NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

INTERNETCONSULTATIE CYBERBEVEILIGINGSWET
Via OVERHEID.NL

Datum : zaterdag 29 juni 2024
Kenmerk : NOREA / VJK / KG Cybersecrurity 202406
Betreft : Bijdrage NOREA op Internetconsultatie Cyberbeveiligingswet

Geachte Collegae,

Bijgaand onze reactie op de consultatie van de Cyberbeveiligingswet. De reactie is opgesteld door de kennisgroep Cybersecurity van NOREA.

Bij het delen van de Internetconsultatie Cyberbeveiligingswet geeft de overheid het volgende aan: Dit wetsvoorstel implementeert de Europese NIS2-richtlijn. De NIS2-richtlijn beoogt de cyberveiligheid in de Europese Unie naar een hoger gemeenschappelijk niveau te brengen door de digitale weerbaarheid van essentiële en belangrijke entiteiten in de lidstaten te versterken. Dit doel wordt in Nederland bereikt door, ter implementatie van deze richtlijn, in dit wetsvoorstel onder meer verplichtingen op te leggen aan entiteiten, zoals het treffen van adequate beveiligingsmaatregelen en het melden van ICT-incidenten.

De kennisgroep Cybersecurity van NOREA heeft de consultatieversie van de Cyberbeveiligingswet bestudeerd en heeft een aantal opmerkingen die wij graag delen.

Positief valt in het bijzonder op:

1. De cybersecurity-wet vraagt organisaties om expliciet cybersecurity-risicoanalyses uit te voeren, en vraagt voortvarend eventuele gaps op te lossen, waardoor essentiële en belangrijke entiteiten worden gestimuleerd zichzelf snel genoeg te beveiligen.

2. Bestuurdersverantwoordelijk voor cybersecurity wordt expliciet benoemd. Dit vraagt dan ook om expliciete verantwoording en expliciete sturing. Hiervoor is adequate verantwoordingsinformatie en training voor bestuurders benodigd. Wij onderkennen dat veel bestuurders vandaag de dag nog niet voldoende zijn

POSTADRES
POSTBUS 242
2130 AE HOOFDDORP

BEZOEKADRES
FRAME OFFICES - PHAROS
MERCURIUSPLEIN 3
2132 HA HOOFFDORP

E-MAIL EN WEBSITE
NOREA@NOREA.NL
WWW.NOREA.NL

OVERIG
TEL: 00 31 (0)88 4960 380
KVK-NR: 40537540
IBAN: NL02ABNA0475165403

uitgerust om de snelheid en kwaliteit van cybersecurity-verbeteringen aan te sturen. Dit benadrukt de behoefte aan expliciete handvatten voor verantwoordingsinformatie en training! Dit ook omdat non-compliance met de Cybersecurity-wet bij een juridisch geschil een versterkende werking zou kunnen hebben op bestuurdersaansprakelijkheid.

Wij onderkennen de volgende uitdagingen:

3. Een belangrijk verbeterpunt voor vele organisaties betreft cybersecurity-risico's met impact op de waardeketen. Dit vraagt aandacht voor activiteiten zoals het classificeren van business partners, het afspreken van beveiligingseisen, evenals het regelmatig controleren van naleving van deze beveiligingseisen. Wij verwachten dat het versterken van de beveiliging van en het houden van inzicht in de beveiliging van derde partijen voor de meeste entiteiten een lange doorloop zal hebben, die niet direct gereed zal zijn ten tijde van de inwerking treden van de cybersecurity-wet. De vraag is dan ook hoe in Nederland wij zullen (kunnen) omgaan met een 'grace'-periode en of dit wenselijk is?

4. In het algemeen is de implementatie van de cybersecurity-wet voor organisaties een grote opgave. Dit geldt in het bijzonder voor kleinere organisaties die veelal niet de kennis, kunde en middelen hebben om de gestelde hoogte van de 'lat' te halen.
   Kleinere organisaties hebben daarom behoefte aan concrete eisen en een duidelijk en werkbaar stappenplan, evenals ene 'grace'-periode. Als wij kijken naar België, dan is daar reeds invulling gegeven aan deze problematiek door expliciet voor verschillend geclassificeerde entiteiten ook verschillende en passende eisen te stellen.
   Op welke wijze zullen in Nederland kleinere organisaties eveneens geholpen worden om de cybersecurity-wet te implementeren?

5. Gegeven de uitdagingen bij het voldoen aan de cybersecurity-wet, en het realiseren van cybersecurity in het algemeen, vragen wij aandacht voor zowel goede informatie-uitwisseling als samenwerking in de keten!

Beveiligingsaudits worden benoemd, deze kunnen worden gevraagd. Als we bijvoorbeeld kijken naar Duitsland, dan kent men reeds KRITIS, waarbij audits worden verwacht voor een vitale infrastructuur. Kan ook voor Nederland duidelijk worden gemaakt wanneer een audit is vereist, welke auditstandaard wordt verwacht, en welke eisen aan de auditor dienen te worden gesteld?

Met vriendelijke groet, mede namens de Kennisgroep Cybersecurity,

Viktor Krul

Viktor J. Krul

Directeur
Telefoon: + 31 (0)88 4960380
Mobiel: + 31 (0)6 20015632
E-mail: v.krul@norea.nl

Bereikbaar van maandag t/m donderdag

Mercuriusplein 3,
Postbus 242,
2130 AE Hoofddorp

Web: www.norea.nl

NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS