

**Minister van Economische Zaken
De heer H.G.J. Kamp**

**Staatssecretaris van Veiligheid en Justitie
De heer dr. K.H.D.M. Dijkhoff**

Den Haag, februari 2017

Betreft: 'Ieder bedrijf heeft digitale zorgplichten: een handreiking voor bedrijven op het gebied van cybersecurity'

Excellenties,

Hierbij bieden wij u, namens de Cyber Security Raad, 'Ieder bedrijf heeft digitale zorgplichten: een handreiking voor bedrijven op het gebied van cybersecurity' aan.

Ieder bedrijf dat gebruik maakt van ICT heeft zorgplichten op het gebied van cybersecurity. Een bedrijf heeft zowel zorgplichten ten opzichte van andere bedrijven als ten opzichte van consumenten. De juiste invulling van zorgplichten is de verantwoordelijkheid van het bestuur of (bij kleinere bedrijven) de directeur.

De CSR heeft geconstateerd dat de toepassing van zorgplichten complex is, terwijl het een belangrijke rol speelt in het verhogen van het cybersecurityniveau van organisaties. De handreiking zorgplichten is door de CSR opgesteld om beter inzicht te geven in de zorgplichten volgens de huidige wet- en regelgeving en hoe hier invulling aan kan worden gegeven in de dagelijkse praktijk. De handreiking is gericht op grotere bedrijven en op brancheorganisaties. Brancheorganisaties kunnen een belangrijke rol spelen in het vergroten van cybersecurity binnen hun achterban. Deze handreiking kan als basis worden gebruikt om de verplichtingen verder uit werken en praktisch toepasbaar te maken bij hun de leden. Ook is de handreiking grotendeels toepasbaar op de overheid.

In het rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity: Nederland digitaal droge voeten', dat vorig jaar oktober is verschenen, wordt het belang van het voldoen aan de randvoorwaarden van cybersecurity onderschreven. Bij een nadere invulling van de zorgplichten moet onder andere helder worden gemaakt wat een consument mag verwachten van de aanbieder en welke maatregelen zij zelf geacht worden te treffen. Daarnaast is het van belang dat er een brede discussie wordt gevoerd over de invulling van de zorgplichten waar het gaat om leveranciers van hard- en software.

Een betere invulling van zorgplichten op het gebied van cybersecurity door het Nederlandse bedrijfsleven is één van de elementen om ervoor te zorgen dat Nederland ook digitaal een *'safe place to do business'* is en blijft. Onlosmakelijk onderdeel daarvan is aandacht voor de privacy aspecten, *'privacy is a licence to do business'*.

Uit onderzoek¹ blijkt dat het stimuleren van zorgplichten effectiever is dan strikte handhaving. Zelfregulering van de zorgplichten binnen sectoren is daarom noodzakelijk. Nederland ICT en het CIO Platform Nederland ondernemen reeds stappen op dit gebied. De Cyber Security Raad is van mening dat dergelijke initiatieven vanuit de private sector moeten worden gestimuleerd. De Rijksoverheid kan een belangrijke bijdrage leveren door invulling te geven aan zorgplichten door bij de inkoop van hard- en software nadrukkelijk te vragen naar producten en diensten waar privacy en *'security by design'* centraal staan.

Advies aan de staatssecretaris van Veiligheid en Justitie

Gezien het internationale karakter van cybersecurity en het feit dat de meeste softwareleveranciers niet in Nederland zijn gevestigd, is het voor een effectieve implementatie van zorgplichten noodzakelijk de wetgeving binnen de EU te harmoniseren. De CSR adviseert het ministerie van Veiligheid en Justitie zich actief in te zetten voor deze harmonisatie van zorgplichten in EU-verband. Tevens is het van belang het onderwerp zorgplichten te agenderen op internationaal niveau.

Advies aan de minister van Economische Zaken

De CSR adviseert het ministerie van Economische Zaken de zelfregulering van zorgplichten binnen het bedrijfsleven te stimuleren en initiatieven op dit vlak te steunen. En het voortouw te nemen in de discussie over de invulling van de zorgplichten waar het gaat om leveranciers van hard- en software.

Wij verzoeken u bijgaande handreiking breed bekend te stellen en te verspreiden.

Deze handreiking is tevens aangeboden aan de voorzitter van VNO-NCW (zie bijgevoegd kopie afschrift) met het verzoek om deze handreiking actief onder de aandacht te brengen bij brancheorganisaties.

Namens de Cyber Security Raad,

Eelco Blok
Co-voorzitter CSR

Dick Schoof
Co-voorzitter CSR

¹ 'Duties of care and diligence against cybercrime', prof. T.F.E. Tjong Tjin Tai e.a., Tilburg University, maart 2015