Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2023-2024

36 270 Regels ter bevordering van de digitale weerbaarheid van bedrijven (Wet bevordering digitale weerbaarheid bedrijven)

C **NOTA NAAR AANLEIDING VAN HET VERSLAG**
Ontvangen 29 april 2024

Het wetsvoorstel heeft in de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

Met belangstelling heb ik kennisgenomen van de vragen en opmerkingen die door de leden van de fractie van JA21 zijn gesteld in het verslag van de vaste commissie voor Economische Zaken en Klimaat van 17 april 2024. In deze nota naar aanleiding van het verslag ga ik graag in op de vragen en opmerkingen, waarbij ik de volgorde van het verslag volg. De tekst van het verslag is schuingedrukt, de beantwoording niet.

Vragen en opmerkingen van de leden van de JA21-fractie

*De fractieleden van **JA21** vragen in hoeverre uitbreiding van bevoegdheden van de minister voor Economische Zaken en Klimaat middels deze wet strikt noodzakelijk is voor het uitvoeren van de taak van het Digital Trust Center (DTC).*

Met het wetsvoorstel bevordering digitale weerbaarheid bedrijven worden de taken en bevoegdheden van de minister van Economische Zaken en Klimaat (EZK) vastgelegd om de niet-vitale bedrijven te kunnen informeren over digitale kwetsbaarheden, dreigingen en incidenten. Deze informatie kan persoonsgegevens bevatten en daarom is een wettelijke verankering van deze taken en bevoegdheden noodzakelijk. De bevoegdheid tot de verwerking van persoonsgegevens vereist namelijk een wettelijke grondslag.

Zij vragen tevens hoe de regering de impact van de Wet bevordering digitale weerbaarheid op bedrijven beoogt te meten. Welke specifieke indicatoren en meetinstrumenten worden ingezet om de verbetering van de digitale weerbaarheid bij bedrijven te kwantificeren?

Het meten van de mate waarin bedrijven cyberweerbaarder zijn geworden is geen sinecure. Daarom gebruikt het Digital Trust Center (DTC) verschillende indicatoren en meetinstrumenten om de digitale weerbaarheid bij bedrijven te kwantificeren. Ten behoeve van de hoofdtaak van het DTC 'het geven van kennis en advies' publiceert het Centraal Bureau voor de Statistiek (CBS) mede op verzoek van het ministerie van Economische Zaken en Klimaat (EZK) jaarlijks de Cybersecuritymonitor[1]. Hierin wordt gerapporteerd over de meest actuele stand van zaken rond de cyberweerbaarheid van bedrijven en huishoudens in Nederland. De cybersecuritymonitor schetst aan de hand van een twintigtal indicatoren een beeld van de cybersecurity in Nederland. Door middel van maatwerktabellen worden hiernaast door het CBS de verschillen in genomen maatregelen gemeten tussen midden- en kleinbedrijven (mkb) en zelfstandigen zonder personeel (zzp'ers) die bekend dan wel verbonden zijn aan het DTC, en mkb'ers en zzp'ers die dat niet zijn. Zo kan een indicatie worden gegeven in hoeverre de producten en diensten van het DTC leiden tot het nemen van meer maatregelen door bedrijven om cyberweerbaarder te worden.
Het DTC maakt binnen haar notificatiedienst gebruik van een vrijwillige feedbackloop om een beeld te krijgen van hoe de notificaties van het DTC worden ervaren en of er opvolging heeft

[1] https://www.digitaltrustcenter.nl/sites/default/files/2023-08/cybersecuritymonitor_2022.pdf

plaatsgevonden. Deze feedback wordt doorlopend gebruikt voor het verbeteren van de dienstverlening van het DTC. De Technische Universiteit Delft zal dit jaar nog starten met een onderzoek voor het DTC, het Computer Incident Response Team voor digitale diensten (CSIRT DSP) en het Nationaal Cyber Security Centrum (NCSC) om te onderzoeken welke notificatiemechanismes het meest effectief zijn om de ontvanger tot opvolging over te laten gaan.

De leden van de JA21-fractie vragen voorts waarom er niet volstaan kan worden met het verstrekken van geanonimiseerde gegevens in plaats van het ontsluiten van persoonsgegeven bij het analyseren van dreigingen dan wel het adviseren tot het nemen van maatregelen.

Via haar website, de DTC community en social media kanalen adviseert het DTC zo veel mogelijk Nederlandse bedrijven tot het nemen van de nodige cybersecuritymaatregelen. Voor een groot deel van deze dienstverlening gaat het om openbare informatie en is dus geen ontsluiting van persoonsgegevens nodig. Echter, als er bij de overheid informatie bekend is over een ernstige cyberdreiging, kwetsbaarheid of incident voor één of meerdere bedrijven dan wil het DTC deze specifieke bedrijven een waarschuwing afgeven.
Deze 'dreigingsinformatie' bestaat uit bijvoorbeeld IP-adressen en/of domeinnamen van kwetsbare systemen. Om Nederlandse niet-vitale bedrijven te kunnen waarschuwen en te voorzien van handelingsperspectief herleidt het DTC, waar mogelijk, tot welke organisatie deze ontvangen dreigingsinformatie behoort. Voor een goede uitvoering van deze taken zal het in voorkomende gevallen noodzakelijk zijn om persoonsgegevens te verwerken.
De organisaties die worden genotificeerd zijn alleen Nederlandse organisaties. Daderinformatie wordt in principe niet verwerkt. Het zou kunnen dat er binnen het handelingsperspectief naar een Indicator of Compromise (IoC)[2] wordt verwezen. Binnen zo'n IoC kan een IP-adres of domeinnaam van een mogelijke dader staan. In de basis zijn de gegevens die worden verwerkt bedrijfsgegevens. Maar in voorkomende gevallen kunnen ook namen, IP-adressen, e-mailadressen en telefoonnummers worden verwerkt welke herleidbaar zijn tot natuurlijke personen. Dat kan bijvoorbeeld het geval zijn bij een eenmansbedrijf of contactpersoon van een bedrijf. Hierbij gaat het om 'gewone' persoonsgegevens waarbij niet meer gegevens worden verwerkt dan strikt noodzakelijk, en deze niet voor andere doeleinden worden gebruikt dan waarvoor zij oorspronkelijk zijn verzameld. Om deze gegevens te mogen verwerken (waaronder ontvangen en verspreiden) is een expliciete wettelijke grondslag op grond van de Algemene verordening gegevensbescherming (AVG) vereist.

De fractieleden van JA21 vragen, gelet op hun zorgen omtrent privacy en gegevensbescherming bij de implementatie van de Wet bevordering digitale weerbaarheid bedrijven, of de regering kan uiteenzetten welke specifieke maatregelen zijn genomen om de bescherming van persoonsgegevens te waarborgen bij het verwerken en delen van informatie tussen de overheid en bedrijven. Hoe wordt verzekerd dat deze maatregelen in lijn zijn met zowel de Algemene Verordening Gegevensbescherming (AVG) als nationale privacywetgeving?

Zoals in de memorie van toelichting bij het wetsvoorstel is aangegeven, volgt de minister van EZK bij de uitvoering van de taken uit dit wetsvoorstel de in het algemeen voor de overheid geldende voorschriften voor informatiebeveiliging zoals de Baseline Informatiebeveiliging Overheid (BIO) en de Richtlijn informatiebeveiliging (IB-richtlijn). De BIO biedt een uniform normenkader voor de beveiliging van de informatiehuishouding van alle overheidsorganisaties waardoor gegevens veilig kunnen worden uitgewisseld.

Met betrekking tot het voorliggende wetsvoorstel is tevens een Data Protection Impact Assessment (DPIA) uitgevoerd. Hierin staan de te verwerken persoonsgegevens en de te nemen maatregelen om deze te beschermen, beschreven. Met de volgende maatregelen wordt verzekerd dat er wordt gewerkt in lijn met zowel de AVG als nationale privacywetgeving:

- Het beperken van toegang van medewerkers tot de informatie binnen hun taak.
- Het vereisen van een screening.

[2] Een Indicator of Compromise (IoC) is een stuk bewijs dat is achtergelaten door een aanvaller of kwaadaardige software die kan worden gebruikt om een beveiligingsincident te identificeren. Met IoC's kunnen organisaties op centrale punten in het netwerk snel zicht krijgen op malafide digitale activiteiten.

- De technische systemen die worden gebruikt voor het verwerken van de gegevens worden periodiek gepentest.[3]
- Het verwerken van gegevens gebeurt uitsluitend op werkstations ten behoeve van de import van data waarna de data direct verwijderd worden en alleen nog in de database worden bewaard.
- De gebruikte systemen en data staan binnen het datacentrum van de overheid - ODC Noord - in een geïsoleerd netwerksegment conform de IB-richtlijn.
- Toegang tot deze data is uitsluitend op basis van 'need to know', dit houdt onder andere in dat medewerkers alleen toegang hebben tot systemen en informatie die verband houden met hun eigen aandachtsgebieden en onderzoeken.
- Het gegeven dat een bedrijf geïnformeerd wordt en het verstrekte advies of handelingsperspectief wordt maximaal 5 jaar bewaard. De onderliggende gegevens, zoals op basis waarvan een bedrijf geïnformeerd is en een handelingsperspectief heeft gekregen, worden maximaal 2 jaar bewaard. Deze termijnen sluiten aan bij de bewaartermijnen van het NCSC.

Zoals opgenomen in de memorie van toelichting is het wetsvoorstel ter advisering aan de Autoriteit Persoonsgegevens (AP) voorgelegd. De AP heeft een blanco advies uitgebracht.

M.A.M. Adriaansens

Minister van Economische Zaken en Klimaat

[3] Een *pentest* is een toets van een of meer computersystemen op kwetsbaarheden. Na afloop kunnen gerichte maatregelen worden genomen om de risico's te beperken.