Aan de heer D.M. van Weel
Minister
Ministerie van Justitie en Veiligheid
Postbus 20301
2500 EH Den Haag

Betreft: Artikel 18 in het concept Cyberbeveiligingsbesluit
Plaats: Breukelen
Datum: 1 september 2025

Geachte heer Van Weel,

NLdigital, de brancheverenigingen van de digitale sector in Nederland, schrijft u naar aanleiding van het onverwacht en laat toegevoegde artikel 18 in het concept-Cyberbeveiligingsbesluit. Als organisatie die zowel Nederlandse als internationale IT-leveranciers vertegenwoordigt, maken wij ons ernstige zorgen over de juridische houdbaarheid, uitvoerbaarheid en proportionaliteit van dit voorstel.

In deze brief behandelen we onze reactie op drie hoofdpunten: ten eerste de fundamentele juridische en uitvoeringstechnische gebreken van het huidige artikel 18 Cyberbeveiligingsbesluit, ten tweede de voorwaarden waar wij denken dat een eventuele bevoegdheid op dit terrein aan moet voldoen, en ten derde ons voorstel voor een beter alternatief gebaseerd op de recente Duitse NIS2-implementatiewet. Wij erkennen de nationale veiligheidsbelangen die ten grondslag liggen aan dit voorstel, maar bepleiten dat hiervoor een juridisch solide, proportionele en uitvoerbare aanpak nodig is die recht doet aan alle betrokkenen.

Juridische tekortkomingen van het huidige voorstel

Het voorliggende artikel 18 Cyberbeveiligingsbesluit bevat naar ons oordeel fundamentele juridische gebreken:

Onvoldoende wettelijke grondslag: De bevoegdheid wordt gebaseerd op een uitbreiding van de zorgplicht uit artikel 21 Cyberbeveiligingswet, maar deze uitbreiding is alleen opgenomen in de Memorie van Toelichting, niet in de wet zelf. Voor een dermate ingrijpende uitbreiding van het begrip en invoering van deze bevoegdheid is een expliciete formeel-wettelijke grondslag noodzakelijk.

Veel te vage beoordelingscriteria: De formulering "gronden zijn te vermoeden dat deze de intentie heeft" is juridisch onhoudbaar vaag. Deze bewoordingen geven ministers praktisch onbegrensde discretionaire ruimte zonder objectieve toetsingskaders. Dit staat op gespannen voet met fundamentele rechtsbeginselen van rechtszekerheid en voorzienbaarheid.

Ontbrekende rechtswaarborgen: Het voorstel bevat geen adequate rechtsbescherming voor leveranciers die door deze maatregelen worden getroffen. Er is geen voorziening voor voorafgaande hoor en wederhoor, geen duidelijke beroepsmogelijkheden en geen transparante procedure voor nadeelcompensatie.

Aantasting rechtszekerheid: Het voorstel leidt tot fundamentele rechtsonzekerheid door inconsistentie met bestaande wetgeving, mogelijke strijd met EU-recht inzake vrij verkeer van goederen en diensten, en onduidelijke procedures voor getroffen leveranciers. Deze cumulatie van gebreken tast de rechtszekerheid aan die essentieel is voor het functioneren van de digitale sector.

NLdigital
De Corridor 5
3621 ZA Breukelen
info@nldigital.nl
+31 (0) 348 - 49 36 36
KVK 3017 4840
NL53 INGB 0662 5905 46

Ondoordachte uitvoering binnen NIS2-kader

De voorgestelde regeling past fundamenteel niet binnen het bestaande NIS2-implementatiekader. De Cyberbeveiligingswet is opgebouwd rondom een risico-gebaseerde aanpak waarbij organisaties zelf risicoanalyses uitvoeren, toezichthouders deze beoordelen en vervolgens eventueel handhaven. Artikel 18 Cbb doorbreekt dit systeem door ministers de mogelijkheid te geven om zeer specifieke, gerichte maatregelen op te leggen die niet passen binnen dit risicoanalyse-toezicht-handhaving model.

Deze systemische inconsistentie leidt tot praktische uitvoeringsproblemen en rechtsonzekerheid voor alle betrokkenen. Het is onduidelijk hoe dergelijke ministeriele interventies zich verhouden tot de eigen verantwoordelijkheid van organisaties voor hun cyberbeveiliging.

Er is uitgelegd dat dit is ontworpen overeenkomstig een bestaande bevoegdheid binnen het Besluit veiligheid en integriteit telecommunicatie (Bvit). Over de juridische houdbaarheid daarvan loopt echter nog een hoger beroep. Daarnaast kent de Regeling veiligheid en integriteit telecommunicatie een expliciete rol voor de minister naast de rol van de toezichthouder, deze losstaande rol bestaat niet voor de minister in de Cyberbeveiligingswet of de NIS2. Het rechtstreeks overnemen uit de Bvit geeft dus geen garantie op juridische houdbaarheid, en heeft een insteek die niet past in het kader van de NIS2.

Tot slot betreft het hier dan ook het oprekken van het zorgplicht-begrip via een toevoeging in de Memorie van Toelichting, dit schept een gevaarlijk precedent voor wat de betekenis van dit begrip kan omvatten. Het ondermijnt de huidige risico-gebaseerde en principle-based benadering van cyberbeveiliging door de organisatie zelf, ten gunste van zeer specifieke rule-based interpretaties door ministers - zonder adequate waarborgen daarop.

Voorwaarden voor proportionaliteit van de bevoegdheid

NLdigital wijst maatregelen die IT-leveranciers beoordelen op basis van de locatie van hun hoofdkantoor principieel af. Dergelijke land-van-herkomstdiscriminatie druist in tegen fundamentele EU-beginselen van non-discriminatie en vrij verkeer van goederen en diensten. Het creëert een gevaarlijk precedent waarbij geopolitieke overwegingen prevaleren boven objectieve, technische veiligheidscriteria. Nederland moet cyberbeveiliging baseren op aantoonbare risico's en verifieerbare standaarden, niet op nationaliteit.

Gegeven dat uitgangspunt erkennen we ook dat er in het huidige geopolitieke klimaat mogelijk behoefte bestaat aan instrumenten ter bescherming van de nationale veiligheid. Wanneer de wetgever kiest voor een dergelijke bevoegdheid, dan stellen wij dat deze tenminste aan de volgende voorwaarden zou moeten voldoen om proportioneel te zijn:

1. **Ultimum remedium-principe** - de bevoegdheid mag uitsluitend worden ingezet nadat alle andere maatregelen zijn uitgeput.
2. **Scherp afgebakende bevoegdheid** met duidelijke, objectieve omstandigheden waaronder de bevoegdheid mag worden ingezet.
3. **Transparantie en bewijslast** - besluiten moeten adequaat gemotiveerd zijn op basis van controleerbare feiten.
4. **Volledige rechtsbescherming** voor zowel afnemers als leveranciers, inclusief beroeps- en verdedigingsmogelijkheden.

5. **Risico-gebaseerde uitvoering in overleg** met gebruikers en afnemers van betreffende producten/leveranciers, waarbij alternatieve maatregelen eerst worden verkend alvorens tot uitsluiting over te gaan.

In het kort: geen protectionisme, ultimum remedium en duidelijk en alleen toegespitst op nationale veiligheid.

Voorstel voor een beter alternatief

VNO-NCW en MKB-Nederland hebben vergelijkbare fundamentele kritiek geuit en stellen dermate stringente voorwaarden - waaronder formeel-wettelijke verankering, nieuwe Raad van State procedure, onafhankelijk voorafgaand toezicht, en wettelijk verankerd ultimum remedium principe - dat implementatie hiervan de facto neerkomt op volledig herontwerp. NLdigital steunt deze minimumeisen, en constateert dat de meest constructieve weg voorwaarts is om artikel 18 te schrappen met een zorgvuldig proces opnieuw te beginnen.

Indien u daarbij een dergelijke bevoegdheid wenst in te voeren, dan is grondige herziening noodzakelijk. Als uitgangspunt zou daarbij kunnen dienen de recente Duitse NIS2-implementatiewet (zie bijlage), die tenminste een juridisch solide en transparant kader biedt. Overigens blijft ook deze aanpak problematisch vanuit non-discriminatie perspectief, maar biedt in ieder geval objectieve criteria en rechtswaarborgen.

Beperkte scope en duidelijke definitie: De regeling is specifiek beperkt tot "kritische componenten" - ICT-producten die worden gebruikt in kritische installaties waarbij verstoringen kunnen leiden tot aanzienlijke aantasting van de functionaliteit of bedreigingen voor de openbare veiligheid. Alleen bij wet aangewezen componenten vallen onder de regeling.

Preventieve meldingsplicht: Exploitanten moeten het geplande eerste gebruik van een kritische component melden bij het Duitse ministerie van Binnenlandse Zaken. Gebruik is niet toegestaan voordat de beoordelingstermijn is verstreken of goedkeuring is gegeven.

Gestructureerde beoordeling met duidelijke termijnen: Het ministerie heeft twee maanden (verlengbaar met nog twee maanden) om een beoordeling uit te voeren. Gedurende deze periode kan gebruik worden verboden als dit de openbare orde of veiligheid in gevaar kan brengen.

Betrouwbaarheidsverklaring van leveranciers: Kritische componenten mogen alleen gebruikt worden als de fabrikant een betrouwbaarheidsverklaring (garantieverklaring) heeft verstrekt. Deze verklaring moet aangeven hoe gewaarborgd wordt dat het component geen technische eigenschappen bezit die specifiek de veiligheid kunnen aantasten. Het ministerie stelt concrete minimumvereisten vast voor deze verklaringen.

Beoordelingscriteria: Op dit punt zien we ook de Duitse wet als problematisch vanuit non-discriminatie perspectief. De criteria omvatten zowel objectieve elementen (eerdere betrokkenheid bij schadelijke activiteiten, niet naleven van verplichtingen) als land-van-herkomst gebaseerde aspecten (staatscontrole door derde landen, alignment met NAVO-doelstellingen) die indruisen tegen onze principiële bezwaren. Wat het Duitse model echter substantieel beter doet is dat deze criteria een duidelijk afgebakend toepassingsgebied hebben (alleen kritieke componenten bij kritieke installaties), dat leveranciers vooraf via de betrouwbaarheidsverklaring kunnen aantonen hoe zij risico's mitigeren, en dat er proportionele escalatiestappen zijn in plaats van directe uitsluiting.

Proportionele escalatie: Bij constatering van onbetrouwbaarheid kunnen stapsgewijs maatregelen worden genomen: eerst verbod van verdere componenten van hetzelfde type, vervolgens alle componenten van dezelfde fabrikant, en alleen in ernstige gevallen alle componenten van die fabrikant.

Discontinuïteit diensten: Het plotseling moeten vervangen van IT-leveranciers kan leiden tot ernstige verstoringen in essentiële en belangrijke dienstverlening. Voor veel digitale infrastructuur zijn alternatieven niet zomaar beschikbaar. Migratietrajecten vergen jaren voorbereiding. Een aanwijzing zonder adequate overgangstermijn kan de dienstverlening die men juist wil beschermen, ontwrichten.

Europese harmonisatie: Het Duitse model sluit bovendien beter aan bij de doelstelling van minimumharmonisatie binnen de EU. Waar de NIS2-richtlijn beoogt een gelijk speelveld te creëren, doorbreekt het Nederlandse voorstel - zoals eerder uiteengezet - het risico-gebaseerde systeem waarin organisaties zelf risicoanalyses uitvoeren en toezichthouders deze beoordelen.

Internationale samenwerking: Een voorspelbare, op criteria gebaseerde benadering zoals in het Duitse model faciliteert ook betere samenwerking met internationale partners, terwijl willekeurige interventies juist het vertrouwen in Nederlandse cybersecurity-governance ondermijnen.

Deze systematische aanpak is niet alleen juridisch houdbaar, maar ook praktisch uitvoerbaar en proportioneel. Het biedt bescherming voor nationale veiligheidsbelangen zonder de gehele digitale sector te ontwrichten, en creëert duidelijkheid voor alle betrokkenen over procedures, criteria en rechtsmiddelen.

Belang van verdedigingsmogelijkheden

Wij benadrukken het cruciale belang van adequate verdedigingsmogelijkheden voor bedrijven. Het huidige voorstel kan leiden tot een aanzienlijk "*chilling effect*" waarbij organisaties preventief bepaalde leveranciers mijden uit vrees voor toekomstige sancties. Dit schaadt niet alleen individuele bedrijven, maar ook de innovatiekracht en concurrentiekracht van de Nederlandse digitale sector als geheel.

De voorgestelde regeling riskeert bovendien de concurrentiepositie van de Nederlandse digitale sector te ondermijnen. Internationale IT-bedrijven kunnen Nederland mijden als vestigingslocatie uit vrees voor onvoorspelbare overheidsinterventie, terwijl Nederlandse bedrijven worden benadeeld ten opzichte van hun Europese concurrenten die niet met dergelijke beperkingen te maken hebben. Dit ondermijnt niet alleen het Nederlandse investeringsklimaat, maar ook de innovatiekracht van onze digitale economie - precies op het moment dat digitale soevereiniteit en technologische autonomie cruciaal zijn voor onze nationale veiligheid.

Conclusie

NLdigital erkent de urgentie van cybersecurity-dreigingen en ondersteunt het doel van nationale veiligheid. Tegelijkertijd zijn wij overtuigd dat dit doel beter kan worden bereikt door een juridisch solide, technisch verantwoorde en economisch proportionele aanpak.

Ook vragen wij aandacht voor de onduidelijke verhouding tot het voorgenomen ABRO (Algemene Beveiligingseisen voor Rijksoverheidsopdrachten) die ook van toepassing verklaard zou worden voor vitale sectoren volgens hierover verstrekte informatie. Als ABRO preventief risico's in de leverancierskete moet mitigeren via objectieve beveiligingseisen, wat is dan nog de toegevoegde waarde van artikel 18? Het stapelen van verschillende regimes zonder duidelijke afbakening creëert alleen meer rechtsonzekerheid.

Ons voorstel: Wij pleiten ervoor om het huidige artikel 18 Cbb te schrappen. Heroverweeg eerst de noodzaak in het licht van de voorgenomen ABRO. En indien de nationale veiligheid een dergelijk artikel noodzakelijk maakt dan zou deze als volgt moeten worden aangevlogen:

- **Gedegen herontwerp** op basis van het Duitse model van 'kritische componenten'.
- **Brede consultatie** met alle betrokkenen over de uitwerking.
- **Adequate waarborgen** voor rechtsbescherming, compensatie en procedurele transparantie.
- **Technische toetsing** van de praktische uitvoerbaarheid en cybersecurity-impact.
- Gebaseerd op **objectieve, technische criteria**.

Constructieve samenwerking: NLdigital stelt zich constructief op en biedt onze expertise aan voor het ontwikkelen van een oplossing die alle belangen evenwichtig behartigt. Wij zijn bereid om in een kort tijdsbestek bij te dragen aan een werkbare, proportionele regeling die zowel de nationale veiligheid als de digitale economie dient.

De urgentie van cybersecurity-dreigingen vereist slagvaardig handelen, maar dit mag niet ten koste gaan van zorgvuldige wetgeving en rechtsstatelijke waarborgen. Met de juiste aanpak kunnen beide doelen worden bereikt.

Hoogachtend,

Rene Corbijn
Adjunct directeur NLdigital

Bijlage – Duitse paragraaf 41

Uit de versie van 23 juni van de Duitse "Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung", pagina 49-51.

§ 41. Untersagung des Einsatzes kritischer Komponenten

(1) Ein Betreiber kritischer Anlagen hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Nummer 23 dem Bundesministerium des Innern vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber kritischer Anlagen nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm der Einsatz nicht untersagt wurde.

(2) Das Bundesministerium des Innern kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen im Benehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob

1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,
2. der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder
3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.

Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern kann die Frist gegenüber der Einrichtung um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.

(3) Kritische Komponenten gemäß § 2 Nummer 23 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der kritischen Anlage abgegeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zweck von Sabotage, Spionage oder Terrorismus, auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können. Das Bundesministerium des Innern legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Funktionsfähigkeit der kritischen Anlage folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von

Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere aus dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 4 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.

(4) Das Bundesministerium des Innern kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist.
Absatz 2 Satz 2 gilt entsprechend.

(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass

1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,
2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,
3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,
4. Schwachstellen oder Manipulationen an seinem Produkt nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber kritischer Anlagen meldet,
5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können, oder
6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können.

(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt

1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und
2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.

(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit den in § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.