STELLING

In artikel 26 (governance) is thans voorzien dat de leden van het bestuur van een Essentiele of Belangrijke onderneming in de zin van de Cyberbeveiligingswet, *aantoonbaar en verplicht* trainingen moeten volgen met als doel:

a. Risico's voor de beveiliging van netwerk- en informatiesystemen te kunnen identificeren;

b. Risicobeheersmaatregelen op het gebied van cyberbeveiliging te kunnen beoordelen; en

c. De gevolgen van de risico's en risicobeheersmaatregelen voor de diensten die door de entiteit worden verleend te kunnen beoordelen.

Daarnaast moeten deze leden van de Raad van Bestuur bedoelde kennis actueel houden en dit kunnen aantonen door middel van het overleggen van een nader te bepalen certificaat.

WEERWOORD, met verzoek tot aanpassing wettekst wetsartikel 26

Cyber Security wordt binnen veel bedrijven geborgd door een team specialisten, met aantoonbare kennis en ervaring op het gebied van Cyber Security. Cyber Security is een snel veranderend en dynamisch vakgebied. Een vakgebied waarvoor specialisten kunnen afstuderen op MBO, HBO en Academisch niveau.

Leden van een Raad van Bestuur worden aangesteld op basis van, voor dat bedrijf, specifieke opleidingsvereisten en ervaring. Voor de uitvoering van verschillende specifieke kennisgebieden, zoals Finance, Operations, Legal, HRM, Procurement, interne Bedrijfsvoering, Communicatie, Health Safety Environment en Quality, etc, laat de Raad van Bestuur zich continue ondersteunen en adviseren door de specifieke, daarvoor opgeleide kennisverantwoordelijken. Dat is zeker ook van toepassing ten aanzien van het vakgebied (Cyber) Security. In dat geval laat de Raad van Bestuurd zich bijstaan door bijvoorbeeld Register Security Experts, Chief Information Security Officers, Security Officers, etc., al dan niet CISM of CISSP gecertificeerd. Ten aanzien van Informatiebeveiliging zijn twee onderwerpen van groot belang.

1. Ten aanzien van Cyber Security dient een onderneming aan te tonen dat het de juiste Cyber Security maatregelen heeft getroffen en wat wordt aangetoond door middel van het afgeven van een daarop van toepassing zijnde certificering, zoals bv het ISO 27001 certificaat. Voor deze certificeringen is het niet alleen van belang dat het bedrijf *in het bezit is* van een management systeem wat van toepassing is op het gebied van (Cyber) Security , maar moet tevens *de werking daarvan worden aangetoond* tijdens een audittraject uitgevoerd door een onafhankelijke Auditor;

2. Daarnaast is het van het grootste belang dat kernfunctionarissen die verantwoordelijk zijn voor de informatiebeveiliging *ten minste maandelijks*, op basis van een cyber-security dashboard, aan de Raad van Bestuur *rapporteren* ten aanzien van Cyber Security en dat alles in de breedte. Dát is het moment waarop binnen de Raad van Bestuur gediscussieerd wordt over Cyber Security. En dat staat uiteraard los van specifieke momenten waarbij sprake is van (cyber) incidenten of bv bij de aanschaf en implementatie van Cyber Security producten of -diensten. Dus het vastleggen, of bijvoorbeeld door middel van de Cyberbeveiligingswet *afdwingen* dat er altijd een directe rapportagelijn is met de Raad van Bestuur, lijkt dan meer logisch dan het volgen van een training op dat vlak. Op die manier kan een Raad van Bestuur zich nooit aan haar verantwoordelijkheid onttrekken en geeft het dus invulling aan de

Zorgplicht zoals de Cyberbeveiligingswet ook voorschrijft. De hoofdtaak van een Raad van Bestuur is immers wat het woord al aangeeft, namelijk het besturen van een onderneming. Dat komt in het gedrang indien voor verschillende (deel)vakgebieden verschillende trainingen moeten worden gevolgd. Dáár hebben de Bestuurders dus Cyber Security experts voor in dienst.

WIJZIGIGSVOORSTEL ARTIKEL 26

- Het wijzigingsvoorstel zou wat ons betreft zijn, dat bedoelde trainingen uitsluitend van toepassing zijn voor die bestuurders *die geen of niet voldoende kennis in huis hebben* om alle afwegingen te maken zoals genoemd onder Artikel 26, lid, A, B en C. Indien een onderneming echter aantoonbaar de beschikking heeft over één of meerdere (Cyber) Security functionarissen, dan vervalt deze verplichting. Daarbij dient tevens te worden opgenomen dat de maandelijkse rapportage lijn in een managementsysteem is gewaarborgd.
- Mocht de wetgever alsdan nog besluiten dat een certificaat noodzakelijk is, dan stellen wij voor dat indien een onderneming een overeenkomst heeft afgesloten met een Cyber Security bedrijf ten aanzien van Managed Detection & Response (het monitoren van de bedrijfseigen netwerken op basis van op risico gebaseerde scenario's) én een overeenkomst heeft afgesloten ten aanzien van Incident Response, bedoelde verplichte trainingen niet van toepassing zijn. Bij de laatste overeenkomst worden immers onder andere playbooks opgemaakt, waarna deze in zogenoemde table-top trainingen de Raad van Bestuur wordt getraind indien zich een ernstige cyber attack heeft voorgedaan.

Wij willen graag op de hoogte te worden gesteld van de reactie van de Wetgever.