Ministerie van Buitenlandse Zaken

Aan de Voorzitter van de
Eerste Kamer der Staten-Generaal
Kazernestraat 52
Den Haag

Ministerie van Buitenlandse Zaken
Rijnstraat 8
2515 XP Den Haag
Postbus 20061
Nederland

www.minbuza.nl

Onze referentie
BZ2520436

Bijlage(n)
1

Datum 1 oktober 2025
Betreft Toezending advies AcICT Transitie ICT-dienstverlening

Geachte voorzitter,

Met deze brief informeren wij uw Kamer over het advies van het Adviescollege ICT-toetsing (hierna: AcICT) over het programma Transitie ICT-dienstverlening. Dit advies hebben wij op 4 februari 2025 van AcICT ontvangen. Hierbij ontvangt u het rapport met de conclusie en de aanbevelingen van AcICT. Bij dit advies hoort nog een vertrouwelijke bijlage. Het integrale advies, dus inclusief die bijlage, is op 3 maart jl. al vertrouwelijk met uw Kamer gedeeld. In deze brief gaan wij in op de conclusie uit het hoofdrapport en beschrijven wij op welke manier opvolging wordt gegeven aan de aanbevelingen.

Aanleiding

Op 14 februari 2011 presenteerde de toenmalige minister van Binnenlandse zaken en Koninkrijksrelaties (BZK) het uitvoeringsprogramma compacte rijksdienst (CRD)[1]. Onderdeel van dit programma was de inrichting van een rijksbrede infrastructuur voor de ondersteunende bedrijfsvoering, inclusief de ICT-dienstverlening. In het programmaplan CRD stond dat alle ministeries (met uitzondering van het ministerie van Defensie) de uitvoering van hun ICT-dienstverlening vanaf 2013 zo veel mogelijk zouden bundelen. Zo werd op 1 januari 2012 het nieuwe Shared Services Center ICT (SSC-ICT) in het leven geroepen, een onderdeel van het ministerie van BZK, met als belangrijkste startkapitaal de ICT-dienstverleningsorganisatie van het toenmalige ministerie van Infrastructuur en Milieu.

Op 1 januari 2015 stapte het ministerie van Buitenlandse Zaken (BZ) in als opdrachtgever voor SSC-ICT, en nam SSC-ICT een groot deel van de ICT-voorzieningen en -diensten over van BZ. Daarbij ging ook een deel van de Directie Informatie Diensten van BZ over naar SSC-ICT, en werd ervan uitgegaan dat SSC-ICT het beveiligings- en beschikbaarheidsniveau zou leveren dat voor het ministerie van BZ vereist is.

[1] Kamerstuk van 14 februari 2011, 31 490 nr. 54.

De samenwerking tussen BZ en SSC-ICT heeft van het begin af aan de nodige struikelblokken gekend. Dat is voor een belangrijk deel toe te schrijven aan de botsing van twee werelden. Aan de ene kant die van een shared services organisatie die is bedoeld om gedeelde, en tot op zekere hoogte identieke diensten te leveren aan verschillende afnemers. Daartegenover staat dat het werk en het werkterrein van BZ met zich meebrengt dat BZ specifieke behoeften heeft, en dat BZ extra bescherming nodig heeft tegen statelijke actoren met een offensief cyberprogramma dat is gericht tegen Nederlandse belangen. Verschillende incidenten hebben gemaakt dat BZ zich in de eerste helft van 2024 genoodzaakt zag om de levering van ICT-diensten te heroverwegen, met als uiterste consequentie het onderbrengen van – een deel van – de door SSC-ICT geleverde diensten bij een of meer andere aanbieders. In dat verband heeft de minister van Buitenlandse Zaken aan AcICT gevraagd om advies uit te brengen over de manier waarop dit moet worden aangepakt.

Advies programma Transitie ICT-dienstverlening

AcICT trekt op basis van hun onderzoek als belangrijkste conclusie dat zij het besluit van BZ om nu te vertrekken bij SSC-ICT te risicovol vinden, vanuit het perspectief van BZ, en met het oog op het rijksbrede belang. Bij deze conclusie zijn ter onderbouwing, kort samengevat, door AcICT de volgende bevindingen meegegeven:

A. Vertrek brengt de urgente verbetering van de informatiebeveiliging in gevaar.
B. Grote kans op herhaling problematiek dienstverlening door onvolwassen besturing BZ.
C. Vertrek belemmert noodzakelijke beveiliging tegen statelijke actoren voor BZ en rijksbreed.

AcICT adviseert op basis van deze conclusie om het vertrekbesluit op dit moment niet door te zetten en eerst de urgente verbetering van de huidige ICT-dienstverlening topprioriteit te geven. Dit advies is door AcICT uitgewerkt in de vorm van vier aanbevelingen:

1. Zorg dat SSC-ICT en BZ de urgente beveiligingsrisico’s terugdringen.
2. Zorg dat de besturing bij BZ fundamenteel verbetert.
3. Realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren.
4. Evalueer na 2 jaar gezamenlijk de opvolging van de adviezen.

Opvolging van het advies

Het advies van AcICT heeft een grote reikwijdte. Er was gevraagd om te adviseren over een programma dat is gestart door BZ, maar veel van de adviezen betreffen logischerwijs ook SSC-ICT, of de samenwerkingsrelatie tussen BZ en SSC-ICT. Als belangrijk puzzelstuk voegt AcICT daar een aanbeveling aan toe die te maken heeft met een rijksbrede verantwoordelijkheid, en die dus vooral is gericht aan BZK, in het bijzonder de directeur-generaal Digitalisering en Overheidsorganisatie (DGDOO). De drie organisatieonderdelen hebben het advies samen bestudeerd, en pakken ook samen de handschoen op die er nu ligt. Zij zien de aanbevelingen als richtinggevend voor de verdere verbetering van de rijksbrede samenwerking op het gebied van ICT-dienstverlening. Dat is concreet uitgewerkt in een programmaplan dat

materieel op 1 juli jl. in uitvoering is genomen: het programma SHIELD (Samenwerkingsprogramma Herziening Informatiebeveiliging En Levering Diensten).

Het programmaplan is opgezet met gebruikmaking van de principes van *Managing Successful Programmes* (MSP). De essentie is onder andere dat, binnen de context van de programmaportfolio, verschillende projecten of andere activiteiten (in het jargon: inspanningen) worden uitgevoerd waarvan de resultaten in samenhang leiden tot concrete baten. De inspanningen zelf vallen niet onder de verantwoordelijkheid van het programma. SHIELD initieert, coördineert en integreert, maar de inspanningen zelf vallen onder verantwoordelijkheid van de staande organisaties, in principe een van de drie samenwerkende organisatieonderdelen: BZ, SSC-ICT en DGDOO.

Voordat SHIELD werd opgezet was een groot aantal inspanningen al van start gegaan. Dat geldt bijvoorbeeld voor het merendeel van de inspanningen die vallen onder verantwoordelijkheid van SSC-ICT. In 2024 zijn daar verschillende trajecten in gang gezet voor het aanpakken van urgente beveiligingskwesties. Inmiddels werpen die hun vruchten af. Daarmee is er nu ook, vanuit het perspectief van risicobeheersing, een natuurlijk moment ontstaan voor openbaarmaking van het advies van AcICT.

BZ en BZK hebben de handen ineengeslagen om, geholpen door het AcICT-advies, hun samenwerking op het ICT-dossier te versterken. Het advies is inmiddels gebruikt als een extra impuls voor de ontwikkeling van maatregelen om onder andere de weerbaarheid tegen statelijke actoren te versterken. De resultaten daarvan komen aan de hele rijksoverheid ten goede. In het vervolg van deze brief is beschreven hoe de verschillende aanbevelingen concreet zijn opgepakt.

Opvolging aanbeveling 1: zorg dat SSC-ICT en BZ de urgente beveiligingsrisico's terugdringen

AcICT adviseert SSC-ICT en BZ om samen urgente beveiligingsrisico's terug te dringen. Daarvoor heeft AcICT concrete maatregelen voorgesteld. De twee organisaties hebben deze voorstellen meegenomen bij de versterking en versnelling van bestaande initiatieven en als basis voor nieuwe, aanvullende maatregelen.

De verschillende initiatieven voor het aanpakken van beveiligingsrisico's zijn bij SSC-ICT ondergebracht in een Integraal Security Programma (ISP), dat in het voorjaar van 2024 van start is gegaan. De activiteiten van het ISP die specifiek zijn voor BZ, zijn ondergebracht in een Agile Release Train (ART BZ). Een deel van de gesignaleerde kwetsbaarheden had te maken met een achterstand in de vernieuwing van – componenten – van de infrastructuur. Voor de vervanging en het up-to-date houden van deze componenten loopt er nu een Life Cycle Management programma (LCM). Daarbij wordt gestuurd op het minimaliseren van risico's; de grootste beveiligingsissues komen als eerste aan de beurt. Naast ISP en LCM wordt er nog een derde programma uitgevoerd: het Integraal Control Framework (ICF). Dat bundelt alle activiteiten op het gebied van compliance en procesvolwassenheid.

AcICT adviseert SSC-ICT en BZ om samen op te trekken bij het aanpakken van beveiligingskwesties. Al enige tijd hadden SSC-ICT en BZ een tactisch security-overleg. Dat is naar aanleiding van het AcICT-advies uitgebreid. In aanvulling daarop wordt momenteel een gezamenlijk team opgezet waarin specifieke deskundigheid van de beide organisaties wordt gecombineerd, om meer focus aan te brengen in de verdere versterking van de informatiebeveiliging.

Specifiek voor de dienstverlening aan BZ bestaat er binnen SSC-ICT een zogenoemd klantteam. Dit klantteam is het centrale aanspreekpunt voor projecten en zogenoemde Niet Standaard Klantvragen (NSK's). Het klantteam is inmiddels ook uitgebreid. In de afgelopen periode heeft deze manier van werken geleid tot een versnelling van – het opstarten van – projecten en het reduceren van de doorlooptijd van de afhandeling van NSK's. Het aanpakken van kwetsbaarheden en beveiligingsissues wordt nu ook aangestuurd door dit klantteam. Zo kunnen BZ en SSC-ICT sneller schakelen, en eerder tot oplossingen komen. Ook op strategisch niveau vindt er intensieve samenwerking plaats in een specifiek voor BZ ingericht Bestuurlijk Overleg (BO). De belangrijkste punten op de agenda zijn de voortgang van de programma's ISP, LCM en ICF, en de samenwerking tussen BZ en SSC-ICT. In het BO wordt de opvolging van het AcICT-advies gemonitord, zowel de maatregelen als de resultaten.

In het licht van het programma SHIELD heeft BZ een voorstel gedaan voor meetwaarden (*metrics*) en streefwaarden (*targets*) waaraan de dienstverlening van SSC-ICT aan BZ zou moeten voldoen. De uitvoeringstoets daarvoor is op dit moment in voorbereiding. Dat is de basis voor de definitieve vaststelling van de targets, en het doorvoeren van de daarvoor benodigde aanpassingen in de dienstverlening. Dit gebeurt binnen de scope van het programma SHIELD. Een van de nieuwe initiatieven binnen het kader van SHIELD is verder het valideren van de door BZ gevraagde dienstverlening in die zin dat wordt nagegaan welke dienstverlening goed past binnen de portfolio en de roadmap van een shared services center als SSC-ICT.

Opvolging aanbeveling 2: zorg dat de besturing bij BZ fundamenteel verbetert

BZ neemt niet alleen ICT-dienstverlening af van SSC-ICT, maar ook van andere leveranciers. In dat laatste geval gaat het bijvoorbeeld om connectiviteitsdiensten in het buitenland. Dit vraagt om zorgvuldige, samenhangende regievoering vanuit de opdrachtgever. In principe is het altijd aan BZ om de 'wat-vraag' concreet te beantwoorden, terwijl de leverancier de 'hoe-vraag' voor zijn rekening moet nemen. Voor SSC-ICT is de laatste vraag de kern van de dienstverlening; onder de motorkap moeten alle verschillende onderdelen, in stelling gebracht voor BZ maar ook voor andere ministeries, in samenhang effectief en efficiënt ingezet kunnen worden. Dat betreft niet zozeer de techniek, omdat er wordt gewerkt met gescheiden omgevingen, maar vooral de kennisbasis en de organisatiekant. Alleen, een complexe 'wat-vraag' is soms het eenvoudigst te formuleren in technische termen. BZ is zich goed bewust van deze valkuil. In de onderdelen van SHIELD die te maken hebben met verbetering van de sturing op de ICT-dienstverlening, waarbij BZ samen optrekt met SSC-ICT, staat het principe van strikte(re) rolscheiding hoog op de agenda. De aanbevelingen die AcICT doet voor het versterken van de besturing zijn gebruikt als evenzovele aanknopingspunten voor de desbetreffende plannen en projecten.

Al in de beginfase van het programma Transitie ICT-dienstverlening heeft BZ ingezien dat versterking van de vraagsturing noodzakelijk is om duurzaam en betrouwbaar te kunnen voorzien in de eigen ICT-behoeften. AcICT reikt daarvoor de volgende trits aan: risicomanagement – specificatie van eisen – regievoering. Dat wordt door BZ gezien als een behulpzaam denkmodel. De aanbeveling om de eisen voor de ICT-dienstverlening – inclusief informatiebeveiliging – vooral in de combinatie van BZ en SSC-ICT beter uit te werken heeft dan ook een prominente plek gekregen in het programma SHIELD. In lijn met het advies van AcICT zullen programma's van eisen categorisch gebaseerd worden op risicoanalyses. Daarvoor sluit BZ zo veel mogelijk aan op een rijksbreed programma dat in het leven is geroepen voor de versterking van het risicomanagement.

Verder is BZ aan de slag gegaan met de manier waarop het opdrachtgeverschap wordt ingevuld. Voor de opdrachtgever-opdrachtnemerrelatie met SSC-ICT doet BZ dat samen met SSC-ICT. Dat is inmiddels zo opgenomen in de jaarplannen van BZ. De belangrijkste elementen daarbij zijn: contractmanagement, portfoliomanagement en architectuur. Daarvoor wordt ook extra capaciteit ingezet. Het resultaat van deze verbeteractie is dat de dienstverlening van alle leveranciers zorgvuldig georkestreerd wordt en dat de BZ-organisatie kan beschikken over passende voorzieningen: op tijd, tegen uitlegbare kosten, en veilig, gebaseerd op risicoanalyses die rekening houden met de bijzondere kenmerken van BZ. AcICT doet ook de oproep om in de aansturing van de opdrachtnemers rolvast en voorspelbaar te zijn, en daarbij de samenhang tussen de verschillende voorzieningen scherp in het oog te houden. BZ beschouwt dat als een speerpunt, en heeft hiervoor inmiddels belangrijke stappen gezet. Richting SSC-ICT is de regievoering op informatiebeveiliging nu gecombineerd met de gebruikelijke regievoering op de afzonderlijke voorzieningen. Er is nu één centraal punt voor het stellen van vragen en het prioriteren van de afhandeling daarvan.

De aanbeveling om de uitvoering van de processen op het gebied van informatiebeveiliging te verbeteren neemt BZ ter harte. Dat gebeurt onder andere door versterking van de regie – voor het onderwerp informatiebeveiliging – op de leveranciers. Zij zullen ervoor moeten zorgen dat de ICT-diensten consequent en navolgbaar zijn afgeleid van de toepasselijke *baselines*. Het verbeteren van de afhandeling van beveiligingsincidenten, waar AcICT voor pleit, heeft BZ meegenomen als onderdeel van het project C-SOC (Centraal Security Operations Center). Dat project gaat over het moderniseren en centraliseren van de huidige SOC-voorzieningen, over alle dienstverleners heen. BZ houdt daarbij rekening met de mogelijkheid dat er op enig moment een rijksbrede, ook voor BZ passende SOC-voorziening beschikbaar komt.

Terecht vraagt AcICT aandacht voor het naleven van de regels op het gebied van accreditatie. Voor BZ is dat essentieel. Ten eerste omdat actieve bescherming tegen statelijke actoren nodig is om de weerbaarheid van de organisatie op peil te houden, maar ook omdat dit een vereiste is om de NATO/EU-accreditatie te behouden. De informatiebeveiligingseisen die hieruit voortvloeien worden daarom onverkort meegenomen als eisen die BZ als opdrachtgever stelt aan de ICT-dienstverlening.

Opvolging aanbeveling 3: realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren

De toenemende cyberdreiging die uitgaat van statelijke actoren vraagt voor de rijksoverheid om een integrale, gezamenlijke aanpak. Die conclusie is bijvoorbeeld te trekken uit het Cybersecuritybeeld 2024, waar ook AcICT naar verwijst. Samenwerking op het gebied van cybersecurity is daarnaast, breder dan binnen het Rijk, noodzakelijk in verband met de ketensamenwerking tussen partijen binnen en buiten de rijksoverheid. Dit betekent dat digitale risico's de grenzen van afzonderlijke ministeries ver overschrijden. Statelijke actoren en cybercriminelen werken steeds intensiever samen, beschikken over geavanceerde intrusietechnieken en maken gebruik van mondiale digitale infrastructuren. Deze actoren zien zogenoemde koppelvlakken en de scheidsvlakken tussen verantwoordelijkheden als dankbare aanvalspunten. We moeten de gelederen dus sluiten.

De oproep om te komen tot een rijksbrede aanpak tegen statelijke actoren wordt dus herkend en van harte onderschreven. AcICT richt zich met zijn aanbeveling in eerste instantie tot BZK, in de verwachting dat verschillende resultaten van die aanpak vervolgens BZ kunnen helpen om zijn doelstellingen te bereiken. De CIO Rijk heeft, in samenwerking met andere onderdelen van de rijksoverheid, al verschillende initiatieven gestart die aansluiten op deze aanbeveling. Bijvoorbeeld het traject Hoog-Gerubriceerde Informatie (HGI), waarover de Staatssecretaris Digitalisering de Tweede Kamer heeft geïnformeerd. Dit moet onder meer leiden tot centrale, gestandaardiseerde dienstverlening op het gebied van hoogbeveiligde voorzieningen. Daarnaast wordt er gewerkt aan de Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO), gebaseerd op de aanpak van het ministerie van Defensie. Verder is er onlangs een kader opgesteld voor het risicomanagement dat van toepassing is op departementoverstijgende ketens. Bij de uitrol daarvan zijn de adviezen van AcICT goed te gebruiken. Op 4 juli jl. heeft de ministerraad ingestemd met een actualisatie van het VIR-BI, wat een kader vormt voor de beveiliging van bijzondere informatie, zoals staatsgeheimen. Tevens is de BIO, de baseline voor de beveiliging van informatie bij de overheid, geactualiseerd, inhoudelijk afgestemd en klaar om als verplicht normenkader vastgesteld te worden. Tot slot is er het programma Versterking SOC-stelsel Rijk (VSSR), dat het functioneren van en de samenwerking tussen SOCs versterkt. Dat gebeurt door bundeling en door het gezamenlijk ontwikkelen van detectieregels. Zo vormen HGI, ABRO, het traject voor risicomanagement en VSSR een solide basis voor de opvolging van de derde aanbeveling van AcICT.

Departementen zijn zelf verantwoordelijk voor het treffen van passende beveiligingsmaatregelen. AcICT geeft terecht aan dat samenwerking en gemeenschappelijke uitgangspunten daarbij nodig zijn. Maar de bescherming van specifieke Te Beschermen Belangen (TBB) tegen statelijke actoren vraagt in veel gevallen om maatwerk. Als er gebruik wordt gemaakt van een breed aanvullend kader bestaat het risico dat het effect onvoldoende is, en dat het onnodig duur wordt. Daarom is in de Baseline Informatiebeveiliging Overheid (BIO) afgezien van een normenkader op BBN3-niveau. Bovendien is in de nieuwe BIO het onderscheid tussen de verschillende basisbeveiligingsniveaus vervallen.

Tegen deze achtergrond, en in aanvulling op de vier eerdergenoemde trajecten, is er een serie van acties in gang gezet. De CIO Rijk zal eerst samen met BZ, SSC-

ICT en gespecialiseerde diensten, op basis van gangbare normen zoals ISO27001, BIO en NATO-normen, een aanvulling op de BIO ontwikkelen. Dit gaat over de actieve bescherming van Departementaal Vertrouwelijke gegevens tegen statelijke actoren. Hierbij worden ook uitgangspunten zoals 'assume breach' en 'Zero Trust' meegenomen. Deze normen en voorschriften worden in eerste instantie toegesneden op de casuïstiek bij BZ, in verband met de urgentie die daar wordt gezien. Naar verwachting kunnen de eerste resultaten aan het einde van dit jaar opgeleverd worden. De tweede stap is dat die aanvulling wordt doorontwikkeld tot een generiek inzetbare handreiking waaruit de ministeries kunnen putten voor het treffen van passende maatregelen om hun TBB's te beschermen tegen statelijke actoren.

Voor de ontwikkeling van deze handreiking is goede interdepartementale samenwerking een belangrijke voorwaarde. Er worden verschillende experts samengebracht: van ministeries, uitvoeringsorganisaties en gespecialiseerde diensten. Zo kunnen domeinkennis, materiedeskundigheid en goede voorbeelden worden gedeeld. BZ speelt daarbij een sleutelrol; AcICT dringt erop aan om de expertise en de kennispositie van BZ goed te benutten voor de opvolging van hun derde aanbeveling. Het resultaat is een breed gedragen kader voor het efficiënt inzetten van generieke beveiligingsmaatregelen, dat tegelijkertijd helpt bij het aanpakken van specifieke beveiligingsuitdagingen.

AcICT adviseert om centrale, gecombineerde dienstverlening op te zetten voor de actieve bescherming van Departementaal Vertrouwelijke gegevens tegen statelijke actoren. Als eerste stap zal BZK een behoefteonderzoek uitvoeren, waarbij wordt meegenomen dat BBN3 komt te vervallen. Vervolgens zal er een business case worden opgesteld om de kosten en de baten van een centrale voorziening in kaart te brengen, en duurzame financiering te kunnen verzekeren.

Opvolging aanbeveling 4: evalueer na 2 jaar gezamenlijk de opvolging van de adviezen

Het overkoepelende advies van AcICT is om topprioriteit te geven aan de urgente verbetering van de huidige ICT-dienstverlening. De vierde aanbeveling die in dat verband wordt gedaan is het gezamenlijk evalueren van de opvolging van het advies, na twee jaar of zoveel eerder als passend wordt gevonden. Daarbij gaat het vooral om de eerste twee aanbevelingen, en dus om wat BZ en SSC-ICT daarmee hebben gedaan: welke maatregelen zijn er genomen, welk effect heeft dat gehad, en welke nieuwe mogelijkheden dienen zich vervolgens aan? AcICT hanteert voor deze evaluatie een vrij ruime termijn. Tegelijkertijd is de urgentie hoog. Het is dus belangrijk om van het begin af aan de vinger goed aan de pols te houden, en het evaluatiemoment als dat mogelijk is wat naar voren te halen.

Aanbeveling 1 (samen urgente beveiligingsrisico's terugdringen) gaat over acute kwesties. BZ en BZK zijn dus voortvarend aan de slag gegaan met dit onderdeel van het AcICT-advies. Beide organisaties hebben vertrouwen in de wenselijkheid van deze koers, en in elkaars goede wil. Dat is ook nodig, want de inhoudelijke opgave is niet gering. Daarbij zal ook de vraag opnieuw worden beantwoord of het principe van een shared services organisatie zich wel verdraagt met het kunnen leveren van gespecialiseerde diensten en het voldoen – voor een enkele opdrachtgever – aan complexe, bijzondere eisen. Op onderdelen geldt mogelijk dat 'nee' verkopen ook

een antwoord is, wat vervolgens voor de opdrachtgever aanleiding is om op zoek te gaan naar een alternatief.

De aanbeveling om de besturing bij BZ te verbeteren is ook belangrijk. De opvolging daarvan wordt gezien als een diepte-investering, die verder gaat dan alleen de dienstverlening die wordt geleverd door SSC-ICT. Er zullen bijvoorbeeld aanpassingen moeten worden gedaan in de organisatie en in de manier van werken. Het programma SHIELD voorziet in een passende systematiek voor het monitoren van de voortgang en de resultaten op dit punt.

AcICT dringt erop aan om het 'vertrekbesluit' uit te stellen, en pas na evaluatie van de verbeteracties opnieuw te bekijken of zo'n besluit nog nodig is. De koppeling die daarmee wordt gemaakt is begrijpelijk. Als aanbeveling 1 (samen beveiligingsrisico's aanpakken) en aanbeveling 2 (besturing door BZ versterken) tot resultaten hebben geleid ligt alle informatie op tafel om een definitief standpunt te kunnen bepalen over het weghalen van – een deel van de – de dienstverlening bij SSC-ICT. Maar dat laat onverlet dat het mogelijk is om eerder al in gezamenlijkheid te bezien of er specifieke diensten zijn die SSC-ICT nu levert aan BZ waarvoor geldt dat het niet in het belang is van BZ en SSC-ICT om die als zodanig te blijven leveren. Die analyse – of validatie, zoals het eerder in deze brief is genoemd – wordt in de komende maanden ter hand genomen binnen het kader van SHIELD.

De activiteiten die door BZ en BZK worden ontplooid om opvolging te geven aan de aanbevelingen 1 en 2 omvatten in feite ook vrijwel alle activiteiten die moeten worden uitgevoerd voor het voorbereiden van een eventuele – gedeeltelijke – ontvlechting. Dat betekent dat BZ een extra reden heeft om zich in te zetten voor het slagen van de maatregelen in het verlengde van deze aanbevelingen. Als dit vervolgens loopt zoals het BZ en SSC-ICT nu voor ogen staat dan is de uitkomst na evaluatie van die maatregelen dat een vertrekbesluit alleen hoeft te worden genomen voor die voorzieningen waarvan in gezamenlijkheid wordt vastgesteld dat die niet goed passen in de portfolio van SSC-ICT. Door op deze manier te werk te gaan (een *no regret* aanpak) treedt er voor BZ geen vertraging op als er vervolgens zou worden besloten tot een al dan niet gedeeltelijke ontvlechting.

Gezien de urgentie van het bovenstaande hebben BZ en SSC-ICT de afspraak gemaakt niet pas twee jaar na het uitbrengen van het advies de genoemde evaluatie uit te voeren, maar dit uiterlijk begin september 2026 te doen. Tot die tijd houden de twee organisaties in de gaten of daarin, al dan niet op onderdelen, nog een versnelling nodig en mogelijk is, bijvoorbeeld op basis van de genoemde validatie (de beantwoording van de vraag wat past binnen de portfolio en roadmap van SSC-ICT). Dat sluit ook aan op het advies van AcICT om elke drie maanden bestuurlijk over de opvolging van het advies te rapporteren.

Tot slot

Aan AcICT is gevraagd advies uit te brengen over een programma van BZ. Vervolgens heeft AcICT zich in zijn beantwoording gericht op twee ministeries, BZ en twee onderdelen van BZK, waarbij een breed terrein aan verbetertrajecten is bestreken. Daarmee ligt er een veelomvattend en betekenisvol advies op tafel. Veel van de bedoelde verbeteringen waren op dat moment al in beeld of zelfs in gang gezet. Maar het advies heeft de verschillende trajecten van nieuwe inzichten

voorzien, en heeft gezorgd voor een nieuwe dynamiek in de onderlinge samenwerking.

BZ en BZK zijn overtuigd van de noodzaak om de investeringen te doen waar AcICT voor pleit. Samen hebben zij daarvoor de nodige plannen uitgewerkt. De verdere uitvoering daarvan is voortvarend ter hand genomen, en BZ en BZK houden samen de vinger aan de pols, om zeker te weten dat het nieuwe elan beklijft en rendeert.

Graag willen wij AcICT dus bedanken voor het advies dat zij ons hebben aangereikt. Het moment bleek goed gekozen, en de uitkomst was behulpzaam. Wij hebben het vertrouwen dat in deze brief duidelijk is toegelicht hoe wij opvolging geven aan het advies van AcICT. Via de gebruikelijke rapportages over de bedrijfsvoering van het Rijk zullen wij u blijven informeren over de voortgang van de verschillende acties en maatregelen in dit verband.

De minister van Buitenlandse Zaken,

D.M. van Weel

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
Herstel Groningen, Koninkrijksrelaties en Digitalisering,

Eddie van Marum

Adviescollege ICT-toetsing

> Retouradres Postbus 16292 2500 BG Den Haag

Ministerie van Buitenlandse Zaken
t.a.v. de minister, de heer drs. C.C.J Veldkamp
Postbus 20061
2500 EB Den Haag

Afschrift aan: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
t.a.v. de staatssecretaris Digitalisering en Koninkrijksrelaties, de heer drs. F.Z. Szabó
Postbus 20011
2500 EA Den Haag

Muzenstraat 95
Den Haag
Postbus 16292
2500 BG Den Haag
adviescollegeicttoetsing.nl

Contactpersoon
info@adviescollegeicttoetsing.nl

Datum
3 februari 2025

Kenmerk
2025-0000122205

Uw kenmerk
BZ2511681

Betreft
Advies programma Transitie ICT-dienstverlening

Geachte heer Veldkamp,

U heeft het Adviescollege ICT-toetsing verzocht een onderzoek uit te voeren naar het programma Transitie ICT-dienstverlening van het ministerie van Buitenlandse Zaken (BZ). De opdrachtgever is de plaatsvervangend secretaris-generaal van uw ministerie. Dit advies sturen we tevens in afschrift aan de staatssecretaris Digitalisering en Koninkrijksrelaties, omdat de onderwerpen die aan bod komen ook betrekking hebben op onderdelen of beleidsterreinen van het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK).

Het advies kan als volgt worden samengevat:

Het ministerie van Buitenlandse Zaken (BZ) heeft een deel van de ICT-dienstverlening bij het Shared Service Center (SSC)-ICT belegd, net als acht andere ministeries. SSC-ICT is een onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Met het nog te starten programma Transitie ICT-dienstverlening beoogt BZ invulling te geven aan een eerder besluit van BZ om te vertrekken bij SSC-ICT en de ICT-dienstverlening te beleggen bij een andere partij.

Conclusie

De belangrijkste conclusie uit het onderzoek is dat wij het besluit van BZ om nu te vertrekken bij SSC-ICT te risicovol vinden, zowel vanuit het perspectief van BZ als vanuit het rijksbrede belang, want:

A. Vertrek brengt de urgente verbetering van de informatiebeveiliging in gevaar.
B. Grote kans op herhaling problematiek dienstverlening door onvolwassen besturing BZ.
C. Vertrek belemmert noodzakelijke beveiliging tegen statelijke actoren voor BZ en rijksbreed.

Advies

Wij adviseren om het vertrekbesluit nu niet door te zetten. Geef eerst de urgente verbetering van de huidige ICT-dienstverlening topprioriteit:

1. Zorg dat SSC-ICT en BZ de urgente beveiligingsrisico's terugdringen.
2. Zorg dat de besturing bij BZ fundamenteel verbetert.
3. Realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren.
4. Evalueer na twee jaar gezamenlijk de opvolging van de adviezen.

Hieronder vindt u eerst een korte beschrijving van het programma Transitie ICT-dienstverlening. Daarna werken we bovenstaande analyse en adviezen nader uit. Wij concentreren ons hierbij op de belangrijkste risico's. In de bijlage vindt u de details van het programma.

Adviescollege ICT-toetsing

Datum
3 februari 2025

Kenmerk
2025-0000122205

Korte omschrijving van het programma Transitie ICT-dienstverlening

Vóór 2015 had BZ een eigen ICT-afdeling. Sinds 2015 maakt BZ gebruik van de ICT-dienstverlening van het Shared Service Center (SSC)-ICT. Bij de overgang naar SSC-ICT heeft BZ circa 100 medewerkers overgedragen. SSC-ICT levert diensten voor werkplekken, housing (fysieke huisvesting van de datacentra) en hosting (alle specifieke hard- en software, inclusief de technische beheeractiviteiten), en verzorgt het beheer van applicaties. SSC-ICT doet dat zowel in Nederland als wereldwijd, op 160 posten en voor drie datacentra in Nederland, Singapore en Noord-Amerika. De directie Informatievoorziening en Digitale Innovatie (IDI) van BZ is verantwoordelijk voor de regievoering op SSC-ICT.

SSC-ICT bestaat sinds 2014. Het is onderdeel van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en opgericht om te zorgen voor meer efficiëntie en samenwerking binnen de rijksoverheid. Negen ministeries maken gebruik van de ICT-dienstverlening van SSC-ICT. Vanuit de gedachte van 'gedeelde diensten' ligt de nadruk bij SSC-ICT op standaarddienstverlening. De ICT-dienstverlening voor BZ wijkt hiervan af omdat BZ wereldwijd werkt, te maken heeft met verhoogde dreiging van statelijke actoren en moet voldoen aan accreditatie-eisen vanuit de Europese Unie (EU) en de NAVO. BZ stelt daarom specifieke eisen, zoals een afgescheiden netwerk, specifieke cryptovoorzieningen en toepassing van BasisBeveiligingsNiveau 3 (BBN3) uit de Baseline Informatiebeveiliging Overheid (BIO)[1] voor de systemen en infrastructuur waar departementaal vertrouwelijke informatie wordt verwerkt.

BZ en SSC-ICT hebben al lange tijd een moeizame onderlinge samenwerking om een aantal redenen, waaronder:

- Er is geen gedeeld beeld van de invulling van de dienstverleningsafspraken. SSC-ICT houdt, in de ogen van BZ, onvoldoende rekening met de eisen en wensen van BZ. In de ogen van SSC-ICT vult BZ het opdrachtgeverschap niet volwassen in.
- Gezamenlijke initiatieven die de afgelopen jaren zijn gestart om de dienstverlening en de beveiliging te verbeteren, hebben niet altijd de gewenste resultaten opgeleverd.
- In 2023 waren er meerdere beveiligingsincidenten die tot verschil van mening leidden. SSC-ICT en BZ dachten niet alleen verschillend over de invulling van hun rol bij deze incidenten, maar ook over noodzakelijke verbetering van de beveiliging.
- Sinds de overgang van BZ naar SSC-ICT in 2015 zijn de ICT-systemen op posten en in datacentra beperkt vernieuwd. Een langlopende discussie over de toerekening van de kosten van de vernieuwing is pas recent afgerond, waardoor de vernieuwing flink is vertraagd.

Eind 2023 heeft BZ eenzijdig besloten om te vertrekken (te 'ontvlechten') bij SSC-ICT. De toenmalige minister van BZ heeft aan de toenmalige staatsecretaris van Digitalisering en Koninkrijksrelaties meegedeeld een 'herziening van de dienstverlening door SSC-ICT aan BZ voor te bereiden'. Dit is in januari 2024 mondeling en in juni 2024 schriftelijk gebeurd. De staatssecretaris heeft hierop nog niet schriftelijk gereageerd.

De invulling van het besluit is door BZ nog niet bepaald. Zo moet BZ nog bepalen of het vertrek voor de hele ICT-dienstverlening geldt of alleen voor de 'kritieke diensten' (waaronder werkplek, housing, specifieke applicaties, crypto-apparatuur en het postennetwerk).

[1] De BIO definieert 3 basisbeveiligingsniveaus (BBN's). BBN2 is het standaardniveau voor de Rijksoverheid. BBN3 vergt aanvullende maatregelen, op basis van organisatiespecifieke risicoanalyses, om weerstand te kunnen bieden tegen statelijke actoren en criminele organisaties. Deze maatregelen of het proces om deze te selecteren zijn niet in de BIO geconcretiseerd.

BZ heeft een eerste projectbrief opgesteld waarin de contouren van het programmaplan Transitie ICT-dienstverlening staan. Een scenario-analyse en een businesscase worden momenteel uitgewerkt. De eerste grove inschatting van BZ is dat de transitie naar een nieuwe dienstverlener vijf jaar gaat duren. Er is nog geen kosteninschatting gemaakt. BZ wil dat lopende en geplande verbeter- en vernieuwingsprojecten bij SSC-ICT gedurende de transitie doorgaan.

BZ neemt niet alleen diensten van SSC-ICT af, maar ook van private aanbieders; bijvoorbeeld een 'Hoog Beveiligde Omgeving (HBO)' van Atos (de huidige HBO1) en Capgemini (de nieuwe HBO2 en Azure cloud). Daarnaast levert British Telecom de netwerkconnectiviteit met de posten.

Conclusie: Doorzetten vertrekbesluit te risicovol

Vanwege de internationale context en de dreiging van statelijke actoren is het noodzakelijk dat de ICT-dienstverlening voor BZ – inclusief de beveiliging – goed op orde is. Dit stelt hoge eisen aan dienstverlener SSC-ICT, aan de besturing vanuit BZ én aan hun onderlinge samenwerking. Beide partijen voldoen nu niet in voldoende mate aan die eisen.

Ondanks meerdere verbeterpogingen in de afgelopen jaren is er, gezien de moeizame relatie tussen beide partijen, weinig concreet perspectief dat de huidige situatie structureel gaat verbeteren. Desalniettemin vinden wij het besluit van BZ om te vertrekken bij SSC-ICT te risicovol, zowel vanuit het perspectief van BZ als vanuit het rijksbrede belang. Wij hebben hiervoor de volgende redenen.

A. Vertrek brengt urgente verbetering informatiebeveiliging in gevaar

De eerste inschatting van BZ is dat de transitie naar een andere dienstverlener vijf jaar gaat duren. BZ en SSC-ICT zitten dus nog een aantal jaren aan elkaar vast. De transitieperiode zal veel schaarse capaciteit en aandacht van zowel SSC-ICT als BZ vergen. Hierdoor is de beschikbare capaciteit beperkt om urgente beveiligingsrisico's in de BZ-dienstverlening vanuit SSC-ICT terug te dringen.
Gezien de aard van deze risico's zijn ze niet in dit publieke advies opgenomen maar in een vertrouwelijke bijlage met een beperkte verspreidingskring.

B. Grote kans herhaling problematiek dienstverlening door onvolwassen besturing BZ

Wij denken dat BZ te optimistisch is over wat de transitie naar een andere ICT-dienstverlener aan verbetering zal brengen. De huidige situatie is namelijk mede ontstaan omdat BZ niet voldoende is toegerust om de besturing van het ICT-domein goed in te richten. Met een transitie naar een nieuwe ICT-dienstverlener is de kans groot dat de problemen met de huidige dienstverlening zich herhalen. Wij constateren het volgende:

- BZ is onvoldoende in staat om concrete eisen aan de ICT-dienstverlening te stellen:
  - De uitvoering van het risicomanagement is niet op orde. BZ kan onvoldoende scherp afbakenen wat voor BZ de kritieke processen en informatiestromen zijn, wat hun dreigingsniveau is en hoe ze zich verhouden tot de verschillende ICT-diensten. Hierdoor kan BZ niet goed bepalen welke ICT-diensten aan een hoger beveiligingsniveau moeten voldoen.
  - BZ stelt eisen op een te hoog abstractieniveau. De specifieke internationale context van BZ vraagt om duidelijke eisen voor leveranciers, zodat zij de mogelijkheid krijgen om de ICT-dienstverlening passend in te richten. BZ is onvoldoende in staat om die eisen concreet te formuleren, waardoor de kans groot is dat dit bij een nieuwe ICT-

dienstverlener opnieuw leidt tot stroeve discussies, misinterpretatie en verschillende verwachtingen.

- De regievoering vanuit BZ op dienstverleners staat nog in de kinderschoenen:
  - Elementaire zaken ontbreken, zoals inzicht in welke ICT-diensten BZ nu precies afneemt van welke dienstverlener of leveranciers. Daarnaast ontbreekt het aan effectieve centrale coördinatie en prioriteitsstelling van opdrachten aan dienstverleners. Daardoor heeft de aansturing in hoge mate een ad hoc karakter.
  - BZ acteert weinig rolvast waardoor samenwerking met SSC-ICT stroef en onvoorspelbaar verloopt. BZ verwacht enerzijds dat de dienstverlener als 'goed huisvader' diensten levert, maar behandelt de dienstverlener anderzijds als een interne IT-afdeling door specifieke ICT-oplossingen voor te schrijven.
- De uitvoering van de interne beveiligingsprocessen bij BZ is niet op orde:
  - BZ leeft haar eigen beveiligingsbaseline onvoldoende na. Zo ontbreekt het bijvoorbeeld aan een sluitend intern auditproces om periodiek de naleving van de beveiligingskaders vast te stellen en verbetermaatregelen te identificeren. Daarnaast is er bij de afhandeling van een significant beveiligingsincident geen onderzoek gedaan naar de grondoorzaak.
  - BZ heeft het accreditatiebeleid onvolledig geïmplementeerd voor systemen waarin nationaal of internationaal (EU/NAVO) gerubriceerde informatie wordt verwerkt. Bij de beoordeling van deze systemen moeten minimaal de relevante (technische) beveiligingskaders als criteria zijn meegenomen, zoals bijvoorbeeld de BIO BBN2-maatregelen. In de praktijk blijkt echter dat dit niet voldoende gebeurt. Bij de beoordeling van de werkplek- en de basis ICT-infrastructuur zijn maatregelen op BBN2-niveau uit de BIO niet expliciet meegenomen.

C. Vertrek belemmert noodzakelijke beveiliging tegen statelijke actoren voor BZ en rijksbreed

Meerdere organisaties binnen de rijksoverheid worstelen – net als BZ – met de beveiliging tegen statelijke actoren en criminele organisaties (BBN3). Daarbij constateren wij dat deze organisaties grote moeite hebben om de benodigde maatregelen in de systemen en infrastructuur te treffen. Bovendien wordt dit vraagstuk urgenter. Zo blijkt uit het Cybersecuritybeeld 2024[2] dat statelijke actoren hun activiteiten in Nederland intensiveren. Ze verbreden daarbij hun capaciteiten, mede door samen te werken met cybercriminelen. Ook zorgt de internationalisering van de IT-markt ervoor dat rijksorganisaties steeds meer afhankelijk worden van buitenlandse leveranciers. Deze hebben dikwijls te maken met andere wetgeving en daar is lastiger toezicht op te houden.

Wij vinden dat een rijksbrede aanpak noodzakelijk is om BBN3 ICT-dienstverlening voor rijksorganisaties, waaronder BZ, goed in te vullen. Wij verwachten dat een vertrek van BZ bij SSC-ICT de totstandkoming van zo'n rijksbrede aanpak belemmert. Wij hebben hiervoor de volgende redenen:

- Voor het ontwerp van BBN3 ICT-dienstverlening moet schaarse specialistische kennis bij verschillende delen van de rijksdienst gebundeld worden. Het gaat om kennis over de modus operandi van aanvallers en over beveiligingstechnieken. Rijksbrede, goede voorbeelden dragen bij aan verdere kennisopbouw. Ter illustratie: specifieke expertise op dit gebied van de AIVD, MIVD en het Nationaal Cyber Security Centrum (NCSC) is schaars. Inbreng vanuit BZ is essentieel gezien de ervaring en de specifieke landenkennis.
- De realisatie van BBN3 ICT-dienstverlening vergt aanzienlijke beheerinvesteringen, bijvoorbeeld in een gespecialiseerd 24/7 *Security Operations Center* (SOC), de ontwikkeling van een BBN3-werkplek en toepassing van cryptografische technieken. Deze investeringen

[2] Zie het NCTV "Cybersecuritybeeld Nederland 2024", beschikbaar op www.nctv.nl.

zijn voor rijksorganisaties zeer kostbaar om individueel te dragen. Dienstverlening wordt zo veel duurder dan nodig. Bovendien ligt een gezamenlijke investering in lijn met de ambitie om ICT-dienstverlening binnen de rijksoverheid te consolideren.

Advies: Geef urgente verbetering van huidige ICT-dienstverlening topprioriteit

Wij adviseren om het vertrekbesluit nu niet door te zetten. Geef eerst de urgente verbetering van de huidige ICT-dienstverlening topprioriteit. Wij hebben daartoe een aantal adviezen geformuleerd.

Randvoorwaardelijk voor de opvolging van deze adviezen is dat BZ en SSC-ICT eerst tot een goede samenwerkingsrelatie komen, met wederzijds respect en begrip voor elkaars situatie en (on)mogelijkheden. Ook moeten beide partijen de intentie hebben om samen de gesignaleerde problematiek op te lossen. Daarvoor is een reset nodig van de huidige relatie op alle niveaus, maar vooral op strategisch en tactisch niveau. Wij kunnen ons voorstellen dat een door beide partijen geaccepteerde onafhankelijke partij een bemiddelende rol bij deze reset vervult. Het is van belang dat de eigenaar van SSC-ICT de ruimte voor deze reset biedt, zeker in het besef dat een groot deel van de te nemen acties ook waardevol zijn voor de andere aan SSC-ICT deelnemende ministeries.

1. Zorg dat SSC-ICT en BZ samen urgente beveiligingsrisico's terugdringen

Gezien de urgente beveiligingsrisico's is het noodzakelijk dat BZ en SSC-ICT constructief gaan samenwerken om de risico's op korte termijn terug te dringen. Wij adviseren om maatregelen te treffen en over de voortgang ervan iedere drie maanden aan de minister van Buitenlandse Zaken en aan de staatssecretaris Digitalisering en Koninkrijksrelaties te rapporteren.
Gezien de aard en details van de maatregelen die wij adviseren, zijn deze niet in dit publieke advies opgenomen maar in een vertrouwelijke bijlage.

2. Zorg dat de besturing bij BZ fundamenteel verbetert

Om tot een meer professionele omgang met ICT-dienstverleners te komen, is het noodzakelijk dat BZ de besturing van het ICT-domein fundamenteel verbetert. Wij adviseren BZ om de volgende maatregelen te treffen:

- Werk de eisen voor de ICT-dienstverlening – inclusief beveiliging – beter uit:
  - Richt een sluitend risicomanagementproces in. Breng de kritieke processen en informatiestromen en bijbehorend dreigingsniveau voor BZ in kaart. Definieer op basis daarvan de specifieke beveiligingsbehoefte.
  - Verbeter het proces voor de specificatie van eisen aan dienstverleners. Stel op basis van de beveiligingsbehoefte duidelijke eisen op waarin de internationale context van BZ en het bijbehorende dreigingsbeeld is meegewogen.
- Breng de regievoering op orde:
  - Verbeter de inrichting van het contractmanagement van BZ, zodat het maken, bewaken en bijsturen van afspraken volgens een gestructureerd en beheerst proces plaatsvindt. Zorg dat BZ centraal inzicht heeft welke ICT-diensten bij welke leverancier worden afgenomen en in hoeverre aan de gemaakte afspraken wordt voldaan door zowel de leverancier als BZ.
  - Acteer rolvast door SSC-ICT en andere dienstverleners als een voorspelbare partner te bevragen en ad hoc sturing te voorkomen. Realiseer binnen het ICT-domein een heldere taakafbakening, inclusief verdeling van verantwoordelijkheden om centrale

coördinatie en prioriteitsstelling te realiseren als het gaat om verzoeken aan dienstverleners.

- Verbeter de uitvoering van de interne beveiligingsprocessen:
  - Zorg voor effectieve naleving van de vereisten uit de BZ-beveiligingsbaseline en een gestructureerd informatiebeveiligingsproces binnen BZ. Verbeter ook de afhandeling van beveiligingsincidenten, waarbij altijd de grondoorzaak wordt onderzocht.
  - Bewaak naleving van de regels vanuit het accreditatiebeleid. Neem in de beoordeling van systemen die gerubriceerde informatie verwerken minimaal de relevante (technische) informatiebeveiligingskaders mee.

3. Realiseer vanuit BZK een rijksbrede aanpak beveiliging tegen statelijke actoren

Gezien de urgentie om beveiliging tegen statelijke actoren en georganiseerde criminaliteit (BBN3) effectief in te vullen, adviseren we BZK met hoge prioriteit een rijksbrede aanpak te realiseren. Maak duidelijk dat dit onderwerp ‘chefsache’ is door het opdrachtgeverschap in het Secretarissen-Generaal Overleg (SGO) te beleggen. We adviseren een rijksbrede aanpak bestaande uit twee onderdelen:

- Realiseer onder aansturing van CIO-rijk binnen zes maanden een uitwerking voor een rijksbreed kader voor de beveiliging tegen statelijke actoren:
  - Mobiliseer specialistische kennis vanuit tenminste de AIVD, MIVD, NCSC, BZ en andere ministeries.
  - Hanteer als uitgangspunt de informatiebeveiligingsnorm ISO27001 en laat het rijksbrede kader daarop aanvullend zijn. Dit is in lijn met de BIO die naar aanleiding van de Europese NIS2-richtlijn (Network and Information Security Directive) wordt vernieuwd.
  - Neem in het kader richtlijnen op voor het risicoanalyseproces ten aanzien van de wijze van selectie van beveiligingsmaatregelen (conform het risicobeoordeling en -behandelingsproces in de ISO27001). Zorg dat in dit risicoanalyseproces de specifieke karakteristieken en technieken van de modus operandi van statelijke actoren en criminele organisaties worden meegewogen, zoals het gebruik van wereldwijde interceptie.
  - Werk een selectie van toepasbare beveiligingsmaatregelen uit. Maak hierbij gebruik van bestaande goede voorbeelden vanuit ministeries, zoals specifieke cryptografische oplossingen, datadiodes voor veilige verbinding met minder veilige netwerken en virtualisatie-oplossingen. Zorg dat deze selectie actueel blijft.
  - Neem detectieregels op om mogelijke inbreuken tijdig te signaleren. Hanteer hiervoor het *Assume Breach*-principe. Dit gaat ervanuit dat niet voorkomen kan worden dat een aanvaller er uiteindelijk in slaagt om een systeem te compromitteren.
- Realiseer stapsgewijs BBN3 ICT-dienstverlening voor rijksbreed gebruik:
  - Bepaal welke overheidspartij het meest geschikt is om BBN3 ICT-dienstverlening te ontwikkelen op basis van het bovenstaande rijksbrede kader.
  - Faciliteer vanuit die overheidspartij de rijksbrede beschikbaarheid van tenminste een BBN3-werkplek. Een goede samenwerking tussen de verschillende ICT-dienstverleners en de datacentra binnen de rijksdienst is daarbij cruciaal.

4. Evalueer na twee jaar gezamenlijk de opvolging van de adviezen

Wij verwachten dat de opvolging van bovenstaande adviezen twee jaar in beslag zal nemen. Wij adviseren:

- Evalueer na twee jaar, of eerder indien opportuun, de opvolging van de adviezen en de effectiviteit van de getroffen maatregelen. Doe dat zowel bij BZ als SSC-ICT. Selecteer hiervoor een partij die onafhankelijk is ten opzichte van BZ en SSC-ICT.

- Bepaal op basis van de uitkomsten van de evaluatie eventuele vervolgstappen. Neem daarin mee hoe om te gaan met het uitgestelde vertrekbesluit. Werk een eventueel scenario voor een transitie dan pas uit, zodat de opbrengsten uit onze adviezen onder 2 (betere besturing BZ) en 3 (rijksbrede aanpak statelijke actoren) meegenomen kunnen worden in de uitwerking.

***

Wij danken alle geïnterviewden voor hun medewerking en openheid. Wij hopen dat we met dit advies een bijdrage kunnen leveren aan zowel het verbeteren van de ICT-dienstverlening bij BZ en SSC-ICT als aan het rijksbreed verbeteren van de weerbaarheid tegen statelijke actoren en criminele organisaties.

Met de meeste hoogachting,
namens het Adviescollege ICT-toetsing,

w.g.

Adri de Bruijn
Voorzitter

w.g.

Sander van Amerongen
Secretaris-directeur

Bijlage

Datum
3 februari 2025

Kenmerk
2025-0000122205

Informatie over programma Transitie ICT-dienstverlening

Nr.	Onderwerp	Toelichting
1.	Projectnaam	Transitie ICT-dienstverlening
2.	Opdrachtgever	Plaatsvervangend secretaris-generaal van het ministerie van Buitenlandse Zaken (BZ)
3.	Startdatum project	Nog niet formeel gestart
4.	Einddatum project	Nog niet bekend
5.	Type project	Transitie van de ICT-dienstverlening naar een andere dienstverlener
6.	Fase Project	Initiatiefase
7.	Totaal budget	Nog niet bekend
8.	Reeds uitgegeven per datum	Niet bekend
9.	Doelstelling	Ontvlechten en herbeleggen van (een nog te bepalen gedeelte van) de dienstverlening geleverd door SSC-ICT aan BZ
10.	Maatschappelijke/ beleidsdoelstelling	Niet gedefinieerd
11.	Meetbare baten	Geen meetbare baten gedefinieerd
12.	Huidige technologie/ architectuur	Grote diversiteit aan hardware en software
13.	Doeltechnologie/- architectuur	Nog niet bekend
14.	Omvang systeem	Niet bekend
15.	Aantal gebruikers	Circa 7600 werkplekgebruikers (ca. 4000 in Nederland en 3600 op buitenlandse posten)
16.	Belanghebbenden	• Medewerkers van BZ binnen en buiten Nederland • Bondgenoten en inlichtingen- en veiligheidsdiensten voor uitwisseling van informatie over geopolitieke ontwikkelingen en dreigingen • Afnemers van ICT-dienstverlening van SSC-ICT
17.	Aanbesteding voorzien	Nog niet bekend, afhankelijk van het te kiezen scenario

Informatie over het uitgevoerde onderzoek

Nr.	Onderwerp	Toelichting
1.	Type onderzoek	Project; conform artikel 7, lid 1 sub a2 Wet Adviescollege ICT- toetsing
2.	Aanmelddatum	22 augustus 2024
3.	Start onderzoek	29 augustus 2024
4.	Afronden onderzoek	5 december 2024
5.	Datum conceptadvies	19 december 2024
6.	Datum definitief advies	3 februari 2025
7.	Eerder onderzoek	Nee
8.	Onderzoeksmethode	Interviews en documentstudie

Ministerie van Buitenlandse Zaken

TER BESLISSING

Aan M
Van
Via
Kopie aan
Afgestemd met

Bescherming persoonlijke levenssfeer

Datum
23 september 2025

Onze referentie
BZ2520436

Opgesteld door

Bescherming persoonlijke levenssfeer

Bijlage(n)
1

nota

Kamerbrief toezending advies AcICT Transitie ICT Dienstverlening

Aanleiding

- Op 22 augustus 2024 is namens de voorganger van M aan het Adviescollege ICT-toetsing (AcICT) gevraagd BZ te adviseren over de aanpak van het programma Transitie ICT-dienstverlening. Dat programma betrof het onderzoeken van de mogelijkheden om de ICT-diensten zoals geleverd door SSC-ICT van andere leveranciers te gaan betrekken. Enkele ernstige incidenten vormden de directe aanleiding daarvoor.
- Op 4 februari jl. heeft AcICT advies uitgebracht over dat programma. In dat advies (met een vertrouwelijke bijlage) stonden aanbevelingen die zowel BZ als BZK betroffen.
- AcICT heeft de wettelijke plicht zo'n advies binnen twee weken te publiceren. BZ en BZK hebben de wettelijke plicht om de beide kamers binnen 4 weken het advies toe te sturen, vergezeld van een bestuurlijke reactie (in de praktijk is deze termijn dus 2 weken, omdat aanbieding aan de kamers, en dus openbaarmaking, logischerwijs niet later kan plaatsvinden dan publicatie door AcICT).
- Uit het oogpunt van nationale veiligheid (getoetst bij AIVD) werd publicatie op dat moment te kwetsbaar gevonden. Met AcICT is toen overeengekomen dat vooralsnog niet zou worden overgegaan tot openbaarmaking. Op 3 maart jl. hebben BZ en BZK wel beide kamers vertrouwelijk geïnformeerd over het advies en hoe daar opvolging aan wordt gegeven.
- Op 1 september jl. heeft AcICT, na afstemming met PSG BZ, besloten om 1 oktober het adviesrapport te gaan publiceren, zonder vertrouwelijke bijlage.
- Weliswaar hebben de betrokken bewindspersonen op 3 maart jl. al voldaan aan hun wettelijke verplichting om de beide kamers te informeren, maar niet-vertrouwelijke toezending van het rapport aan de kamers (zonder de vertrouwelijke bijlage), gelijktijdig met de publicatie van het rapport door AcICT, ligt in de rede. Daarbij past een bestuurlijke reactie.

Geadviseerd besluit

Akkoord gaan met toezending van het advies van AcICT aan de beide kamers (zonder de vertrouwelijke bijlage), vergezeld van een bestuurlijke reactie (identieke brieven voor beide kamers). De bestuurlijke reacties worden samen met de Stas BZK ondertekend.

Kernpunten

- AcICT adviseert om het voornemen van BZ op dit moment niet door te zetten en eerst de urgente verbetering van de huidige ICT-dienstverlening topprioriteit te geven.
- Door de betrokken partijen (BZ, en de onderdelen DG Digitalisering en Overheidsorganisatie, DG Vastgoed en Bedrijfsvoering Rijk en SSC-ICT van BZK) wordt in de Kamerbrief invulling gegeven aan het advies van AcICT.
- Een vertrekbesluit (voor alle BZ dienstverlening van SSC-ICT of een deel daarvan) wordt daarmee in feite uitgesteld. De in de reactie beschreven activiteiten m.b.t. de aanbevelingen zijn voor de komende tijd in elk scenario (blijven of – al dan niet gedeeltelijk – vertrekken) vereist.
- De door AcICT aanbevolen evaluatie met alle partijen, na uiterlijk twee jaar, zal duidelijk maken of van het vertrekbesluit afgezien kan worden of dat, maar dan door alle partijen begrepen en onderschreven, ontvlechting voor bepaalde delen van de ICT-dienstverlening de betere optie is.
- In de bestuurlijke reactie wordt verder aangegeven dat, gezien de voortgang op de verschillende dossiers, er nu een natuurlijk moment is ontstaan om over te gaan tot publicatie van het advies van AcICT.
- Het besluit tot toezending van het adviesrapport aan de kamers is goed beschouwd een pro forma aangelegenheid, dit gezien het besluit van AcICT tot openbaarmaking van het advies.