Het Bericht

WWW.RATHENAU.NL • 2013, nummer 6

Rathenau Instituut

Voer haalbaarheidstoets op ICT-projecten in

Beleidsmakers overschatten de mogelijkheden van ICT, blijkt uit de studie voor het Europees Parlement *Security of eGovernment Systems*. Het goed functioneren van ICT-systemen vraagt niet alleen om betere systeembeveiliging en privacybescherming, maar ook om scherpere keuzes in politieke doelstellingen. Die moeten daarom in de ontwerpfase getoetst worden op hun haalbaarheid.

Deze aanbeveling volgt uit een onderzoek voor het Europees Parlement van het Rathenau Instituut en zijn Europese zusterorganisaties DBT en ITAS naar politieke aandachtspunten rond digitalisering van overheidsdiensten. Ze onderzochten drie cases: digitale aanbestedingsprocedures, elektronische patiëntendossiers en het biometrisch paspoort. De conclusies zijn ook relevant voor de besluitvorming over Nederlandse ICT-projecten.

Digitalisering van administraties en online dienstverlening kunnen leiden tot kostenbesparing voor de overheid en groter gemak voor burgers. Daarvoor is het wel nodig dat de systeembeveiliging verbetert en dat er meer aandacht uitgaat naar privacybescherming.

Daarnaast zijn beleidsmakers vaak te ambitieus als het om ICT-projecten gaat. Zo wil de EU digitale aanbestedingen verplicht stellen vanaf 2016. Dat lijkt te hoog gegrepen: op dit moment verloopt slechts vijf procent van de procedures digitaal, en het is de vraag of volledige digitalisering voldoende betrouwbaar is. Ook bij de invoering van het biometrisch paspoort zijn de technische implicaties ervan onderschat. EU-standaarden voor de kwaliteit van de biometrische gegevens ontbreken, waardoor het systeem niet naar behoren functioneert.

Een haalbaarheidstoets in de ontwerpfase van ICT-projecten moet uitwijzen of de diverse ontwerpeisen, zoals systeembeveiliging, gebruiksgemak en interoperabiliteit, wel verenigbaar zijn. Verschillende systeemvarianten, met elk een andere invulling van de ontwerpeisen, moeten tegen elkaar worden afgewogen. Dit dwingt tot een kritische reflectie op het eigenlijke doel dat het ICT-systeem moet dienen en gaat verder dan de huidige ‘Privacy Impact Assessments’ en ‘Gateway Reviews’.

Vanwege het grote maatschappelijke belang van ICT-projecten, zou de haalbaarheidstoets verplicht moeten worden. Voor de uitvoering ervan kan gedacht worden aan een onafhankelijke instantie als het College Bescherming Persoonsgegevens of aan een MER(milieueffectenrapportage)-achtige constructie. Van belang is dat onafhankelijke deskundigen en belanghebbenden bij de toets worden betrokken en dat de resultaten openbaar worden gemaakt. Kamerleden moeten inzicht krijgen in de uitkomsten en de te maken afwegingen.

Het Rathenau Instituut bestudeert het wetenschapssysteem en de maatschappelijke effecten van nieuwe technologieën en ondersteunt het maatschappelijk debat en de politieke oordeelsvorming hierover.

AANBEVELINGEN

- **Haalbaarheidstoets ICT-projecten**
  Om te hoge politieke ambities rond ICT-projecten te voorkomen, dient kritisch naar de ontwerpeisen en politieke doelstellingen te worden gekeken. De overheid moet in de ontwerpfase de haalbaarheid van ICT-beloftes door onafhankelijke experts en stakeholders laten onderzoeken. Dit maakt vooraf duidelijk of de ontwerpeisen wel verenigbaar zijn, en stelt beleidsmakers in staat doelstellingen tijdig bij te stellen.

- **Minimum beveiligingsniveau**
  Om veilig gebruik van ICT-systemen te bevorderen, moeten ICT-systemen aan een minimum beveiligingsniveau voldoen. Denk op korte termijn aan de verplichte toepassing van een standaardpakket aan beveiligingsprotocollen en -maatregelen door systeembeheerders. Op langere termijn is isolatie van systeemkritische componenten nodig, zodat die bijvoorbeeld niet steeds in verbinding staan met internet.

- **Privacy by Design**
  Opslag en verwerking van persoonsgegevens maakt burgers kwetsbaar. Privacygevoelige informatie verdient hogere bescherming, zowel in juridisch als in technologisch opzicht. De overheid moet meer gebruik maken van bestaande technieken om data te minimaliseren (‘Privacy by Design’). Zo geven ‘attribute-based credentials’ alleen de strikt noodzakelijke informatie door. Daarnaast dient Privacy by Design gestimuleerd te worden door de opzet van een kennisbank met praktijkvoorbeelden en mogelijke systeemarchitecturen, al dan niet in Europees verband.

Overheid & ICT: lessen uit Europa

***Security of eGovernment Systems,* een nieuwe studie voor het Europees Parlement naar het gebruik van grootschalige ICT-systemen, maakt duidelijk dat politici niet alleen sterker moeten inzetten op systeembeveiliging en privacybescherming, maar ook op meer realiteitszin in de besluitvorming rond ICT-projecten. Dit vraagt om meer dan 'Privacy Impact Assessments' en 'Gateway Reviews'. Het betekent: standaard onderzoek doen naar de haalbaarheid van ICT-beloftes.**

Biometrisch paspoort
Bij de EU-brede invoering van het biometrisch paspoort zijn de technologische consequenties ervan structureel onderschat. De verwachting dat het ePaspoort de grenscontrole sterk zou verbeteren, kan daardoor niet worden waargemaakt. Zo ontbreken EU-brede standaarden voor de kwaliteit van pasfoto's en vingerafdrukken. Te vaak hebben EU-lidstaten gekozen voor snelle, gebruiksvriendelijke procedures, ten koste van de kwaliteit van de biometrische gegevens. Dit leidt tot hogere foutmarges bij grenscontroles. De in paspoorten opgenomen vingerafdrukken blijken in praktijk bovendien moeilijk bruikbaar, omdat niet alle lidstaten hun beveiligingssleutels willen uitwisselen. Als gevolg hiervan functioneert het huidige systeem gebrekkig.

Daarnaast besloot een aantal lidstaten, waaronder Nederland, de verzamelde data ook te gebruiken voor opsporing en terrorismebestrijding. Het idee dat dat in één moeite door zou kunnen, geeft blijk van onvoldoende inzicht in technologische vereisten. De huidige kwaliteit van de afgenomen gegevens voor het biometrisch paspoort is namelijk te laag voor opsporingsdoeleinden.

Rechtsbescherming onvoldoende
Burgers hebben momenteel te weinig juridische middelen om zich tegen systeemfouten te verweren. Een betere afstemming van de privacywetgeving in EU-verband is hiervoor noodzakelijk. Daarnaast moet de overheid standaard 'Privacy by Design' in haar ICT-systemen toepassen. Denk hierbij aan minimalisatietechnieken (waardoor alleen data verstrekt worden die relevant zijn voor een specifiek doel) of aan technieken die voorkomen dat data uit geanonimiseerde bestanden door 'data mining' alsnog tot personen te herleiden zijn. Een voorbeeld is 'attribute based credentials' waarbij slechts onderdelen van de identiteit van een persoon worden uitgewisseld (zoals 'ouder dan 18' of 'nationaliteit is Nederlands'). Nu wordt vaak om volledige identiteitsgegevens gevraagd. 'Privacy by Design' kan sterk worden gestimuleerd door de opzet van een (Europese) kennisbank.

Digitaal aanbesteden
Ook bedrijven moeten erop kunnen rekenen dat bedrijfsgevoelige informatie niet op straat komt te liggen. De EU wil in 2016 alle aanbestedingen verplicht digitaliseren. Opnieuw een voorbeeld van grote politieke ambities. Het is onduidelijk of volledige digitalisering voldoende betrouwbaar is, terwijl aanvallen op netwerken steeds ingenieuzer worden. Diverse organisaties, waaronder de NAVO, hebben daarom besloten om met papieren eindcontracten te blijven werken. Het is dus de vraag of volledige digitalisering altijd de beste oplossing is.

SAMENVATTING

***eGovernment* wordt als een belangrijk middel gezien in de modernisering van de overheid. Om het vertrouwen van burgers in digitale overheidsdiensten niet te beschamen, dient de privacy beter beschermd te worden en zou het algehele niveau van systeembeveiliging moeten stijgen. Dit blijkt uit de studie *Security of eGovernment Systems*, uitgevoerd in opdracht van het Europees Parlement.**

De studie richt zich op de complexe samenhang tussen systeemontwerp, beleidsdoelen en gebruiksrisico's. De verschillende eisen die er aan een ICT-systeem worden gesteld kunnen onderling botsen. Dit vraagt om een zorgvuldige weging van het doel dat een systeem moet dienen, de data die daarvoor nodig zijn – en welke data dus *niet* – en de vereiste mate van systeembeveiliging, privacybescherming, gebruiksgemak en interoperabiliteit (uitwisselbaarheid van gegevens). Uit de studie blijkt dat deze weging nu onvoldoende gebeurt.

Weging van ontwerpeisen en beleidsdoelen – en daarmee: de keuze tussen systeemvarianten – vereist meer dan de uitvoering van 'Privacy Impact Assessments' (PIA's) en 'Gateway Reviews'. PIA's moeten worden aangevuld met een verplichte haalbaarheidstoets om de besluitvorming rond ICT-projecten te verbeteren. Onafhankelijke deskundigen en stakeholders dienen hierbij te worden betrokken. Kamerleden moeten inzicht krijgen in de resultaten en in de te maken afwegingen.

COLOFON: Het Bericht is een uitgave van het Rathenau Instituut. Redactie: L. Kool, G. Munnichs en C. Boland. Het Bericht is gebaseerd op het rapport *Security of eGovernment Systems. Final Report*, Science and Technology Options Assessment (STOA), Europees Parlement, 2013. Dit Bericht en het rapport staan ook op www.rathenau.nl.

Rathenau Instituut