Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Vragen om als bestuurder te stellen aan de CISO

Verbeter samen de cyberveiligheid van je organisatie

Factsheet | versie 1.1 | juli 2024

Deze factsheet helpt jou als bestuurder om het juiste gesprek te hebben met de CISO en zo grip te krijgen op de cyberveiligheid van je organisatie. Het doel van deze factsheet is dan ook niet zozeer het opleveren van een checklist om compliant te zijn, maar om de belangrijke dialoog tussen bestuurder en CISO op gang te helpen. De vragen en bijbehorende subvragen in dit document zijn gespreksstarters op een aantal belangrijke onderwerpen. Zo ga je niet alleen het gesprek aan, maar versterk je ook de bestaande relatie, samenwerking en het vertrouwen tussen jou en de CISO. Deze 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 Vulnerabilty Disclosure
- Dunea
- Cyberveilig Nederland

Intentie en randvoorwaarden

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 alle vragen passend zijn voor jouw organisatie. Het kan natuurlijk ook voorkomen dat naast deze vragen er nog meer onderwerpen en vragen relevant zijn binnen de organisatie.
3. Het kan zijn dat binnen de organisatie OT-systemen voorkomen. 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.

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.

1. *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. Ze worden niet veroordeeld en gestraft voor fouten, maar worden aangemoedigd om van fouten te leren. Een positieve veiligheidscultuur kan leiden tot een open aanspreekcultuur op onveilig gedrag en een constructieve dialoog over veilig en wenselijke gedragingen. 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 positieve veiligheidscultuur?
2. Wat is er (nog) nodig om een positieve veiligheidscultuur te creeëren?
3. In hoeverre is er managementsupport voor een (security-)melding?
4. Wat kan ik als bestuurder doen om te zorgen voor een positieve veiligheidscultuur?
5. Hoe hoog is het aantal veiligheidsmeldingen en hoe kunnen we als organisatie onze meldingsbereidheid verhogen?
6. Welke veilige escalatiemogelijkheden zijn er voor de medewerkers als een melding onvoldoende prioriteit krijgt?

2. *Kennis en vaardigheden*

Met als hoofdvraag *"In hoeverre beschik ik over de juiste kennis en vaardigheden met betrekking tot cybersecurity om er zeker van te zijn dat onze digitale weerbaarheid op een passend niveau is?"* is het nodig dat de bestuurder en de CISO dezelfde taal spreken. Deze vraag is erop gericht om de bestuurder te helpen met het in kaart brengen van de kennis en vaardigheden nodig voor het nemen van verantwoordelijkheid. Tegelijkertijd kan deze vraag de CISO helpen bij het goed uitleggen van de boodschap aan 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. Wat voor kennisniveau is benodigd binnen de rest van de organisatie?
4. In hoeverre zijn opleidingen en trainingen nodig voor de organisatie?

3. 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. Onder de NIS2 is de bestuurder verantwoordelijk, maar misschien is het niet duidelijk wat die taak eigenlijk betekent. Door het stellen van deze vraag zorg je voor transparantie. Bovendien kun je het gebruiken als een plan van aanpak om vervolgstappen te bespreken en het managen van verwachtingen.

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 de TBVn voor ons allebei duidelijker maken?
5. Wat heb je nodig om ervoor te zorgen dat het management voldoende mensen en middelen toewijst om de doelstellingen te realiseren?
6. Welke mechanisme is er binnen de organisatie om de cybersecuritystrategie te borgen en goedkeuring van beleid rondom risicomanagement door management?

4. Aandacht management

Met als hoofdvraag *"Welke onderwerpen met betrekking tot cybersecurity laten we periodiek op de bestuursagenda terugkomen en hoe borgen we de kwaliteit van de informatie en gesprekken over dit onderwerp?"* helpen we de bestuurder en de CISO in het duidelijk naar elkaar uitspreken en samen zorgen voor de juiste omgeving waarin op het juiste moment, op de juiste manier over de juiste onderwerpen gesproken waardoor impactvol handelen mogelijk is. Het periodiek toevoegen van cybersecurity aan de bestuursagenda geeft de mogelijkheid om de samenwerking en relatie van de bestuurder en CISO te versterken en zorgt ervoor dat je als 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 helpen bij het voeren van een diepgaander gesprek over dit onderwerp. Houd rekening bijvoorbeeld met de volwassenheid van de organisatie, wat er nog gedaan moet worden met betrekking tot de vorm en frequentie van de contactmomenten.[1]

1. Met welke frequentie staat cybersecurity op de agenda om te borgen dat er voldoende voortgang is op dit onderwerp?
2. Hoe kunnen we elkaar het beste op de hoogte houden over wat we van elkaar nodig hebben?
3. Welke rol en taak heeft de CISO wanneer deze aansluit bij bestuursvergaderingen?

5. Risico's

Met de hoofdvraag *"Hoe zorgen we ervoor dat we de risico's goed in kaart hebben en weten hoe we deze kunnen beheersen??"* wil je weten wat de grootste risico's zijn voor de organisatie en hoe er naast de CISO, de omgang is vanuit de hele organisatie. 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 helpen om een diepgaander gesprek te voeren over dit onderwerp.

[1] 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.

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. Welke van deze risico's zijn incidenteel en/of structureel?
6. Hoe identificeren en berekenen we de kans en impact en hoe maken we onderscheid in de verschillende soorten risico's en watvoor een rol speel ik hierin?
7. Welke restrisico's zijn er? Zijn deze acceptabel? Zijn de restrisico's met de toezichthouder besproken?

6. Te beschermen belangen

Met de hoofdvraag *"Hoe bepalen we onze te beschermen belangen en hoe zorgen we ervoor dat die veilig blijven?"* is het de 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 zijn: klantgegevens, productiemethoden/bedrijfsprocessen, gegevens over medewerkers, financiële gegevens, bepaalde besturingssystemen of de reputatie van de 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 helpen om over dit onderwerp een diepgaander gesprek te voeren.

1. Wat zijn onze belangrijkste assets en processen?
2. Welke maatregelen hebben we getroffen om deze te beschermen? Wat is de status van deze maatregelen en welke moeten nog nemen om tot een acceptabel weerbaarheidsniveau te komen?
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 dan een noodvoorzieningenplan (back-up/redundancy systemen) en een incidenresponse plan? Zo ja, zien deze eruit?

7. "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?

8. 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 de belangrijkste thema's zijn 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?

Tot slot

Neem ook eens een kijkje in de vier nieuwste publicaties van het NCSC met handvatten voor de bestuurder en de CISO.

In de publicatie van '*Hoe breng ik mijn te beschermen belangen in kaart*' bieden wij praktische handvatten die je kunt gebruiken om de 'te beschermen belangen' (TBB's) van jouw organisatie in kaart te brengen. Wanneer je jouw te beschermen belangen in kaart hebt gebracht kun je deze vervolgens gebruiken om bijvoorbeeld een risicoanalyse uit te voeren.

De publicatie '*Hoe breng ik mijn dreigingen in kaart*' biedt praktische handvatten voor jouw organisatie om dreigingen in kaart te brengen ter voorbereiding op de NIS2-richtlijn. De NIS2-richtlijn bevat een zorgplicht die jouw organisatie verplicht om de eerder genoemde risicoanalyse uit te voeren. Op basis van deze risicoanalyse kun je beoordelen wat passende maatregelen zijn om de continuïteit van diensten te waarborgen en informatie te beschermen.

Allereerst beantwoorden je vraag '*Hoe krijg ik grip op mijn security controls?*'. Security controls zijn beheersmaatregelen die gericht zijn om jouw beveiligingsrisico's te beperken door een (digitale)aanval te voorkomen. Deze publicatie helpt je om grip te krijgen op jouw security controls.

Leestip

Wil je nog meer inspiratie opdoen over hoe je als bestuurder de cyberveiligheid binnen je organisatie kunt verbeteren? 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
info@ncsc.nl
@ncsc_nl

Juli 2024