Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

> 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
2660476

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

Datum 6 augustus 2019
Onderwerp Onderzoeksrapport WODC kwetsbaarheden industriële controle systemen

Met deze brief bied ik uw Kamer het in opdracht van mijn ministerie door het WODC opgeleverde onderzoeksrapport *'Online Discoverability and Vulnerabilities of ICS/SCADA Devices in the Netherlands'* aan, over de online vindbaarheid en kwetsbaarheid van digitale industriële controlesystemen in Nederland. Dergelijke systemen, ook wel bekend als ICS/SCADA[1] systemen, worden onder andere gebruikt voor de besturing van processen in de vitale infrastructuur. Als deze systemen worden gehackt kunnen aanvallers de besturing ervan overnemen met in potentie grote nadelige gevolgen.

De onderzoekers hebben aangetoond dat het relatief gemakkelijk is om via het internet ICS/SCADA systemen te lokaliseren. Zij wisten door inzet van een bepaalde methode rond de duizend ICS/SCADA systemen in Nederland te lokaliseren. Ongeveer zestig van de gevonden systemen bevatte één of meerdere kwetsbaarheden. Of deze systemen aan vitale infrastructuur toebehoorden hebben de onderzoekers niet kunnen aantonen. Desalniettemin is het een belangrijk signaal over kwetsbaarheden in ICS/SCADA-systemen, zeker aangezien het aantal kwetsbaarheden in werkelijkheid hoger kan liggen. De zorgen hierover zijn al langer bekend. Het NCSC heeft in dit kader onder meer in 2015 een tweetal uitgebreide adviezen gepubliceerd.

De resultaten van het onderzoek onderschrijven de noodzaak om te werken aan de verhoging van de digitale weerbaarheid van Nederland. Op 12 juni jl. bood ik uw Kamer het Cybersecurity Beeld Nederland 2019 aan met daarbij mijn beleidsreactie.[2] Het CSBN2019 schetste een zorgwekkend beeld van een digitale weerbaarheid die achter dreigt te lopen bij de digitale dreiging. Ik schreef uw Kamer daarom dat dit kabinet zich onder mijn regie de komende periode inzet om de weerbaarheid structureel te verhogen. De verdere implementatie van de maatregelen uit de Nederlandse Cybersecurity Agenda en de uitwerking van het programma van continue en adaptieve risicobeheersing zullen daaraan bijdragen. Inzicht verkrijgen in het weerbaarheidsniveau en kwetsbaarheden is daarvan een essentieel onderdeel. In datzelfde kader zal de uitvoering van de door uw Kamer

[1] Industrial Control Systems (ICS) worden gebruikt voor het aansturen van fysieke processen. Deze systemen worden doorgaans beheerd met een SCADA systeem (Supervisory Control and Data Acquisition) dat (1) instructies kan versturen aan het controlesysteem, (2) informatie biedt over metingen van diverse sensoren en (3) als alarmsysteem kan fungeren wanneer er iets misgaat.

[2] Brief CSBN 2019 en voortgangsrapportage NCSA (Kamerstuk 26643, nr. 614)

aangenomen motie van de leden Verhoeven en Laan-Geselschap om te scannen op kwetsbaarheden daar ook aan bijdragen.[3]

Wat de vindbaarheid en kwetsbaarheid van ICS/SCADA systemen zelf betreft, doen de onderzoekers in hun rapport enkele aanbevelingen. Deze zijn, zoals zij zelf aangeven, tamelijk eenvoudig uit te voeren. Deze maatregelen zijn bovendien in lijn met adviezen die het Nationaal Cyber Security Centrum (NCSC) eerder uitbracht. In 2015 publiceerde het NCSC twee factsheets over de beveiliging van ICS. De factsheet '*Uw ICS/SCADA- en gebouwbeheersystemen online*' beschrijft de risico's van het koppelen van dergelijke systemen aan internet en de maatregelen die organisaties kunnen treffen om deze systemen beter te beveiligen. Met behulp van de tweede factsheet, '*Checklist beveiliging van ICS/SCADA-systemen*', kunnen organisaties bepalen of hun ICS afdoende zijn beveiligd. De checklist omvat maatregelen tegen de meest voorkomende kwetsbaarheden en beveiligingsproblemen. In welke mate de aanbevelingen over aanvullend onderzoek en discussie worden meegenomen zal mede in de uitwerking van het programma van continue en adaptieve risicobeheersing worden bezien.

Het NCSC zal organisaties binnen de vitale infrastructuur en hun toezichthouders over de publicatie van het onderzoeksrapport informeren en de risico's van het koppelen van ICS/SCADA-systemen aan het internet opnieuw bij hen onder de aandacht brengen. Tevens kan het NCSC organisaties binnen de vitale infrastructuur adviseren bij het treffen van de in het rapport voorgestelde maatregelen. Vanuit mijn coördinerende rol voor nationale veiligheid en als stelselverantwoordelijke voor cybersecurity blijf ik regie voeren op het verhogen van de weerbaarheid en op verdere intensivering van de cybersecurity aanpak.

De Minister van Justitie en Veiligheid,

Ferd Grapperhaus

[3] Motie van de leden Verhoeven en Laan-Geselschap over het op kwetsbaarheden scannen van overheidssystemen in de vitale infrastructuur (Kamerstuk 30 821, nr. 85)