TWEEDE KAMER DER STATEN-GENERAAL **2**

Vergaderjaar 2025-2026

36 764 **Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (PbEU 2022, L 333) (Cyberbeveiligingswet)**

Nr. 14 **AMENDEMENT VAN HET LID EL BOUJDAINI**
Ontvangen 20 maart 2026

De ondergetekende stelt het volgende amendement voor:

In het voorgestelde artikel 51 wordt na het tweede lid een lid ingevoegd, luidende:

2a. De CSIRT's werken voor de doeltreffende en doelmatige uitvoering van hun taken uit hoofde van deze wet samen met de burgemeesters en de voorzitters van de veiligheidsregio's, gelet op hun taken op het gebied van de handhaving van de openbare orde respectievelijk op het gebied van de crisisbeheersing, en wisselen in het kader van die samenwerking alle daarvoor noodzakelijke gegevens over cyberdreigingen, kwetsbaarheden en incidenten uit, waaronder persoonsgegevens.

Toelichting

De burgemeester is op grond van de Gemeentewet verantwoordelijk voor de handhaving van de openbare orde binnen de gemeente. De voorzitter van de veiligheidsregio is belast met de crisisbeheersing op regionaal niveau. Cyberincidenten bij organisaties in de gemeente, zoals ziekenhuizen, energiebedrijven of vervoerders, kunnen directe gevolgen hebben voor de openbare orde, bijvoorbeeld door uitval van essentiële diensten zoals openbaar vervoer, verkeerslichten of ICT bij ziekenhuizen. Om hierop te anticiperen en de gevolgen te beperken, moeten de burgemeester en de voorzitter van de veiligheidsregio tijdig beschikken over relevante informatie. Het wetsvoorstel voor de Cyberbeveiligingswet (Cbw) regelt dat Computer Security Incident Response Teams (CSIRT's, voor de meeste essentiële en belangrijke entiteiten is de Minister van Justitie en Veiligheid, in de praktijk het Nationaal Cyber Security Centrum, het CSIRT) beschikken over informatie over cyberdreigingen, kwetsbaarheden en incidenten bij essentiële en belangrijke entiteiten. Het wetsvoorstel biedt echter geen grondslag om deze informatie te delen met de burgemeester of de voorzitter van de veiligheidsregio, wanneer die informatie niet ziet op de cyberveiligheid van de gemeentelijke organisatie zelf, maar op dreigingen en incidenten bij andere organisaties binnen de gemeentegrenzen die de openbare orde kunnen raken.

De regering heeft in de nota naar aanleiding van het verslag bevestigd dat de Cbw hiervoor geen grondslag biedt en verwijst naar het Bestuurlijk convenant digitale veiligheid gemeenten. Dit betekent dat de burgemeester bij incidenten zonder nationale opschaling geen informatie kan ontvangen over dreigingen en incidenten bij organisaties in de gemeente, ook niet wanneer die incidenten de openbare orde raken of kunnen raken. Indiener acht alleen een convenant binnen dit kader onvoldoende, omdat het geen wettelijke grondslag biedt voor het delen van informatie die op grond van de Cyberbeveiligingswet bij de Minister van Justitie en Veiligheid (in de praktijk: het Nationaal Cyber Security Centrum (NCSC)) en de andere CSIRT's berust.

In de nota naar aanleiding van het verslag wordt bovendien gesuggereerd dat geen zinvolle informatie aan de burgemeester kan worden verstrekt omdat de meldtermijn van 72 uur maakt dat deze zelf al eerder op de hoogte kan zijn van de lokale impact van een cyberdreiging of veiligheidsincident. Indiener deelt deze opvatting niet, omdat organisaties binnen uiterlijk 24 uur een vroegtijdige waarschuwing dienen te geven en er sprake is van maximumtermijnen, zodat er over het algemeen sneller dan binnen 72 uur informatie beschikbaar is. De CSIRT's hebben daarnaast ook een eigen monitoringscapaciteit, wat kan leiden tot nieuwe signalen. Niet ieder incident komt voorts in de openbaarheid en bereikt de burgemeester, terwijl ook bij cyberincidenten waar de burgemeester wel via eigen kanalen van op de hoogte raakt, de informatie relevant kan zijn, bijvoorbeeld omdat deze scenario's valideert of juist uitsluit.

De NIS2-richtlijn verzet zich niet tegen deze informatiedeling. Artikel 9, eerste lid, van de richtlijn verlangt dat lidstaten zorgen voor samenhang tussen het kader voor cybercrisisbeheersing en bestaande kaders voor nationale crisisbeheersing. De burgemeester en de veiligheidsregio zijn in Nederland de aangewezen partijen voor crisisbeheersing op lokaal en regionaal niveau. Daarnaast rekenen de artikelen 10, derde lid, en 11, derde lid, onderdeel b, van de richtlijn het verstrekken van informatie aan "relevante belanghebbenden" uitdrukkelijk tot de taken van het CSIRT. Dit amendement voorziet in de wijziging van het voorgestelde artikel 51 van de Cbw, waarbij de burgemeester en de voorzitter van de veiligheidsregio expliciet worden toegevoegd als ontvangers van informatie van het CSIRT. Het gaat daarbij zowel om actuele informatie over dreigingen, incidenten en kwetsbaarheden bij organisaties binnen de gemeentegrenzen die kunnen leiden tot lokale ontwrichting, als om strategische informatie, zoals dreigingsbeelden en risicoanalyses, die de burgemeester in staat stelt gericht samen te werken met lokale essentiële en belangrijke organisaties en preventiemaatregelen te treffen waar dat raakt aan de openbare orde in de gemeente.

Op de verstrekking van vertrouwelijke informatie zijn de waarborgen van het voorgestelde artikel 66 van de Cbw onverkort van toepassing. Ten overvloede merkt de indiener op dat het nadrukkelijk gaat om het kunnen verstrekken van informatie en dat de gedeelde informatie relevant moet zijn voor de uitoefening van de taken van de burgemeester en de voorzitter van de veiligheidsregio op het gebied van openbare orde en respectievelijk crisisbeheersing. De voorwaarden voor deze informatiedeling kunnen nader uitgewerkt worden in een convenant tussen de betrokken partijen.

El Boujdaini