Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2023-2024

36 263 Tijdelijke regels inzake specifieke wettelijke voorzieningen voor het uitvoeren van onderzoeken door de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen alsmede voorzieningen inzake de mogelijkheid tot vaststelling van een nieuwe eindtermijn voor gebruik door de diensten van in het kader van hun taakuitvoering met bijzondere bevoegdheden verworven bulkdatasets en de invoering van een bindende toets ex ante van verleende toestemmingen voor de real time interceptie van verkeers-en locatiegegevens (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen)

30 821 Nationale veiligheid

F[1] **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 6 februari 2024

Middels deze brief informeer ik uw Kamer over het nieuwsbericht dat China via malware bij het ministerie van Defensie spioneert. Inmiddels is het nader onderzoek ten behoeve van attributie afgerond en maakt het kabinet om redenen van het vergroten van weerbaarheid nationaal en internationaal de informatie openbaar.

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft Chinese cyberspionage in Nederland blootgelegd. De MIVD ontdekte geavanceerde Chinese malware die dit mogelijk maakt. De aangetroffen malware installeerde een 'achterdeurtje' door gebruik te maken van een bekende kwetsbaarheid in FortiGate-apparaten. Een Chinese statelijke actor is hiervoor verantwoordelijk. Dit stelt de MIVD op basis van eigen inlichtingen vast. Via een publicatie op 6 februari op de website van het Nationaal Cybersecurity Centrum (NCSC) is een technisch rapport van de MIVD gedeeld met details over de Chinese malware met bijbehorend handelingsperspectief. Defensie heeft haar interne maatregelen opnieuw tegen het licht gehouden om dit soort acties zo veel mogelijk te voorkomen.

China's cybercapaciteiten zijn significant. De MIVD wijst er in de jaarverslagen op dat Nederland doorlopend wordt geconfronteerd met digitale aanvallen, uitgevoerd door landen met een offensief cyberprogramma, waaronder China, Rusland, Noord-Korea en Iran. Dit is de eerste keer dat de MIVD een technisch rapport over de werkwijze van Chinese hackers openbaar maakt. Zo draagt Defensie bij aan het verhogen van cyberweerbaarheid. De MIVD treedt nu naar buiten, aangezien er grondig en zorgvuldig onderzoek nodig was om uit te zoeken van wie deze malware afkomstig is.

De MIVD heeft in samenwerking met het NCSC kenmerken van de aangetroffen malware gedeeld met relevante nationale en internationale partners in het cybersecuritydomein. Tot dan toe waren de kenmerken van de malware nog niet bekend bij partners. De MIVD vraagt organisaties die deze malware aantreffen om zich te melden bij het NCSC. Zo kan de Chinese spionagecampagne worden

[1] De letter F heeft alleen betrekking op 36 263.

tegengegaan. Het rapport van de MIVD biedt technisch handelingsperspectief op de onderzochte malware. Het NCSC biedt daarnaast algemeen handelingsperspectief.

Een gelijkluidende brief heb ik verstuurd aan de Tweede Kamer.

De minister van Defensie

drs. K.H. Ollongren