> Retouradres Postbus 16950 2500 BZ Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Programma Nederland Digitaal Veilig

Turfmarkt 147
2511 DP Den Haag
Postbus 16950
2500 BZ Den Haag
www.nctv.nl

Ons kenmerk
2634396

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 25 juni 2019
Onderwerp Kamerbrief kwetsbaarheden scan nav AO Nationale Veiligheid 20 juni 2019

Deze brief is een reactie aan uw Kamer op de vraag van het lid Verhoeven (D66), gesteld tijdens het AO Nationale Veiligheid van 20 juni jl., over de wenselijkheid van een scan van kwetsbaarheden in de context van cybersecurity en het belang van publiek private samenwerking daarbij. Het scannen op kwetsbaarheden zal onderdeel uitmaken van de structurele en adaptieve risicobeheersing zoals aangekondigd in mijn reactie op het Cybersecurity Beeld Nederland (CSBN) 2019 aan uw Kamer op 12 juni jl.

In voorgenoemde brief aan uw Kamer, waarin ik u tevens informeerde over de voortgang van de Nederlandse Cybersecurity Agenda (NCSA), schreef ik dat het CSBN 2019 een zorgwekkend beeld schetst, waarbij de weerbaarheid achter dreigt te lopen bij de ontwikkelingen ten aanzien van de digitale dreiging. Dit vraagt om actie. Met de implementatie van de eerste NCSA maatregelen is het afgelopen jaar een goede start gemaakt, maar naast de voortzetting van de aanpak zoals aangekondigd in de NCSA is extra inspanning nodig. Daarom wordt gezamenlijk met de betrokken departementen en onder mijn regie voor alle vitale sectoren ingezet op structurele en adaptieve risicobeheersing.

Een belangrijk onderdeel van de structurele en adaptieve risicobeheersing is het verkrijgen van inzicht in kwetsbaarheden van digitale systemen van vitale sectoren om het niveau van de digitale weerbaarheid te kunnen beoordelen en passende beheersmaatregelen te kunnen treffen. Dit inzicht kan op verschillende manieren worden verkregen. Het voorgestelde breed, publiek-private, oefen- en testprogramma van dit kabinet moet onder meer leiden tot meer inzicht in de kwetsbaarheden. Door op structurele basis en in gezamenlijkheid digitale systemen te testen zal beter zicht op de kwetsbaarheden ontstaan. Ook het opnieuw beoordelen welke belangen in de digitale ruimte het meest van invloed zijn op de nationale veiligheid en of organisaties zich voldoende bewust zijn van de daarbij behorende kwetsbaarheden zal daaraan bijdragen. Dat dit in publiek-privaat verband gebeurt, is gezien de belangrijke rol van private vitale organisaties essentieel.

In mijn brief schreef ik u ook reeds over de ontwikkeling en inrichting van een gezamenlijke vulnerability scanning faciliteit voor de Rijksoverheid onder coördinatie van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Hiermee kunnen alle systemen van de Rijksdienst die zijn verbonden met het internet worden gecontroleerd op bekende kwetsbaarheden. Samen met mijn collega bewindspersonen van de betrokken departementen zal ik, mede op basis

van de ervaringen die daarmee worden opgedaan, bezien in welke mate deze methodiek toegepast kan worden bij de vitale sectoren.

Om de digitale weerbaarheid te verhogen werkt dit kabinet de komende periode hard verder aan het implementeren van de maatregelen uit het NCSA en zet het in op structurele en adaptieve risicobeheersing. De komende maanden zullen de plannen aangekondigd in mijn brief van 12 juni jl. onder regie van de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) in samenwerking met de betrokken departementen en de vitale sectoren verder worden uitgewerkt. Scannen op en verkrijgen van inzicht in kwetsbaarheden zullen daar onderdeel van uitmaken, samenwerking met de private sector zijn bij de uitvoering daarvan van groot belang. Ik zie het voorstel voor een scan van kwetsbaarheden dan ook als ondersteuning van beleid en zal uw Kamer hierover in samenhang met de voortgang van de NCSA blijven informeren.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus