Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

35 570 XVI Vaststelling van de begrotingsstaten van het Ministerie van Volksgezondheid, Welzijn en Sport (XVI) voor het jaar 2021

Nr. 190 **BRIEF VAN DE ALGEMENE REKENKAMER**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 mei 2021

Op 2 december 2020 werden we door de voorzitter van de Tweede Kamer verzocht (Kamerstuk 35 570 XVI, nr. 37) een nadere analyse uit te voeren over de informatiebeveiliging bij het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) naar aanleiding van de in uw Kamer aangenomen motie van het lid Van den Berg (Kamerstuk 35 470 XVI, nr. 13). Wij hebben op 12 januari 2021 uw Kamer geïnformeerd dat wij aan dit verzoek kunnen voldoen (Kamerstuk 35 570 XVI, nr. 182).

Separaat aan de uitkomsten van ons onderzoek over 2020 bij het Ministerie van Volksgezondheid, Welzijn en Sport, begrotingshoofdstuk XVI van de Rijksbegroting (Kamerstuk 35 830 XVI, nr. 2) bieden we u daarom middels deze brief de antwoorden op de door de Tweede Kamer gestelde onderzoeksvragen.

Centraal staat de vraag hoe de ITorganisatie van het Ministerie van VWS met betrekking tot informatiebeveiliging is vormgegeven qua systemen, processen en procedures en hoe deze in de praktijk functioneert. Wij beantwoorden dat aan de hand van vijf deelvragen die de Tweede Kamer in haar verzoek noemt.

1. Hoe zijn de ICTorganisatie, de ICTsystemen, de governance en de processen en procedures met betrekking tot het voorkomen van incidenten en datalekken bij VWS vormgegeven en hoe wordt daar in de praktijk invulling aan gegeven?

Naast het kerndepartement kent het Ministerie van VWS verschillende decentrale onder delen en uitvoeringsorganisaties, zoals de Inspectie Gezondheidszorg en Jeugd, het RIVM en het CAK. Deze decentrale concernonderdelen hebben eigen ITsystemen en organisaties. Relevant te weten is dat de grootste informatiebeveiligingsrisico's bij de decentrale concernonderdelen te vinden zijn: het kerndepartement heeft namelijk

kst-35570-XVI-190
ISSN 0921 - 7371
's-Gravenhage 2021

geen bedrijfskritische ITsystemen. Voor bedrijfskritische systemen gelden op basis van de Baseline Informatiebeveiliging Overheid (BIO) striktere eisen omdat de impact van uitval of misbruik door onbevoegden groot is op de continuïteit van de bedrijfsvoering.
De verantwoordelijkheid voor informatiebeveiliging ligt bij de Minister van VWS. Hij mandateert de taken die horen bij deze verantwoordelijkheid aan de secretarisgeneraal (SG). De secretarisgeneraal is bijvoorbeeld verplicht om ieder jaar een *incontrolverklaring* aan te leveren bij de *chief information officer*-Rijk van het Ministerie van Binnenlandse Zaken van Koninkrijksrelaties. De overige taken op het terrein van informatiebeveiliging mandateert de secretarisgeneraal naar de plaatsvervangend secretarisgeneraal (pSG). Voor het vervullen van deze taken krijgt de psg ondersteuning van de *chief information officer* (cio) van VWS en de *chief information security officer* (ciso). De beveiligings ambtenaar (bva) houdt toezicht op het concernbrede informatiebeveiligingsbeleid en heeft een signalerende en adviserende rol.
Lijnmanagers dienen de informatiebeveiliging van de onder hen vallende informatie in processen, ketens en systemen goed te organiseren.
Om de gehele VWSorganisatie centraal te monitoren en alle onderdelen te kunnen adviseren is er een concernciso. In onze verantwoordingsonderzoeken informatie beveiliging hebben wij de afgelopen jaren aanbevolen om deze wijze van sturing, organisatie en monitoring op informatiebeveiligingsrisico's te verbeteren. In de praktijk zien we hier verbetering bij het Ministerie van VWS. Wij constateren dat er een goed lopend proces rond de *incontrolverklaring* is en dat er werkbezoeken en gesprekken over informatiebeveiliging bij de verschillende onderdelen plaatsvinden. Het ontbreekt echter nog aan volledig centraal inzicht in de informatiebeveiligingsrisico's bij de SG.

Ten aanzien van incidenten heeft de ciso van het VWSconcern centraal overzicht van de belangrijkste informatiebeveiligingsincidenten en gemelde datalekken. Over de incidenten en datalekken wordt gesproken in een informatiebeveiligingsexpertoverleg (het IBX).
Zo kan de Minister van VWS gerichter sturen, bijvoorbeeld als blijkt dat er relatief veel datalekken gemeld worden bij een bepaald organisatieonderdeel.
In een draaiboek is vastgelegd wat de taken zijn indien er sprake is van een datalek, zoals de ciso, de functionaris gegevensbescherming (fg) en de bva. Het draaiboek beschrijft wanneer er met welke doelgroep gecommuniceerd moet worden. Zo staat beschreven dat de pSG wordt geïnformeerd bij het optreden van een (zeer) ernstig incident en dat de Autoriteit Persoonsgegevens (AP) over een datalek wordt geïnformeerd op aangeven van de Functionaris Gegevensbescherming. Uit het incidentregister blijkt dat bij de verschillende datalekken de AP inderdaad is geïnformeerd.

2. Wat is het niveau van informatiebeveiliging, ook in vergelijking tot andere ministeries?

Voor een vergelijking van de oordelen van informatiebeveiliging tussen ministeries verwijzen wij naar ons rapport bij het Jaarverslag 2020 van Binnenlandse Zaken en Koninkrijksrelaties (BZK) (Kamerstuk 35 830 VII, nr. 2) en naar de Staat van de Rijksverantwoording 2020 (Kamerstuk 35 830, nr. 3). Hierin staan overzichten van de door ons onderzochte ministeries en Hoge Colleges van Staat, waarin ook de ontwikkeling door de jaren heen is te zien. Dit jaar beoordelen we de informatie beveiliging bij 5 van de 12 onderzochte ministeries als onvolkomenheid, waaronder bij het Ministerie van VWS. In de manier waarop de Minister van VWS het incidentmanagement het afgelopen jaar inrichtte, onderscheidt de organisatie zich positief van de andere onderzochte ministeries en Hoge

Colleges van Staat. Op andere onderdelen van informatie beveiligingsaspecten constateren we dat de risico's op de informatiebeveiliging nog onvoldoende beheerst worden.

3. Wat is de cultuur binnen organisaties op het VWSterrein wat betreft het melden van en omgaan met incidenten en datalekken? Hoe zijn op centraal niveau binnen VWS het zicht en de regie op incidenten en datalekken?

In onze reactie op het verzoek van 2 december voor dit onderzoek gaven wij aan geen cultuuraudit te doen bij (de medewerkers van) het Ministerie van VWS. Toch kunnen we op basis van ons onderzoek wel aangeven dat er een positieve ontwikkeling is binnen het Ministerie van VWS. Verantwoordelijken bij het Ministerie van VWS kunnen hun rol beter invullen doordat de verantwoordelijkheden ten aanzien van de informatiebeveiliging inmiddels helder zijn beschreven (zie vraag 1). Ook blijkt dat sleutelfunctionarissen meer in gesprek willen met de medewerkers over informatiebeveiligingsrisico's, vanuit het besef dat menselijk gedrag hierin essentieel is. Activiteiten om het bewustzijn over risico's te vergoten, zoals *phishing*-simulaties, dragen bij aan een cultuur waarin informatie beveiliging een belangrijk onderwerp is.

4. Welke tekortkomingen heeft de Algemene Rekenkamer in haar verantwoordingsonderzoeken op het punt van informatiebeveiliging op VWSterrein gesignaleerd? Tot welke aanbevelingen heeft dit geleid en (hoe) is daar opvolging aan gegeven?

Ieder jaar rapporteert de Algemene Rekenkamer over de opvolging van de gedane aanbevelingen van het voorgaande jaar. Daarom verwijzen we voor het antwoord op deze vraag naar de tussen 2017 en 2021 gepubliceerde rapporten bij het jaarverslag van het Ministerie van VWS. De opvolging van de aanbevelingen uit het verantwoordingsonderzoek 2019 is hier eerder al aan bod gekomen.

5. Ziet de Algemene Rekenkamer, ook gezien datalekken die in 2020 zijn opgetreden, nog mogelijkheden voor verbetering van de informatiebeveiliging op VWS-terrein?

We constateren over het jaar 2020 op het gebied van incidentmanagement, waaronder incidenten in de vorm van datalekken, een grote verbetering op het concernniveau ten opzichte van vorig jaar. De aanbeveling die wij vorig jaar hebben gedaan om het incidentmanagement te verbeteren is door het Ministerie van VWS opgevolgd.

Algemene Rekenkamer

drs. A.P. (Arno) Visser,
president

drs. C. (Cornelis) van der Werf,
secretaris