

Vergaderjaar 2020–2021

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 731

BRIEF VAN DE MINISTER-PRESIDENT, MINISTER VAN ALGEMENE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 december 2020

Het Bureau ICT-toetsing (BIT) heeft in de periode mei t/m augustus 2020 onderzoek verricht naar het programma AZ Next bij het Ministerie van Algemene Zaken (AZ). Dit programma heeft ten doel de Werkplekdienstverlening, het Document Management Systeem en de voor deze diensten benodigde IT-infrastructuur volledig te vervangen.

Op 16 november 2020 ontving AZ per post het definitieve advies¹. Dit bestaat uit drie hoofdadviesen. Verder doet het BIT een aantal constatering en benoemt het diverse zorgpunten. In deze brief zet ik uiteen hoe AZ deze punten adresseert en de beschreven risico's mitigeert.

Aanloop naar het BIT advies

AZ is in januari 2019 gestart met het onderzoeken van de mogelijkheden om in het kader van life cycle management, groot onderhoud uit te voeren rond de Werkplekdienstverlening, het Document Management Systeem en de ICT infrastructuur. Allereerst heeft er een brede inventarisatie plaatsgevonden naar (standaard)oplossingsmogelijkheden die door andere departementen worden gebruikt. Vervolgens is onafhankelijk advies aan Gartner gevraagd over de potentiële oplossingsrichting en is bezien in hoeverre deze aan de gebruikerswensen kan voldoen. Tenslotte is de tijd besteed aan het regelen van de benodigde financiering. In februari 2020, vóórdat de daadwerkelijke uitvoering van het programma zou kunnen starten, is contact gezocht met het BIT. In april 2020 is de aanvraag ingediend om het AZ Next programma door het BIT te laten toetsen en het BIT is daarmee in mei 2020 gestart. Mei 2020 was daarmee voor het BIT het peilmoment. Aanvullende documenten die door AZ Next na het peilmoment zijn geformuleerd zijn door het BIT niet in het advies betrokken.

De samenwerking tussen AZ en BIT is goed verlopen.

¹ Raadpleegbaar via www.tweedekamer.nl

De daadwerkelijke uitvoering van AZ Next is aangehouden totdat het definitieve BIT advies is afgegeven en wordt nu verder vorm gegeven met inachtneming van de inhoud van het advies. Overigens heeft het AZ Next programma enige vertraging opgelopen door de COVID-19 pandemie, die maakte dat thuiswerken bij AZ in korte tijd moest worden ingericht, terwijl op kantoor werken voorheen voor 100% de norm was.

Belangrijkste punten van het BIT advies:

Na bestudering van de documentatie van AZ Next en mede op basis van diverse interviews van betrokkenen heeft het BIT een aantal adviezen, constatering en zorgpunten geformuleerd.

Hieronder wordt eerst ingegaan op de drie hoofdadvies, en daarna op de overige zorgpunten en constatering:

Beperk het aantal veiligheidsniveaus tot twee

Het BIT pleit ervoor niet teveel te differentiëren in beveiligingsniveaus. Dit zou het programma en de uiteindelijke IT-omgeving te complex maken. Tevens geeft het BIT aan dat door de manier waarop AZ haar beveiligingsanalyse heeft uitgevoerd, de behoeften van de meest beveiligingskritische gebruikers bepalend zijn voor de uitkomst (een hoog beveiligingsniveau). Zij stelt dat dit belemmerend werkt voor delen van de AZ-organisatie die een lagere beveiligingsbehoefte hebben.

Het advies van het BIT geeft AZ aanleiding om hier nader naar te kijken en om het Nationaal Bureau voor Verbindingsbeveiliging te vragen om hierover te adviseren. Naar de aard van de werkzaamheden van delen van de organisatie van AZ dienen haar informatie en IV systemen beschermd te worden tegen statelijke actoren. AZ verwerkt informatie van verschillende beveiligingsniveau's, variërend van «Openbaar» t/m Staatsgeheim Zeer Geheim (STG ZG). Daarom beschikt AZ over een Staatsgeheime werkplek én een werkplek die geschikt is voor Departementaal Vertrouwelijke (Dep V) informatie. De (verzameling van) informatie die wordt verwerkt op de Dep V werkplek verdient volgens AZ weerbaarheid tegen statelijke actoren. Daar hoort het Basis Beveiligings Niveau 3 (BBN3) bij, dat ervoor zorgt dat statelijke actoren «niet binnen kunnen komen».

Tegelijk wil AZ de diensten, afdelingen en medewerkers die niet of nauwelijks gevoelige informatie verwerken (ongeveer de helft van het ministerie) zo min mogelijk beperken. Deze groep is gebaat bij een meer open werkplek. De enige manier om zowel recht te doen aan de noodzakelijke beveiliging als bepaalde afdelingen daarbij te ontzien, is differentiëren in aangeboden beveiligingsniveau's.

Het NBV, een autoriteit op het vlak van Informatie beveiliging, wordt bij deze keuzes en de uitwerking hiervan nauw betrokken en geeft onafhankelijk advies. Om de onderbouwing verder te versterken voert AZ een Kwetsbaarheidanalyse Spionage (KVAS analyse) uit. Daarnaast worden de diverse implementatie-opties voor het gewenste veiligheidsniveau op haalbaarheid en impact op de primaire en secundaire processen van AZ onderzocht en aan de leden van de Bestuursraad ter besluitvorming voorgelegd. Daarmee wordt op basis van *onderbouwde* scenario's gekozen voor een goed bij AZ passend aantal beveiligingsniveaus.

Ga pas tot inkoop over als de impact en beveiligingskwaliteit akkoord zijn

Het BIT adviseert geen hardware of software aan te schaffen zolang het programma AZ Next nog niet volledig is uitgewerkt. Daarbij doelt het

onder meer op een nog vast te stellen beveiligingsniveau en het nog onvoldoende rekening houden met gebruikerswensen.

Dit advies wordt opgevolgd. Een NBV-advies inzake beveiligingskwaliteit is aangevraagd en in behandeling. Een impactanalyse op de primaire en secundaire processen is gestart, de resultaten ervan worden aan de leden van de Bestuurs Raad van AZ voorgelegd. Eind gebruikers van de ICT en IV systemen worden betrokken om de impact beter te kwantificeren. Pas daarna wordt besloten wat precies voor het gekozen beveiligingsniveau moet worden ingekocht.

Een uitzondering op «het uitstellen van inkoop» betreft de vervanging van IT-componenten die vanwege hun levensduur een continuïteits risico voor het primair proces dreigen te vormen.

Verstevig de programmaorganisatie en maak een goede planning

Het BIT adviseert de aansturing van het programma AZ Next te versterken. De deelprojecten sluiten volgens het BIT onvoldoende op elkaar aan en onderlinge afhankelijkheden worden onvoldoende onderkend.

Dit advies, dat samenhangt met het peilmoment van het BIT in mei 2020, is inmiddels opgevolgd. Er is een overkoepelende planning met financieel overzicht opgesteld, die strak wordt gemonitord, de «Quality Assurance» en Project Management Ondersteuning voor het programma is ingeregeld en de senior stuurgroep op niveau Bestuursraad is ingesteld.

Overige constatering en zorgpunten

Het BIT benoemt in haar advies -in aanvulling op bovenstaande drie hoofdadvisen- nog een aantal zorgpunten en doet nog een aantal constatering:

Recente keuze voor derde beveiligingsniveau verhoogt complexiteit

Een potentieel scenario voor AZ is de (voorlopige) keuze om de «standaard» werkplek op te splitsen in een normaal beveiligingsniveau (BBN2) en een hoog beveiligingsniveau (BBN3). Daarnaast blijft een STG-omgeving gehandhaafd. Het BIT pleit ervoor de standaard werkplek niet te splitsen omdat dit tot hogere complexiteit voor gebruikers leidt.

Het splitsen van de IT-omgeving van AZ in een BBN2 en BBN3 beveiligingsvariant is één van de mogelijke opties. AZ onderzoekt ook andere scenario's op haalbaarheid en impact op de primaire en secundaire processen van AZ. De scenario's worden ter besluitvorming voorgelegd aan de Bestuursraad. Zie verder het eerste hoofdadvis, in het bijzonder de alinea die start met de rol van het NBV, onderaan pagina 2.

Alternatieven zijn niet onderzocht

Het BIT doelt hier voornamelijk op het afnemen van dienstverlening van een SSO. Het niet afnemen van dienstverlening van een SSO was begin 2018 een weloverwogen gezamenlijke beslissing van AZ en de betrokken SSO. Dit was het resultaat van de ervaringen van voorgaande jaren, het betreffende besluit is genomen in de periode *voorafgaand* aan de start van het programma AZ Next. Het opnieuw in overweging nemen van een dergelijke dienst zou de doorlooptijd én complexiteit van het programma aanzienlijk verhogen (punten waar het BIT al voor waarschuwt) en wordt momenteel als niet haalbaar gezien, mede vanwege de personele

consequenties. De inhuizing naar het Binnenhof na de renovatie is een natuurlijk moment om aansluiting bij een SSO te heroverwegen.

Beveiligingskwaliteit is nog niet getoetst

In het kader van het onderzoek naar verschillende scenario's voor beveiligingsvarianten stelt AZ een eigen concept weerbaarheidsnormenkader op. Volgens het BIT staat niet vast of dit normenkader daadwerkelijk de gewenste beveiliging tegen statelijke actoren biedt.

Om dit vast te stellen vraagt AZ het NBV het op te stellen normenkader te beoordelen. Daarbij beantwoordt het de vraag of weerstand tegen statelijke actoren wordt bereikt. Het NBV benoemt tevens de door AZ te mitigeren risico's. Tijdens en na de implementatie van dit normenkader toetst de Auditdienst Rijk (ADR) opzet, bestaan en werking van de genomen maatregelen. Het NBV adviseert daarnaast over het ontwerp van AZ Next. Dit komt tevens tegemoet aan een behoefte van de CTIVD en TIB, twee organisaties die sinds enkele jaren ICT dienstverlening van AZ afnemen en daarbij hoge beveiligingsniveaus behoeven.

Keuze voor BBN3 beïnvloedt doorlooptijd en inkoop negatief

Het BIT stelt dat de keuze voor een voor AZ noodzakelijk beveiligingsniveau de doorlooptijd van de inkoop van hardware en software verlengt. Te meer omdat een toetsing door de AIVD voorzien is. AZ beaamt dat onderzoek naar en de keuze voor een hoog beveiligingsniveau tijd kost. Tijd is echter geen reden het niet te doen. Advies van de AIVD acht AZ daarbij noodzakelijk. Indien nodig past AZ de planning van het programma aan.

Het BIT stelt verder dat de keuze voor BBN3 de inkoop compliceert wat betreft het kunnen stellen van eisen, flexibiliteit van inkoop en kosten. Er is nog geen keuze gemaakt m.b.t. het vereiste veiligheidsniveau. Deze keuze en de implicaties hiervan worden onderzocht, waarbij het NBV nauw wordt betrokken. Een door het BIT aanbevolen maatregel om binnen de leveranciersketen ongewenste elementen te weren is het geheim verklaren van (delen) van het programma, zodat cruciale elementen worden geleverd door vertrouwde fabrikanten en/of leveranciers.

Tot slot twijfelt het BIT aan het streven van AZ om producten die voor haar omgeving met een hoog beveiligingsniveau worden aangeschaft ook binnen het Staatsgeheime netwerk in te kunnen zetten. AZ erkent dat mogelijk niet alle componenten die het aanschaf in de Staatsgeheime omgeving hergebruikt kunnen worden. Hergebruik is dan ook een streven, maar geen vast gegeven.

Onzeker of tijdig wordt voldaan aan behoeften van gebruikers

Het BIT geeft aan dat het programma te weinig rekening houdt met de behoeften van gebruikers. Het risico bestaat dat gebruikers in negatieve zin verrast worden door beperkingen in functionaliteit. Dit betreft zowel de werkplek, het DMS als architectuurkeuzes.

Mede naar aanleiding van deze constatering van het BIT heeft AZ workshops met eindgebruikers georganiseerd en wordt er een klantenraad ingericht. De informatie die dit oplevert over wensen en eisen van gebruikers wordt voorgelegd aan de stuurgroep op Bestuursraad-niveau, waarin het primair proces is vertegenwoordigd. Na goedkeuring worden de resultaten verwerkt en opgenomen in het programma.

Lage planningskwaliteit verhoogt kans op uitloop

Het BIT pleit voor een geformaliseerd en steviger ingericht projectmanagement met bijbehorende overkoepelende planning voor de drie deelprojecten. Het stelt onder meer dat de voortgang van projecten niet goed is vast te stellen, doorlooptijden te optimistisch zijn ingeschat en dat niet bekend is welke inzet vanuit de AZ-organisatie nodig is. Onzekerheden in de planning brengen volgens het BIT een financieringsrisico met zich mee.

Vanwege deze constatering heeft AZ de planning en coördinatie van het programma AZ Next verbeterd. De opdrachtnemer, verantwoordelijk voor het AZ Next programma is benoemd, evenals een onafhankelijke Quality Assurance en een Project Management Officer. Er wordt nauwlettend gestuurd op het behalen van de overkoepelende planning inzake tijd en geld. Voortgangsrapportages zijn verder geprofessionaliseerd. Deze zorgen t.b.v. de stuurgroep voor meer inzicht in de verschillende projecten en onderlinge afhankelijkheden.

Het programma AZ Next is meer dan een technische verbetering. AZ erkent dat de klantorganisatie hier integraal onderdeel van is en benodigd is bij onder meer het (eventueel) aanpassen van werkprocessen, de content migratie, trainingen, etc. De eerder genoemde klantenraad gaat dit adresseren en benodigde acties worden in de planning opgenomen.

Tot slot is AZ zich bewust van de gesignaleerde financieringsrisico's voor het totaal van de benodigde investering en de spreiding van de kosten over de jaren heen. In overleg met het Ministerie van Financiën heeft inmiddels een doorschuif van 2 mln. euro aan middelen van 2020 naar 2021 plaatsgevonden. Binnen het totale project is een risico-opslag voorzien, waarvan de spreiding in de tijd nader wordt bekeken. De financiële beheersing van het programma is inmiddels verbeterd door een Taskforce met vertegenwoordiging uit de afdelingen Financiën en Inkoop.

Tot slot

Ik vertrouw erop dat de acties en voornemens van AZ, zoals geschetst in deze brief, afdoende invulling geven aan het BIT-advies.

De Minister-President,
Minister van Algemene Zaken,
M. Rutte