Cyberbeveiligingsbesluit - AMvB – consultatieversie en de bijbehorende Cyberbeveiligingsbesluit - nota van toelichting – consultatieversie.

Consultatie: Techniek Nederland

Door: Team Advies Advies@techniekNederland.nl

Datum 28 maart 2025

Techniek Nederland, als vereniging van de Technische Installatie Branche (TIB) en elektrotechnische Detailhandel onderschrijft het belang van een algemeen gedeeld bewustzijn en gezamenlijke inspanning voor maximaal benodigde cybersecurity in de keten waarin onze leden opereren. Vrijwel iedere installatie en veel apparaten hebben heden ten dage enige vorm van online connectie of afhankelijkheid. De kwetsbaarheid en risico's die hiermee gepaard gaan moeten onderkend en ondervangen worden.

Wij zijn er ons van bewust dat dit een gezamenlijke opgave is en dat enige regulering hieromtrent gestoeld moet zijn op dat uitgangspunt en tevens rekenschap geeft van de extra belasting die deze grote uitdaging met zich meebrengt. Wetgeving zal derhalve praktisch en werkbaar moeten zijn en geen oneerlijk speelveld creëren, dan wel een onmogelijke taak opleggen uitgedrukt in tijd, geld, personele beschikbaarheid of andere vorm.

Vrijwel alle leden in onze branche kunnen op enige manier te maken krijgen met deze wet, al dan niet via hun opdrachtgevers die direct onder de wet zullen vallen. Daarmee is met name het wettelijk kader van de toeleveringsketen van art. 10 van toepassing voor beoordeling en commentaar.

Art. 10 lid 2 Cbb

Het gebruik van het woord "actueel" in dit lid is niet specifiek genoeg om werkbaar te zijn. In de keten is er behoefte aan een uniform uitgangspunt waar partijen zich in hun bedrijfsvoering op kunnen voorbereiden en welke over en weer zij kunnen implementeren. Techniek Nederland stelt zich, zoals andere brancheverenigingen, op het punt dat een jaarlijks evaluatie en vastlegging voldoende zouden moeten zijn.

Daarmee blijven de afspraken en de controle actueel, maar wordt geen der betrokken partijen opgezadeld met een onnodige terugkerende administratieve last. Een last die dan ook eerder het risico loopt om te veranderen in een repeterende formaliteit met risico van voldoende urgentie en grondigheid. Dit proces is niet gebaat bij een terugkerende invuloefening maar juist bij een jaarlijkse deugdelijke analyse en verslaglegging.

Nota van toelichting

Onder de toelichting op art 10 Ccb inzake de verdere uitwerking van art 21 lid 3 sub d Cbw, wordt teruggevallen op een tweetal voorbeelden waaruit duidelijk zou worden wanneer activiteiten onder de reikwijdte van dit artikel vallen.

Ondanks de waardering voor de inspanning om in de toelichting het speelveld beter te duiden is er in de praktijk eerder behoefte aan een duidelijkere definitie van de grens van wel naar niet. Dit in plaats van een voorbeeld op basis van twee uitersten die, los van de inhoud zelf, die in zichzelf evident zijn. Er is behoeft, bij voorkeur aan de hand van praktijk voorbeelden, voor de markt duidelijk te krijgen waar de grens ligt en hoe voorkomende gevallen en omstandigheden beoordeeld zouden moeten worden in een potentieel grijs gebied.

Klaarblijkelijk is bij de toelichting hier een eerste aanzet voor gegeven en het lijkt dan ook mogelijk om juist de grens beter te kunnen definiëren. Een oplossing die zeer wenselijk is.

Hierbij merken wij op dat door de steeds verdere integratie en verbondenheid van systemen en werkprocessen, het zeer lastig zal blijken om de grens goed te definiëren. In dat geval is het wenselijk om dan beter geen voorbeelden op te nemen, maar een opdracht om per specifiek geval een toetsingskader met een duidelijk uitgangspunt voor een situatie-afhankelijke risicobeoordeling. Partijen weten dan waaraan te toetsen waardoor van leverancier tot leverancier risico's en bijbehorende maatregelen kunnen worden geïdentificeerd, vastgelegd en aangepakt.

Gewogen risico, passende inspanning qua maatregelen

Daarnaast pleiten wij voor een werkwijze waarbinnen de individuele aanpak de gelegenheid biedt voor een werkwijze waarbij een schaal gehanteerd kan worden van weinig risico en minder maatregelen naar groot risico naar zware maatregelen. Hiermee is er ruimte om het systeem proportioneel te laten functioneren en de bijkomende lasten in de pas te houden en de aanpak werkbaar.

Maak gebruik van NIS2 Quality mark van Samen Digitaal Veilig

In de toelichting op art. 10 lid 2 Cbb wordt melding gemaakt van de op leveranciers van toepassing zijnde cyberbeveiligingseisen en de eis dat er cyberveilig gewerkt wordt. Wij constateren dat in dit geval de markt ook gebaat is bij een duidelijke standaard.

Techniek Nederland heeft ten bate van de cyberveiligheidseisen met anderen in Samen Digitaal Veilig de NIS2 Quality mark ontwikkeld die mede van toepassing is op onze branche en die in 3 niveaus is verdeeld. Dit sluit aan op de vereisten van de nu toepasselijke wetgeving en de uitgangspunten van de Ccb. Dit zou derhalve uitstekend als uitgangspunt of benchmark kunnen dienen als (vereiste) certificering of als uitgangspunt voor cyberveilig

werken in de keten. Dit NIS2 Quality mark opnemen zou voor onze en andere branches helpen om een duidelijke benchmark te hebben.

Vervangen van leveranciers

Het lijkt ons onjuist, in welke vorm dan ook, dat de overheid een opening te creëert om contract beëindiging te faciliteren. Het uitgangspunt moet zijn dat de AMvB praktisch uitvoerbaar is, dat de vereisten werkbaar zijn en dat er op individuele basis een goede beoordeling gemaakt kan worden met passende maatregelen waardoor partijen juist samen kunnen blijven werken. Continuïteit van bestaande rechtsrelaties moeten er juist niet door geschaad worden.

Algemeen:

De leden van onze branche zijn cruciaal in het draaiende houden van Nederland. Ook in de weerbaarheid van de samenleving spelen zij een belangrijke rol. Vanuit die positie komen er reeds vele verplichtingen, uitdagingen en vereisten op de leden af. In algemene zin roepen wij daarom op om de AMvB zodanig in te richten dat er vooral sprake is van een heldere en werkbare situatie in de praktijk waarbij onnodige extra lasten op bedrijfsvoering worden voorkomen.

Essentieel hierin is, zoals eerder aangegeven, dat lagere risico's met lagere inspanningen gepaard gaan en zo oplopend naar een maximale inspanning als een situatie daarom vraagt.

Mochten de besluiten van de AMvB er in resulteren dat de keten op slot raakt en toeleveranciers worden afgesneden via de verplichtingen, dan levert dan niet alleen een op korte termijn onwerkbare situatie op waar de Cyberveiligheid niet bij gebaat is, maar het zou ook nog een ernstige marktverstoring teweegbrengen. Onze leden opereren immers op allerlei niveaus en van Eenmanszaak tot grote internationale speler, allen in een zorgvuldig evenwicht maar niet allen met dezelfde middelen.