



Nationaal Cyber Security Centrum  
*Ministerie van Justitie en Veiligheid*

# Vragen om als bestuurder te stellen aan de CISO

Om samen de cyberveiligheid van je organisatie te verbeteren

Dit factsheet helpt bestuurders om in gesprek gaan hebben met hun CISO en zo grip te krijgen op 'cybersecurity'. Het doel van dit product is dan ook niet zozeer het opleveren van een checklist om compliant te zijn maar juist jou als bestuurder te helpen het gesprek aan te gaan met de CISO. De vragen en bijbehorende subvragen in dit document zijn gesprekstarters op een aantal belangrijke onderwerpen om niet alleen het gesprek aan te gaan, maar ook de bestaande relatie, samenwerking en vertrouwen tussen jou en de CISO te versterken. Dit factsheet probeert jou als bestuurder in een positie te brengen om overzicht te hebben op de uitvoering van maatregelen op het gebied van cyberbeveiligingsrisico's en om deze te begrijpen en goed te keuren. (NIS2, Artikel 20, lid 1).

## Doelgroep

Deze publicatie is geschreven voor bestuurders die behoefte hebben om grip te krijgen op de uitvoering van maatregelen op het gebied van cyberbeveiligingsrisico's en de samenwerking met de CISO te verbeteren in het kader van NIS2.

## Deze publicatie is tot stand gekomen met bijdragen van:

- Digital Trust Centre, ministerie van Economische Zaken en Klimaat
- ABN AMRO
- Tesorion
- CIO Platform Nederland
- CIZ
- Dutch Institute for Vulnerability Disclosure
- Dunea
- Cyberveilig Nederland

## NIS2

Artikel 20, lid 1 (Governance): richt zich tot het bestuur van organisaties. Het bestuur dient de maatregelen, bedoeld in artikel 21, lid 2 goed te keuren en toe te zien op de uitvoering ervan (NIS2).

In Nederland zal de NIS2-richtlijn geïmplementeerd worden in de vorm van de Cyberbeveiligingswet. Op het moment dat de Cyberbeveiligingswet wordt aangenomen, zal deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangen.

## Belangrijke punten

Het beoogde doel van dit product is het samenbrengen van jou, de bestuurder en de CISO om de bestaande onderlinge band te versterken. Hierbij zijn een paar punten ter overweging:

1. De vragen in dit document zijn geen vragen die een keer gesteld worden om een checklist af te vinken. Ze dienen puur als middel om de gesprekken tussen CISO en bestuurder vorm te geven.
2. Deze vragen zijn niet de enige onderwerpen waarover gesproken kan of moet worden. Elke organisatie is uniek en zodoende kan het zijn dat niet al deze vragen passend zijn voor jouw organisatie. Het kan natuurlijk ook voorkomen dat naast deze vragen er nog meer onderwerpen/vragen relevant zijn binnen de organisatie.
3. Het kan voorkomen dat binnen jouw organisatie ook gebruik wordt gemaakt van OT-systemen. De verantwoordelijkheid van OT-systemen ligt niet altijd bij de CISO. In dat geval is het van toegevoegde waarde om de persoon die hier wel verantwoordelijk voor is te betrekken bij het gesprek of hier apart een gesprek mee te voeren.

### Positief veiligheidscultuur

Met als hoofdvraag *“Hoe zorg jij als CISO voor een positieve veiligheidscultuur met betrekking tot cybersecurity en hoe kan ik als bestuurder hieraan bijdragen?”* richt deze vraag zich op de cultuur van de organisatie. Het succesvol borgen van cybersecurity binnen een organisatie valt of staat met de medewerkers. Bij een positieve veiligheidscultuur kan er gedacht worden aan een omgeving waarin medewerkers geen drempel ervaren bij het bespreekbaar maken van zorgen en waarin medewerkers bewust en alert zijn. Niet worden veroordeeld en gestraft voor fouten, maar juist kunnen leren van deze fouten. Een goed voorbeeld vanuit de bestuurder draagt hier positief aan bij.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. In hoeverre is er binnen de organisatie sprake van een positief veiligheidscultuur?
2. Wat is er (nog) nodig om een positieve veiligheidscultuur te creëren?
3. In hoeverre is er managementsupport voor een (security-)melding?
4. Welke veilige escalatie mogelijkheden zijn er voor de medewerkers als een melding onvoldoende prioriteit krijgt?
5. Wat kan ik als bestuurder doen om te zorgen voor een positieve veiligheidscultuur?
6. Hoe kunnen we als organisatie ons meldingsbereidheid verhogen?

### Kennis en vaardigheden

Met als hoofdvraag *“In hoeverre beschik ik over de juiste kennis en vaardigheden met betrekking tot cybersecurity om verzekeren dat onze digitale weerbaarheid op een passend niveau is?”* is het nodig dat de bestuurder en de CISO er zeker van zijn dat ze dezelfde taal spreken. Deze vraag is erop gericht om de bestuurder te helpen in kaart te brengen wat voor kennis en vaardigheden er nodig zijn om de verantwoordelijkheid te kunnen nemen. Tegelijkertijd kan deze vraag de CISO helpen de boodschap goed uit te leggen zodat het landt bij de bestuurder.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. Over welke kennis en vaardigheden moet ik beschikken om mijn rol als bestuurder goed in te kunnen vullen?

2. Wat zijn de grootste obstakels op het gebied van kennis waar we ons op moeten richten?
3. Welke kennisniveau is benodigd binnen de rest van de organisatie?
4. In hoeverre zijn er opleidingen en trainingen nodig voor de rest van de organisatie?

### Verantwoordelijkheid

Met als hoofdvraag *“Op welke manier kan ik invulling geven aan mijn verantwoordelijkheid voor cybersecurity binnen de organisatie?”* gaat het vooral om eigenaarschap en rolverdeling. Met de NIS2 is de bestuurder verantwoordelijk, maar misschien is het niet duidelijk wat die verantwoordelijkheid eigenlijk inhoudt. Door deze vraag te stellen zorg je voor transparantie en kun je het gebruiken als een plan van aanpak om vervolgstappen te bespreken en verwachtingen te managen.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. Wat verandert er met de NIS2 met betrekking tot mijn verantwoordelijkheid?
2. Wat zijn de meest urgente zaken waar ik mij op moet richten?
3. Wat heb je als CISO van mij nodig om voldoende grip op jouw eigen taken, bevoegdheden en verantwoordelijkheden (TBV) te hebben?
4. Hoe kunnen we onze TBV voor ons allebei verduidelijken?
5. Wat heb je nodig om ervoor te zorgen dat het management voldoende mensen en middelen toewijst om de doelstellingen te realiseren?
6. Welke mechanismes zijn er binnen de organisatie om te borgen dat de cybersecuritystrategie en beleid rondom risicomanagement goedgekeurd worden door management?

### Agendering

Met als hoofdvraag *“Welke onderwerpen met betrekking tot cybersecurity moeten we periodiek op de bestuursagenda laten terugkomen en hoe borgen we de kwaliteit van de informatie en gesprek hierover?”* willen we de bestuurder en de CISO helpen om duidelijk naar elkaar uit te spreken hoe er samen voor gezorgd kan worden dat er op het juiste moment en op de juiste manier over de juiste onderwerpen gesproken wordt zodat er impactvol gehandeld kan worden. Het periodiek terug laten komen van cybersecurity op de bestuursagenda geeft de mogelijkheid om de samenwerking en relatie van de bestuurder en CISO te versterken en zorgt ervoor dat de

bestuurder op de hoogte blijft en de benodigde verantwoordelijkheid kan (blijven) nemen. Cruciaal is dat de CISO aansluit wanneer de onderwerpen met betrekking tot cybersecurity worden besproken met de verantwoordelijke bestuurder.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren. Hou rekening bijvoorbeeld met de volwassenheid van de organisatie, wat er nog gedaan moet worden met betrekking tot de form en frequentie van de contactmomenten.<sup>1</sup>

1. Met welke frequentie moeten wij dit onderwerp op de agenda hebben staan om te borgen dat er voldoende voortgang is op dit onderwerp?
2. Hoe kunnen we het beste elkaar op de hoogte houden wat we van elkaar nodig hebben?

#### Risico's

Met de hoofdvraag "Hoe zorgen we ervoor dat we de risico's goed in kaart hebben en weten we hoe we deze kunnen beheersen?" wil je weten wat de grootste risico's zijn voor de organisatie en hoe er niet alleen maar vanuit de CISO, maar vanuit de hele organisatie ermee om wordt gegaan. Deze vraag biedt focus en creëert een moment om duidelijk de prioriteiten van elkaar te horen om vervolgens een beslissing te nemen.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. Wat heeft de CISO nodig om voldoende inzicht te krijgen in de risico's en dreigingen die we als organisatie lopen?
2. Wat moet ik als bestuurder weten om voldoende inzicht te krijgen in de Cybersecurityrisico's van deze organisatie?
3. Worden er risicoanalyses uitgevoerd, zo ja wat zijn op hoofdlijnen de onderwerpen en uitkomsten van de uitgevoerde risicoanalyses?
4. Wat zijn onze grootste risico's en dreigingen en hebben we hier voldoende grip op?
5. Zijn deze risico's incidenteel of structureel?

6. Hoe identificeren, berekenen we de kans en impact en maken we nu onderscheid in de verschillende soorten risico's en wat voor een rol moet ik hierin spelen?
7. Welke restrisico's zijn er? Zijn de restrisico's met de toezichthouder besproken?

#### Te beschermen belangen

Met de hoofdvraag "Hoe bepalen we onze te beschermen belangen en hoe zorgen we ervoor dat die veilig blijven?" is het bedoeling om inzichtelijk te krijgen wat de huidige getroffen maatregelen zijn voor de te beschermen belangen van de organisatie. Te beschermen belangen zijn zaken die cruciaal zijn voor dienstverlening van jouw organisatie. Voorbeelden van te beschermen belangen kunnen zijn: klantgegevens, productiemethoden, gegevens over jouw medewerkers, financiële gegevens, bepaalde besturingssystemen of de reputatie van jouw organisatie. Met deze vraag krijg je als bestuurder inzicht in zowel de te beschermen belangen, de getroffen maatregelen en de overwegingen die hierbij een rol hebben gespeeld.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. Wat zijn onze belangrijkste assets en processen?
2. Wat is de status van de maatregelen die we al hebben genomen en die we nog moeten nemen?
3. Welke maatregelen nemen we niet en waarom nemen we deze maatregelen niet?
4. Wie is er verantwoordelijk voor de getroffen maatregelen?
5. Is er een overzicht van de maatregelen die zijn geïmplementeerd om de systemen (inclusief hun fysieke omgeving) en gegevens van de organisatie te beschermen?
6. Hoe houden we zicht op uitvoering / naleving van de overeengekomen maatregelen?
7. Stel het gaat onverhoopt mis, hebben we een noodvoorzieningsplan? Zo ja, hoe ziet dit plan eruit?

<sup>1</sup> Eventueel kan de ISO 27001, hoofdstuk 9,3 geraadpleegd worden voor informatie over afstemmomenten en hoe deze vormgegeven kunnen

worden om de toepasbaarheid, adequaatheid en effectiviteit te meten.

### “Continuous in control” proces

Met als hoofdvraag “Hoe richten we ons “continuous in control” proces in voor cybersecurity?” richt deze vraag zich op het onderbrengen van een continu proces voor cybersecurity gebaseerd op analyses, maatregelen, monitoring en evaluaties en niet een eenmalige investering. Het doel van deze vraag is om als bestuurder meer grip te krijgen op de overkoepelende strategie die binnen de organisatie wordt toegepast omtrent cybersecurity, als dit binnen de organisatie plaatsvindt. Anders kan deze vraag dienen als gesprekstarter voor het inrichten van een strategie op cybersecurity.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. Hebben wij als organisatie een cybersecuritystrategie? Zo ja, hoe ziet deze eruit?
2. In hoeverre zijn onze beheersmaatregelen in lijn met veelgebruikte cybersecurity normen?
3. Hoe komen we tot een gedragen continuous in control proces voor cybersecurity binnen onze organisatie?
4. Wie hebben we hiervoor nodig en wat is mijn rol, waar kan ik helpen?

### Wet-en regelgeving

De hoofdvraag “Als we alles uitvoeren wat we net hebben besproken; voldoen we dan aan de huidige wet- en regelgeving op het gebied van cybersecurity? Wat moeten we mogelijk nog doen?” stel je aan het einde van je gesprek om ervoor te zorgen dat alles is besproken en er wordt gewerkt dat de organisatie voldoet aan de huidige wet- en regelgeving. De CISO moet weten wat er van hen wordt verwacht en de juiste tools hebben om de organisatie te voldoen aan de wetgeving en wat de positie is van de organisatie als geheel ten opzichte van de huidige wet- en regelgeving.

#### Voorbeeldvragen

Hieronder staan een aantal voorbeeldvragen die kunnen helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. Wat heb je nodig als CISO om voldoende te begrijpen wat er van onze organisatie wordt verwacht in het kader van wet- en regelgeving en hoe kan ik je hierbij ondersteunen?
2. Welke specifieke maatregelen hebben we al genomen om te voldoen aan de wettelijke vereisten met betrekking tot cyberbeveiliging?
3. Wat moet er gebeuren om de huidige tekortkomingen aan te pakken en wat heb jij als CISO van mij nodig?

4. Kun je me vertellen hoe onze organisatie omgaat met de aansprakelijkheid van bestuursorganen in geval van het niet naleven van de zorg- en meldplicht zoals beschreven in de NIS2?
5. Welke vraag heb ik je niet gesteld, maar zou je wel willen dat ik je gevraagd had?

### Leestip

Wil je nog meer inspiratie opdoen op hoe je als bestuurder cybersecurity binnen je organisatie kunt bellen? Lees dan de door de Cyber Security Raad ‘[Handreiking Cybersecurity voor de bestuurder](#)’.

**Uitgave**

Nationaal Cyber Security Centrum (NCSC)  
Postbus 117, 2501 CC Den Haag  
Turfmarkt 147, 2511 DP Den Haag  
070 751 5555

**Meer informatie**

[www.ncsc.nl](http://www.ncsc.nl)  
[info@ncsc.nl](mailto:info@ncsc.nl)  
[@ncsc\\_nl](https://www.instagram.com/ncsc_nl)

Juli 2024