Raad van de EU

PRESS
NL

PERSMEDEDELING
904/15
08/12/2015

Eerste EU-brede regels voor een betere cyberbeveiliging: akkoord met het EP

Op 7 december 2015 bereikte het Luxemburgse voorzitterschap van de Raad een informeel akkoord met het Europees Parlement over gemeenschappelijke regels ter versterking van de **netwerk- en informatiebeveiliging (NIB)** in de hele EU.

De nieuwe richtlijn behelst verplichtingen op het gebied van cyberbeveiliging voor **exploitanten van essentiële diensten** en **aanbieders van digitale diensten**. Deze exploitanten/aanbieders zullen maatregelen moeten nemen voor het beheer van cyberrisico's en moeten belangrijke beveiligingsincidenten melden, maar voor beide categorieën gelden verschillende regelingen.

Xavier Bettel, premier van Luxemburg, minister van Communicatie en Media en voorzitter van de Raad, zei hierover het volgende: "Dit is een belangrijke stap naar een meer gecoördineerde aanpak van cyberbeveiliging in heel Europa. Alle actoren, zowel publieke als particuliere, zullen extra inspanningen moeten leveren, vooral door een betere samenwerking tussen de lidstaten en betere beveiligingsvoorschriften voor exploitanten van infrastructuur en digitale diensten".

Strengere regels voor essentiële exploitanten

De richtlijn noemt een aantal **kritieke sectoren** waarin exploitanten van essentiële diensten actief zijn, zoals energie, vervoer, financiën en gezondheidszorg. Binnen deze sectoren bepalen de lidstaten, aan de hand van duidelijke criteria die in de richtlijn zijn bepaald, welke exploitanten essentiële diensten verrichten. Voor deze exploitanten zullen de voorschriften en het toezicht strenger zijn dan voor aanbieders van digitale diensten. Dat is functie van de hoogte van het risico die elke onderbreking in hun diensten teweeg kan brengen voor de samenleving en de economie.

Een eenvormiger regeling voor aanbieders van digitale diensten

De volgende digitale diensten vallen onder de richtlijn**: platformen voor e-commerce, zoekmachines en clouddiensten**.

Aanbieders van digitale diensten zijn gewoonlijk actief in veel lidstaten. Om ervoor te zorgen dat zij in de hele EU op vergelijkbare wijze worden behandeld, zullen de regels gelden voor alle exploitanten die zulke diensten verrichten, met uitsluiting van kleine ondernemingen.

Nationale en EU-kaders ter bestrijding van cyberdreigingen

Elke lidstaat moet een of meer nationale autoriteiten aanwijzen en een strategie voor de aanpak van cyberaangelegenheden opstellen.

De lidstaten zullen ook hun samenwerking op het gebied van cyberbeveiliging opvoeren. Er zal een samenwerkingsgroep op EU-niveau worden ingesteld om de strategische samenwerking en de uitwisseling van beste praktijken tussen de lidstaten te ondersteunen. Er zal een netwerk van nationale responsteams computerbeveiliging (Computer Security Incident Response Teams (CSIRTs)) worden opgezet ter bevordering van de operationele samenwerking. Zowel de groep als de teams moeten tevens het vertrouwen tussen de lidstaten helpen versterken.

Termijnen

De lidstaten beschikken over 21 maanden na de inwerkingtreding van de richtlijn om de nodige nationale bepalingen aan te nemen. Na deze periode hebben zij nog eens 6 maanden om te bepalen welke exploitanten essentiële diensten verrichten.

Hoe wordt dit wetgeving?

Wat de Raad betreft, moet het akkoord nog worden bevestigd door de lidstaten. Het voorzitterschap zal op 18 december de overeengekomen tekst ter goedkeuring voorleggen aan de ambassadeurs van de lidstaten in het Comité van permanente vertegenwoordigers (Coreper). Om de procedure af te ronden is de formele aanneming door de Raad en het Parlement vereist.

- Verbeteren van cyberbeveiliging in de hele EU

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press