Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 775 VII Vaststelling van de begrotingsstaten van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (VII) voor het jaar 2018

Nr. 47

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 22 december 2017

In het Verantwoordingsdebat over het jaar 2016 (Handelingen II 2016/17, nr. 81, items 3 en 6) is een aantal toezeggingen gedaan rond het thema informatiebeveiliging bij de overheid. Naar aanleiding van dit debat heeft uw Kamer op 6 juni 2017 de motie Aukje de Vries (VVD) aangenomen (Kamerstuk 34 725, nr. 5; Handelingen II 2016/17, nr. 83, item 10).

Deze toezeggingen hebben geleid tot een brief over de stand van zaken bij drie departementen waarvan de Algemene Rekenkamer (AR) een onvolkomenheid voor informatiebeveiliging had geconstateerd en waarvan de AR had aangegeven te twijfelen of deze ministeries deze onvolkomenheid ernstig genoeg namen. Deze brief heeft uw Kamer – conform toezegging – voor het zomerreces ontvangen (Kamerstuk 34 550 VII, nr. 50)

Met deze brief informeer ik uw Kamer, mede namens de Staatssecretaris van BZK, over het rijksbrede beleid ten aanzien van informatiebeveiliging en de toezegging om te worden geïnformeerd over uitvoering van de motie van het lid De Vries. De motie:

1. Verzoekt de regering, zich maximaal in te spannen om voor eind 2017 de onvolkomenheden op het gebied van informatiebeveiliging weg te werken;
2. Verzoekt de regering tevens, te verkennen wat er nodig is voor een goede toekomstbestendige informatiebeveiliging bij de overheden en de daaraan gelieerde instellingen, op het gebied van
   (1) organisatie,
   (2) rol en mandaat van de coördinerend Minister,
   (3) personeel,
   (4) maatregelen,
   (5) maar ook aanpassing van het afsprakenkader op basis van ontwikkelingen en bedreigingen,

kst-34775-VII-47
ISSN 0921 - 7371
's-Gravenhage 2017

en de Tweede Kamer hierover voor eind 2017 te informeren.

Om zowel aan de toezeggingen als de motie te voldoen, heb ik deze brief gestructureerd op basis van de verschillende onderwerpen van de motie (organisatie, rol en mandaat van de coördinerend Minister, personeel, maatregelen, aanpassing van het afsprakenkader op basis van ontwikkelingen en bedreigingen). Per onderwerp ga ik in op zowel het beleid als initiatieven die vanaf de afgelopen zomer reeds in gang zijn gezet of waarvoor een dergelijk voornemen bestaat. Een aantal van onderstaande nieuwe initiatieven zult u eveneens terugvinden in de herziene strategische i-agenda.

Onvolkomenheden

De door de AR geconstateerde onvolkomenheden moeten de ministeries zelf oplossen. Maar ik vind, net als uw Kamer, coördinatie op dit punt belangrijk. De CIO Rijk agendeert daarom dit jaar de geconstateerde onvolkomenheden in de CIO gesprekken die hij halfjaarlijks met de CIO's van de ministeries voert. Ter voorbereiding op de lopende ronde van deze gesprekken is nu ook formeel gesproken met de Chief Information Security Officers (CISO's) van de ministeries. Het beeld dat uit deze gesprekken naar voren komt, is dat alle ministeries serieus werk maken van het oplossen van geconstateerde onvolkomenheden. Daartoe in gang gezette initiatieven daartoe hebben soms meer tijd nodig om effect te sorteren; de AR zal begin 2018 hierover oordelen. Enkele collega-ministers zullen voorts uw Kamer zelf informeren over hun initiatieven.

Toekomstbestendige informatiebeveiliging

In absolute zin bestaat een 100% toekomstbestendige informatiebeveiliging niet. De dreigingen en kwetsbaarheden van 10 jaar geleden zijn anders dan nu. De dreiging van statelijke actoren is bijvoorbeeld nu veel meer manifest dan toen. Het Cyber Security Beeld Nederland (CSBN) onderstreept de voortdurende verandering van dreigingen en kwetsbaarheden. Informatiebeveiliging is daarom een cyclisch proces, dat telkens moet inhaken op nieuwe ontwikkelingen. Daarom kan deze brief niet uitputtend zijn: ook in 2018 kunnen er nieuwe initiatieven nodig zijn die nu niet kunnen worden voorzien.

Omdat informatiebeveiliging een cyclisch proces is, is dit het uitgangspunt van het rijksbrede informatiebeveiligingsbeleid binnen de rijksdienst. Dit uitgangspunt komt terug in verschillende rijksbreed geldende voorschriften.

Afsprakenkader & Maatregelen

Het huidige fundament van de interdepartementale regelgeving wordt gevormd door het Voorschrift Informatiebeveiliging Rijksdienst 2007[1] (VIR). De grondgedachte van dit voorschrift is dat informatiebeveiliging op meerdere manieren tot stand kan komen, mits dit op basis van bewuste keuzes gebeurt. Informatiebeveiliging vormt een integraal onderdeel van de bedrijfsvoering en is daarmee een managementverantwoordelijkheid, met als politiek eindverantwoordelijke de betreffende vakminister. Voor elk informatiesysteem[2] wordt vooraf door het betreffende lijnmanagement op basis van een risicoafweging bepaald welke specifieke

[1] Jaartallen bij de afsprakenkaders verwijzen naar het jaar van herziening en niet naar het jaar van ontstaan.

[2] Een informatiesysteem is in de context van VIR een samenhangende (logische) groepering van gegevensverwerkende processen en gegevensverzamelingen.

beveiligingsmaatregelen de organisatie treft. Een afweging voor een systeem met open data zal anders zijn dan een afweging voor een systeem met gevoelige persoonsgegevens. Het cyclisch karakter van informatiebeveiliging en de eigen verantwoordelijkheid zijn uitgangspunten van het VIR.

Voor informatie waarvoor een verhoogde mate van vertrouwelijkheid (waaronder staatsgeheime informatie) is vereist, geldt een aanvullende regeling: het Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2013 (VIR-BI). Het VIR-BI bevat regels, gericht op de bescherming van de vertrouwelijkheid. Het is een aanvulling op het VIR waarin beveiliging van informatie in het algemeen binnen de rijksdienst is geregeld.

Voortvloeiend uit het VIR is de Baseline Informatiebeveiliging Rijksdienst (BIR). De BIR is allereerst een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de Rijksdienst. Daarnaast concretiseert de BIR een aantal normen tot verplichtingen:
– vanwege wet- en regelgeving, voor zover het de beveiliging van informatie(systemen) betreft;
– vanwege de gemeenschappelijk veiligheid van informatieketens;
– omdat deze altijd fundamenteel zijn voor een veilige informatievoorziening.

De BIR beoogt de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de Rijksdienst te bevorderen, zodat deze bedrijfsonderdelen erop kunnen vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de Rijksdienst, in lijn met wet- en regelgeving, passend beveiligd zijn.

De Interdepartementale Commissie Bedrijfsvoering Rijks (ICBR) heeft op 28 november 2017 ingestemd met een grondig herziene en gemoderniseerde Baseline Informatiebeveiliging Rijk (BIR). In de herziene BIR staat de aanpak centraal waarbij diepgang van het risicomanagement, beveiliging, verantwoording en toezicht proportioneel zijn aan het te beschermen belang en een realistische inschatting van dreigingen. Om de hanteerbaarheid en de efficiëntie van de BIR te vergroten, kent de BIR drie basisbeveiligingsniveaus (BBN).

Het hoogste BBN is nieuw en is het gevolg van de toename van steeds geavanceerdere dreigingen van statelijke actoren en georganiseerde criminelen. Dit niveau is significant hoger dan het beschermingsniveau van de oude BIR. De maatregelen worden in 2018 aan de BIR toegevoegd en zijn gebaseerd op toepasselijke NAVO kaders.

Onderdeel van de nieuwe BIR is een set van handreikingen die behulpzaam kunnen zijn bij de toepassing van de BIR. Deze set kan en zal in 2018 verder worden aangevuld. In de telkens veranderende praktijk van informatiebeveiliging ligt dat ook voor de hand. Dat is ook de reden waarom in de BIR de mogelijkheid is ingebouwd om halfjaarlijks de BIR zelf aan te passen, mede op basis van de uitvoeringspraktijk bij de ministeries.

Versterken operationele samenwerking

In de afgelopen jaren is een duidelijke operationele samenwerking tot stand gekomen tussen ICT-dienstverleners binnen het Rijk, alsook tussen deze dienstverleners en het Nationaal Cyber Security Centrum (NCSC) op het gebied van informatiebeveiliging. Dit heeft onder andere geleid tot een beschrijving en formalisering van deze samenwerking–ook wel aangeduid met de term Joint Security Operations Centers (Joint

SOC's)–en een pilot van het Nationale Detectie Netwerk (NDN). Ik wil deze samenwerking verder uitbouwen. De Chief Technology Officers Raad (CTO-raad) neemt hierin samen met het NCSC het voortouw om effectiviteit van preventie te vergroten en snelheid bij het oplossen van veiligheidsproblemen te verhogen. Daarbij past ook de uitbouw van het Threat Intel Platform van het NCSC.

Personeel

i-bewustzijn en i-vaardigheden

Aan de basis van informatiebeveiliging moet de wil, vaardigheid en mogelijkheid staan om veilig te handelen; daarvoor is het noodzakelijk dat men zich bewust is van de digitale dreigingen, de eigen rol en mogelijke consequenties/risico's van het eigen handelen en de daarmee samenhangende (bedrijfs)risico's. Het treffen van beveiligingsmaatregelen heeft geen zin als mensen er omheen werken omdat dat makkelijker is.

Via iBewustzijnRijk heb ik reeds geïnvesteerd in het verhogen van ICT vaardigheden en bewustzijn bij ambtenaren van de rijksdienst en de medeoverheden. Voor de Rijksdienst heb ik dit punt verplicht gesteld in de nieuwe BIR.

Het merendeel van de ambtenarenpopulatie is niet opgegroeid met ICT en heeft digitale vaardigheden gaandeweg op eigen kracht verkregen. Ik vind daarom dat het vergroten van ICT-veiligheidsbewustzijn onderdeel moet zijn van het vergroten van algemene digitale vaardigheden voor personeel van de Rijksdienst. Een positief bijeffect is dat bestaande ICT beter en efficiënter wordt benut.

Dit betekent onder andere een voortzetting en uitbreiding van bestaande curricula voor beleidsmedewerkers, leidinggevenden en opdrachtgevers van projecten, waarbij onderzocht wordt of curricula verplicht gesteld kunnen worden. Voorzien wordt een aanpassing van de kernprofielen van topmanagers in de rijksdienst op kennis en begrip van digitale ontwikkelingen. Een kwartiermaker is gestart met de uitvoering van de aanbeveling van de Studiegroep Informatiesamenleving en Overheid (Kamerstuk 26 643, nr. 460) om een nieuwe ICT-opleidingsvoorziening in te richten, analoog aan de Rijksacademie voor Financiën en Bedrijfsvoering, met de werktitel RADIO (Rijksacademie voor Digitalisering en Informatisering Overheid).

ICT personeel

De Rijksdienst kan in deze tijd niet meer zonder goed ICT personeel, zowel op de ministeries, dicht bij de beleidsmakers, als in de uitvoering. Dit is ook in de kabinetsreactie van januari 2015 op het Eindrapport van de Tijdelijke commissie ICT aangegeven. Echter, de bezetting van I-functies binnen de rijksdienst is een uitdaging, zowel vanwege schaarste op de markt als vanwege de vergrijzing bij de rijksdienst.

De urgentie voor het versterken van de positie van het Rijk als ICT-werkgever is groot. De belangrijkste aanleiding hiervoor zijn de (geprognosticeerde) tekorten aan eigen ICT-personeel bij het Rijk en de afhankelijkheid van externe inhuur. Deze tekorten zijn in algemene zin het grootst voor developers en architecten, maar bestaan ook voor meer specialistische functies zoals security specialisten, data- en informatieanalisten en ethical hackers.

Uw Kamer heeft onlangs een brief ontvangen over de positie van het Rijk als ICT-werkgever.

Organisatie & Rol en mandaat BZK

Bovengenoemd beleid en initiatieven vloeien voort uit mijn verantwoordelijkheid voor de coördinatie op het gebied van de informatievoorziening in de openbare sector als geheel (artikel 5, Besluit informatievoorziening in de rijksdienst 1990). Voor de Rijksdienst heb ik de bevoegdheid om na overleg met de ministers kaders vast te stellen ter bevordering van de eenheid, de kwaliteit of de efficiëntie van de bedrijfsvoering door de ministeries (artikel 2 lid 1, Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst). Hiertoe behoren ook de kaders ten aanzien van de informatiebeveiliging bij de rijksdienst.

De coördinerende taak leidt er toe dat ik de effectiviteit van vastgestelde kaders monitor. Waar nodig vraag ik bij andere ministers aandacht voor het in acht nemen van vastgestelde kaders (ex artikel 2 lid 2, Coördinatiebesluit organisatie en bedrijfsvoering rijksdienst). Hieruit vloeit voort dat–zoals eerder genoemd–de CIO Rijk in zijn halfjaarlijkse gesprekken met de CIO's informatiebeveiliging formeel agendeert naar aanleiding van de bij de ministeries geconstateerde onvolkomenheden.

De uitvoering van de kaders bij de ministeries hoort niet bij de rol en het mandaat van de Minister van BZK. De ministers zijn immers zelf verantwoordelijk voor hun ministerie en dus ook voor de informatiebeveiliging bij hun ministerie. En alleen zij kunnen een goede afweging maken van de gewenste betrouwbaarheidseisen van hun informatiesystemen.

Toezicht

Ik heb formeel geen toezichthoudende taak, maar houd niettemin toezicht op de naleving van de rijksbreed geldende kaders. Ik laat de ministeries jaarlijks een in control verklaring (ICV) opleveren waarin zij aangeven welke zeer hoge risico's zij onderkennen. Dit vormt mede input voor de eerder genoemde formele gesprekken van CIO Rijk met de andere ministeries.

De CIO Rijk geeft ook jaarlijks opdracht aan de Auditdienst Rijk tot het verrichten van departementale informatiebeveiligingsonderzoeken en een rapportage waarin de hoofdlijnen van de resultaten van deze onderzoeken staan. Deze rapportage is mede input voor het bepalen van de effectiviteit van vastgestelde kaders.

Tot nu toe werd gekeken naar de sturing en de implementatie van de BIR, met name bij enkele kritieke informatiesystemen. Dat gaf weliswaar inzicht in het al dan niet voldoen aan losse maatregelen, maar gaf weinig inzicht gaf in de volwassenheid van informatiebeveiliging.

Daarom heb ik, samen met de Auditdienst Rijk, in het najaar van 2017 gekozen voor een nieuwe opzet van de jaarlijkse departementale informatiebeveiligingsonderzoeken. In de nieuwe opzet van de IB-onderzoeken wordt de focus nu gelegd op de beheersing van het informatiebeveiligingsproces binnen het ministerie. In het onderzoek wordt ook gekeken hoe het ministerie zelf het controlemechanisme heeft ingericht. Het beoogde resultaat is per ministerie een volwassenheidsmeting op generieke themas met aanbevelingen hoe te komen tot een hoger niveau.

Interdepartementale afstemming

Beleidskaders worden in interdepartementaal overleg vastgesteld. Dergelijk overleg staat ook ten dienste aan het monitoren van de effectiviteit van beleid. Ook wordt interdepartementaal op diverse manieren veelvuldig kennis gedeeld over informatiebeveiliging.

Onder voorzitterschap van de Directeur-Generaal Overheidsorganisatie vindt overleg plaats in de Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR). Voor onderwerpen op het gebied van informatievoorziening en ICT adviseert het beraad van de departementale CIO's, het CIO Beraad onder voorzitterschap van de CIO Rijk, aan de ICBR.

Op zijn beurt adviseert de Subcommissie Informatie Beveiliging (SIB) aan het CIO-beraad over rijksbrede onderwerpen op het gebied van informatiebeveiliging. Het gaat daarbij om bijvoorbeeld het vaststellen (en de herziening) van rijksbrede kaders, beleid en tools voor informatiebeveiliging (IB). In de SIB is een aantal departementen vertegenwoordigd, alsook het Nationaal Cyber Security Centrum (NCSC, onderdeel van het Ministerie van Justitie en Veiligheid) alsmede het Nationaal Bureau Verbindingsbeveiliging (NBV, onderdeel van de Algemene Inlichtingen en Veiligheidsdienst), het Integraal Beveiligingsberaad rijksoverheid (IBR) en het Centrum voor Informatiebeveiliging en Privacy (CIP).

Momenteel kijk ik naar de herinrichting van dit overleg om de rijksbrede informatiebeveiligingsstrategie nog beter te agenderen en de verbinding te leggen met de Nationale Cyber Security Agenda.

Informatiebeveiliging bij medeoverheden

Ook medeoverheden zijn in beginsel zelf verantwoordelijk voor de eigen informatiebeveiliging. Zo hebben gemeenten in 2013 de resolutie «informatiebeveiliging basis voor een professionele gemeente» omarmd. De afgelopen jaren wordt in het gemeentelijk domein hard gewerkt aan het verbeteren van informatiebeveiliging. Bij de informatiebeveiligingsdienst voor gemeenten (IBD) zijn inmiddels alle gemeenten aangesloten, het merendeel daarvan heeft informatie met IBD gedeeld op basis waarvan zij gericht geïnformeerd kunnen worden over actuele dreigingen. De betreffende informatie krijgt IBD vanuit het NCSC én signalen uit het gemeentelijk veld. Naast de gemeenten zelf onderhoudt ook de IBD relaties met leveranciers van gemeentelijke software. Ook dreigingsinformatie vanuit softwareleveranciers wordt via IBD met gemeenten gedeeld. Op die manier zijn gemeenten in staat snel en adequaat te reageren.

Gemeentelijke informatiebeveiliging reikt verder dan de aansluiting bij IBD. Belangrijk is om het «eigen huis op orde» te krijgen én te houden. Gemeenten hebben met de resolutie het specifieke normenkader informatiebeveiliging omarmd. Deze Baseline Informatiebeveiliging Gemeenten (BIG) is inmiddels de de facto standaard binnen het gemeentelijk domein. Gemeenten implementeren de BIG zelfstandig en worden daarbij door de IBD ondersteund met handreikingen, regiosessies en kwalitatieve helpdesk. De BIG is net als de Departementale Baseline (BIR) een afgeleide van de internationaal erkende standaard NEN/ISO 27001 en 27002.

Inmiddels hebben alle betrokken overheidslagen (te weten Rijk/ZBO's, provincies, gemeenten en waterschappen) zich gecommitteerd aan een op de Code voor Informatiebeveiliging (NEN-ISO IEC 27002:2007 nl) gebaseerde baseline per sector of overheidslaag, zoals NEN7510 (in de zorg), BIR (voor het Rijk), BIG (voor gemeenten), BIWA (voor water-

schappen), of IBI (voor provincies). De vervolgstap is het neerzetten van één baseline voor de gehele overheid, de Baseline Informatiebeveiliging Overheid (BIO). Deze wordt op basis van BIR 2017 opgesteld en zal naar verwachting volgend jaar worden opgeleverd. De andere baselines zullen hiervan afgeleid worden en zullen daardoor eenvoudiger worden. Het gevolg is administratieve lastenverlichting bij gegevensuitwisseling met en tussen overheidsorganisaties, immers er behoeft slechts aan één veiligheidsregime te worden voldaan in plaats van aan vier.

De ministerraad heeft op 15 december ingestemd met het wetsvoorstel Digitale Overheid. Het wetsvoorstel richt zich op het verbeteren van de digitale overheid door regels te geven over de toegang van burgers en bedrijven tot on-line dienstverlening bij de (semi)overheid. In het wetsvoorstel is voorts de bevoegdheid opgenomen om overheidsbrede toepassing van bepaalde open standaarden, waaronder informatiebeveiligingsstandaarden, te verplichten via algemene maatregel van bestuur.

Informatiebeveiliging is mensenwerk en vraagt bestuurlijke aandacht en awareness. De afgelopen twee jaar heeft een bestuurlijke visitatiecommissie 120 gemeenten bezocht. De commissie heeft bij de bezochte gemeenten een belangrijke impuls gegeven aan dit bestuurlijke bewustzijn. Bij de bezochte gemeenten is door de commissie stevig doorgeprikt op de bestuurlijke betrokkenheid bij het thema en heeft bemiddelend gewerkt in de communicatie tussen de gemeentelijke beveiligingsfunctionaris (CISO) en Bestuurder. Naast het belang van deze communicatie wijst de commissie ook op het risico van de voortschrijdende techniek en wijst op de noodzaak om hierop een gemeentelijk antwoord te vinden; enerzijds door het zoeken van (intergemeentelijke) samenwerking anderzijds door te wijzen op de noodzaak van aansluiting bij IBD. De visitatiecommissie dringt ook aan op de vorming van CISO netwerken én (bestuurlijke) leerkringen rond het thema informatiebeveiliging.

De IBD voert op haar beurt een verkenning uit naar de een werkwijze die meer proactief risico's signaleert. In samenwerking met VNG werkt IBD aan een toolkit voor CISO's om de communicatie tussen bestuurder en CISO verder te optimaliseren. Daarnaast wordt ingezet op een meer actieve benadering van bestuurders door onder meer het uitbrengen van een gemeentelijke maandmonitor informatiebeveiliging. Ook wordt gewerkt aan een uitbreiding van de communicatie tussen IBD en gemeenten bij actuele dreigingen specifiek gericht op de bestuurder. Tot slot wordt gewerkt aan een gemeentelijk dreigingsbeeld dat in navolging van het nationaal cybersecuritybeeld jaarlijks wordt uitgebracht.

In de eerder genoemde resolutie hebben gemeenten ook afgesproken transparant te zijn over informatiebeveiliging en daarover in het jaarverslag te rapporteren aan de gemeenteraad. Met gemeenten en departementale toezichthouders is gewerkt aan een gestroomlijnde verantwoordingssystematiek die kan voldoen aan deze informatieverstrekking aan de gemeenteraad. De systematiek is gebaseerd op de BIG. De informatiebehoefte van departementale toezichthouders voor specifieke domeinen is aangepast op deze verantwoordingssystematiek; met de betreffende toezichthouders is overeenstemming over deze nieuwe wijze van verantwoording. Alle gemeenten werken in 2017 volgens deze systematiek waarin zes stelsels zijn samengebracht. De verantwoordingscyclus sluit per 1 mei 2018. Deze wijze van verantwoorden geeft niet alleen invulling aan de verantwoordelijkheid van college voor informatiebeveiliging, maar geeft ook de gemeenteraad een instrument in handen om daarop toezicht te houden. In een verder weg

liggend perspectief geeft de systematiek kansen om gemeentelijke leercycli informatiebeveiliging invulling te geven.

Informatiebeveiliging is nooit af en vereist dat telkens met gezond verstand in regelgeving, beveiligingseisen, maatregelen en toezicht worden aangepast. In die context constateer ik dat alle partijen bij de overheid betrokken zijn om de informatie(systemen) bij de overheid te beveiligen en veilig te houden.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren