Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

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

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag

Kenmerk
2020-0000533724

Uw kenmerk

5 oktober 2020
Betreft: Brief n.a.v. AO Digitalisering 1 juli

Tijdens het AO Digitalisering op 1 juli 2020 stelde het lid Van Dam (CDA) vragen over het artikel in de Volkskrant van 1 juli jl. "Half jaar na Citrix-crisis zijn 25 Nederlandse organisaties gehackt. En ze weten zelf van niets".[1] In dat artikel werd gemeld dat uit onderzoek bleek dat minstens 25 organisaties zijn gehackt naar aanleiding van het Citrix-lek. De heer Van Dam vroeg zich af of de situatie nu helemaal in control is.

Na het lek bij Citrix heeft het NCSC de betrokken Rijksorganisaties onder meer geadviseerd om forensisch onderzoek uit laten voeren om eventuele uitbuiting uit te sluiten. Volgens de Rijksbrede afspraken in de Baseline Informatiebeveiliging Overheid (BIO) dienen nieuwe dreigingen (aanvallen) binnen geldende juridische kaders gedeeld te worden binnen de rijksoverheid, waaronder met het NCSC.[2] Op basis van de mij nu bekende informatie zijn rijksoverheidsorganisaties in control naar aanleiding van het Citrix incident waar de Volkskrant op 1 juli over berichtte.

Elk departement is zelf verantwoordelijk voor het op orde hebben van de eigen informatiebeveiliging. Hiervoor worden onder coördinatie van BZK kaders en richtlijnen opgesteld, zoals de BIO. Over de implementatie van de BIO en andere bovenbedoelde richtlijnen rapporteren rijksoverheidsorganisaties aan de departementale CIO's en aan de CIO Rijk.

In dit verband wijs ik graag nog op de toezeggingen die zijn gedaan naar aanleiding van de evaluatie van het Citrix incident en het WRR-rapport Voorbereiden op Digitale Ontwrichting.[3] Zo zullen binnen de Rijksoverheid naast de al bestaande richtlijnen en kaders bindende afspraken worden gemaakt op bestuurlijk en politiek niveau over het 'pas toe of leg uit' principe. Organisaties binnen de Rijksoverheid moeten dan bij dringende beveiligingsadviezen van het NCSC aan de CIO Rijk uitleg geven wanneer zij deze niet opvolgen. Ook wordt het rijksbrede beeld van de bij rijksoverheidsorganisaties in gebruik zijnde netwerk en informatiesystemen verbeterd door afspraken te maken in het informatiestatuut over welke informatie hierover organisaties met de CIO Rijk delen.

[1] Kamerstukken II 2019/2020, 26643 nr. 707
[2] BIO 12.4.1.4
[3] Kamerstukken II 2019/2020, 26643 nr. 673

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Kenmerk
2020-0000533724

Ik zal uw Kamer op de hoogte houden over de uitvoering van deze toezeggingen via de periodieke voortgangsrapportages van de Strategische I-agenda voor de Rijksdienst.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops