onderzoek verdiepingsvragen gesteld over OT.

Managementsamenvatting

- Van de aangeschreven 70 Brzo-bedrijven hebben er 39 deelgenomen aan het onderzoek.
  - 13 Brzo-bedrijven zijn onderzocht door middel van het afnemen van een diepte-interview.
  - 26 Brzo-bedrijven hebben deelgenomen middels het invullen van een self-assessment.

- De volwassenheidsscore tussen de verschillende organisaties verschilt sterk. Het valt op dat er een positieve correlatie lijkt te zijn tussen volwassenheid en de omvang van een organisatie.

- Van alle onderzochte Brzo-bedrijven is 1 op de 4 onvoldoende in staat om cybersecurity risico's te mitigeren.

- Cybersecurity maatregelen op het gebied van OT-systemen lopen achter bij maatregelen voor IT-systemen. Brzo-bedrijven onderkennen veelal het onderwerp, echter verschilt het implementatieniveau per organisatie sterk. 4 Op de 10 Brzo-bedrijven hebben geen of alleen op ad-hoc basis maatregelen genomen en missen daarmee structuur en borging.

- Het isoleren van OT omgevingen is een belangrijke preventieve maatregel. 1/3 van de Brzo-bedrijven scoort lager dan een 1 op een schaal van 1 t/m 5. Dit betekent dat zij hun OT-omgevingen niet hebben geïsoleerd of niet weten waar zij staan ten opzichte van deze maatregel.

- De verschillen tussen DCMR-codering, MARS-codering en provincies zijn kleiner. Aanwezige positieve verschillen tussen deze groepen worden veelal veroorzaakt door enkele Brzo-bedrijven die groter zijn in omvang.

- Diepte-interviews en self-assessments laten een gelijk beeld zien met de kanttekening dat self-assessments gemiddeld hoger scoren dan diepte-interviews.

Toelichting

Cyber security in IT-omgevingen en OT-omgevingen bestaat door het gebruik en de toepassing van concepten. Binnen deze concepten gaat het dan om enerzijds de toepassing van cybersecurity elementen en het beschrijven er van, maar anderzijds ook om het gebruiken van concepten om een uitgebreide cybersecurity aanpak en programma te formuleren.

Voorbeelden van deze concepten zijn het toepassen van ‘defense in depth’ en een principe als ‘least privilege’. Het concept ‘defense in depth’ houdt in dat er meerdere maatregelen nodig zijn om cybersecurity risico’s te mitigeren en beveiliging niet afhankelijk te maken van één enkele maatregel. Bij ‘least privilege’ gaat het erom dat gebruikers precies voldoende rechten krijgen om hun rol/functie uit te kunnen oefenen. Effectief en efficiënt toepassen van deze ‘defense in depth’, ‘least privilege’ en andere concepten vereist een risico gebaseerde aanpak. Weten waartegen verdedigd moet worden is hierbij van groot belang. De volwassenheid van een organisatie geeft aan in hoeverre zij in staat is deze concepten toe te passen, te documenteren en te specificeren voor en door iedere individuele organisatie.

Uit het onderzoek blijkt dat circa 40% van de organisaties een volwassenheidsniveau van 2 of lager scoort. Dit betekent dat standaarden, procedures, hulpmiddelen en methoden nog niet volledig zijn geïmplementeerd en/of beschreven binnen de desbetreffende organisatie. Ook ontbreekt er consistentie in de toepassing en/of de documentatie en vindt er nog niet in alle gevallen procesverbetering plaats. Een lagere volwassenheidsscore betekent dus over het algemeen dat organisaties minder ‘in control’ zijn over hun cybersecurity aanpak.

Binnen dit onderzoek is er gekeken naar hoe risicomanagement is ingericht en welke structuren er zijn aangebracht om verdere maatregelen te implementeren. Dit valt binnen de categorie ‘governance’. Een erg groot deel van de organisaties scoort hier laag. Hiermee is deze categorie een duidelijk aanknopingspunt om verbeteringen binnen organisaties structureel en uitgebreid aan te pakken.

2. Werkwijze

Aanpak van het onderzoek

Opdracht: DCMR heeft Fox-IT gevraagd om voor zowel Operational Technology (OT) als Information Technology (IT) een cybervolwassenheidsbeeld vast te stellen voor de Brzo-bedrijven in Zuid-Holland en Zeeland.

Methode: Fox-IT heeft diepte-interviews (13 organisaties) en self-assessments (26 organisaties) afgenomen aan de hand van een vragenlijst die door Fox-IT is opgesteld en afgestemd met DCMR. De uitkomsten van de self-assessments en diepte-interviews zijn geaggregeerd tot een eindresultaat.

Vragenlijst: De vragenlijst bestaat uit 33 vragen en deze zijn onderverdeeld in de categorieën governance, preventie, detectie en response. Deze categorieën bieden inzicht in de gelaagdheid van de beveiliging.

Implementatieniveaus: Het antwoord/toelichting op de vragen indiceren op welk volwassenheidsniveaus (0 – 5) een organisatie zich bevindt op de verschillende maatregelen, categorieën en overall.

Samenstelling vragenlijst

Hieronder de bronnen die een rol hebben gespeeld bij de samenstelling van de vragenlijst.

TNO: De initiële versie van deze vragenlijst is ontwikkeld door TNO voor een vergelijkbaar onderzoek voor het Ministerie van Infrastructuur en Waterstaat.

Ethische hackers Fox-IT: Uit praktijkervaringen van ethische hackers van het Fox-IT RedTeam zijn vragen toegevoegd over hoe zij digitaal toegang verkrijgen tot organisaties.

CIS Top 20: De CIS Top 20 is ontwikkeld door het Center for Internet Security en bevat maatregelen om de weerbaarheid te vergroten tegen cyberaanvallen.

OT-perspectief: Het OT-perspectief is onderdeel van het assessment mede door middel van vragen afkomstig uit een werksessie met stakeholders betrokken bij het onderzoek.

Uitleg implementatieniveaus

Per categorie zijn er een aantal onderwerpen vastgesteld. Per onderwerp wordt het implementatieniveau bepaald op basis van een 5-punts schaal. Voor het bepalen van de score in deze 5-punts schaal worden de definities van het CMMI-model aangehouden. Deze schaal start bij 0 (niet geïmplementeerd) en loopt door naar maximaal 5 (volledige geïmplementeerd).

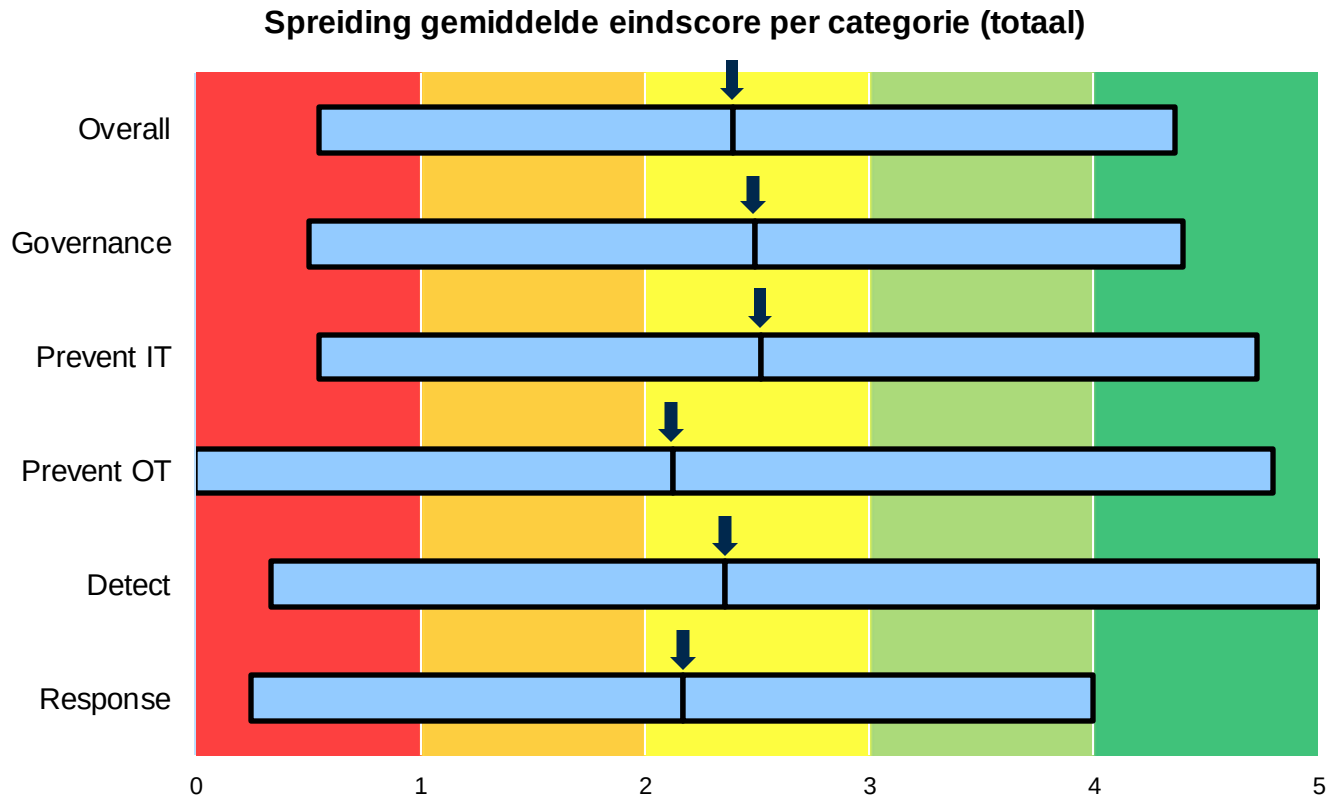
0 Niet bestaand	De maatregel is niet geïmplementeerd. De organisatie is niet in staat om aan te geven waar ze staan ten opzichte van deze maatregel (voorbeeld; verklaren waarom de maatregel niet relevant is of juist verplicht is). De maatregel, en de geassocieerde risico's, representeert mogelijk een "unknown" voor de organisatie.
1 Initieel / Ad-hoc	De organisatie herkent het risico waarvoor de maatregel bedoeld is. De maatregel is gedeeltelijk geïmplementeerd, het is voornamelijk handwerk en/of wordt niet consistent uitgevoerd.
2 Herhalend maar intuïtief	De maatregel wordt over het algemeen consistent geïmplementeerd; maar kan afhankelijk zijn van de kennis en toewijding van een kleine groep personeel. De basis beleidsstukken en documentatie in context van de (voorbeeld; werkinstructies) maatregel zijn er, wat zorgt voor een bepaalde mate van consistentie. Auditing en compliancy mechanismes zijn gelimiteerd, wat betekent dat wanneer er wordt afgeweken van gedocumenteerde normen dit niet altijd worden gedetecteerd.
3 Gedefinieerd	De maatregel is in detail gedocumenteerd, op een manier waarop de uitvoering consistent is. De maatregel heeft een formeel erkende eigenaar wie verantwoordelijk is voor de effectiviteit en verbetering. In het geval van handmatige maatregelen: de maatregel is zeer herhaalbaar, op een manier dat wanneer twee mensen dezelfde taak zouden krijgen, het resultaat hetzelfde zou zijn.
4 Beheerst en meetbaar	De maatregel is hoofdzakelijk geautomatiseerd, met als basis gedocumenteerde business rules welke voortkomen uit het beleid van de organisatie. De maatregel is onderhevig aan management bij uitzondering (voorbeeld; foutcondities) en management toezicht (voorbeeld; audits). KPI's en geassocieerde prestatie doelstellingen zijn gedefinieerd voor de maatregel; waar op wordt gerapporteerd; en enige onder prestatie wordt verholpen.
5 Geoptimaliseerd	In het vervolg van "4 – Beheerst & Meetbaar". De organisatie kan het volgende bewijs laten zien: - Proactief continue verbetering in relatie tot de maatregel. - Het resultaat van de investering in de securitymaatregel.

3. Cybervolwassenheidsbeeld

3.1 Overall Cybervolwassenheidsbeeld

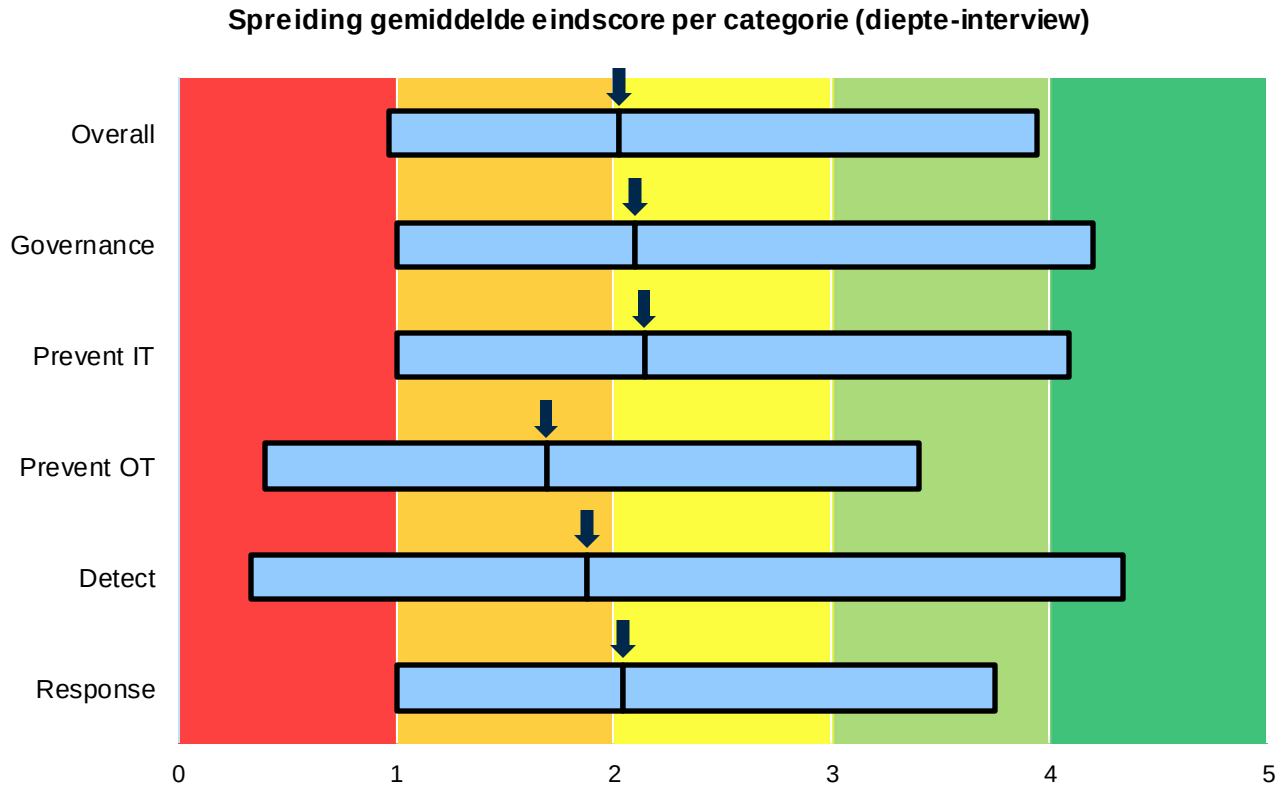
Overall cybervolwassenheidsbeeld (totaal)

In het overall beeld zijn de diepte-interviews en de self-assessments gecombineerd om tot een totaalbeeld te komen. Overall laten de diepte-interviews en de self-assessments een gelijk beeld zien. In dat beeld is te constateren dat de categorie ‘preventie’ op OT-gebied minder volwassen is dan de overige categorieën. Afwijkend is de categorie ‘response’ welke in diepte-interviews relatief licht hoger scoort dan bij de self-assessments. 4 Op de 10 organisaties heeft beperkt tot geen maatregelen ten aanzien van de OT-omgeving.



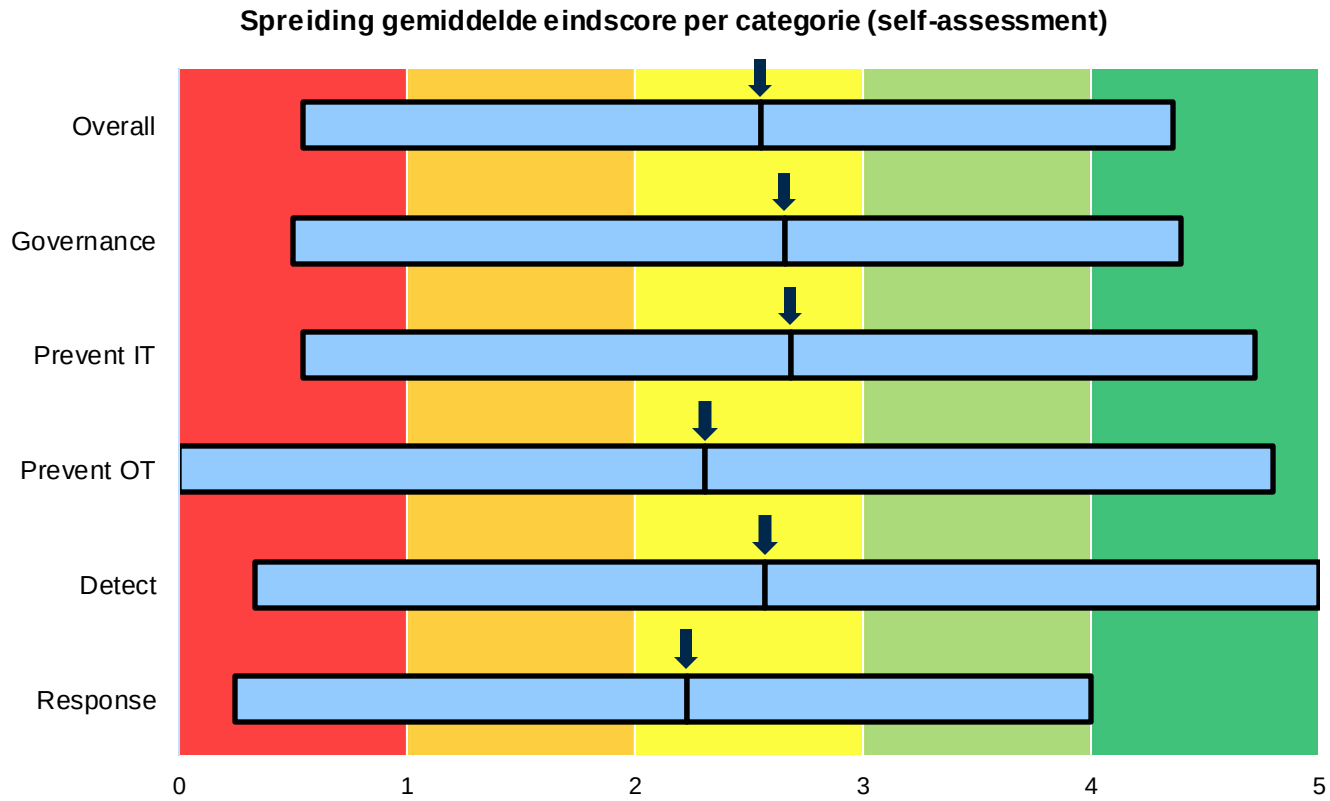
Overall cybervolwassenheidsbeeld (diepte-interviews)

De diepte-interviews hebben plaatsgevonden door bij de geselecteerde organisaties Fox-IT een interview af te laten nemen aan de hand van de vragenlijst. Tijdens diepte-interviews is er gelegenheid om op onderwerpen door te vragen en worden de scores vastgesteld door medewerkers van Fox-IT. Onderstaande weergave geeft het gemiddelde, de minimale score en de maximale score weer binnen de groep organisaties waarmee een diepte-interview heeft plaatsgevonden. Het valt op dat er een positieve correlatie lijkt zijn tussen volwassenheid en de omvang van een organisatie.



Overall cybervolwassenheidsbeeld (self-assessments)

Self-assessments zijn zelfstandig ingevuld door de geselecteerde organisaties. Voor deze organisaties is gebruik gemaakt van dezelfde vragenlijst als voor de organisaties waarbij een diepte-interview is afgenomen. Organisaties zijn gevraagd om aan de hand van de omschreven volwassenheidsniveaus per maatregel zichzelf een score te geven en daarbij een toelichting te geven om deze score te onderbouwen. Fox-IT heeft deze self-assessments beoordeeld en indien nodig na overleg met de organisatie aangepast. Enkele self-assessments zijn later opgevolgd door diepte-interviews. Het beeld dat voor de totale groep self-assessments ontstaat is dat organisaties zichzelf positiever beoordelen dan Fox-IT doet bij een diepte-interview.



Overall cybervolwassenheidsbeeld

- Het overall beeld toont een zeer diverse aanpak van cybersecurity bij de onderzochte organisaties. Enkele organisaties tonen een zeer volwassen en gedegen aanpak in alle categorieën, echter daar tegenover staan ook enkele organisaties waarbij het onderwerp cybersecurity maar beperkt wordt behandeld en er dus een lage volwassenheid wordt gescoord. 1 Op de 4 organisaties behandeld cybersecurity op ad-hoc basis of ongestructureerd.

- Ten aanzien van de OT-omgeving is dit gevonden verschil groter. De spreiding van de hoogste en laagste scores zijn hier groter, maar wat bovenal opvalt is dat enkele organisaties een lage volwassenheid scoren. 4 Op de 10 van de onderzochte organisaties scoort op het gebied van OT een 2 of lager, wat aangeeft dat maatregelen niet, op ad-hoc basis of herhalend maar intuïtief worden geïmplementeerd. Structuur en borging ten aanzien van OT-maatregelen ontbreekt in deze groep.

- In het algemeen wordt er onderkend dat cybersecurity ook van belang is voor OT-omgevingen. Voor de te nemen maatregelen wordt er veelal gekeken naar standaarden en best practices. De fase waarin organisaties zich bevinden ten aanzien van de implementatie van maatregelen verschilt.

- Het self-assessment toont een gelijk beeld als de diepte-interviews binnen de verschillende categorieën. In alle self-assessments is de volwassenheid op het gebied van OT lager ten opzichte van de overige categorieën. Organisaties geven daarmee aan dat OT-maatregelen minder volwassen zijn geïmplementeerd dan overige maatregelen.

- In de self-assessments scoren organisaties binnen de categorie ‘response’ lager dan in de diepte-interviews. Dit is mogelijk te verklaren door de positieve waardering voor generieke incident response capaciteiten tijdens diepte-interviews.

Overall cybervolwassenheidsbeeld

Categorie: Governance (1/2)

- Binnen de categorie ‘governance’ worden maatregelen onderzocht die sturing geven aan cybersecurity maatregelen.
- Overall scoort de categorie ‘governance’ gemiddeld een 2,5. Hierbij is het gemiddelde voor diepte-interviews een 2,1 en voor self-assessments een 2,6. Dit geeft aan dat organisaties het onderwerp herhalend maar intuïtief behandelen en niet consistent geborgd hebben in de organisatie.
- Enkele organisaties tonen zich volwassen op het gebied van cybersecurity risk management, een kwart scoort een 4 of hoger waarmee deze organisaties de processen beheersen, meetbaar hebben gemaakt en in sommige gevallen hebben geoptimaliseerd. Veelal is het een apart behandeld onderwerp of wordt het geïntegreerd in het enterprise risk management. Daartegenover staan een kwart van de organisaties die een 1 scoren en daarmee cybersecurity risk management ad-hoc benaderen.
- De gebieden risk management, anticiperen op dreigingen en security organisatie scoren een licht hoger gemiddelde dan de overige governance onderdelen.
- Met name leveranciersmanagement scoort lager. Deze laatste is van belang wanneer organisaties het beheer van de IT- en/of OT-omgeving uitbesteden aan leveranciers. Een positieve relatie tussen uitbesteding en volwassenheid is niet geconstateerd.

Overall cybervolwassenheidsbeeld

Categorie: Governance (2/2)

- Het bekend zijn met en het volgen van good practices scoort gemiddeld het hoogst binnen deze categorie. Organisaties geven met deze score aan dat good practices zijn geborgd en consistent worden geïmplementeerd. Het feit dat deze categorie gemiddeld het hoogst scoort en andere categorieën die duiding geven aan de invulling van good practices lager scoren, geeft een beeld dat deze score niet wordt onderbouwd binnen de categorieën ‘preventie’, ‘detectie’ en ‘response’.

- De omvang en achtergrond van een organisatie lijken mede bepalend te zijn voor de implementatie van maatregelen van de bijbehorende controls. Hier is een duidelijke positieve correlatie te zien.

Overall cybervolwassenheidsbeeld

Categorie: Preventie IT

- Binnen de categorie ‘preventie IT’ worden maatregelen onderzocht die het aanvallers bemoeilijkt om toegang te krijgen tot informatiesystemen.

- Overall scoort de categorie ‘preventie’ gemiddeld een 2,4. Hierbij is het gemiddelde voor diepte-interviews een 2,2 en voor self-assessments een 2,6. Dit geeft aan dat organisaties het onderwerp niet consistent geïmplementeerd hebben in de organisatie.

- Patch management scoort bovengemiddeld. 95% scoort daarbij een 2 of hoger wat aangeeft dat deze maatregel wel consistent is geïmplementeerd. Door veel organisaties wordt het belang van tijdig patchen onderkend en wordt gestreefd naar het tijdig en volledig installeren van patches.

- Het toepassen van encryptie scoort beduidend lager. Een kwart van de respondenten geeft aan geen encryptie toe te passen. Encryptie wordt met name toegepast om vertrouwelijkheid en in mindere mate integriteit te waarborgen, waarbij het bij de onderzoeksgroep met name draait om beschikbaarheid van systemen.

Overall cybervolwassenheidsbeeld

Categorie: Preventie OT

- Binnen de categorie ‘preventie OT’ worden maatregelen onderzocht die het aanvallers bemoeilijkt om toegang te krijgen tot OT informatie systemen.
- De maatregelen binnen de categorie ‘preventie OT’ scoren lager dan het gemiddelde (2,2). Dit is van toepassing op zowel de self-assessments als de diepte-interviews. Gemiddeld de helft van de organisaties scoort een 2 of lager. ‘Preventie OT’ is hiermee bij een grote groep organisaties niet consistent geïmplementeerd.
- Het beheer van de OT-omgevingen heeft expliciete aandacht. Door de complexiteit van OT-omgevingen is een consistente en effectieve implementatie uitdagend.
- Het isoleren van OT omgevingen is een belangrijke preventieve maatregel. 1/3 van de organisaties scoort lager dan een 1. Dit betekent dat zij hun OT-omgevingen niet hebben geïsoleerd of niet weten waar zij staan ten opzichte van deze maatregel.

Overall cybervolwassenheidsbeeld

Categorie: Detectie

- Binnen de categorie ‘detectie’ zijn maatregelen onderzocht die aangeven of organisaties detectietechniek en –processen hebben ingericht voor het ontdekken van kwetsbaarheden, afwijkende zaken en de opvolging van alerts.
- Het verkregen beeld in de diepte-interviews en de self-assessments is bijna identiek. De diepte-interviews scoren iets lager dan de self-assessments.
- Een kwart van de organisaties heeft geen maatregelen geïmplementeerd voor het detecteren van kwetsbaarheden in hun omgeving.
- Eén op de tien organisaties heeft geen detectie op cybersecurity om afwijkende gebeurtenissen tijdig op te merken en hier op te reageren.

Overall cybervolwassenheidsbeeld

Categorie: Response

- Binnen de categorie ‘response’ is onderzocht of organisaties in staat zijn om te kunnen reageren op incidenten. De maatregelen richten zich op het hebben van plannen en procedures, het hebben van adequate back-ups en het testen van dit geheel.

- Tussen de self-assessments en de diepte-interviews zijn vrijwel geen verschillen te constateren en dit is daarmee een verschil ten opzichte van de andere categorieën. Dit is mogelijk te verklaren omdat de incident response processen voor fysieke veiligheid tijdens diepte-interviews positief zijn beoordeeld.

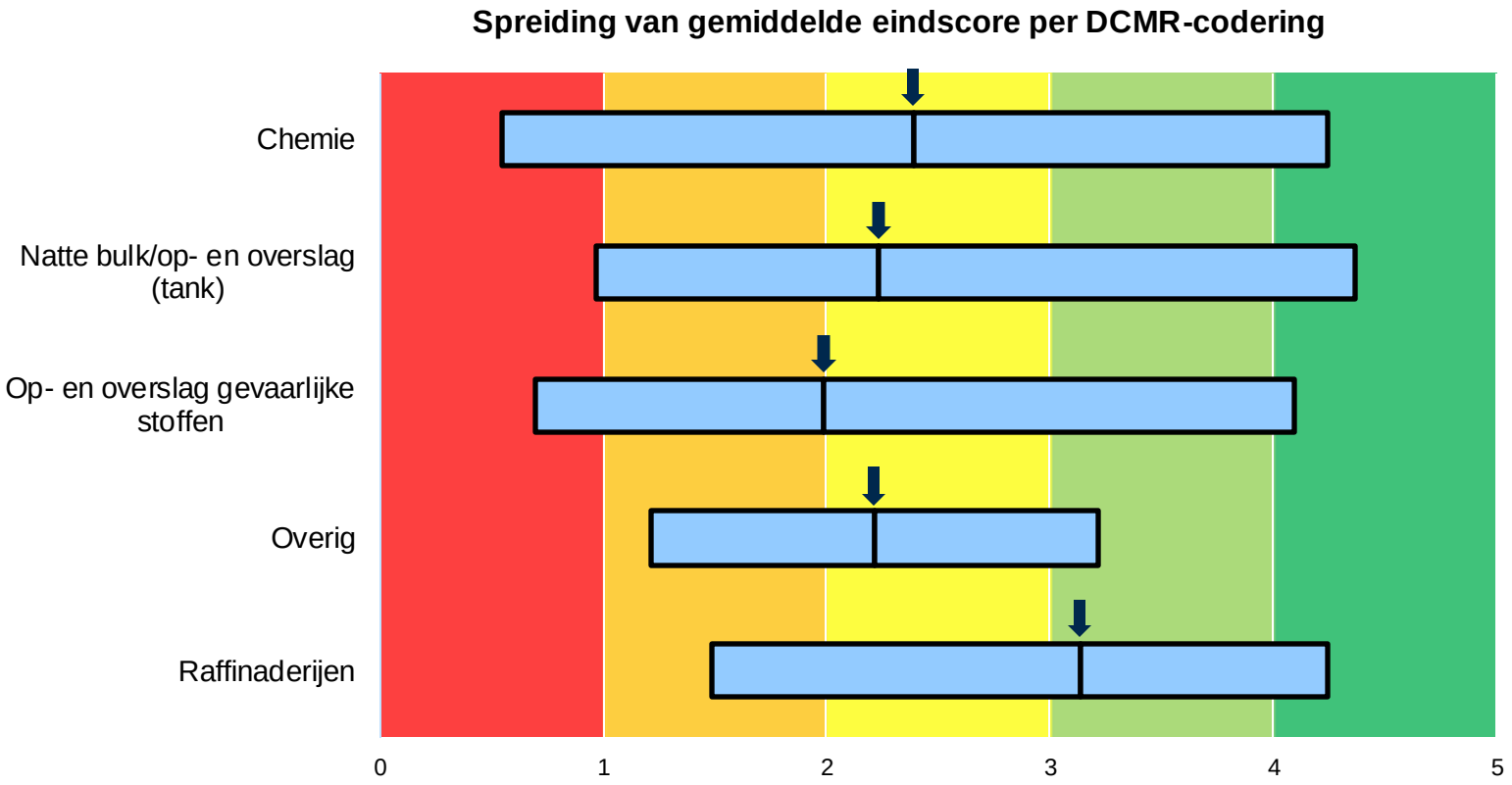
- De categorie ‘response’ scoort in lijn met de andere categorieën. Dit is met name te duiden doordat iedere organisatie maatregelen heeft ten aanzien van back-ups en deze de overige vragen in de categorie naar boven bijstelt.

- De onderdelen incident response, continuïteitsplan en crisisplan scoren één op de vijf organisaties een 0 waarmee organisaties aangeven geen maatregelen te hebben ten aanzien incidenten en crisisafhandeling.

3.2 Cybervolwassenheidsbeeld per DCMR-codering

Cybervolwassenheidsbeeld per DCMR-codering

De branches binnen de DCMR-codering laten een gelijk beeld zien als het overall beeld. Afwijkingen in positieve zin zijn te verklaren door de een beperkte groep onderzochte organisaties in combinatie met een grote vertegenwoordiging van multinationals in deze groep.



Cybervolwassenheidsbeeld per DCMR-codering

- Ten aanzien van de verschillende Brzo-sectoren is het beeld ongeveer gelijk. Een uitzondering op dit beeld is de sector ‘Raffinaderijen’ welke gemiddeld bijna 0,6 punt hoger scoort dan de overige sectoren.

- Deze afwijking ten aanzien van de sector ‘Raffinaderijen’ is tweeledig te verklaren. Ten eerste betreft het een kleine (n=4) groep van organisaties die onderzocht zijn. Ten tweede zien we over het algemeen dat enkele grote multinationals een hoge mate van volwassenheid tonen. Deze multinationals zijn ook vertegenwoordigd in deze kleine groep organisaties wat de gemiddelde volwassenheid verhoogt.

- Over de verschillende assen van ‘governance’, ‘preventie’, ‘detectie’ en ‘response’ valt op dat de sector ‘Op- en overslag gevaarlijk stoffen’ lager scoort op de gebieden ‘detectie’ en ‘response’ met een afwijking van minimaal 0,5 punt ten opzicht van de overige sectoren.

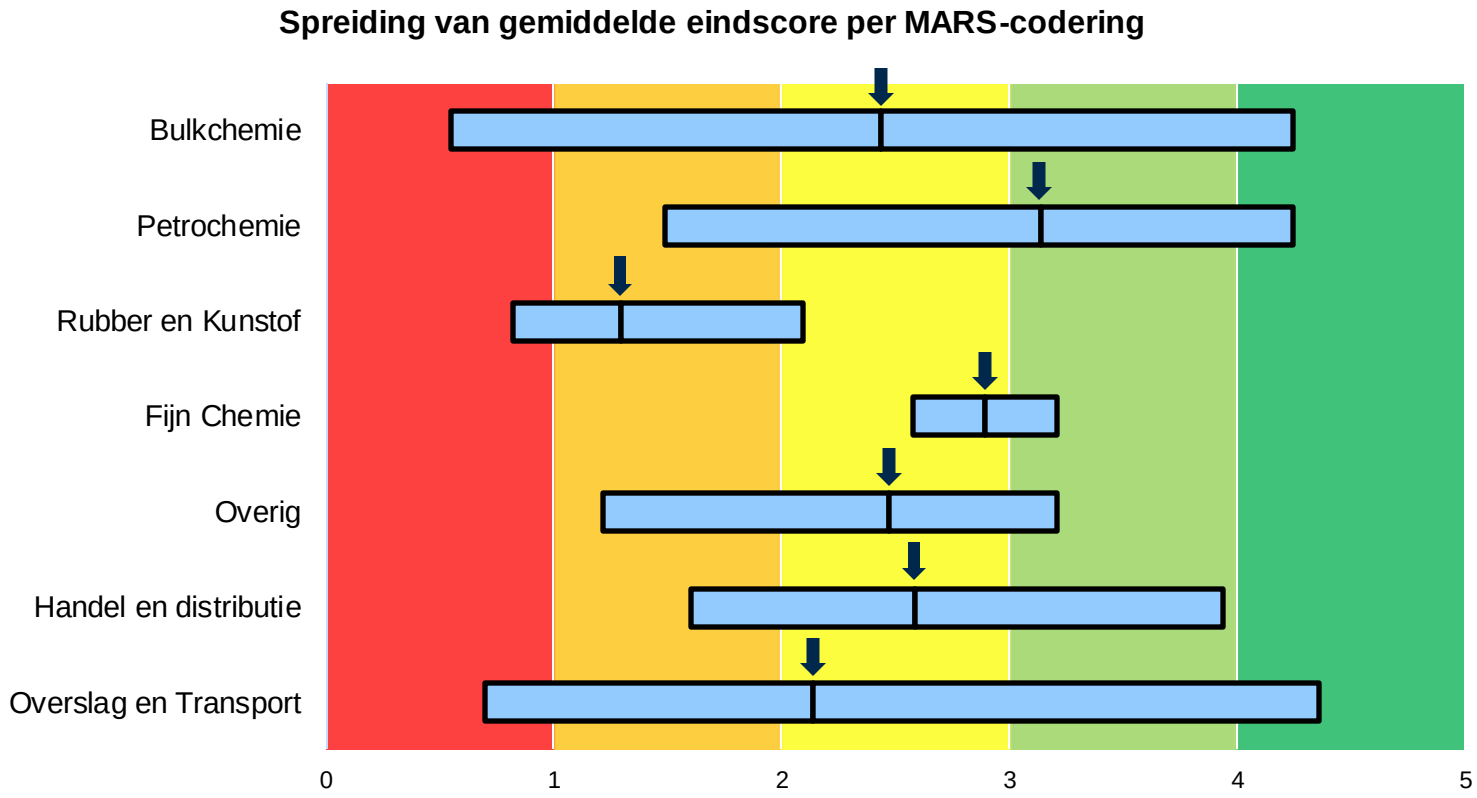
- Daartegenover staat dat de sector ‘Raffinaderijen’ met name in de categorie ’Governance’ hoger scoort met een verschil van minimaal 0,9 punt.

3.3 Cybervolwassenheidsbeeld per MARS-codering*

* MARS = Major Accident Reporting System. Dit is een meldingssysteem om ongevallen te rapporteren aan de Europese Commissie.

Cybervolwassenheidsbeeld per MARS-codering

De branches binnen de MARS-codering geven een divers beeld. Verschillen kunnen veelal worden verklaard door de achtergrond van de organisaties en de omvang van de organisaties. Conclusies zijn lastig vast te stellen gezien de diversiteit onder de onderzochte respondenten.



Cybervolwassenheidsbeeld per MARS-codering

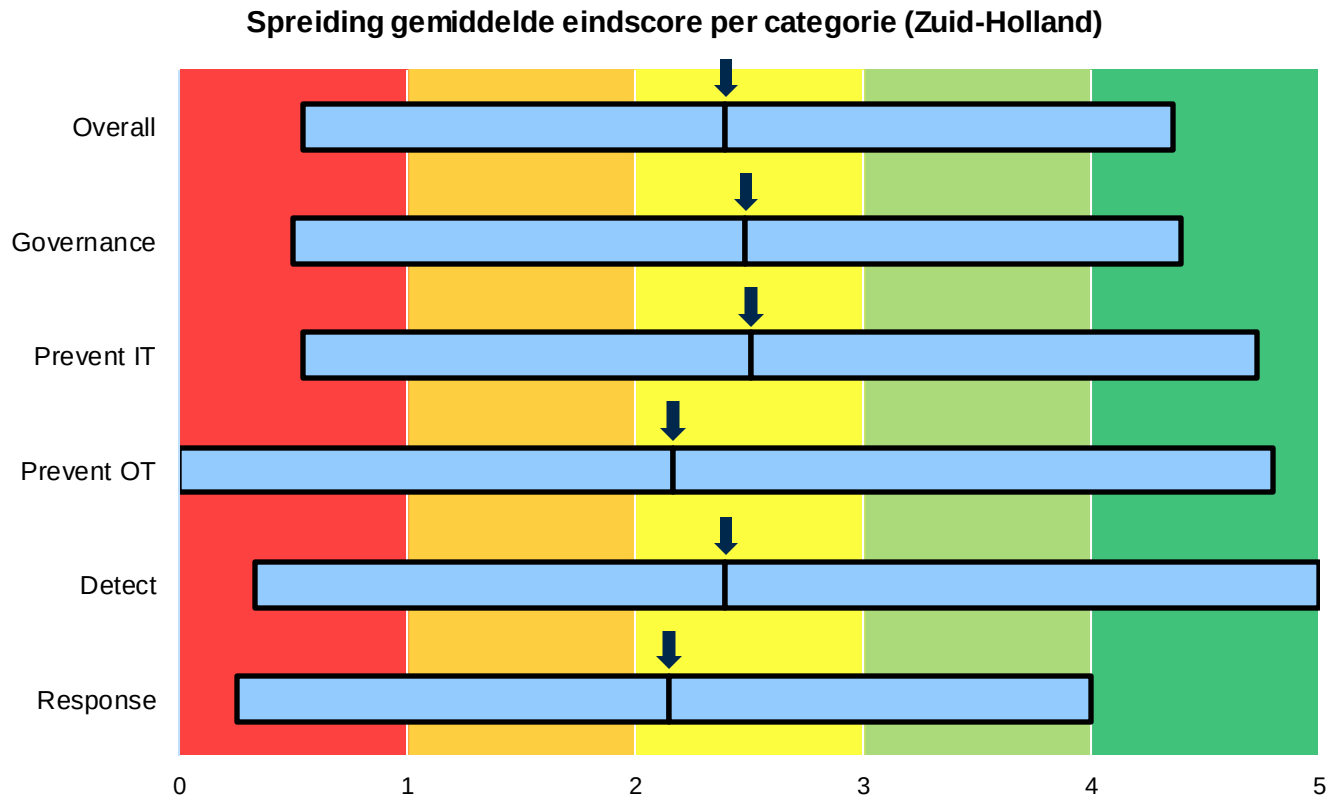
- De MARS-codering ‘overig’ bevat de MARS categorieën 5, 7, 11 en 19.
- De MARS-codering ‘Petrochemie’ bevat dezelfde respondenten als de sector ‘Raffinaderijen’ en daarmee is ook dezelfde toelichting van toepassing als bij de toelichting op sectoren.
- De MARS-codering ‘Rubber en kunststof’ scoren over de gehele linie beduidend lager dan de overige categorieën. Hierbij wordt over alle assen lager gescoord en is er geen significant onderscheidt tussen diepte-interviews en self-assessment waar te nemen.
- De MARS-codering ‘Fijne chemie’ is een kleine steekproef met n=2. Beide organisaties scoren gemiddeld hoger over alle categorieën, met uitzondering van ‘Preventie OT’ welke 0,6 punt lager is dan het gemiddelde.
- Ten aanzien van de MARS-codering ‘Handel en distributie’ (n=10) valt op dat 2 respondenten het gemiddelde nadrukkelijk naar boven halen. Zonder deze 2 respondenten zou het gemiddelde 0,5 punt lager uitvallen.

3.4 Cybervolwassenheidsbeeld per provincie

Cybervolwassenheidsbeeld per provincie

Provincie: Zuid-Holland

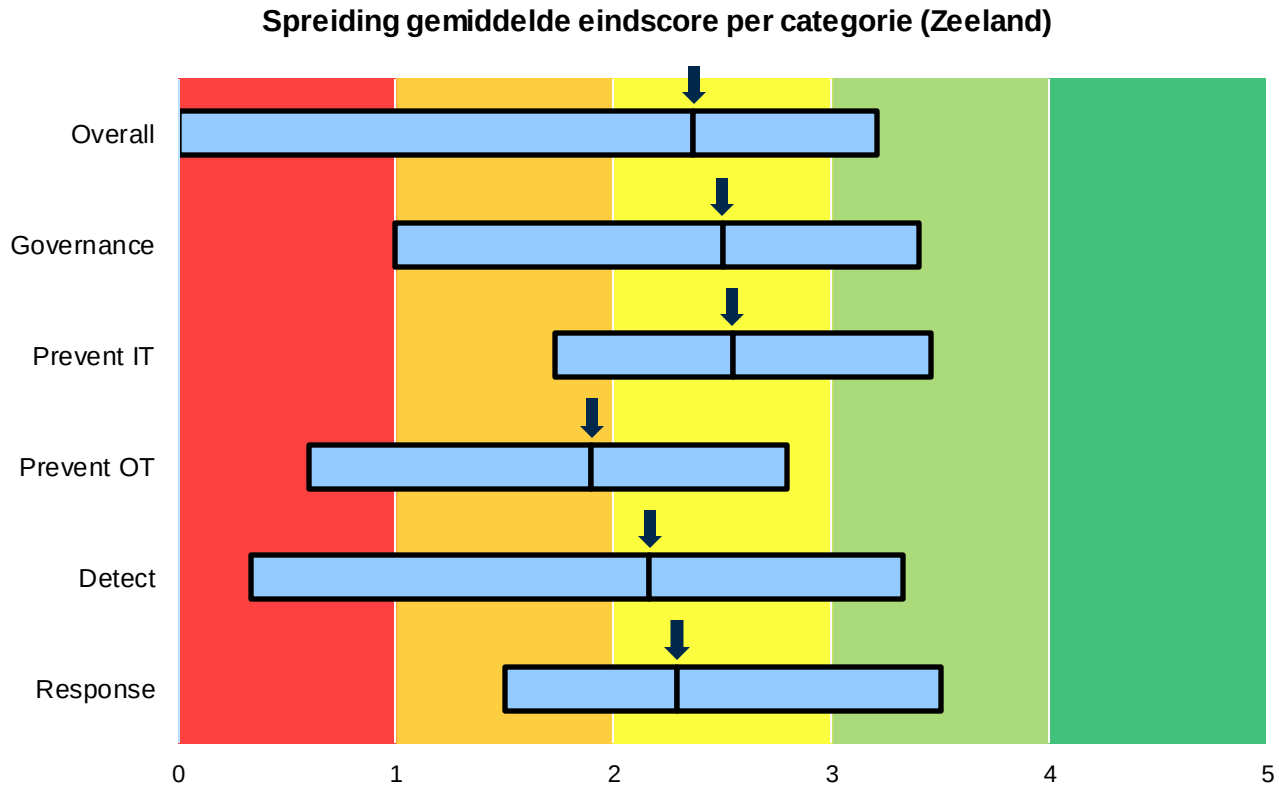
Het beeld van de provincie Zuid-Holland vertoont, door de grootte van de onderzoeksgroep, een gelijk beeld als het overall beeld. Daarmee is ook voor 4 op de 10 organisaties van toepassing dat zij beperkt tot geen maatregelen hebben op het gebied van OT. 1 Op de 4 heeft in algemene zin beperkte maatregelen ten aanzien van cybersecurity.



Cybervolwassenheidsbeeld per provincie

Provincie: Zeeland

Voor de provincie Zeeland zijn geen conclusies vast te stellen. Het beeld wordt vertekend door een beperkte groep organisaties die ook nog een beperkte verdeling heeft over de diverse sectoren.



Cybervolwassenheidsbeeld per provincie

- Beide provincies laten een gelijk beeld zien ten aanzien van de gemiddeld waardes.
- De provincie Zuid-Holland laat een grotere spreiding zien in de scores dan de provincie Zeeland. Dit is met name te verklaren is de omvang van de groep. Zuid-Holland heeft met 33 deelnemers een grotere groep dan Zeeland met 6 deelnemers.
- Zuid-Holland is daarmee vergelijkbaar met de algehele groep van organisaties, inclusief de constateringen die ten aanzien van de groep gedaan kunnen worden.
- Zeeland is naast de kleine groepsomvang ook beperkt in de verdeling over drie branches binnen de DCMR-codering.

Documentbeheer

Version Control	
Classification	COMMERCIAL.RESTRICTED.DCMR
Client Name	DCMR Milieudienst Rijnmond
Document Title	Eindrapportage Cybervolwassenheidsonderzoek DCMR v0.92
Author	Martijn Eikelenboom| Business Security Consultant | Fox-IT Risk Management and Governance Christiaan Huijers | Business Security Consultant | Fox-IT Risk Management and Governance
QA Review	René Ouwehand | Business Security Consultant | Fox-IT Risk Management and Governance René Valstar | Business Security Consultant | Fox-IT Risk Management and Governance

Revision History			
Issue Number	**Issue Date**	**Issued By**	**Change Description**
0.1	23-03-2021	Christiaan Huijers	Initieel document
0.2	03-05-2021	Martijn Eikelenboom	Concept
0.3	04-05-2021	René Valstar	Q&A Concept
0.4	05-05-2021	Martijn Eikelenboom	Feedback verwerkt
0.9	11-05-2021	René Ouwehand	Finale review & Definitief Concept
0.92	15-06-2021	René Valstar	Tweede concept
1.0	20-07-2021	René Valstar	Definitief rapport

FOX IT
part of nccgroup

FOX-IT Risk Management & Governance

Fox-IT Risk Management & Governance (RM&G) ondersteunt organisaties in het digitale tijdperk met als doel de cyberveiligheid te verbeteren. De gespecialiseerde adviseurs van RM&G maken inzichtelijk welke beslissingen cruciaal zijn voor het bereiken van een effectieve cybersecurity bestendigheid. Daarbij worden organisaties geholpen te voldoen aan hun cybersecurityvereisten, waarbij kenmerken en (on)mogelijkheden in acht worden genomen. Onze business security consultants combineren zowel technische als niet-technische (organisatorische) vaardigheden en bieden passende en doelgerichte oplossingen voor cybersecurity uitdagingen. De kern van de ondersteuning van RM&G is hun pragmatische aanpak: ondersteuning en oplossingen zijn evenredig, specifiek, uitvoerbaar en op maat gemaakt.

Contactinformatie

+31 15 284 7999
Olof Palmestraat 6, Delft

Postbus 638, 2600 AP Delft
Nederland