CSR Cyber Security Raad

Bezoekadres
Turfmarkt 147
2511 DP Den Haag

Postadres
Postbus 20011
2500 EA Den Haag

I www.cybersecurityraad.nl
T 070 751 5555

Monitoring Commissie Corporate Governance Code
t.a.v. Prof. Dr. J.A. van Manen
Postbus 20401
2500 EK Den Haag

Contactpersoon
mw. drs. E.C. van den Heuvel
Secretaris CSR
T 06-51095594
E e.c.van.den.heuvel@nctv.minvenj.nl

Den Haag, 31 maart 2016

Onderwerp: tekstvoorstel Corporate Governance Code

Geachte prof. dr. J.A. van Manen,

In het kader van de consultatie over de nieuwe corporate governance code vraagt de Cyber Security Raad aandacht voor het thema cybersecurity en verzoeken wij u dit thema te borgen in de nieuwe corporate governance code.

Als eerste stellen wij de Cyber Security Raad aan u voor. Daarna schetsen wij het belang van cybersecurity voor het bedrijfsleven. Wij sluiten af met een voorstel voor een tekstaanpassing voor de nieuwe code.

Cyber Security Raad

De Cyber Security Raad (CSR) is een nationaal en onafhankelijk adviesorgaan van het Kabinet en bestaat uit vertegenwoordigers van publieke en private organisaties en wetenschap. De CSR zet zich op strategisch niveau in om de cybersecurity in Nederland te verhogen.

De CSR heeft als opdracht gevraagd en ongevraagd advies te geven aan het Kabinet over het tijdig en effectief inspelen op nieuwe technologische ontwikkelingen en de rollen en verantwoordelijkheden in het cyberdomein. Ook agendeert de raad prioritaire thema's op het terrein van cybersecurity voor onderzoek. Daarnaast borgt de CSR publiek-private samenwerking op strategisch niveau in het cybersecurity domein en levert een bijdrage aan awareness over cybersecurity binnen overheid, vitale infrastructuur en bedrijfsleven.

Kansen en risico's cybersecurity

De CSR staat op het standpunt dat nieuwe technologische ontwikkelingen veel kansen met zich meebrengen, bijvoorbeeld voor leefcomfort, efficiënte bedrijfsvoering en het creëren van andere banen. Nieuwe technologieën zijn een belangrijke drijfveer voor innovatie en economische groei. Echter, nieuwe technologische ontwikkelingen brengen ook risico's en dillema's met zich mee.

De risico's hebben betrekking op veiligheid en beveiliging op allerlei niveaus binnen de organisatie, zowel op technisch vlak als op dat van de menselijke factor.

De afgelopen jaren krijgt Nederland steeds vaker te maken met digitale (spionage) aanvallen die een dreiging vormen voor de nationale veiligheid en die de economische belangen kunnen schaden[1]. De gevolgen voor bedrijven kunnen enorm zijn: ze kunnen bijvoorbeeld hun concurrentiepositie (ongemerkt) verliezen omdat hun belangrijkste informatie – 'kroonjuwelen' – gestolen is, ze kunnen door het verlies van privacygevoelige informatie grote imagoschade oplopen en ze kunnen een verstoring krijgen van de business continuïteit als gevolg van een cyberaanval.

Cybersecurity is voor bedrijven een belangrijke randvoorwaarde om de economische kansen die zich voordoen te kunnen blijven benutten. Het is van belang dat een onderneming cybersecurity niet alleen als ICT-vraagstuk ziet, maar ook aandacht heeft voor cultuur, de menselijke factor en fysieke beveiliging. Aandacht voor bewustwording bij medewerkers is onmisbaar om het cybersecurity-level in het bedrijfsleven omhoog te krijgen.

Wat bedrijven kunnen doen

Nederlandse bedrijven moeten future proof zijn en de economische kansen die zich voordoen volop benutten. Bedrijven dienen de digitale infrastructuur en het informatiemanagement op orde te hebben. Van organisaties wordt verwacht dat ze een betrouwbare digitale dienstverlening hebben. Risicomanagement en snel en effectief weer door kunnen gaan na een incident (bijvoorbeeld door redundantie in systemen en goede training) dragen hier aan bij. Ook verwacht men dat privacy en verantwoorde omgang met big data goed geborgd zijn. Digitale gezondheid vraagt én verdient daarom dezelfde aandacht als bijvoorbeeld de financiële en operationele gezondheid van organisaties.

Cybersecurity heeft alles te maken met strategie, bedrijfsvoering, financiën en business continuïteit van een onderneming. Bestuurders en toezichthouders horen dit onderwerp daarom hoog op de strategische agenda te hebben, inzicht te hebben in het digitale veiligheids- en weerbaarheidsniveau van hun organisatie en daarop maatregelen te nemen. Dit is in het belang van hun eigen bedrijf, in het belang van andere bedrijven in de keten en in het belang van de Nederlandse samenleving waarin burgers moeten kunnen vertrouwen op digitaal veilige software, hardware, producten en diensten.

---

[1] Cybersecuritybeeld Nederland
CSBN 2015

Er komt steeds meer wet- en regelgeving op het terrein van netwerkbeveiliging en cybersecurity. Dit gebeurt zowel op nationaal als op Europees niveau. Deze wet- en regelgeving brengt verplichtingen voor ondernemingen met zich mee, bijvoorbeeld rondom het melden van datalekken of de bescherming van persoonsgegevens. Ondernemingen zullen op strategisch niveau in de board sturing moeten geven aan het tijdig en correct implementeren van deze compliance mechanismen. Cybersecurity is ook om die reden een belangrijk vraagstuk voor organisaties.

Voorstel CSR aan de Commissie Corporate Governance Code

De CSR wil de herziening van de Nederlandse corporate governance code gebruiken om het thema cybersecurity een plaats te geven binnen de principes en best practices van de code. Daarom stelt de raad voor dat u – gezien de noodzaak om cybersecurity in het bedrijfsleven en in de samenleving op een hoger niveau te krijgen – dit thema borgt in de tekst van de Nederlandse corporate governance code.

Wij doen u de suggestie aan de hand om een wijziging op te nemen in **paragraaf 1.5.1**. **Taken en verantwoordelijkheden auditcommissie**, ***onderdeel iii*** . Wij stellen voor de daar genoemde taak aan te vullen met de volgende tekst:

iii. de toepassing van informatie en communicatietechnologie van de vennootschap, ***in het bijzonder de beheersing van risico's op het gebied van cybersecurity.***

Graag vernemen wij uw reactie.

Namens de Cyber Security Raad

De voorzitters,

Dick Schoof

Eelco Blok