Corporategovernanceverbinding met cybersecurity nader gereguleerd

Koster, H.

WETENSCHAP

Corporategovernanceverbinding met cybersecurity nader gereguleerd

H. Koster

1 Inleiding

In beste practice 1.1.1 van de Nederlandse Corporate Governance Code is vastgelegd dat het bestuur een visie op duurzame langetermijnwaardecreatie van de vennootschap en de met haar verbonden onderneming ontwikkelt en een daarbij passende strategie formuleert. Bij het vormgeven van de strategie dient onder meer aandacht te worden besteed aan de impact van nieuwe technologieën en veranderende businessmodellen.[1] Het geven van aandacht aan nieuwe (en bestaande) technologieën op het terrein van corporate governance, vanuit onder meer het perspectief van strategie en risicobeheersing, is onderdeel van cybersecurity.[2] Op dit terrein doen zich de nodige actuele ontwikkelingen voor. Ik noem het wetsvoorstel Wet bevordering digitale weerbaarheid bedrijven, dat momenteel in de Eerste Kamer in behandeling is.[3] Voorts wijs ik op de aanstaande implementatie in Nederlandse wetgeving van de 'Network and Information Security Directive' (hierna: NIS 2-richtlijn).[4] Deze richtlijn vervangt de eerste 'NIS'-richtlijn, die in Nederland is geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (Wbni).[5] De Nederlandse overheid heeft aangekondigd dat er in 2024 ter implementatie een consultatievoorstel wordt gepubliceerd.[6] In dit artikel bespreek ik deze beide (voorgestelde) regelingen en hun verbinding met corporate governance.

1 Zie hierover ook C.D.J. Bulten, B.P.F. Jacobs & C.J.H. Jansen, Cybersecurity: Chefsache?!, Ondernemingsrecht 2021/79.

2 Cybersecurity kan (bijv.) worden omschreven als de praktijk van het beschermen van informatiesystemen, netwerken en programma's tegen digitale aanvallen.

3 Voluit: wetsvoorstel Regels ter bevordering van de digitale weerbaarheid van bedrijven. Zie Kamerstukken 36270.

4 Richtlijn (EU) 2022/2555 van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148. De NIS 2-richtlijn maakt deel uit van de op 1 maart 2021 door de Europese Commissie gepresenteerde Digital Decade en is onderdeel van een pakket van wetgeving uit Europa voor een 'digital single market'. Andere onderdelen zijn onder meer de Cyber Security Act, de Cyber Resilience Act, de Cyber Solidarity Act en de Digital Operational Resilience Act.

5 Richtlijn (EU) 2016/1148 van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie.

6 Dat is ten tijde van het schrijven van dit artikel begin mei 2024 nog niet gepubliceerd. De Europese lidstaten moeten de NIS 2-richtlijn uiterlijk op 17 oktober 2024 in de eigen wetgeving hebben geïmplementeerd.

Onderneming en Financiering 2024 (32) 2
doi: 10.5553/OenF/157012472024032002002

2 Wetsvoorstel Wet bevordering digitale weerbaarheid bedrijven

Het wetsvoorstel Wet bevordering digitale weerbaarheid bedrijven regelt de taken en bevoegdheden van de minister van Economische Zaken en Klimaat (hierna: de minister) op het gebied van de verbetering van de digitale weerbaarheid van het niet-vitale bedrijfsleven in Nederland. In dat kader is relevant het binnen het Ministerie van Economische Zaken en Klimaat (hierna: het Ministerie) in 2017 opgerichte Digital Trust Center (hierna: DTC). Dit centrum is er om niet-vitale bedrijven en maatschappelijke organisaties te kunnen informeren en adviseren over en concrete hulp en ondersteuning te kunnen bieden bij het verbeteren van hun cybersecurity en bij het afslaan van aanvallen door hackers. DTC kent twee hoofdtaken.[7] Ten eerste informatie en advies geven en ten tweede samenwerking tussen bedrijven op het gebied van digitale weerbaarheid bevorderen. Door DTC wordt nu met name algemene informatie over digitale dreigingen en incidenten aan het niet-vitale bedrijfsleven gegeven.

Uit onderzoek van het Centraal Bureau voor de Statistiek blijkt dat de digitale weerbaarheid van ondernemingen nog geen vanzelfsprekendheid is.[8] Door de verder doordringende digitalisering zou de potentiële schade aan het bedrijfsleven, zoals door ransomwareaanvallen en hacken, bij het achterblijven van digitale veiligheid en beveiliging steeds groter worden. Bovendien levert digitalisering ook nieuwe onderlinge afhankelijkheden op bij bedrijven, niet alleen tussen digitale systemen, maar ook in de digitale leveranciersketen.[9] Het belang van digitale veiligheid en beveiliging groeit aldus. De onveiligheid van een onderneming kan via de verbindingen in deze keten ook de onveiligheid elders in de keten beïnvloeden.[10] Bedrijven hebben de overheid gevraagd om te zorgen voor (meer) informatiedeling vanuit de overheid in situaties dat zij beschikt over relevante informatie over dreigingen, kwetsbaarheden en incidenten. Thans informeert de overheid op basis van de Wbni alleen specifieke doelgroepen binnen het Nederlandse bedrijfsleven, te weten vitale bedrijven en digitale dienstverleners. Op basis van het wetsvoorstel kunnen straks ook niet-vitale bedrijven informatie van de overheid ontvangen. De minister benoemt daarbij dat verwacht mag worden dat ondernemingen bij een voor hen concrete bedreiging eerder naar hun digitale weerbaarheid zullen kijken dan bij een algemene waarschuwing.[11] Voorts zal door DTC bij informatie over een specifieke dreiging een zo praktisch mogelijk handelingsperspectief worden aangereikt, opdat het bedrijf ook weet welke vervolgstap(pen) het kan nemen.[12] Voor de uitbreiding van deze informatievoorziening wordt in het wetsvoorstel een verdere inbedding van de taken en bevoegdheden van de minister vastgelegd. Het wetsvoorstel creëert, naast de reeds bestaande bevoegdheden op grond van de Wbni, aldus een nieuwe wettelijke taak voor de minister. Het wetsvoorstel bevat daartoe

7 Zie www.digitaltrustcenter.nl/.
8 Zie www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019.
9 Kamerstukken II 2022/23, 36270, nr. 3, p. 1.
10 Zie www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.
11 Kamerstukken II 2022/23, 36270, nr. 3, p. 1-2.
12 Kamerstukken II 2022/23, 36270, nr. 3, p. 2.

onder meer bepalingen over het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten en het samenwerken met andere bestuursorganen en organisaties. In dat kader mogen persoonsgegevens worden verwerkt. Ook voorziet het wetsvoorstel in een wettelijke grondslag om bij andere (publiekrechtelijke) organisaties de voor de taakuitoefening noodzakelijke gegevens op te vragen alsmede in de mogelijkheid van derden om in reactie daarop zo nodig ook persoonsgegevens te verstrekken aan de minister.

Door in de situatie waar de overheid over (acute) dreigingsinformatie beschikt deze aan niet-vitale bedrijven te verstrekken, biedt de overheid dergelijke bedrijven de kans om met deze informatie zelf te beoordelen of en in welke mate zij maatregelen moeten treffen voor de mitigatie van een kwetsbaarheid, voor de afwering van een dreiging of voor de oplossing van een daadwerkelijke inbreuk. Dit is ook belangrijk voor de Nederlandse economie.[13] De ondernemingen kunnen dan bewuste, op risico's gebaseerde keuzes maken over de te nemen maatregelen op het gebied van digitale beveiliging. Hierbij kan worden gedacht aan voorlichting door trainingen voor personeel, specifieke IT-beveiligingsmaatregelen, maar ook aan maatregelen voor de bedrijfscontinuïteit of de inhuur van gespecialiseerde diensten.[14]

3 Network and Information Security Directive (NIS 2-richtlijn)

De NIS 2-richtlijn is de opvolger van de NIS-richtlijn. Met de NIS-richtlijn werd nagestreefd om de cyberbeveiliging en de weerbaarheid in EU-lidstaten te verbeteren. Sindsdien hebben de ontwikkelingen evenwel niet stilgestaan, onder andere door de verdergaande digitale transformatie en de toenemende onderlinge (grensoverschrijdende) verbondenheid van de samenleving. Dit veroorzaakt volgens de Europese wetgever een toename van het aantal cyberincidenten en de omvang, de complexiteit, de frequentie en de impact ervan.[15] Een herziening van de NIS-richtlijn werd daarom noodzakelijk geacht. De NIS 2-richtlijn brengt meer sectoren, entiteiten en activiteiten onder de reikwijdte van de regeling. Ook komen er strengere beveiligingsnormen en meldingsvereisten voor incidenten. De NIS 2-richtlijn behelst daartoe de nodige nieuwe verplichtingen. De richtlijn ziet op risico's die netwerk- en informatiesystemen bedreigen, zoals cyberbeveiligingsrisico's. Bovendien is het idee dat de komst van de NIS 2-richtlijn bijdraagt aan meer Europese harmonisatie en een hoger niveau van cybersecurity bij bedrijven en organisaties. Er is voorts minder vrijheid voor lidstaten om entiteiten binnen het toepassingsbereik te plaatsen of om ze erbuiten te laten.

De scope van de NIS 2-richtlijn is (met name) vastgelegd in twee bijlagen bij de richtlijn met een opsomming van zeer kritieke (bijlage 1) en andere kritieke sectoren (bijlage 2). Voor de vraag of een organisatie binnen de reikwijdte van de

13 Kamerstukken II 2022/23, 36270, nr. 3, p. 3.

14 Kamerstukken II 2022/23, 36270, nr. 3, p. 3.

15 European Commission, Frequently Asked Questions: Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), beschikbaar via: digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive.

doi: 10.5553/OenF/157012472024032002002

NIS 2-richtlijn valt, is van belang of een organisatie actief is in een van de sectoren genoemd in de bijlagen. Is dat het geval, dan wordt vervolgens naar de omvang van de organisatie gekeken. De NIS 2-richtlijn ziet op middelgrote of grote organisaties, met als ondergrens vijftig medewerkers en/of een jaarlijkse omzet van in elk geval € 10 miljoen.[16] Kleinere entiteiten die actief zijn in een (zeer) kritieke sector kunnen niettemin toch onder de scope vallen. Dat ziet op entiteiten die een sleutelrol hebben in de samenleving, economie of bepaalde sectoren, dan wel bepaalde diensten leveren die een sleutelrol vervullen, denk aan aanbieders van openbare communicatienetwerken of -diensten, domeinnaamdiensten en centrale en regionale overheidsinstanties.

Onder de NIS 2-richtlijn vervalt het onderscheid tussen aanbieders van essentiële diensten en digitale diensten van de NIS-richtlijn. Dit verschil bleek achterhaald. Is de NIS 2-richtlijn van toepassing, dan geldt dat gekeken moet worden of de organisatie als 'essentiële' of als 'belangrijke' entiteit kan worden aangemerkt. Dit onderscheid is vooral relevant voor het toezicht op de entiteit. Er is sprake van een (pro) actief toezicht voor essentiële entiteiten en een reactief toezicht voor belangrijke entiteiten. Uitgangspunt daarbij is dat alle organisaties die niet gelden als een essentiële entiteit, aangemerkt worden als belangrijke entiteit. Essentiële entiteiten zijn in elk geval grote organisaties die in een zeer kritieke sector opereren en bepaalde sleutelrolorganisaties. Organisaties die in zeer kritieke sectoren opereren, zijn onder meer energieleveranciers, vervoersbedrijven (waaronder luchtvaartmaatschappijen), kredietinstellingen, bepaalde zorgaanbieders, drinkwaterbedrijven, aanbieders van digitale infrastructuur, zoals aanbieders van datacenterdiensten, cloudcomputingdiensten en entiteiten die zich bezighouden met het beheer van (b2b) ICT-diensten. Naast essentiële entiteiten onderscheidt de richtlijn ook belangrijke entiteiten. Deze worden nader geduid in art. 3 lid 2 NIS 2-richtlijn. De enigszins lastig te lezen omschrijving luidt: 'Voor de toepassing van deze richtlijn worden entiteiten van een in bijlage I of II bedoeld type die niet in aanmerking komen als essentiële entiteiten krachtens lid 1 van dit artikel, als belangrijke entiteiten beschouwd. Hiertoe behoren entiteiten die door lidstaten aangemerkt zijn als belangrijke entiteiten krachtens artikel 2, lid 2, punten b) tot en met e).'

Het vierde hoofdstuk van de NIS 2-richtlijn bevat verplichtingen op het terrein van risicobeheersmaatregelen en rapportages. Van belang is dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen dienen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

16 Zie art. 2 lid 1 NIS 2-richtlijn jo. art. 2 van de bijlage bij Aanbeveling 2003/361/EG.

De maatregelen voor het beheer van cyberbeveiligingsrisico's en de rapportageverplichtingen die in de NIS 2-richtlijn zijn vastgesteld, zijn van toepassing op de relevante essentiële en belangrijke entiteiten, ongeacht of deze entiteiten het onderhoud van hun netwerk- en informatiesystemen intern uitvoeren of uitbesteden.[17] De NIS 2-richtlijn kent voor het waarborgen van beveiliging bij organisaties een principle-based benadering.[18]

Met de NIS 2-richtlijn moet een cultuur van risicobeheer worden bevorderd en ontwikkeld, die risicobeoordelingen en de uitvoering van op de risico's afgestemde maatregelen voor het beheer van cyberbeveiligingsrisico's behelst.[19] Beklemtoond wordt ook dat maatregelen voor het beheer van cyberbeveiligingsrisico's moeten voorzien in een systemische analyse, waarbij rekening wordt gehouden met de menselijke factor, om een volledig beeld te krijgen van de beveiliging van het netwerk- en informatiesysteem.[20] Ook dienen leden van bestuursorganen van essentiële en belangrijke entiteiten een opleiding te volgen, opdat zij voldoende kennis en vaardigheden verwerven om (1) risico's te kunnen identificeren en (2) risicobeheerspraktijken op het gebied van cyberbeveiliging te kunnen beoordelen met het oog op de diensten die door de entiteit worden verricht. De idee is dat bestuurders daardoor bewuster worden van de uitdagingen die samenhangen met cybersecurity.

De NIS 2-richtlijn kent strengere beveiligingsverplichtingen en deze omvatten in elk geval:

a beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b incidentenbehandeling;
c bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningenplannen, en crisisbeheer;
d de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
e beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
f beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
g basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
i beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;

17 Overweging 83 NIS 2-richtlijn.
18 Zie hierover N.M. Brouwer & J.J.H. van Mil, Cybersecurity in Europa. De herziene Netwerk- en Informatiebeveiligingsrichtlijn (NIS 2), NJB 2023/674, p. 748.
19 Overweging 77 NIS 2-richtlijn.
20 Overweging 78 NIS 2-richtlijn.

doi: 10.5553/OenF/157012472024032002002

j wanneer gepast, het gebruik van multifactorauthenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

Nieuw is dat de NIS 2-richtlijn voorschrijft dat gereguleerde entiteiten ook maatregelen moeten treffen om de toeleveringsketen te beveiligen.[21] Dit ziet op de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners. Het ziet derhalve op rechtstreekse leveranciers of dienstverleners. In verband hiermee bepaalt de richtlijn voorts dat de lidstaten ervoor zorgen dat de entiteiten, wanneer zij overwegen welke maatregelen passend zijn, rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.[22] Dit roept de vraag op of in het kader van de beoordeling van de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken het ook om niet-rechtstreekse partijen gaat. Voor de reikwijdte kan dat nogal een verschil uitmaken.

Op basis van de herziene regeling over rapportageverplichtingen dienen essentiële en belangrijke entiteiten ieder incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten onverwijld te melden. Organisaties kennen overigens op grond van de Algemene verordening gegevensbescherming (AVG) al beveiligings- en meldplichten.[23] De AVG-regeling kent evenwel een andere focus. Bij de AVG-regeling ligt de focus op de vertrouwelijkheid en integriteit van persoonsgegevens,[24] terwijl de NIS 2-richtlijn ziet op de continuïteit van netwerken en diensten. Die meldplicht is onder de NIS 2-richtlijn uitgebreid. Bepaald is dat entiteiten ieder significant incident melden aan de bevoegde autoriteit. Een cyberincident moet daarnaast ook bij het Computer Security Incident Response Team (CSIRT) worden gemeld, dat vervolgens hulp en bijstand kan verlenen.[25] Er is sprake van een 'incident' bij een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens, of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. Deze omschrijving is meeromvattend dan de definitie onder de NIS-richtlijn, waar een daadwerkelijk schade-effect nodig was. Er is sprake van een significant incident als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroor-

21 Art 21 lid 2 onder d NIS 2-richtlijn.

22 Art 21 lid 3 NIS 2-richtlijn.

23 Zie over de gelijkenissen en verschillen tussen beide regelingen L. Viergever & G. van Til, NIS 2 en de AVG: werk aan de winkel?, Computerrecht 2023/166.

24 Zie J.A. Hofman, De beveiliging van persoonsgegevens, Deventer: Wolters Kluwer 2022, par. 7.3.5.5.

25 In art. 23 lid 1 NIS 2-richtlijn is vastgelegd dat elke lidstaat ervoor zorgt dat essentiële en belangrijke entiteiten elk incident dat aanzienlijke gevolgen heeft voor de verlening van hun diensten als bedoeld in lid 3 (significant incident) onverwijld melden bij hun CSIRT of, indien van toepassing, hun bevoegde autoriteit. Ik ga ervan uit dat bij beide gemeld moet worden, maar de richtlijn vindt een van beide dus al voldoende.

zaakt of kan veroorzaken, dan wel andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken. Is hiervan sprake, dan dient onverwijld en in elk geval binnen 24 uur na kennisname van het significante incident een vroegtijdige waarschuwing te worden gegeven. Daarbij moet worden geduid of sprake is van een onrechtmatige of kwaadwillende oorzaak en van mogelijke grensoverschrijdende gevolgen. Ook onverwijld en in ieder geval binnen 72 uur na kennisname van het significante incident moet een (grondige) incidentmelding worden gedaan. Daarin moet een initiële beoordeling van het incident, met inbegrip van de ernst en de gevolgen ervan, worden opgenomen. Vervolgens dient uiterlijk binnen een maand na de incidentmelding een eindverslag te worden ingediend met daarin onder meer een gedetailleerde omschrijving van het incident en de genomen cybersecuritymaatregelen. Zijn ontvangers van een verleende dienst mogelijk ook door het incident getroffen, dan dienen zij ook onverwijld geïnformeerd te worden over de maatregelen die zij kunnen treffen. Wat onverwijld hier inhoudt, is evenwel niet nader ingevuld en wordt dus in eerste instantie aan de betrokken entiteit overgelaten om te beoordelen. Ten slotte, om tegen te gaan dat situaties strategisch niet gemeld worden, is bepaald dat een melding niet leidt tot een verhoogde aansprakelijkheid.

De nationale bevoegde autoriteit dient bepaalde onderzoeksbevoegdheden te hebben, zoals het kunnen uitvoeren van inspecties, audits en beveiligingsscans en het opvragen van informatie, gegevens en andere documenten. De NIS 2-richtlijn verplicht de lidstaten om te zorgen voor effectieve, evenredige en afschrikkende sancties. Dat kan strafrechtelijk of administratief zijn. Er moet daarbij rekening worden gehouden met de ernst en aard van de overtreding en voorts met factoren zoals de veroorzaakte schade, samenwerking met de bevoegde autoriteit en andere omstandigheden. Er kunnen administratieve boetes worden opgelegd van maximaal € 7 miljoen of 1,4% van de wereldwijde jaaromzet voor belangrijke entiteiten en € 10 miljoen of 2% van de jaarlijkse wereldwijde omzet van essentiële entiteiten, afhankelijk van wat hoger is. Ook kunnen andere maatregelen worden getroffen. Zoals al hiervoor genoemd, is er sprake van een (pro)actief toezicht voor essentiële entiteiten en een reactief toezicht voor belangrijke entiteiten en dat betekent dat er meer maatregelen mogelijk zijn bij essentiële entiteiten. Voor zowel essentiële als belangrijke entiteiten wordt genoemd het geven van waarschuwingen en bindende aanwijzingen of het gebieden om (een) bepaalde gedraging(en) te staken. Als een waarschuwing, bindende aanwijzing of bepaald gebod niet doeltreffend blijkt te zijn, dan kunnen bevoegde autoriteiten een termijn opleggen om alsnog het geconstateerde nalevingsprobleem op te lossen of aan de eisen van de bevoegde autoriteit te voldoen. Gebeurt dat niet, dan kan de bevoegde autoriteit bij een essentiële entiteit een certificering of vergunning tijdelijk opschorten of daarom verzoeken bij de rechter. Ook kan bij een essentiële entiteit een natuurlijk persoon met leidinggevende verantwoordelijkheden op het niveau van de algemeen directeur door het bevoegde orgaan of de rechter tijdelijk worden verboden om leidinggevende functies in de desbetreffende essentiële entiteit uit te voeren. Voorts kan bij een essentiële entiteit – derhalve proactief – een controlefunctionaris worden aange-

wezen die gedurende een bepaalde periode duidelijk omschreven taken heeft om erop toe te zien dat de betrokken entiteit aan art. 21 en 23 NIS 2-richtlijn voldoet.

De NIS 2-richtlijn is duidelijk gericht op het waarborgen van een hoge mate van verantwoordelijkheid voor de risicobeheersmaatregelen en rapportageverplichtingen op het gebied van cyberbeveiliging op het niveau van de essentiële en belangrijke entiteiten. In een van de overwegingen bij de richtlijn wordt daarover nog toegelicht dat de bestuursorganen van de essentiële en belangrijke entiteiten de risicobeheersmaatregelen op het gebied van cyberbeveiliging goedkeuren en toezicht dienen te houden op de uitvoering ervan.[26] De NIS 2-richtlijn bevat daarnaast twee (nieuwe) bepalingen over aansprakelijkheid. De NIS-richtlijn bevat geen bepalingen hierover. Ten eerste wordt in art. 20 lid 1 NIS 2-richtlijn over aansprakelijkheid van het bestuur van essentiële en belangrijke entiteiten gemeld:

> 'De lidstaten zorgen ervoor dat de bestuursorganen van essentiële en belangrijke entiteiten de door deze entiteiten genomen maatregelen voor het beheer van cyberbeveiligingsrisico's goedkeuren om te voldoen aan artikel 21, toezien op de uitvoering ervan en aansprakelijk kunnen worden gesteld voor inbreuken door de entiteiten op dat artikel.'

Ten tweede wordt in art. 32 lid 6 NIS 2-richtlijn bepaald dat (mogelijk onder meer) bestuurders van entiteiten die onder de NIS 2-richtlijn vallen persoonlijk aansprakelijk kunnen worden gesteld. Deze aansprakelijkheidsbepaling ziet alleen op essentiële entiteiten. Deze bepaling luidt:

> 'De lidstaten zorgen ervoor dat elke natuurlijke persoon die verantwoordelijk is voor of optreedt als wettelijke vertegenwoordiger van een essentiële entiteit op basis van de bevoegdheid om deze te vertegenwoordigen, de bevoegdheid om namens deze entiteit beslissingen te nemen of de bevoegdheid om controle uit te oefenen op deze entiteit, de bevoegdheid heeft om ervoor te zorgen dat deze entiteit deze richtlijn nakomt. De lidstaten zorgen ervoor dat dergelijke natuurlijke personen aansprakelijk kunnen worden gesteld voor het niet nakomen van hun verplichtingen om te zorgen voor de naleving van deze richtlijn.'

Naar huidig Nederlands recht is de aansprakelijkheid van bestuurders (vooral) gebaseerd op art. 6:162 van het Burgerlijk Wetboek (BW) (in combinatie met art. 2:9 BW), op grond waarvan een bestuurder, gelet op zijn verplichting tot een behoorlijke taakvervulling, persoonlijk een voldoende ernstig verwijt moet kunnen worden gemaakt. De tekst lijkt de mogelijkheid open te laten dat deze NIS 2-richtlijn-aansprakelijkheid niet alleen voor statutaire bestuurders relevant is, maar ook voor anderen die beslissingen kunnen nemen, zoals mogelijk leden van een *executive committee*. Ook wordt gewezen op personen die bevoegdheid hebben om controle uit te oefenen op een entiteit. Dat roept de vraag op of dit ook ziet op bepaalde aandeelhouders en/of mogelijk (ook) op leden van de raad van commissarissen.

26 Overweging 137 NIS 2-richtlijn.

Het hangt ervan af hoe de tekst gelet op tekstonderdelen alsmede de samenhang daarvan gelezen moet worden. Ik ben benieuwd hoe de Nederlandse wetgever deze aansprakelijkheid gaat implementeren. Het lijkt mij in elk geval niet onvoorstelbaar dat deze bepaling tot daadwerkelijke (massa)schadeclaims zal gaan leiden bij bestuurders van essentiële entiteiten met cyberincidenten. Daarbij kan ook worden gedacht aan het verhaal van opgelegde boetes.

4 Afronding

In dit artikel heb ik vanuit het perspectief van corporate governance het voorstel voor de Wet bevordering digitale weerbaarheid bedrijven en de NIS 2-richtlijn besproken. Deze beide regelingen dragen zeker bij aan meer duidelijkheid over hetgeen van bedrijven verwacht wordt op het terrein van cybersecurity. Ik vind de verdere invulling van cybersecurity vanuit corporategovernanceperspectief een positieve ontwikkeling. Zoals in dit artikel ook aangestipt, verwacht ik dat de NIS 2-richtlijn nog de nodige vragen zal oproepen, zoals de reikwijdte van de regeling over de aansprakelijkheid van bestuurders en anderen. Ook de scope van de beveiliging van de toeleveringsketen lijkt nog niet geheel duidelijk. Nadat beide regelingen in werking zijn getreden, zullen er vermoed ik ook nog wel de nodige vragen opkomen. Kortom, cybersecurity zal ons nog wel even bezighouden.

doi: 10.5553/OenF/157012472024032002002