Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

BTG reactie internetconsultatie Min JenV NIS2-richtlijn

Datum: 28-06-2024

Versie: 1.00 Definitief

Inleiding

BTG is de Brancheverenigingvoor ICT en Telecommunicatie Grootgebruikers in Nederland. BTG behartigt sinds 1986 de belangen van Nederlandse bedrijven en instellingen die op grote schaal gebruikmaken van bedrijfscommunicatie. BTG vertegenwoordigt haar leden bij binnen- en buitenlandse toezichthouders. De vereniging telt ruim 180 leden binnen zowel het bedrijfsleven als de overheid. BTG verbindt organisaties in hun gezamenlijke belangen in het domein van ICT en Telecommunicatie. BTG organiseert daartoe structurele lobby tussen overheid, leveranciers en leden en biedt haar leden een netwerk voor ontmoeting en kennisdeling. BTG signaleert trends en vertaalt deze in relevante inhoud en activiteiten. Ledenvoordeel wordt gerealiseerd door bundeling van vraag en daarop gebaseerde dienstverlening.

BTG heeft binnen de vereniging de focus op een aantal kennisgebieden met expertise groepen waar BTG leden bij aangesloten zijn. In deze expertise groepen worden de ledenbelangen geformuleerd, kennis uitgewisseld en ervaringen gedeeld. In Figuur 1 is een overzicht gegeven van de BTG expertise groepen.

Figuur 1. Overzicht van de BTG expertise groepen

Cyber Security is voor alle leden van BTG van essentieel belang zowel de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) en de nieuwe cyberbeveiligingswet.

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

De voorliggende reactie op de consultatie van het ministerie van Ministerie van Justitie en Veiligheid betreffende het wetsvoorstel voor de implementatie in Nederland van de Europese NIS2-richtlijn, is in onderling overleg met de BTG leden tot stand gekomen van zowel de vraagzijde als de aanbodzijde van de markt. De BTG vertegenwoordigt de belangen van ICT gebruikers aan de vraagzijde van de markt. Indien er op een onderwerp een belangenverschil is tussen de vraag- en aanbodzijde van markt dan is in deze reactie het gebruikersbelang opgenomen.

Deze BTG reactie is niet namens de publieke telecommunicatie operators in Nederland opgesteld.

Inhoudelijke reactie BTG

De Network and Information Security (NIS2) -richtlijn is opgesteld door de Europese Unie en in november 2022 gepubliceerd. Het heeft als doel de beveiliging van netwerk- en informatiesystemen te verbeteren en de digitale en economische weerbaarheid binnen de Europese Unie te versterken tegen groeiende bedreigingen.
In Nederland heeft de omzetting van deze Europese richtlijn naar nationale wetgeving geresulteerd in een wetsvoorstel in de vorm van de Cyberbeveiligingswet, die naar verwachting in Q2 of Q3 2025 in werking zal treden. Op het moment dat de Cyberbeveiligingswet wordt aangenomen, zal deze de huidige Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangen.

De internetconsultatie voor het wetsvoorstel is inmiddels gestart en eindigt 1 juli 2024, waarna alle reacties worden geëvalueerd en mogelijke aanpassingen aan het wetsvoorstel worden doorgevoerd, voordat het wetsvoorstel naar de Tweede Kamer gaat.

In dit document reageert BTG op de consultatie genaamd "Start van de Cyberbeveiligingswet", vanuit het standpunt van haar leden. (exclusief publieke telecommunicatie operators)

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

Artikel 8, essentiële entiteit van rechtswege

Lid 1d en 1e
Volgens deze twee leden worden aanbieders van openbare elektronische communicatienetwerken/ communicatiediensten, die in aanmerking komen als middelgrote onderneming, gezien als essentiële entiteit. Dit komt niet overeen met de figuur op pagina 17 van de NIS2-richtlijn Informatiebrochure.

Advies BTG: verduidelijk of corrigeer de betreffende teksten.

Artikel 12, belangrijke entiteit van rechtswege

Lid 1c en 1d
Volgens deze twee leden worden aanbieders van openbare elektronische communicatienetwerken/ communicatiediensten, die in aanmerking komen als kleine of micro-onderneming onderneming, gezien als belangrijke entiteit. Dit komt niet overeen met de figuur op pagina 17 van de NIS2-richtlijn Informatiebrochure.

Advies BTG: verduidelijk of corrigeer de betreffende teksten.

Artikel 17, aanwijzing en taken CSIRT

Lid 2d
Van de forensische gegevens die door het CSIRT bij uitoefening van haar taken worden verzameld en geanalyseerd is niet helder of deze gegevens van de betrokken entiteit altijd worden verzameld of dat deze slechts worden verzameld wanneer een entiteit een verzoek doet tot ondersteuning bij een incident.

Advies BTG: leg vast of het CSIRT in de uitvoering van haar taken zoals scanning van gegevens, deze forensische gegevens continu verzamelt, of dat zij dit enkel doet bij verzoek tot onderzoek van de gegevens van een entiteit. Leg tevens vast of en in welke gevallen en onder welke voorwaarden forensische gegevens van de entiteit door het CSIRT kunnen worden verzameld en verwerkt.

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

Lid 7
Welke gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema's en taxonomieën worden hier bedoeld? Het kan namelijk zijn dat een entiteit doelbewust niet meewerkt. Is het CSIRT in de positie de entiteit te dwingen mee te werken en deze standaarden toch te gebruiken?

Advies BTG: geef een verduidelijking, de wet vereist dat er gemeenschappelijke of gestandaardiseerde praktijken, classificatieschema en taxonomieën gebruikt dienen te gaan worden. De vraag is welke?

Artikel 21, nationaal plan voor grootschalige cyberbeveiligingsincidenten en crisisrespons

Ten aanzien van de beveiliging van de toeleveringsketen (punt d) wordt in artikel 21, tweede lid, onderdeel d, en derde lid, NIS2-richtlijn aangegeven dat dit met inbegrip is van beveiliging gerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners.

Advies BTG: het heeft de voorkeur om de scope te verduidelijken. Is dit enkel de rechtstreekse leverancier/dienstverlener of mogelijk de gehele keten?

Artikel 23, zorgplicht

Het ontbreekt in de wet aan een uitputtende opsomming van de minimale risicobeperkende technische, operationele en organisatorische maatregelen voor de beveiliging van netwerk- en informatiesystemen. De NIS2 biedt meerdere specifieke richtlijnen hiervoor. Op dit moment, met deze wetgeving, kunnen de vereiste maatregelen onvolledig worden aangepakt, wat het voor entiteiten bemoeilijkt zich aan de wet te voldoen.

Advies BTG: een verduidelijking geven hoe dit verwerkt gaat worden in de amvb.

Een ander vraagstuk betreft de internationale aanpak voor uitvoering van de zorgplicht. Binnen de Cyberbeveiligingswet is er geen uniforme aanpak beschreven voor het vervullen van de zorgplicht met betrekking tot cybersecurity, zoals wel bepaald in de NIS2-richtlijn. Elk lidstaat interpreteert en implementeert deze verplichting op zijn eigen manier, wat kan leiden tot inconsistenties en onduidelijkheid voor de entiteiten binnen de telecommunicatie, die actief zijn in meerdere EU-landen.

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

Het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) biedt echter een gestandaardiseerde risico-gebaseerde benadering die kan dienen als een bruikbaar kader voor alle entiteiten binnen de EU om aan de zorgplicht te voldoen. Door ENISA's aanpak te volgen, kunnen entiteiten op EU-niveau een uniforme aanpak hanteren, wat zorgt voor consistentie en rechtszekerheid. Bovendien helpt een uniforme methodiek ook toezichthouders bij het vervullen van hun taken, omdat zij een gemeenschappelijk referentiekader hebben om naleving te beoordelen.

Advies BTG: neem de risico-gebaseerde aanpak van ENISA als verplichte aanpak op.

Artikel 26, governance

In de Cyberbeveiligingswet is opgenomen dat het bestuur van een entiteit wordt geacht in staat te zijn toe te zien op de cyberbeveiligingsbeheersmaatregelen, de uitvoering ervan en de beoordeling ervan. Tevens wordt het bestuur geacht over kennis en vaardigheden te beschikken om risico's voor de beveiliging van netwerk- en informatiesystemen te identificeren.
Dit zijn echter taken die binnen een entiteit door speciaal daarvoor (hoog) opgeleide en ervaren medewerkers worden uitgevoerd. Dit zijn geen taken die kunnen worden uitgevoerd door mensen die hiertoe niet bekwaam zijn. Het management van een entiteit heeft andere taken. Zij zijn weliswaar eindverantwoordelijk voor de cyberbeveiligingsbeheersmaatregelen, maar zijn niet verantwoordelijk voor de uitvoering. Het bestuur moet echter wel zorgen voor voldoende kennis om te kunnen beoordelen hoe groot de kans is op het optreden van het risico en wat daarbij dan de impact zal zijn (ondanks dat deze al gegeven zijn door het risk-team). In realiteit is deze risicobeoordeling al uitgevoerd door de mensen in de business en hoeft het bestuur slechts aan te geven of zij met de hoogte van de risicobepaling en de voorgestelde beheersmaatregelen akkoord gaat, danwel het risico accepteert danwel het risico uitbesteedt.

Advies BTG: verwijder punt a uit lid 2, en behoudt wel de punten b en c uit lid 2. In deze laatste punten gaat het namelijk over het daadwerkelijk beoordelen van de beheersmaatregelen

Ook dient er meer expliciet aangegeven te worden wat precies "een sufficiënt kennislevel" is. Er wordt aangegeven dat aantoonbare actuele kennis en vaardigheden gevraagd worden. Dat roept de vraag op wat een minimaal kennisniveau is. Is dat een globale, korte risk-cursus bijvoorbeeld via YouTube, of een officieel erkende cursus? Wat is de definitie van het minimale niveau van kennis om de risico mitigerende maatregelen te kunnen beoordelen? Daarbij

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

kunnen bepaalde cursussen of scholing aangewezen worden, waar entiteiten of individuen aan kunnen deelnemen. Hiermee wordt ook direct het risico gemitigeerd naar het niveau dat alle managementleden van entiteiten tenminste een evenredig minimaal level aan kennis vergaren.
Daarnaast kan het zijn dat kleinere entiteiten niet de resources hebben om het management nog eens extra te laten scholen op cyberrisico's en bijhorende maatregelen. Een geldelijke ondersteuning in de vorm van subsidie voor de hierboven genoemde aangewezen scholing, zou hiervoor een optie kunnen zijn evenals een scholing van overheidswege.

Advies BTG: neem concreet op welke opleidingen minimaal door het bestuur moeten zijn gevolgd om te kunnen voldoen aan de eisen in artikel 26. Daarnaast zou de overheid de kosten voor die entiteiten met een maximum aantal medewerkers bij een maximaal bedrag aan gerealiseerde omzet, geheel dienen te dragen. Of biedt vanuit de overheid een scholing aan.

Artikel 27, meldplicht significante incidenten

Compliance met de meldplicht kan flinke administratieve last leggen op de betrokken entiteiten, vooral als het gaat om incident detectie, assessment en notificatie, allen op korte termijn (72u). Dit kan zorgen voor een erg verstoorde incident managementproces en/of business continuïteit.

Advies BTG: wanneer er zich een significant incident voordoet is het alle hens aan dek voor de entiteit om de schade zoveel mogelijk en zo snel mogelijk te beperken. Om hulpverlening zo snel mogelijk op gang te helpen is een meldplicht, waarbij een eerste melding gedaan wordt van het incident, om dit binnen 24 uur te doen.
Een optie zou kunnen zijn om een eerste melding binnen 24 uur te doen en de volledige melding binnen 72 uur te doen.

Voor het melden van informatie over incidenten, bijna-incidenten, cyberdreigingen en kwetsbaarheden op het meldpunt, dient natuurlijk het waarborgen van de veiligheid en integriteit van de gedeelde gegevens op het platform centraal te staan. Het is cruciaal om ongeautoriseerde toegang of inbreuken te voorkomen. Hoe zorgt het CSIRT ervoor dat de veiligheid en integriteit aantoonbaar gewaarborgd blijft? Hoe krijgen de entiteiten daar assurantie van? Welke aantoonbare maatregelen neemt het CSIRT Zelf?

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

Advies BTG: neem op dat het CSIRT transparant moet zijn over de informatiebeveiligings-maatregelen die zij zelf heeft geïmplementeerd om de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens van de entiteiten te borgen. Het streven naar één handeling is essentieel om de administratieve last te beperken.

Artikel 30, tussentijds verslag

Er staat een spelfout in deze zin. "*Eem* essentiële entiteit" dient "*Een*" te worden.

Artikel 89, wijziging Telecommunicatiewet

Net als in artikel 23, dienen er in artikel 89 meer richtlijnen te komen voor de passende en evenredige technische, operationele en organisatorische maatregelen om de risico's voor de beveiliging van de diensten te beheersen. De maatregelen die hier genoemd staan, dienen verduidelijking te krijgen. "...versleuteling, teneinde de gevolgen van beveiligingsincidenten op gebruikers en op andere netwerken en diensten zo laag mogelijk te houden." is hierbij te globaal. Er wordt genoemd dat er rekening gehouden dient te worden met desbetreffende Europese en Internationale normen, maar dit is heel globaal. Welke normen? Om een uniforme aanpak te behouden in Nederland en inconsistenties te vermijden dienen er meer concrete richtlijnen gegeven te worden.

Advies BTG: formuleer duidelijke richtlijnen nogmaals in artikel 23 en in Telecommunicatiewet artikel 11a1. Daarbij adviseert BTG ook het gebruik van specifieke Europese en internationale normen als kader te benoemen met als doel inconsistenties en onduidelijkheid te voorkomen.

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

Verdere suggesties vanuit BTG:

- *Verplichting tot het gebruik van geavanceerde beveiligingstechnologieën: De wetgeving kan entiteiten verplichten om geavanceerde beveiligingstechnologieën te gebruiken, zoals encryptie, access control en monitoring, om hun netwerken en systemen te beschermen*

- *Verplichting tot het delen van cyberbedreigingsinformatie: De wetgeving kan entiteiten verplichten om cyberbedreigingsinformatie met elkaar en met de bevoegde autoriteiten te delen.*

- *Verplichting tot het uitvoeren van regelmatige pentesten: De wetgeving kan entiteiten verplichten om regelmatige pentesten uit te voeren om de kwetsbaarheid van hun netwerken en systemen te testen.*

- *BTG streeft een zo goed mogelijk geharmoniseerde NIS2 transpositie na. Dit komt ten goede aan de werking van de interne markt. Ondanks dat er veel details missen vanwege het nog ontbreken van secundaire regelgeving is BTG benieuwd in welke mate dit is te verwachten? Zeker vanwege de tekst in het hoofdlijnenakkoord van de nieuwe regeringscoalitie staat onder het sub-hoofdstuk "Solide overheidsfinanciën, economie & vestigingsklimaat": geen nieuwe nationale koppen op Europees beleid; daar waar mogelijk bestaande koppen, die zorgen voor extra regeldruk, schrappen.*

- *De volledige impact van de wet is onduidelijk omdat er veel details nog worden uitgewerkt. Wordt de secundaire regelgeving aangeboden ter consultatie en wanneer wordt dit verwacht?*

Pelmolenlaan 10
3447 GW Woerden
+31(0)88-35 32 222
officemanager@btg.org

Additioneel algemeen oordeel

Hoewel NIS2 zich voornamelijk richt op cybersecurity, kan er overlap zijn met gegevensbeschermingsvoorschriften zoals de GDPR/AVG. Entiteiten kunnen uitdagingen tegenkomen bij het navigeren door het snijvlak van deze regelgevingen en het waarborgen van naleving van beide kaders.
Ook kunnen entiteiten uitdagingen tegenkomen bij het integreren van nieuwe beveiligingsmaatregelen in hun bestaande infrastructuur en operaties, wat mogelijk kan leiden tot verstoringen in de dienstverlening. Het vinden van een balans tussen de beveiligingseisen en de noodzaak om ononderbroken interne- en externe diensten te handhaven, is een belangrijke uitdaging.

Advies BTG: zet extra support op, bijvoorbeeld bij de bevoegde autoriteit, voor de uitdagingen die entiteiten hebben bij het navigeren naar compliance met deze nieuwe wetgeving.

In het specifieke geval van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving wordt vrijstelling gegeven aan bepaalde aspecten van de wet. Op dit moment is het onduidelijk in welke specifieke gevallen er vrijstelling wordt gegeven.

Advies BTG: Voeg hierom meer expliciete richtlijnen aan de artikelen die vrijstelling kunnen genereren zodat het voor deze entiteiten duidelijker navigeren is binnen de kaders van de wet.