Goed bestuur begint bij goed geïnformeerd zijn

Opleidingsplicht verkleint risico op bestuurdersaansprakelijkheid bij cyberincidenten

Een cyberincident kan leiden tot bestuurdersaansprakelijkheid. Als u denkt dat dit risico ver weg is, bijvoorbeeld omdat u uw ICT heeft ondergebracht bij een professionele partij, dan hebben Jeroen van Helden, Menno de Wijs en Sonja Geldermans slecht nieuws voor u. Die tijd is voorbij, vanwege een aanzienlijk wetgevingspakket dat door de EU is uitgevaardigd.

ICT-SYSTEMEN ZIJN VOOR VEEL BEDRIJVEN EN INSTELLINGEN ESSENTIEEL, DAT WEET DE EU OOK. Een ICT-gerelateerd incident heeft al snel significante sociale en economische gevolgen. Vanwege de toenemende afhankelijkheid van ICT, en een toename van de cyberdreigingen, poogt de EU met steeds verdergaande wetgeving bedrijven en instellingen weerbaarder te maken voor dreigingen op cybergebied. Voorbeelden van deze wetgeving zijn:

- Algemene verordening gegevensbescherming (AVG): de bekende privacyregels.
- Network and Information Security richtlijn (NIS2): cybersecurityregels voor ondernemingen in kritieke sectoren.
- Digital Operational Resilience Act (DORA): cybersecurityregels voor financiële ondernemingen.
- AI Verordening: regelgeving voor de ontwikkeling en het gebruik van AI-systemen.
- Cyber Resilience Act (CRA): cybersecurityeisen aan hardware en software producten.

Op het eerste gezicht lijkt deze wetgeving uitsluitend op bedrijven en instellingen zelf te zien. Een bestuurder die dat denkt, vergist zich. De wet- en regelgeving kan ook gevolgen hebben voor de persoonlijke positie van bestuurders. Om dat uit te leggen, nemen we eerst een duik in het leerstuk van bestuurdersaansprakelijkheid. Vervolgens staan we stil bij enkele concrete verplichtingen uit de recente EU-wetgeving die belangrijke gevolgen hebben voor de positie van bestuurders. Wij ronden af met een aantal voorbeelden uit de praktijk.

Bestuurdersaansprakelijkheid

Het is de taak van het bestuur om de vennootschap te besturen en het beleid van de onderneming te bepalen. Het bestuur is verplicht om deze taak op een behoorlijke wijze te vervullen. Gaat er wat mis, dan is het uitgangspunt dat alleen de onderneming de schade draagt. Bestuurders zijn in beginsel niet persoonlijk aansprakelijk. Toch is het wel mogelijk dat een bestuurder ook in privé aansprakelijk is voor han-

delingen of nalaten van het bedrijf of de instelling waarvan hij of zij bestuurder is. Dat is niet nieuw, het is onder andere mogelijk als de bestuurder een ernstig verwijt kan worden gemaakt ten aanzien van de wijze waarop hij of zij zijn bestuurstaak heeft vervuld. Deze ernstig-verwijtnorm wordt onder andere ingevuld door wet- en regelgeving.

Het bestuur is collectief verantwoordelijk voor de uitvoering van de bestuurstaak en in principe dus ook collectief persoonlijk aansprakelijk. Het is aan een individuele bestuurder om aan te tonen dat hem in een concreet geval geen ernstig verwijt valt te maken. Het enkele feit dat cybersecurity in de onderlinge taakverdeling bij een andere bestuurder is neergelegd, doorgaans de chief information security officer (CISO), is op zichzelf onvoldoende om aansprakelijkheid te ontlopen.

Verplichtingen bestuurders

De nieuwe wetgeving verlangt van bestuurders dat zij kennis hebben van

Een verstandige bestuurder voldoet aan de opleidings-verplichtingen

digitale diensten, ICT en, meer recent, AI, en dat zij actief op deze onderwerpen sturen. De beheersing van risico's op het gebeid van ICT en cybersecurity zijn dus steeds meer een onderdeel geworden van de 'behoorlijke taakvervulling' door het bestuur. De focus ligt op bewustwording van de risico's die een bedrijf op dat gebied loopt en het op orde brengen van de interne organi-

Beeld: Shutterstock

Een bestuurder kan in privé aansprakelijk zijn voor handelingen of nalaten van het bedrijf of de instelling

satie en governance. De DORA en NIS2 maken daarvan expliciet een taak én verantwoordelijkheid voor het bestuur. Het bestuur kan zich niet langer verschuilen achter een IT-afdeling of haar eigen onwetendheid, in tegendeel.

Concrete voorbeelden zijn:

- Het bestuur moet beschikken over voldoende kennis en vaardigheden om ICT-risico's te kunnen identificeren en beheersen;[1]
- Het bestuur moet regelmatig opleidingen volgen over ICT-risicobeheersing; [2]
- Het bestuur moet zorgdragen voor AI-geletterdheid van medewerkers die met AI-systemen werken;[3]
- Het bestuur moet het informatiebeveiligingsbeleid goedkeuren;[4]
- Het bestuur moet toezien op implementatie van het informatiebeveiligingsbeleid.[5]

Beleid goedkeuren en toezien op implementatie

Het bestuur dient de risico's die de organisatie loopt op het gebied van cyberdreigingen in kaart te brengen, beheersmaatregelen vast te stellen en erop toe te zien dat de maatregelen daadwerkelijk in de organisatie worden geïmplementeerd. Dit is niet een eenmalige exercitie voor het bestuur. De weerbaarheid tegen cyberdreigingen moet een terugkerend onderwerp zijn op de agenda van het bestuur en dient te zijn ingebed in een plan-do-act-check cyclus.

Opleidingen

Om op een goede manier uitvoering te kunnen geven aan voornoemde verplichtingen, dienen de leden van het bestuur bovendien te beschikken over voldoende kennis en vaardigheden op het gebied van ICT. Het gaat hierbij niet noodzakelijkerwijs om technische kennis van ICT, maar wel om kennis van de dreigingen die er zoal zijn op het gebied van cyber, de technische en organisatorische maatregelen die je als organisatie kunt treffen om je te beschermen tegen die dreigingen en de wijze waarop je risicoanalyses maakt en stuurt op het onderwerp digitale weerbaarheid.

Om het belang van voldoende kennis en vaardigheden bij het bestuur verder te onderstrepen, wordt aan de leden van het bestuursorgaan de verplichting opgelegd om aantoonbaar opleidingen te volgen op het gebied van ICT-risicobeheersing. Een dergelijke verplichting lijkt een Europese trend te zijn. Zo is die verplichting tot opleiding bijvoorbeeld terug te vinden in de AI-verordening (art. 4), de NIS2-richtlijn (art. 20 lid 2) en de DORA (art. 5 lid 4). Door middel van een certificaat kunnen bestuurders aantonen dat zij aan hun opleidingsverplichting hebben voldaan.

Verzwaarde zorgplicht

Deze en andere verplichtingen leiden ertoe dat bestuurders in de praktijk te maken krijgen met een verzwaarde zorgplicht om ICT-risico's te beheersen. Het ontbreken van passende beheers- en controlesystemen, of het (structureel) niet voldoen aan opleidingsverplichtingen, kan resulteren in een ernstig verwijt en daarmee bestuurdersaansprakelijkheid. Een verstandige bestuurder zorgt er dus voor dat hij of zij aan de opleidingsverplichtingen voldoet, dat er een deugdelijk ICT-beleid is geïmplementeerd én dat de

bestuurdersaansprakelijkheids-verzekering op orde is. De schade van een cyberincident kan enorm zijn: de bedrijfsvoering komt stil te liggen, systemen of data moeten worden hersteld, afnemers dienen schadeclaims in, er moet misschien losgeld worden betaald, om nog maar te zwijgen over de reputatieschade. Daarnaast kunnen de toezichthoudende instanties forse, omzet gerelateerde boetes opleggen, wanneer een entiteit zich niet aan beveiligingsverplichtingen of aanverwante meldplichten blijkt te hebben gehouden. Onder omstandigheden kan een bestuurlijke boete ook rechtstreeks aan een bestuurder worden opgelegd. Zelfs faillissement is niet ondenkbaar. De curator zal dan onderzoeken of de bestuurder(s) persoonlijk aansprakelijk kan worden gesteld voor het tekort van het faillissement.

Amerikaanse toestanden?

In de Verenigde Staten loopt men vaak voorop en daar zijn al talloze rechtszaken gevoerd tegen bestuurders vanwege cyberaanvallen. Voorbeelden zijn procedures na de aansprakelijkstelling van de bestuurders van bijvoorbeeld Target, Home Depot, Wendy's en Yahoo. In het geval van Home Depot heeft dit geresulteerd in een schikking om een vonnis af te wenden. Onderdeel van de schikking was dat Home Depot alsnog maatregelen zou nemen om de cybersecurity te verbeteren.

Het lijkt slechts een kwestie van tijd voordat ook in Nederland bestuurders rechtstreeks aansprakelijk worden gesteld bij cyberincidenten. In dat kader mag niet onvermeld blijven dat het sinds de inwerkingtreding van de WAMCA in 2020, in Nederland mogelijk is om collectief schadevergoeding te vorderen. Dit heeft de laatste jaren geleid tot diverse massaclaims voor o.a. overtredingen van de AVG, al dan niet in verband met datalekken. Het is goed denkbaar dat er in de nabije toekomst massaclaims gaan volgen tegen organisaties die hun digitale weerbaarheid niet op orde hadden, en dat bestuurders in die procedures worden betrokken.

Niet simpel

Het moge duidelijk zijn dat de druk op bestuurders vanuit diverse richtingen toeneemt om toegerust te zijn voor de uitdagingen in het digitale domein. Nieuwe EU wet- en regelgeving introduceert nieuwe verplichtingen, met specifieke verantwoordelijkheden voor het bestuur, die bij schending kunnen leiden tot bestuurdersaansprakelijkheid. Bestuurders dienen zich te realiseren dat zij niet simpelweg aan alle wet- en regelgeving kunnen voldoen door hun ICT onder te brengen bij professionele partijen; ook dan moeten zij zelf het ICT-risico in kaart brengen, beleid goedkeuren, toezien op de implementatie daarvan, passende contractuele afspraken maken met die ICT-leveranciers en relevante opleidingen volgen, om zo bestuurdersaansprakelijkheid te voorkomen.

[1] Artikel 20 lid 2 NIS2 en Artikel 5 lid 4 DORA.
[2] Artikel 20 lid 2 NIS2 en Artikel 5 lid 4 DORA.
[3] Artikel 9 lid 5 AI Verordening
[4] Artikel 20 lid 1 NIS2 en Artikel 5 lid 2 DORA.
[5] Artikel 20 lid 1 NIS2 en Artikel 5 lid 2 DORA.

Sonja Geldermans is advocaat ondernemingsrecht en aanbestedingsrecht bij De Clercq Advocaten Notariaat.

Jeroen van Helden is advocaat IT, Privacy & Cybersecurity bij De Clercq Advocaten Notariaat.

Menno de Wijs is advocaat aanbestedingsrecht bij De Clercq Advocaten Notariaat.

Reacties en bijdragen

Voor reacties en nieuwe bijdragen van IT-experts:
Tanja de Vrede
020-2467230
t.d.vrede@agconnect.nl