Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

Aanhangsel van de Handelingen

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

2427

Vragen van de leden **Snels** en **Van der Lee** (beiden GroenLinks) aan de Ministers van Financiën en van Economische Zaken en Klimaat over *het bericht «IT-controleurs: te weinig investeringen in cyberbeveiliging»* (ingezonden 25 april 2018).

Antwoord van Staatssecretaris **Keijzer** (Economische Zaken en Klimaat), mede namens de Minister van Financiën (ontvangen 14 juni 2018).

Vraag 1
Heeft u kennisgenomen van het artikel «IT-controleurs: te weinig investeringen in cyberbeveiliging», waaruit blijkt dat in accountantsverklaringen nog te weinig aandacht wordt gegeven aan cyberbeveiliging en ICT?[1] Zo ja, wat is uw oordeel over dit artikel?

Antwoord 1
Ja, ik heb kennisgenomen van het artikel. Ik deel de mening van de opsteller van het artikel dat het belangrijk is dat bedrijven meer aandacht besteden aan cybersecurity. Digitale veiligheid is een topprioriteit voor dit kabinet. Die prioriteit wordt in zeven stevige ambities uiteengezet in de Nederlandse Cybersecurity Agenda (NCSA) die 20 april jl. naar de Tweede Kamer is gestuurd (Kamerstuk 26 643, nr. 536). Daarin benadrukt dit kabinet het belang van investeringen in en intensivering van cybersecurity, zowel door de overheid als door het bedrijfsleven.
Ik zie dat cybersecurity steeds hoger op de agenda staat van verschillende private en publieke organisaties en dat bedrijven in toenemende mate investeren in het versterken van hun digitale weerbaarheid. Het wisselt echter in welke mate aandacht aan cybersecurity wordt besteed. Voor een veilig klimaat in het digitale domein mag en moet van bedrijven verwacht worden dat zij hun verantwoordelijkheid nemen en hun bijdrage leveren om Nederland samen digitaal veilig te maken en te houden. Het is dan ook belangrijk dat publieke en private partijen blijvend voldoende aandacht besteden aan cybersecurity. In dit kader kunnen audits een bijdrage leveren aan het cybersecure maken van publieke organisaties en ondernemingen. De Nederlandse Beroepsorganisatie van Accountants (NBA) heeft over dit

[1] https://fd.nl/ondernemen/1251117/it-controleurs-te-weinig-investeringen-in-cyberbeveiliging

ah-tk-20172018-2427
ISSN 0921 - 7398
's-Gravenhage 2018

onderwerp een publieke management letter gepubliceerd met concrete adviezen over hoe organisaties cybersecurity op kunnen pakken.[2]

Vraag 2
Klopt het dat in accountantsverklaringen expliciet aandacht gegeven moet worden aan de belangrijkste onderwerpen bij een bedrijf, die door het bedrijf zelf worden voorgesteld en worden gecontroleerd door de accountant? Zo nee, waarom niet? Zo ja, deelt u de mening dat cyberbeveiliging en ICT in het huidige technische tijdperk vrijwel altijd tot de belangrijkste onderwerpen bij een bedrijf horen?

Antwoord 2
Ik deel de mening dat cybersecurity een belangrijk onderwerp is voor publieke en private organisaties en voor ondernemingen steeds belangrijker wordt, gezien de verdergaande digitalisering van de maatschappij. Dit is bijvoorbeeld terug te zien in de Nederlandse corporate governance code uit 2016, waarin is opgenomen dat de raad van commissarissen van beursvennootschappen toezicht dient te houden op het bestuur ten aanzien van de toepassing van informatie- en communicatietechnologie door de vennootschap, waaronder risico's op het gebied van *cybersecurity*. Middelgrote en grote ondernemingen dienen in het bestuursverslag een beschrijving te geven van de voornaamste risico's, waarmee de rechtspersoon wordt geconfronteerd.[3] In deze tijd zullen ICT-gerelateerde risico's daar regelmatig deel van uitmaken. De accountant gaat vervolgens na of er in het bestuursverslag materiële onjuistheden zijn gebleken, waarbij hij zich mede baseert op de kennis die hij bij het onderzoek van de jaarrekening over de onderneming heeft gekregen en neemt dit oordeel op in de accountantsverklaring. De accountant moet verder in het verslag dat hij van zijn onderzoek uitbrengt aan bestuur en commissarissen (ook wel «management letter» genoemd) ten minste melden wat hij bij zijn onderzoek heeft opgemerkt over de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking. Voor wat betreft de wettelijke controle van organisaties van openbaar belang (beursvennootschappen, banken en verzekeraars) geldt daarnaast op grond van Europese wetgeving[4] dat de accountant in zijn controleverklaring een beschrijving dient te geven van de kernpunten van de controle (de als meest significant ingeschatte risico's op een afwijking van materieel belang). Ook daaronder kunnen risico's op het gebied van cybersecurity vallen.[5]

Vraag 3
Klopt het dat er in Nederland nog geen regels zijn voor accountants om te controleren of (beursgenoteerde) bedrijven maatregelen treffen op het gebied van cyberbeveiliging? Zo nee, waarom niet? Zo ja, bent u van plan om dergelijke regels in te voeren?

Antwoord 3
Zoals ook in het antwoord op vraag 2 is aangegeven, bestaat er regelgeving op het gebied van financiële verslaggeving op basis waarvan aandacht moet worden besteed aan belangrijke risico's voor de rechtspersoon. In het kader van de controle van de jaarrekening beoordeelt een accountant de risico's voor de financiële verslaggeving en de continuïteit. Daaronder kunnen ook cybercrime en cybersecurity vallen. Naast de in antwoord 2 vermelde regelgeving dient zowel een onderneming als de accountant bijvoorbeeld melding te maken van zaken die de continuïteit van de onderneming in gevaar kunnen brengen (artikelen 2:384 lid 3 en 2:393 lid 5 onder h van het Burgerlijk Wetboek).
Daarnaast worden op dit moment andere beleidsinstrumenten ingezet om bedrijven bewust te maken van cybersecurity risico's en om ze te helpen deze risico's te adresseren. Ik wil organisaties verder vooralsnog de ruimte geven

---

[2] https://www.nba.nl/globalassets/projecten/kennis-delen-pmls/cybersecurity/pml-cybersecurity.pdf

[3] Artikel 2:391, eerste lid, Burgerlijk Wetboek.

[4] Artikel 10 en 11 van de Verordening (EU) nr. 537/2014 van het Europees parlement en de Raad van 16 april 2014 betreffende specifieke eisen voor de wettelijke controles van financiële overzichten van organisaties van openbaar belang (PbEU 2014, L 158).

[5] Artikel 2:393, vierde lid, Burgerlijk Wetboek.

om zelf de juiste instrumenten te kiezen om hun bedrijf cybersecure te maken. Bij veel bedrijven zie je nu al dat audits worden uitgevoerd om te kijken hoe goed bedrijven beveiligd zijn. Dit zijn uitvoerige audits waar gebruik wordt gemaakt van praktische instrumenten. Ook worden andere vrijwillige middelen als *Coordinated Vulnerability Disclosure* en *penetration testing* ingezet door bedrijven om de weerbaarheid van IT-systemen te testen.

Vraag 4
Deelt u de mening dat het belangrijk is om niet achter te lopen op de realiteit wat betreft regelgeving? Zo nee, waarom niet? Zo ja, bent u bereid om te onderzoeken of regelgeving voor toezichthouders wat betreft controle op niet alleen de aanwezigheid van maatregelen maar ook op de effectiviteit van maatregelen op het gebied van cyberbeveiliging ingevoerd zou kunnen worden?

Antwoord 4
Het is belangrijk dat de overheid duidelijke kaders biedt, die aansluiten bij recente ontwikkelingen. Daarvoor is er doorlopend aandacht voor de nadere ontwikkeling en de evaluatie van regelgeving, ook op het gebied van cybersecurity. Op dit moment wordt er nieuwe cybersecurity regelgeving geïmplementeerd als gevolg van de Netwerk- en Informatiebeveiligingsrichtlijn (NIB). Het doel van deze richtlijn is om eenheid en samenhang te brengen in Europees beleid, door de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen. Het niveau van netwerk- en informatiebeveiliging verschilt momenteel per lidstaat. Dit leidt tot een sterk wisselend niveau van paraatheid bij incidenten en een ongelijk niveau van bescherming van consumenten en bedrijven. Mede door deze fragmentatie wordt er geen informatie over dreigingen en incidenten uitgewisseld tussen de lidstaten. De NIB-richtlijn verplicht lidstaten dan ook hun paraatheid te verbeteren en beter met elkaar samen te werken. Daarnaast worden partijen die essentiële diensten aanbieden en digitale dienstverleners verplicht om passende en evenredige technische en organisatorische maatregelen te nemen om hun ICT adequaat te beveiligen tegen inbreuken van buitenaf en beveiligingsrisico's te beheersen. Verder moeten zij passende maatregelen nemen om incidenten te voorkomen en, als zich toch incidenten voordoen, de gevolgen daarvan zo veel mogelijk beperken. Ook moeten zij ernstige incidenten met aanzienlijke gevolgen melden bij de nationale bevoegde autoriteit of het CSIRT (Computer Security Incident Response Team). Het is aan de aangewezen toezichthouders om per sector te bepalen op welke wijze zij het toezicht zullen vormgeven. Toezichthouders kunnen daarbij audits voorschrijven.