Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2016–2017

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1927

Vragen van het lid **Hijink** (SP) aan de Minister van Economische Zaken en de Staatssecretaris van Veiligheid en Justitie over *het bericht dat bedrijven nog te weinig doen aan digitale veiligheid* (ingezonden 7 april 2017).

Antwoord van Minister **Kamp** (Economische Zaken) mede namens de Staatssecretaris van Veiligheid en Justitie (ontvangen 23 mei 2017). Zie ook Aanhangsel Handelingen, vergaderjaar 2016–2017, nr. 1740.

Vraag 1
Kent u het bericht «Bedrijven doen nog te weinig aan digitale veiligheid» van de Cyber Security Raad (CSR)?[1]

Antwoord 1
Ja.

Vraag 2
Welke inspanningen onderneemt u nu om bedrijven op de hoogte te stellen van hun zorgplichten ten aanzien van digitale veiligheid?

Antwoord 2
Op 5 april jl. heeft de Cyber Security Raad de handreiking *Ieder bedrijf heeft digitale zorgplichten* gepubliceerd. Deze handreiking bevat een overzicht van generieke zorgplichten die bedrijven hebben op het gebied van cybersecurity. Deze handreiking geeft mij aanleiding om, in aanvulling op eerdere voorlichting over veilig internetten, bedrijven nog eens via diverse kanalen expliciet op de hoogte te stellen van deze zorgplichten. Hierover zal actief worden gecommuniceerd, onder andere via brancheorganisaties, het ondernemersplein en veiliginternetten.nl.

Vraag 3
Welke middelen heeft u om deze zorgplichten te handhaven en in welke mate maakt u hiervan gebruik?

[1] https://www.cybersecurityraad.nl/010_Actueel/Advies_zorgplichten_bedrijven.aspx

ah-tk-20162017-1927
ISSN 0921 - 7398
's-Gravenhage 2017

Antwoord 3
De Cyber Security Raad maakt in haar handreiking een onderscheid tussen zorgplichten op het gebied van de veilige verwerking van persoonsgegevens, zorgplichten betreffende het gebruik van ICT en zorgplichten in verband met producten of diensten met een ICT toepassing. Indien een bedrijf persoonsgegevens verwerkt, heeft het zorgplichten op grond van de Wet bescherming persoonsgegevens. Op de naleving van deze plichten wordt krachtens dezelfde wet toezicht gehouden door de Autoriteit Persoonsgegevens.
De krachtens het Burgerlijk Wetboek (BW) bestaande zorgplichten op het gebied van het gebruik van ICT en zorgplichten in verband met producten of diensten met een ICT toepassing kunnen door (private) partijen via de rechter worden afgedwongen. De Autoriteit Consument en Markt ziet toe op de naleving van de wetten en regels op het gebied van consumentenrecht. Overigens bestaan er ook sectorspecifieke zorgplichten. Bijvoorbeeld wordt nu gewerkt aan de totstandbrenging van de implementatiewetgeving van de Netwerk- en informatiebeveiligingsrichtlijn. Daarin worden voor aanbieders van essentiële diensten en digitale dienstverleners zorgplichten betreffende de continuïteit van hun dienstverlening alsook handhaving van de naleving daarvan geregeld. Hierover wordt de Kamer op reguliere wijze door de Staatssecretaris van Veiligheid en Justitie geïnformeerd.

Vraag 4
Welke middelen heeft u om bedrijven op hun zorgplicht te wijzen en welke middelen gebruikt u om bedrijven hierbij te ondersteunen?

Antwoord 4
Hiervoor wordt verwezen naar het antwoord op vraag 2.

Vraag 5
Hoe heeft u opvolging gegeven aan het in oktober 2016 verschenen advies Verhagen van de CSR?[2] Is hierbij ruimte gecreëerd voor sturing vanuit de overheid?

Antwoord 5
Tijdens de behandeling van de begroting van het Ministerie van Veiligheid en Justitie is toegezegd opvolging te gegeven aan het advies van Verhagen.[3] Middels het organiseren van een aantal ronde tafels wordt het gesprek aangegaan met vertegenwoordigers van het bedrijfsleven en andere relevante maatschappelijke actoren, zoals aanbevolen door Verhagen. Deze gesprekken dienen om publiek-private samenwerking op het gebied van cybersecurity te bevorderen, waarbij sturing vanuit de overheid een aandachtspunt is. De uitkomsten van de gesprekken worden betrokken bij de doorontwikkeling van de cybersecurity strategie.

Vraag 6
Hoeveel bedrijven negeren bewust hun verantwoordelijkheden voor wat betreft cybersecurity? Hoeveel van deze bedrijven wentelen de aansprakelijkheid via ontsnappingsclausules af? Hoe handhaaft u op dergelijke, volgens de CSR, illegale ontsnappingsclausules?

Antwoord 6
Er bestaat geen inzicht in het aantal bedrijven dat hun verantwoordelijkheid voor wat betreft cybersecurity bewust negeert of ontsnappingsclausules hanteert. In het antwoord op vraag 3 is ingegaan op de handhaving van zorgplichten.

Vraag 7
Welke mogelijkheden hebben consumenten en ondernemers om verwijtbare schade te verhalen op leveranciers? In welke mate wordt hiervan gebruik gemaakt en tot welke schadevergoedingen leidt dit?

---

[2] https://www.cybersecurityraad.nl/010_Actueel/20161006_Cybersecurity-advies_Verhagen.aspx
[3] Handelingen II 2016/2017, nr. 30, item 12, blz 11.

Antwoord 7
Een leverancier die een product levert dat niet voldoet aan de overeenkomst, is hiervoor jegens de koper aansprakelijk. Consumenten en ondernemers kunnen in dit geval op grond van het Burgerlijk Wetboek aanspraak maken op herstel, vervanging of schadevergoeding. Komen partijen hier onderling niet uit, dan kunnen ze zich zo nodig tot de rechter wenden. Er bestaat geen inzicht in welke mate hiervan gebruik wordt gemaakt en tot welke schadevergoedingen dit leidt.

Vraag 8
Verwacht u dat zelfregulering afdoende is om ervoor te zorgen dat bedrijven hun zorgplichten serieus neemt? Zo nee of indien dit niet voldoende blijkt te zijn, bent u bereid aanvullende wettelijke maatregelen te nemen om de risico's voor burgers en bedrijven in te perken?

Antwoord 8
Uit onderzoek komt naar voren dat het stimuleren van zorgplichten effectiever is dan strikte handhaving.[4] Met het actief onder de aandacht brengen van de door de Cyber Security Raad gepubliceerde handreiking *Ieder bedrijf heeft digitale zorgplichten* wordt afnemers en leveranciers inzicht gegeven in de bestaande generieke zorgplichten en hoe zij hier in de dagelijkse praktijk invulling aan kunnen geven. Transparantie hierover is een belangrijke eerste stap om zelfregulering te stimuleren. Zoals in het antwoord op vraag 3 aangegeven, gaat het niet alleen om zelfregulering maar bestaan er ook wettelijke zorgplichten.

Vraag 9
Hoe groot is de bekendheid van bedrijven met de meldplicht datalekken? Hoe vindt toezicht op en handhaving van naleving van deze meldplicht plaats? Is de Autoriteit Persoonsgegevens in staat om meldingen van datalekken snel en zorgvuldig te verwerken en te monitoren?

Antwoord 9
De meldplicht datalekken is per 1 januari 2016 in werking getreden. Deze meldplicht houdt in dat organisaties en bedrijven binnen 72 uur een melding moeten doen bij de Autoriteit Persoonsgegevens (AP) zodra er sprake is van een inbreuk op de beveiliging met ernstige nadelige gevolgen (of de aanzienlijke kans daarop) voor de bescherming van persoonsgegevens. De AP heeft daar een meldloket voor ingericht. Ook moet de betrokkene van een inbreuk in kennis worden gesteld, indien deze inbreuk waarschijnlijk ongunstige gevolgen heeft voor diens persoonlijke levenssfeer.
Om de meldplicht datalekken breed onder bedrijven bekend te stellen, is over de meldplicht geregeld gecommuniceerd via diverse kanalen, waaronder veiliginternetten.nl en het ondernemersplein. Tevens heeft de AP beleidsregels uitgebracht. Deze beleidsregels zijn bedoeld om organisaties te helpen bij het bepalen of er sprake is van een datalek dat zij bij de AP, en eventueel aan betrokkenen, moeten melden.
Vanaf de inwerkingtreding monitort de AP de effecten van de invoering van de meldplicht datalekken. Daarbij wordt bezien in hoeverre de meldplicht extra capaciteitsinzet van de AP zal vergen. De uitkomsten van de monitoring tot nu toe laten zien dat de met de meldplicht datalekken gemoeide werklast binnen het huidige budget van de AP kan worden opgevangen. Overigens voorziet de Algemene verordening gegevensbescherming (AVG), die in mei 2018 werking zal krijgen en in de plaats van de Wet bescherming persoonsgegevens zal treden, ook in een meldplicht bij datalekken. De AP heeft adviesbureau AEF de opdracht gegeven de gevolgen van de implementatie van de AVG, waaronder de daarin opgenomen meldplicht datalekken, in kaart te brengen.

[4] *Duties of care and diligence against cybercrime*, prof. T.F.E. Tjong Tjin Tai e.a. (2015).