Bureau ICT-toetsing
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Ministerie van Algemene Zaken
T.a.v. de minister-president, minister van Algemene Zaken, de heer drs. M. Rutte
Postbus 20001
2500 EA Den Haag

Bureau ICT-toetsing

Muzenstraat 95
Den Haag
Postbus 20011
2500 EA Den Haag
www.bureauicttoetsing.nl

Contactpersoon
BIT@rijksoverheid.nl

Kenmerk
2020-0000634883

Uw kenmerk
4124070

Datum	29 oktober 2020
Betreft	Definitief BIT-advies programma AZ-Next

Geachte heer Rutte,

U heeft het Bureau ICT-toetsing (BIT) verzocht een toets uit te voeren op het programma AZ-Next. De opdrachtgever is de secretaris-generaal van het ministerie van Algemene Zaken (AZ). Hieronder vindt u een korte beschrijving van het programma. Daarna geven we de conclusie van de toets, en onze analyse en adviezen. Wij concentreren ons hierbij op de belangrijkste risico's van het programma.

AZ heeft een eigen IT-afdeling met ruim 40 medewerkers die zelf ruim 70 systemen beheren, zowel functioneel als technisch. De gebruikers van de systemen stellen uiteenlopende eisen aan informatiebeveiliging. De infrastructuur kent nu twee niveaus van beveiliging: AZ-Standaard en AZ-Staatsgeheim.

AZ heeft de afgelopen jaren minder onderhoud uitgevoerd, naar eigen zeggen vanwege een mogelijke overdracht van IT-diensten naar SSC-ICT. In 2018 is deze overdracht afgeblazen. AZ-Next moet nu groot onderhoud uitvoeren. Het programma bestaat uit drie sterk met elkaar samenhangende projecten:
- Het infra-project migreert de ICT van het primaire datacenter naar een nieuwe locatie en renoveert de ICT in het secundaire datacenter.
- Het werkplek-project vervangt de 650 werkplekken van AZ. Dit project wil de infrastructuur gebruiken die het infra-project zal opleveren.
- Het DMS-project vervangt het huidige documentmanagementsysteem (DMS) door OpenText. Dit project wil de infrastructuur en werkplekken van beide andere projecten gaan gebruiken.

Het programma wil infrastructurele oplossingen verwerven via zogenaamde mini-competities op basis van de bestaande raamovereenkomsten voor hard- en software. De contracten voor *Firewalls* en het *Document Management Systeem* zijn inmiddels gegund. Mogelijk wil AZ-Next een tweede *Document Management Systeem* verwerven en een contract afsluiten met een *Security Operations Center* (SOC) dat het *Security Information & Event Management* (SIEM) voor AZ kan uitvoeren.

AZ-Next is gestart in januari 2019. De gebruikers gaan volgens de planningen van het werkplek-project en het DMS-project eind 2021 de werkplek en het DMS in gebruik nemen. In de zomer van 2021 wil AZ (tijdelijk) van het Binnenhof naar het Catshuis verhuizen. De IT-dienstverlening moet dan doorlopen.

Volgens uw aanmeldingsbrief is de begroting € 27 miljoen voor de komende 6 jaar. Het ministerie van Financiën financiert hiervan € 14 miljoen.

De BIT-toets is uitgevoerd tussen april en juli 2020. De conclusie van onze toets luidt als volgt:

AZ-Next neemt een aanzienlijk risico door te snel in eigen beheer een nieuwe IT-infrastructuur te realiseren op basis van een complexe beveiligingsarchitectuur. Het programma wil de inkoop van infrastructurele componenten starten, nog voordat de impact van deze architectuur voor AZ is bepaald en zonder dat voldoende zeker is of het resultaat de gebruikersbehoeften kan invullen. Dit kan leiden tot de aanschaf van ongeschikte producten, tot vertraging en extra kosten.

Bovendien kan het ontbreken van een overkoepelende planning en onvoldoende gecoördineerde aansturing op de drie sterk van elkaar afhankelijke projecten leiden tot verdere vertraging.

Wij adviseren AZ-Next eerst de beveiligingsarchitectuur te vereenvoudigen en de impact daarvan af te stemmen met de gebruikersorganisatie. En om pas tot inkoop over te gaan na onafhankelijke toetsing van de architectuur. Ook raden wij aan planmatiger te werk te gaan en hiertoe de programmaorganisatie te verstevigen.

Hieronder lichten wij onze analyse en adviezen toe.

AZ-NEXT NEEMT ONNODIG RISICO'S MET COMPLEXE INFRASTRUCTUUR

Het programma AZ-Next heeft ruim een jaar gewerkt aan het ontwerp van een nieuwe IT-infrastructuur op basis van een complexe beveiligingsarchitectuur. Nu deze architectuur gereed is, wil men snel tot realisatie overgaan en de inkoop opstarten. Wij vinden dat het programma daar nog niet klaar voor is. Er zijn nog te veel onzekerheden over de beveiligingsarchitectuur en de aansluiting op gebruikerswensen. Ook ontbreekt een overkoepelende planning en wordt de aansturing op de drie deelprojecten onvoldoende gecoördineerd.

A. Te veel onzekerheden over complexe beveiligingsarchitectuur

AZ hecht terecht waarde aan een goed beveiligde IT-infrastructuur. Deze moet gebaseerd zijn op een uitgewerkte beveiligingsarchitectuur waarin het niveau van beveiliging is afgestemd op het gebruik en de beveiligingsrisico's. AZ-Next loopt het risico te snel een onnodig complexe beveiligingsarchitectuur met veel nadelen te realiseren. Dit onderbouwen we als volgt:

Noodzaak hoog beveiligingsniveau BBN3 voor AZ-standaard staat niet vast
AZ heeft een Baseline Informatiebeveiliging Overheid (BIO) beveiligingsanalyse uitgevoerd op AZ-Standaard, het deel van de infrastructuur dat gebruikt wordt door het gros van de gebruikers. Binnen de gebruikerspopulatie bestaan zowel gebruikers met hoge beveiligingsbehoeften, zoals het Kerndepartement, als met gebruikelijke beveiligingsbehoeften, zoals de Dienst Publiek Communicatie (DPC) en de Wetenschappelijke Raad voor het Regeringsbeleid (WRR). Bij een BIO-beveiligingsanalyse zijn de behoeften van de meest beveiligingskritische gebruikers bepalend voor de uitkomst. Op basis van de analyse heeft AZ er

daarom voor gekozen geheel AZ-Standaard op een hoger niveau te beveiligen dan in de huidige situatie. AZ-Next hanteert daarvoor het in de BIO gespecificeerde Basisbeveiligingsniveau 3 (BBN3)[1]. Dat beveiligingsniveau is fors hoger dan het binnen de rijksoverheid gebruikelijke BBN2. Het hanteert strenge eisen uit onder meer de NAVO-standaard *NATO Restricted* en vereist volledig preventieve bescherming tegen aanvallen van “statelijke actoren of gelijkwaardige beroeps-criminelen”. BBN3 beperkt gebruikers inherent in mogelijkheden om informatie uit te wisselen met gebruikers op een lager beveiligingsniveau, en is daarnaast ook duur en tijdrovend om te implementeren. AZ heeft, mede gelet op deze forse consequenties, de keuze voor BBN3 te beperkt gemotiveerd.

Recente keuze voor derde beveiligingsniveau verhoogt complexiteit
In juni 2020, in de eindfase van deze toets, is ons mondeling meegedeeld dat het vereiste beveiligingsniveau voor AZ-Standaard wordt gesplitst in BBN2[2] voor DPC en de WRR, en BBN3 voor het Kerndepartement en de onafhankelijke commissies. Het niveau AZ-Staatsgeheim blijft ongewijzigd. Dit betekent drie beveiligings-niveaus in plaats van twee. Dit kan serieuze nadelen hebben die niet zijn onderzocht. Zo gebruiken DPC, WRR en kerndepartement gedeelde systemen (zoals het DMS) en moeten ze informatie kunnen uitwisselen. Het kan betekenen dat gebruikers meerdere computers krijgen waartussen moet worden geschakeld afhankelijk van de informatie die wordt bewerkt.

Alternatieve zijn niet onderzocht
Potentieel aantrekkelijke alternatieven, die de ICT-complexiteit en de kosten kunnen reduceren, zijn niet onderzocht. Dit betreft onder meer het onderbrengen van alle BBN3-informatie in de infrastructuur met beveiligingsniveau AZ-Staatsgeheim, de afname van diensten van shared service organisaties (SSO's) voor een gedeelte van de dienstverlening, en de afname van standaard BBN2-diensten voor uitsluitend DPC en WRR.

Beveiligingskwaliteit is nog niet getoetst
AZ-Next laat, ondanks de hoge ambities die uit de beveiligingsarchitectuur spreken, veel onzekerheid bestaan over de vraag of de gewenste beveiligingswinst wel echt behaald zal worden. In de aanpak missen we namelijk twee belangrijke toetsen die deze zekerheid aanzienlijk kunnen verhogen:

- Onafhankelijke toetsing op de beveiligingsarchitectuur. Die is verplicht volgens de BIO en het eigen AZ-informatiebeveiligingsbeleid. Het is ook de gangbare praktijk om beveiligingszwakheden die over het hoofd zijn gezien zichtbaar te maken.
- De commissies TIB en CTIVD zijn onafhankelijk en eindverantwoordelijk voor hun eigen informatiebeveiliging en werken met informatie van inlichtingen-diensten. Noch de commissies, noch de diensten hebben vastgesteld of laten toetsen in hoeverre de oplossing die AZ-Next wil bieden veilig genoeg is. Wij verwachten dat sommige gemaakte beveiligingskeuzes niet acceptabel zijn voor hen.

[1] NB: AZ-Staatsgeheim is gebaseerd op het Voorschrift Informatiebeveiliging voor Bijzondere Informatie (VIR-BI).
[2] BBN2 maakt een open samenwerking mogelijk met de buitenwereld die niet realiseerbaar is met BBN3. DPC en WRR zijn hiermee geholpen.

Keuze voor BBN3 beïnvloedt doorlooptijd en inkoop negatief
Wij denken dat de keuze voor toepassing van BBN3 een negatieve impact heeft op de doorlooptijd en inkoop die mogelijk vermeden kan worden, om de volgende redenen:

- Toepassing van BBN3 vergt, naar onze inschatting, minimaal 6 maanden meer tijd, zeker als AZ de toetsing door de AIVD wil laten uitvoeren.
- De keuze voor BBN3 compliceert de inkoop. In de raamovereenkomsten kunnen slechts beperkt aanvullende betrouwbaarheidseisen worden gesteld aan leveranciers. En BBN3 beperkt de mogelijkheid om diensten flexibel en tegen lagere kosten in te kopen.
- Het programma neemt aan dat de producten die worden ingezet voor niveau BBN3 ook ingezet kunnen worden voor het niveau AZ-Staatsgeheim. We twijfelen hieraan, omdat de eisen voor AZ-Staatsgeheim hoger liggen. De kans bestaat dat AZ-Next in een later stadium alsnog aparte producten voor AZ-Staatsgeheim moet kopen.

B. Onzeker of tijdig wordt voldaan aan behoeften van gebruikers

De programmateamleden zijn goed op elkaar ingespeeld en voeren een actieve onderlinge dialoog. Maar het programma maakt te weinig concrete afspraken met de gebruikersorganisatie over de eisen en wensen waar de te realiseren werkplek en het DMS aan moeten voldoen. De kans is groot dat een belangrijk deel van de gebruikers in een later stadium in negatieve zin verrast gaat worden door onverwachte beperkingen in de geboden gebruikersfunctionaliteit, waarvoor dan nog oplossingen gevonden moeten worden. Wij leiden dat af uit het volgende:

- Alleen DPC heeft een memo met gebruikerseisen en –wensen opgesteld die getoetst kunnen worden. AZ-Next heeft niet duidelijk gemaakt welke van de van DPC ontvangen eisen en wensen ingevuld kunnen of zullen worden.
- Met geen van de gebruikers is geverifieerd of de gemaakte keuzes in de architectuur en het pakket van eisen voor de mini-competities tot een voor hen acceptabele oplossing zullen leiden.
- Het is onbekend hoeveel maatwerk moet worden gerealiseerd in het DMS. Een pakket van eisen en wensen waarmee kan worden vastgesteld waar maatwerk nodig is en wat met de standaardfunctionaliteit kan worden afgedekt ontbreekt. De leverancier van het DMS heeft in oktober 2019 gebruikers geïnterviewd. Dit heeft slechts een globaal beeld opgeleverd van gebruikerseisen en roept nieuwe vragen op bij AZ, die nog niet beantwoord zijn. Dat kan veel impact hebben op de implementatieplanning.

C. Lage planningskwaliteit verhoogt kans op uitloop

AZ is een klein ministerie dat een groot programma uitvoert. Een programma van deze omvang vergt meer geformaliseerd en steviger ingericht projectmanagement en een goede planning. De aansturing op de drie sterk van elkaar afhankelijke deelprojecten wordt nu te weinig gecoördineerd. De planning van het programma schiet daardoor tekort en het ontbreekt aan inzicht in de voortgang. Dit leiden wij af uit het volgende:

- Een overkoepelende programmaplanning, waarin de verwachte opleverdatum van eind 2021 wordt onderbouwd, ontbreekt. De infra- en DMS-projecten hebben bovendien beide hun eigen planningen. Het werkplek-project heeft er zelfs twee. Ook de architect heeft een eigen planning. De planningen zijn verouderd en onderling inconsistent. De DMS- en werkplekprojecten hebben bijvoorbeeld de reeds opgetreden vertraging van 3 maanden in het infra-

project niet vertaald naar hun eigen planningen, terwijl die vertraging wel rechtstreeks doorwerkt.
- De voortgang in de drie projecten is niet goed vast te stellen. Voortgangsrapportages geven niet aan hoeveel vertraging verwacht wordt en of activiteiten tijdig zijn afgerond. De rapportages worden niet besproken in een stuurgroep onder voorzitterschap van de opdrachtgever.
- Een aantal doorlooptijden is optimistisch ingeschat. Dit geldt voor doorlooptijden van aan beveiliging gerelateerde activiteiten, voor verwachte levertijden en voor doorlooptijden van het inrichten van meerdere ontwikkel-, test- en acceptatieomgevingen. Daarnaast verwacht het programma dat de standaardinstellingen van de kant-en-klare (“turnkey”) oplossingen van leveranciers nauwelijks aangepast hoeven te worden op het gebruik bij AZ. Wij denken dat hiervoor te weinig tijd wordt ingeruimd.
- De benodigde inzet vanuit de AZ-organisatie ontbreekt in de planning. De gebruikers verwachten vooral “een nieuwe computer” maar weten niet dat ze met hulp van het programma ook nieuwe werkprocessen moeten ontwikkelen, rollen en verantwoordelijkheden moeten aanscherpen, documenten moeten migreren, en tijd moeten investeren in testen en trainingen. Het risico bestaat dat onderdelen van AZ hier straks te weinig tijd voor kunnen vrijmaken.

De onzekerheden in de planning brengen een financieringsrisico met zich mee. Dit betreft niet alleen de totale omvang van de benodigde investering, maar ook de spreiding van uitgaven over de jaren heen. Zo komt de meerjarenraming van FEZ de komende drie jaar € 4 miljoen lager uit dan die van het programma.

ADVIES: VEREENVOUDIG DE BEVEILIGINGSARCHITECTUUR EN VERSTEVIG DE PROGRAMMAORGANISATIE

De risico’s van de complexe architectuur kunnen worden gereduceerd. Wij adviseren AZ-Next de beveiligingsarchitectuur minder complex te maken. Wij verwachten dat twee beveiligingsniveaus volstaan. De consequenties van de door AZ gekozen beveiligingsarchitectuur moeten vervolgens in beeld worden gebracht. Laat daarna de beveiligingsarchitectuur onafhankelijk toetsen en ga pas tot inkoop over als de resultaten hiervan verwerkt zijn. Om dit in goede banen te leiden moet AZ-Next planmatiger te werk gaan en de programmaorganisatie verstevigen. Onze adviezen werken we hieronder in meer detail uit.

1. Beperk het aantal beveiligingsniveaus tot twee

Wij adviseren AZ-Next de keuze om binnen de AZ-Standaard-infrastructuur te differentiëren tussen BBN2 en BBN3 te heroverwegen, en om te kiezen voor één beveiligingsniveau voor AZ-Standaard, naast AZ-Staatsgeheim. Wij verwachten dat AZ het meest gediend is met een beveiligingsniveau dat boven BBN2 ligt maar onder BBN3. AZ-Next kan dit niveau specificeren op basis van bijvoorbeeld een Kwetsbaarheidsanalyse Spionage van de AIVD, waarin tevens wordt gekeken naar de impact op gebruikers, kosten en doorlooptijd. Eventueel kan informatie waarvoor bescherming minimaal op niveau BBN3 noodzakelijk is, ondergebracht worden in het AZ-Staatsgeheime netwerk. Dit leidt tot een minder complexe en uiteindelijk goedkopere architectuur. Wij verwachten dat daarmee op termijn ook, als meer rijksbrede, gestandaardiseerde voorzieningen voor werkplekken met een

verhoogd beveiligingsniveau beschikbaar komen, een overgang naar een shared service organisatie binnen bereik komt.

2. Ga pas tot inkoop over als impact en beveiligingskwaliteit akkoord zijn

Wij adviseren AZ-Next pas tot inkoop over te gaan als het de architectuur onafhankelijk heeft laten toetsen, en de consequenties voor gebruikers, kosten en doorlooptijd bepaald en afgestemd zijn. Dan kan AZ bovendien een wijze van inkopen kiezen die beter past bij de gekozen beveiligingsarchitectuur.

- Als AZ-Next de keuze voor BBN3 handhaaft, adviseren wij na toetsing door de AIVD de inkoop zodanig vorm te geven dat in de offerteaanvraag extra eisen kunnen worden gesteld aan de betrouwbaarheid van de leveranciers (zoals het ministerie van Defensie dat doet via zijn Algemene Beveiligingseisen Defensieopdrachten).
- Komt AZ-Next uit op één niveau BBN2, dan is de AIVD-toetsing niet nodig. AZ kan dan een SSO benaderen óf een mini-competitie starten bij mantelpartijen.

3. Verstevig de programmaorganisatie en maak een goede planning

Om het programma beter te beheersen en bovenstaande in goede banen te leiden, adviseren we het volgende:

- Wijs een programmamanager aan die verantwoordelijkheid neemt voor het eindresultaat van het programma AZ-Next. Laat de programmamanager een integrale planning opstellen met heldere mijlpalen en laat hem periodiek verantwoording afleggen over de voortgang.
- Start met de bijeenkomsten van de in de programmabeschrijving beschreven senior stuurgroep, onder voorzitterschap van de opdrachtgever.
- Laat gebruikerseisen en –wensen in de stuurgroep accorderen, en neem besluiten over de scope op basis van impact-analyses in aanwezigheid van een senior gebruiker die optreedt namens alle gebruikers.
- Verstevig de financiële beheersing. Laat het programma een meerjaren-begroting opstellen en afstemmen met FEZ. Zorg voor adequate afspraken over financiering per jaar en richt een rapportage in waarin de werkelijke kosten beoordeeld kunnen worden ten opzichte van de afspraken met FEZ.
- Maak vaart met het aanstellen van een quality assurance-functionaris zoals voorzien in de programmabeschrijving.

* * *

Tot slot danken wij alle geïnterviewden voor hun medewerking en openheid. Wij hopen dat wij met dit advies een bijdrage kunnen leveren aan het beheerst uitvoeren van AZ-Next.

Met de meeste hoogachting,
Namens het Bureau ICT-toetsing,

Sander van Amerongen
wnd. Hoofd BIT