NIS2: akkoord bereikt over het aanscherpen van regelgeving over cyberbeveiliging

Het Europees Parlement en de Raad van de Europese Unie bereikten recentelijk een politiek akkoord over de ontwerprichtlijn betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging (de Ontwerp NIS 2 Richtlijn). Met de invoering van de NIS 2 richtlijn zal de huidige regelgeving op het gebied van cyberbeveiliging, die voortvloeit uit de NIS richtlijn, worden aangescherpt. Het doel van de NIS 2 richtlijn is om de Europese Unie weerbaarder te maken tegen cyberaanvallen. Na formele goedkeuring zal de Ontwerp NIS 2 Richtlijn de huidige NIS richtlijn vervangen en dient deze door de lidstaten te worden omgezet in nationale wetgeving.

Emelien Kadijk Versluis, Viviënne

3 oktober 2022

De NIS 2 richtlijn brengt gevolgen met zich voor bedrijven binnen verschillende sectoren (1). Daarom gaan wij in deze blog in op de belangrijkste verschillen ten opzichte van de huidige richtlijn.

Huidige NIS richtlijn en implementatie

Op dit moment is de NIS richtlijn – *richtlijn (EU) 2016/1148 van 16 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie* – van kracht. Het doel van deze richtlijn is om Europa digitaal veiliger te maken door het versterken van weerbaarheid tegen cyberincidenten en het beperken van gevolgen van cyberincidenten.

Nederland heeft de huidige NIS richtlijn geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (de Wbni). De Wbni is van toepassing op vitale aanbieders en digitale dienstverleners. Vitale aanbieders bieden diensten aan in sectoren die van essentieel belang zijn voor

het goed functioneren van de samenleving, zoals de zorg, het vervoer en de energiesector. Zo kan een energieleverancier een vitale aanbieder zijn. Onder digitale dienstverleners vallen rechtspersonen die digitale diensten aanbieden. Een online zoekmachine kan daarvan een voorbeeld zijn.

De Wbni bevat twee belangrijke plichten voor vitale aanbieders en digitale dienstverleners. Ten eerste moeten incidenten worden gemeld bij het Agentschap Telecom en bij het Computer Security Incident Response Team voor digitale dienstverleners (opgericht door het ministerie van Economische Zaken en Klimaat). Een incident in de zin van de Wbni is een gebeurtenis met een schadelijk effect op de beveiliging van netwerk- en informatiesystemen. Ten tweede is er de zorgplicht op grond waarvan vitale aanbieders en digitale dienstverleners technische en organisatorische maatregelen moeten nemen om de risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen.

Aanleiding Ontwerp NIS 2 Richtlijn

De huidige NIS richtlijn biedt volgens de Europese Raad en het Europees Parlement onvoldoende antwoord op de toenemende incidenten in verband met de digitalisering van de maatschappij, zoals cyberaanvallen.
Cyberincidenten kunnen grote schade toebrengen aan de economie en de samenleving. Een hoog niveau van cyberbeveiliging is daarom essentieel voor de veiligheid van de Europese Unie en van haar burgers, bedrijven en instellingen. De lidstaten dienen samen te werken om een toereikend niveau van cyberbeveiliging te bereiken en in stand te houden.

Belangrijkste wijzigingen

De Ontwerp NIS 2 richtlijn wijkt op verschillende punten af van de huidige NIS richtlijn. De Ontwerp NIS 2 richtlijn heeft onder meer tot doel om een hoger niveau van cyberbescherming te waarborgen en om verschillen in het niveau van cyberbeveiliging tussen lidstaten uit te bannen. Om dat doel te bereiken, wordt de lijst met sectoren en activiteiten waarvoor cyberbeveiligingsverplichtingen gelden uitgebreid. Verder krijgen de nationale toezichthouders meer rechtsmiddelen toebedeeld om handhaving van de regelgeving te waarborgen.

Uitbreiding toepassingsgebied

Het toepassingsgebied van de richtlijn wordt uitgebreid door nieuwe sectoren toe te voegen die van groot belang zijn voor de maatschappij. Op dit moment zijn de NIS richtlijn en de Wbni van toepassing op digitale dienstverleners en op vitale aanbieders in belangrijke sectoren. De Ontwerp NIS 2 richtlijn

voegt hier sectoren aan toe, zoals afval(water)beheer, post- en koeriersbedrijven, overheidsdiensten en platforms voor sociale netwerken. De Ontwerp NIS 2 richtlijn zal van toepassing zijn op middelgrote en grote ondernemingen binnen al die sectoren.

De Ontwerp NIS 2 richtlijn maakt geen onderscheid meer tussen vitale aanbieders en digitale dienstverleners, maar deelt ondernemingen in de volgende categorieën in: essentiële en belangrijke ondernemingen. De nationale autoriteiten krijgen verdergaande bevoegdheden ten opzichte van *essentiële ondernemingen* (binnen onder meer de energiesector) dan ten opzichte van *belangrijke ondernemingen* (zoals post- en koeriersdiensten).

Versterken en stroomlijnen beveiligings- en rapportagevereisten

De Ontwerp NIS 2 richtlijn versterkt de beveiligings- en rapportagevereisten voor bedrijven door verplichtingen op te leggen in het kader van risicobeheersing. De richtlijn bevat daartoe een lijst met minimale beveiligingselementen die in elk geval moeten worden toegepast door zowel essentiële als belangrijke ondernemingen. Nieuw ten opzichte van de huidige richtlijn is onder meer de verplichting om cyberbeveiligingsrisico's in toeleveringsketens en relaties met leveranciers aan te pakken.

Verder bevat de Ontwerp NIS 2 richtlijn preciezere bepalingen over (de procedure voor) incidentmeldingen bij het Computer Security Incident Response Team, dan wel de nationale autoriteit.

Toezicht en handhaving

Tot slot beschrijft de Ontwerp NIS 2 richtlijn in meer detail de bevoegdheden die nationale autoriteiten dienen te hebben bij de uitoefening van hun toezicht- en handhavingstaken. Lidstaten moeten ervoor zorgen dat de toezichthouder (onder meer) de mogelijkheid krijgt om bindende instructies en bevelen te geven en administratieve boetes op te leggen. De maximale hoogtes van deze boetes moeten de lidstaten stellen op ten minste EUR 10 miljoen of 2% van de totale wereldwijde omzet, afhankelijk van welk bedrag hoger is. Dit wijkt af van de huidige NIS richtlijn, waarin geen minimale boetehoogtes zijn opgenomen. De maximale boete die op dit moment op grond van de Wbni kan worden opgelegd, bedraagt EUR 5 miljoen.

Volgende stappen

Vermoedelijk zal de inwerkingtreding van de Ontwerp NIS 2 richtlijn nog even op zich laten wachten. Het Comité van permanente vertegenwoordigers dient de tekst nog goed te keuren. Na invoering van de richtlijn hebben lidstaten 21 maanden de tijd om de bepalingen in hun nationale recht om te zetten.

Voor bedrijven kan het lonen om alvast te onderzoeken of zij onder de werkingssfeer van de Ontwerp NIS 2 richtlijn zullen vallen. Indien dat het geval is, dienen er namelijk stappen te worden gezet richting een hoog niveau van cyberbeveiliging.

https://www.rijksoverheid.nl/actueel/nieuws/2022/07/22/nieuwe-europese-richtlijn-moet-veiligheid-verhogen