

4.2 Informatiseringsbeleid Rijk

2011 was het jaar van de bewustwording van kwetsbaarheid. Zo herinnert iedereen zich de hack bij Diginotar en de lekke websites in 'Lektobor'. De rijksoverheid ondernam verschillende acties om informatie beter te beveiligen. Ook nam de rijksoverheid maatregelen rondom de bescherming van privacy, zoals opgenomen in de kabinetsreactie op het WRR-rapport iOverheid. Ook zijn in 2011 de cloud strategie en de I-strategie tot stand gekomen en is het Rijks ICT-dashboard gelanceerd.

4.2.1 Rapportage grote en risicovolle ICT-projecten

Elk jaar rapporteert het Rijk over grote ICT-projecten met een meerjarig budget van meer dan twintig miljoen euro en over kleinere risicovolle ICT-projecten. De lijst van deze projecten komt tot stand op basis van een uniform selectiemechanisme voor het Rijk. Nieuw is dat vermeld wordt of een project privacygevoelige gegevens bevat of dat er meer data aan zijn gekoppeld. Dit heeft het kabinet besloten (26 643, nr. 216) naar aanleiding van het WRR-rapport iOverheid. Net als vorig jaar zijn ook de projecten van de publiekrechtelijke zelfstandige bestuursorganen (zbo's) in het selectiesysteem opgenomen. De rapportagegegevens uit de bijlage grote ICT-projecten zijn ook terug te vinden op het Rijks ICT-dashboard (www.rijksictdashboard.nl).

Naar aanleiding van de motie Van der Burg c.s. (33 000 VII nr. 15) is bij de projecten in de rapportage nu ook informatie opgenomen over de in het projectplan vermelde (maatschappelijke) relevantie: kwalitatieve en/of kwantitatieve baten en de doelen in het regeerakkoord waaraan het project bijdraagt. Verder is de in het projectplan vermelde informatie over de verwachte kosten van de fase van beheer opgenomen in de rapportage. Ten slotte geeft het projectplan antwoord op de vraag of de aard van de vermelde contracten wel of niet is gewijzigd. Indien dit laatste het geval is, wordt toegelicht wat er is gewijzigd. De bovenstaande informatie is in de rapportage opgenomen onder het veld projectomschrijving van de projecten.

Rapportagegegevens

Eind 2011 werden 49 grote en risicovolle ICT-projecten uitgevoerd bij het Rijk. De totale meerjarig geraamde kosten van deze ICT-projecten bedragen € 2.409 miljoen. Deze rapportage omvat twaalf nieuwe projecten ten opzichte van de rapportage over 2010. De meerjarige kostenschattingen van de 26 projecten die al in 2010 liepen en die ook in 2012 doorlopen namen eind 2011 netto toe met 1,7% ten opzichte van de vorige jaarrapportage. De Tweede Kamer is al ingelicht over de grootste toenames die aan deze stijging ten grondslag liggen. Alle herijkingen zijn met toelichting opgenomen in de bijlage. Ter vergelijking met de vorige jaarrapportage: de meerjarige kostenschattingen van de 23 projecten die al in 2009 liepen en die in 2011 doorliepen namen eind 2010 toe met 11,4%.

Beheersing ICT-projecten

Net als voorgaande jaren hebben de ministeries in deze jaar-rapportage per project de meerjarige kosten en doorlooptijd vermeld. Ook geven zij aan of de projectplannen volgens de afspraken zijn opgesteld en of er externe kwaliteitstoetsen zijn uitgevoerd. Deze afspraken gaan over de inhoud van de projectplannen (zoals doelstelling, besturing, businesscases, planning, beheersing en informatievoorziening) en over de aanpak van externe kwaliteitstoetsen (zoals Gateway Reviews, ICT-haalbaarheidstoetsen, externe en interne audits). Deze jaarrapportage bevat ook informatie over elf projecten die in 2011 zijn afgerond, inclusief de gerealiseerde uitgaven.

Bevindingen auditdiensten

De rapporterende ministeries en publiekrechtelijke zbo's hebben hun rapportage voorzien van een nota van bevindingen van de eigen audit- of accountantsdienst over het totstandkomingsproces. Het beoordeelde proces heeft vooral betrekking op de volledige en juiste identificatie, registratie en selectie van de beoogde projecten en de tijdige oplevering (en publicatie) van de gevraagde gegevens daarover. Uit de nota's van bevindingen blijkt dat dit proces steeds professioneler wordt uitgevoerd. De aanbevelingen gaan onder andere in op een verdere professionalisering van het projectportfoliomangement, de documentatie van het proces en een beter beheersbare aansluiting op de financiële administraties. Deze aanbevelingen zullen worden meegenomen in de opmaat naar de volgende jaarrapportage.

4.2.2 Gateway Review

De Nederlandse rijksoverheid gebruikt de reviewmethode OGC Gateway™ om meer grip te krijgen op risicovolle programma's en projecten. Met deze methode kunnen ministeries per mijlpaal toetsen of een programma of project klaar is voor de volgende fase. Collega-ervaringsdeskundigen (peers) voeren deze compacte reviews in één werkweek uit.

In 2011 zijn 36 Gateway Reviews uitgevoerd. Daarmee is de resultaatafspraken van 35 Gateway Reviews in 2011 gehaald. Afgelopen jaar zijn meer dan vijftig collega's opgeleid tot reviewer. De totale pool van opgeleide Gateway Reviewers bestaat nu uit ruim 250 personen. De reviewers werken voornamelijk in dienst van de (rijks)overheid.

Bureau Gateway introduceerde in 2011 twee nieuwe Gateway Reviewtypes: de *Starting Gate* en de *Health Check*. De *Starting Gate* is ontwikkeld naar aanleiding van de wens om de uitgangspunten voor de start van een programma of project te toetsen. De *Health Check* kan op elk moment worden uitgevoerd. In de *Health Check* wordt bekeken hoe het functioneren van een organisatie of keten van organisaties kan worden verbeterd.

In 2011 werkte Bureau Gateway samen met de grote vier gemeenten aan een pilot met de Gateway Reviewmethode. De

gemeentesecretarissen van de vier grote gemeenten Amsterdam, Den Haag, Utrecht en Rotterdam zijn van plan een vervolg te geven aan hun Gateway-pilot.

4.2.3 De Digitale Werkomgeving Rijksdienst (DWR)

De Digitale Werkomgeving Rijksdienst (DWR) wil de rijksmedewerker op elk moment, elke plaats en elk apparaat op een veilige wijze toegang geven tot de digitale informatie en applicaties die hij voor zijn werk nodig heeft. Hiervoor is een aantal instrumenten ontwikkeld. De generieke kantoorautomatisering DWR-cliënt biedt kantoorapplicaties zoals tekstverwerking en presentaties. Het Rijksportaal is een intranet voor alle ministeries. Met DWR-SWF (samenwerkingsfunctionaliteit) kunnen rijksmedewerkers digitaal samenwerken. Deze functionaliteit omvat onder meer een wiki, blog, chatapplicatie en mogelijkheden om bestanden te delen.

In 2011 zijn er enkele duizenden DWR-cliëntwerkplekken bijgekomen. Daarmee komt het totaal op ruim 15.000; het streven voor eind 2012 is 20.000 werkplekken. In 2011 zijn in totaal zes ministeries aangesloten op het Rijksportaal. Dat is vier minder dan voorzien. Het Ministerie van Economische Zaken, Landbouw en Innovatie is na technische problemen bij DWR begin 2012 alsnog aangesloten. Ook het Ministerie van Volksgezondheid, Welzijn en Sport sluit begin 2012 alsnog aan. Het Ministerie van Infrastructuur en Milieu en het Ministerie van Veiligheid en Justitie hebben nog geen datum afgegeven waarop zij aansluiten op het Rijksportaal.

4.2.4 Rijkspas

Rijkspas heeft tot doel een veilige, flexibele, effectieve en efficiënt geregelde fysieke en digitale toegang tot de rijksoverheid te bewerkstelligen. Rijkspas wil de flexibiliteit van medewerkers vergroten, de beveiliging van rijksobjecten standaardiseren en – waar nodig – op een hoger plan brengen. De Rijkspas heeft drie niveaus:

- departementale fysieke toegang;
- interdepartementale fysieke toegang;
- logische toegang (toegang tot informatie en systemen).

Uit medio 2011 hebben medewerkers van negen van de elf ministeries een Rijkspas als vervanger van de oude departementale toegangspas. Veiligheid en Justitie volgt in het voorjaar van 2012, Defensie in 2015. Daarbij wordt de voor Defensie vereiste functionaliteit meegenomen. Daarnaast beschikken ook enkele Hoge Colleges van Staat, waaronder de Tweede Kamer, over de Rijkspas. Medewerkers van de kerndepartementen met een Rijkspas kregen in 2011 toegang tot vijf ministeries die gebruikmaken van de Rijkspas. In 2012 gaan ook de andere ministeries dat doen voor medewerkers binnen de Haagse beleidskern. De mogelijkheid van logische toegang (de toegang tot de digitale werkplek) met de Rijkspas kwam voorzichtiger op gang bij enkele departementen, uitvoeringsorganisaties en Hoge Colleges van Staat, waaronder

de Tweede Kamer. In het Rijkspas Werkplan 2012 staat het voornemen om de departementale en interdepartementale fysieke toegang te voltooien binnen de rijksdienst, ook buiten de Haagse beleidskern.

4.2.5 Archiefachterstanden

In 2009 heeft het kabinet vastgesteld dat er tussen 1976 en 2005 circa achthonderd strekkende kilometers archiefachterstanden zijn ontstaan, waarvan circa driehonderd kilometers intensief moeten worden bewerkt. Per 1 januari 2011 is de batenlastendienst Doc-Direkt gestart om samen met het Nationaal Archief deze archiefachterstanden in tien jaar weg te werken. Hiervoor wordt de capaciteit van Doc-Direkt in deze periode uitgebreid met 160 fte en die van het Nationaal Archief met vijftien fte.

Doc-Direkt heeft in 2011 8,2 kilometers archiefachterstand ingehaald. De streefwaarde is een gemiddelde van dertig kilometer per jaar. Doc-Direkt heeft een langere aanloopfase nodig gehad om tot volledige productie te komen, onder meer omdat het aanbod vanuit de ministeries achterbleef, de archieven intensievere bewerking vergden en er nog onafgeronde projecten lagen van de voorlopers van Doc-Direkt.

Om vast te stellen in hoeverre de oorspronkelijke schattingen van de achterstand kloppen en na te gaan of de vernieuwde selectiemethode goed en effectief is, vindt een tussentijdse evaluatie plaats, die kan leiden tot herijking van de benodigde capaciteit (29362, nr. 156).

4.2.6 Personeel en kwaliteit

De pool voor ICT-projectmanagement die opgericht is voor het hele Rijk, I-Interim Rijk, is in 2011 gegroeid tot veertig fte's. I-Interim Rijk vermindert niet alleen de externe ICT-inhuur. De pool is vooral ingericht om cruciale projectmanagementposities met eigen deskundigheid in te kunnen vullen en tegelijk te borgen dat die deskundigheid wordt ontwikkeld en gedeeld.

Het curriculum voor CIO-adviseurs is in samenwerking met de Rijksacademie voor Financiën, Economie en Bedrijfsvoering in 2011 voortgezet. In 2011 hebben 44 adviseurs het curriculum afgerond. Daarnaast zijn aansluitend op het nieuwe functiegebouw voor de rijksdienst cursussen georganiseerd voor tien opdrachtgevers van ICT-projecten.

4.2.7 Beschermen van privacy en informatiebeveiliging

Beschermen van privacy

Naar aanleiding van het rapport iOverheid van de Wetenschappelijke Raad voor het Regeringsbeleid besloot het kabinet om de maatregelen om grote ICT-projecten te beheersen uit te breiden met maatregelen om de privacy te beschermen. Zo moet in een projectplan vanaf nu beargumenteerd worden aangegeven of een privacy-effectbeoordeling nodig is. De

opdrachtgever en de departementale CIO houden hiermee ook rekening bij het opstellen van het risicoprofiel van het project. Dat risicoprofiel is medebepalend voor de vraag of het project wordt gerapporteerd in de Jaarrapportage Bedrijfsvoering Rijk.

Informatiebeveiliging

De hack bij DigiNotar veroorzaakte een crisis. Het vertrouwen in de door DigiNotar uitgegeven certificaten werd opgezegd. Microsoft en Firefox plaatsten DigiNotar op de lijst met onbetrouwbare leveranciers van certificaten. Hierdoor waren de bezitters van door DigiNotar uitgegeven certificaten genoodzaakt over te stappen op certificaten van andere leveranciers. Voor de zogeheten SSL-certificaten (Secure Sockets Layer) die in websites worden toegepast, moest deze vervanging zo snel mogelijk plaatsvinden.

Om een tweede DigiNotar-crisis te voorkomen, zijn verschillende maatregelen getroffen of voorbereid. Het gaat om preventieve maatregelen ter voorkoming van een dergelijke crisis, maar ook om maatregelen om het probleem sneller op te lossen. Daarbij kan worden gedacht aan acties, waardoor de afhankelijkheid van één leverancier wordt beperkt.

Voor de rijksdienst is in 2011 gewerkt aan de normenkaders van de Baseline Informatiebeveiliging Rijk (BIR). Deze baseline gaat gelden voor alle onderdelen van de rijksdienst en vervangt vijf interdepartementale normenkaders en de individuele baselines van de rijksdienst. Waar nodig kunnen departementen en diensten extra normen aan de BIR toevoegen, afgestemd op hun specifieke beveiligingseisen.

Eind 2011 is een verkenning uitgevoerd naar de inrichting van één ICT-beveiligingsfunctie die een geharmoniseerd ICT-beveiligingsbeleid voor het hele Rijk gaat uitvoeren. Daarbinnen zijn overigens wel verschillende beveiligingsniveaus mogelijk. De verkenning geeft inzicht in de wijze waarop de informatiebeveiligingsfunctie binnen de Rijksdienst is georganiseerd. Maar ook inzicht in welke behoeften er nog zijn en welke nieuwe behoeften ontstaan als gevolg van het inrichten van de compacte Rijksdienst en één ICT-infrastructuur.

In het algemeen overleg van 10 april jongstleden over cyber security is toegezegd om de Tweede Kamer te informeren over de inzet van hogescholen en universiteiten bij zogenaamde penetratietesten (hacktesten). Het is te kort dag om u hierover nu reeds te informeren, dit komt in de volgende rapportage. Dit geldt ook voor de uitkomsten van controles door OPTA en Policy Authority bij de certificatenleveranciers.

4.2.8 Samenwerking met de markt en sourcing

Samenwerking met de markt

In samenwerking met ICT-Office is in 2011 een convenant opgesteld ter bevordering van de samenwerking met de ICT-markt, dat 26 januari 2012 is ondertekend. Dit convenant is een herijking van de Gemeenschappelijke verklaring uit 2007,

aangevuld met nieuwe afspraken. Nieuw is de inzet van de ICT-Marktspiegel (in een vroeg stadium van een project precompetitief overleg met de ICT-markt), implementatie van Publiek Private Samenwerkingsvarianten, talentbehoud en ontwikkeling van personeel. Waar wenselijk of nodig worden ook andere organisaties (zoals MKB-Nederland, CIO Platform, Platform voor de InformatieSamenleving, etcetera) betrokken bij de verschillende onderdelen van het convenant.

Sourcing

Het Rijk ontwikkelde in 2011 een afwegingskader voor generieke ICT om te bepalen wat en onder welke voorwaarden er in eigen huis wordt gedaan en waar de markt in beeld komt. Kostenafwegingen spelen daarbij een rol, maar ook risicoafwegingen en de wens om de ICT-verboddeling van de I-infrastructuur stapsgewijs te verminderen. Het afwegingskader wordt vanaf 2012 gebruikt.

4.2.9 Webrichtlijnen

In november 2011 is een sanering aangekondigd (26643 nr. 215) van de websites die onder verantwoordelijkheid van de Rijksoverheid vallen. Deze sanering heeft tot doel alle rijksoverheidswebsites aan de webrichtlijnen te laten voldoen vóór 1 januari 2013.

De eerste fase van de saneringsoperatie is bijna afgerond. Dit betrof de inventarisatie van de websites waarvoor de rijksoverheid verantwoordelijk is, met inbegrip van die van de zbo's. Het gaat volgens opgave van de departementen om bijna 1.000 websites in 2012. Van deze websites zijn er 60 getoetst op het voldoen aan de webrichtlijnen. Van de getoetste websites voldoet het merendeel van de websites van de rijksoverheid niet aan de webrichtlijnen.

De tweede fase van de saneringsoperatie is gaande. Dit betreft een indeling van de websites van de Rijksoverheid in drie categorieën:

- opheffing van websites die over hun houdbaarheidsdatum heen zijn;
- integratie in één van de drie platforms: rijksoverheid, Rijksportaal of overheid.nl, of
- zelfstandig voortbestaan, al of niet geclusterd met andere websites (onder voorwaarde dat de overblijvende sites volledig voldoen aan de webrichtlijnen).

In het Algemeen Overleg van 1 maart 2012 is afgesproken dat de Tweede Kamer na de zomer over de voortgang wordt geïnformeerd.

4.2.10 I-strategie en cloud strategie

I-strategie

In november 2011 presenteerde de minister van BZK namens het kabinet de Informatiseringsstrategie (I-strategie) aan de Tweede Kamer (26643, nr. 216). Deze I-strategie wordt uitgevoerd in de

periode 2012-2015. Met de I-strategie voor het Rijk wil het kabinet de ICT van de rijksoverheid verbeteren. Het streefbeeld van de I-strategie krijgt handen en voeten in de vorm van deze ambitie:

- een meer samenhangende informatie-infrastructuur;
- een platform voor tijd-, plaats- en apparaatonafhankelijk werken;
- beheersing van grote en risicovolle projecten.

Er zijn zeven thema's gedefinieerd om dit streefbeeld te realiseren:

- aanbodstructurering;
- sourcing;
- sturings- en verantwoordingsinstrumenten;
- I-infrastructuur voor de rijksambtenaar;
- personeel en kwaliteit;
- vertrouwen en beveiliging van informatie;
- samenwerking met de markt.

In de I-strategie komen drie lijnen samen: de uitwerking en uitvoering van het onderdeel informatisering uit het uitvoeringsprogramma Compacte Rijksdienst, doorontwikkeling van bestaand beleid en aanvullingen daarop.

Cloud strategie

In 2012 is de cloud strategie (26643, nr. 179) aan de Tweede Kamer aangeboden als reactie op de motie Van der Burg. De implementatie van deze strategie is verder geïntegreerd in de I-strategie die in november 2011 aan de Tweede Kamer is verzonden.