Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA 's-Gravenhage

DG Digitalisering & Overheidsorganisatie
IFHR & CIO Rijk

Turfmarkt 147
2511 DP Den Haag

Onze referentie
2025-0000542953

Uw referentie

Bijlage(n)
1

Datum 12 september 2025
Betreft Beleidsreactie rapport van Kwetsbaar naar Weerbaar; Geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties.

Hierbij bied ik u aan, mede namens de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, het bijgevoegde ABDTOPConsult rapport 'Van Kwetsbaar naar weerbaar. Geleerde lessen uit dreigende acute en langdurige uitval van uitbestede ICT-dienstverlening bij overheidsorganisaties.' In deze brief benoem ik de bevindingen, bezie ik de bredere context van de situatie en schets ik de noodzakelijke vervolgaanpak. Daadkrachtig opvolging geven door het kabinet aan de benoemde aanbevelingen is van belang, voor de continuïteit en wendbaarheid van cruciale (dienstverlenings)processen van de overheid.

Nederland behoort tot de top vijf van meest gedigitaliseerde landen in Europa. Voor het kunnen uitvoeren van dienstverlening aan burgers, bedrijven en voor de werking van de overheid zelf zijn Nederlandse overheden sterk afhankelijk geworden van ICT-leveranciers. Voor primaire en secundaire processen van (uitvoerings-)organisaties speelt ICT een cruciale rol, hiermee wordt bijgedragen of wordt mogelijk gemaakt dat gegevensuitwisseling, transacties, besluitvorming en dienstverlening aan burgers en bedrijven correct en efficiënt verlopen.

Kernboodschap uit het rapport voor politiek en bewindspersonen
Het rapport geeft de volgende kernboodschap voor de politiek en bewindspersonen: "Burgers moeten kunnen rekenen op een betrouwbare overheid. Het is de verantwoordelijkheid van de politiek, bewindspersonen en de ambtelijke top om overheden weerbaar te maken tegen langdurige uitval van ICT-diensten. Maak daarom een politieke afweging om de digitale weerbaarheid van overheidsorganisaties op orde te krijgen in de juiste verhouding ten opzichte van het realiseren van nieuw beleid. Maak substantieel budget beschikbaar om rijksfaciliteiten te bouwen die de overheid minder kwetsbaar maken voor ICT-risico's met betrekking tot leveranciers, geopolitieke ontwikkelingen en cyber".

Bevindingen op overheidsbreed niveau
In 2024 had de sterk verslechterende financiële situatie van een grote internationale ICT-leverancier tot een landelijke crisissituatie kunnen uitgroeien. Het geconstateerde risico betrof verstoring van overheidsdienstverlening op meerdere aspecten, van financiële en zorg gerelateerde dienstverlening, werkende infrastructuur tot rechtspraak, openbaar ministerie en politietaken.

Dit rapport onderzoekt niet de ICT-leverancier betrokken bij deze 'bijna-crisis', wat slechts de aanleiding was voor het onderzoek. Deze casus is in een ander traject door benodigde acties beheerst. Het onderzoek richt zich wel op de lessen die in algemene zin geleerd kunnen worden uit de hiervoor genoemde situatie en geeft aanbevelingen.

Uit het rapport blijkt dat de weerbaarheid van overheden tekortschiet als grote ICT-incidenten niet binnen korte tijd worden opgelost. De oorzaken van incidenten zijn uiteenlopend, de overeenkomst is dat de ICT in het primaire proces van de overheidsorganisaties acuut en voor langere tijd niet beschikbaar is. Bestaande structuren, kennis en maatregelen worden onvoldoende gehanteerd voor het mitigeren van het risico op en de impact van acute en langdurige uitval van ICT. Gezien de huidige geopolitieke verhoudingen nemen de risico's van acute uitval van ICT-dienstverlening toe. Het Cybersecuritybeeld Nederland[1] benadrukt de dreiging van grootschalige uitval en noemt hierbij expliciet het risico van een 'digitale monocultuur', waarin vele organisaties afhankelijk zijn van een klein aantal aanbieders.

Het rapport doet constateringen op verschillende thema's:

- Ten aanzien van bestaand beleid is geconstateerd dat het huidige rijksbrede ICT-sourcingsbeleid, de bijbehorende afwegingskaders en vooral de toepassing daarvan in de praktijk overheidsorganisaties onvoldoende beschermen tegen continuïteits- en concentratierisico's. Daarnaast bestaan er geen eenduidige overheidsbrede definities of afwegingskaders van wat kritieke, cruciale of vitale ICT-dienstverlening is, waardoor onduidelijk is welke kaders wel of niet van toepassing zijn.

- Ten aanzien van kennis en expertise met betrekking tot acute continuïteits- en concentratierisico's blijkt dat deze centraal binnen de rijksoverheid beperkt aanwezig zijn. Er is ook onvoldoende kennisdeling op nationaal en internationaal niveau.

- Ten aanzien van toetsing blijkt dat er onvoldoende onafhankelijke toetsing bij individuele overheden op de beheersing van risico's is, bij acute of langdurige uitval en concentratierisico's van uitbestede kritieke of vitale ICT-dienstverlening.

- Ten aanzien van monitoring blijkt dat er rijksbreed niet voldoende wordt gemonitord bij afgesloten contracten (bij kritieke of vitale ICT-diensten) en de daarbij behorende leveranciers. Continuïteits- en concentratierisico's worden

[1] CSBN 2024, NCTV.

niet centraal gemonitord. Slechts een beperkt aantal leveranciers wordt centraal gemonitord door rijksbreed strategisch leveranciers-management en categoriemanagement.

- Ten aanzien van faciliteiten is geconstateerd dat de organisaties in het Rijk in noodsituaties wel terugvallen op de afspraken ten aanzien van crisisbeheersing (onder leiding van NCTV), maar niet tot nauwelijks op gezamenlijke voorzieningen. In een 'bijna-crisissituatie', de zogenaamde 'lauwe fase', bestaat geen vastgestelde rijksbrede organisatie en/of governance om snel te anticiperen. In de eerdergenoemde recente casus is een passende governance opgezet.

Geopolitieke, markt-, leveranciers- en cyberrisico's kunnen tot onverwachte verstoring in het ICT-landschap leiden en daarmee tot abrupte, langdurige verstoring van de digitale dienstverlening aan maatschappij, burgers en bedrijven. Een verhoogde digitale weerbaarheid draagt bij aan de maatschappelijke weerbaarheid. Dit maakt het een maatschappelijke opgave voor álle overheden.

Bevindingen op het niveau van individuele overheidsorganisaties
ICT-dienstverlening is bij de meeste overheidsorganisaties vergaand uitbesteed. Door deze ontwikkeling is uitbestede ICT-dienstverlening onderdeel geworden van de kerntaken en de primaire processen voor dienstverlening aan burgers, bedrijven en maatschappij. Hiermee is het belang van effectieve ICT- en leveranciersrisico's beheersing toegenomen.

Primaire processen blijken niet bestand tegen abrupte en langdurige uitval van (uitbestede) ICT-diensten. Bij individuele overheidsorganisaties zijn bevindingen geconstateerd ten aanzien van beperkte informatieplanning en afwezigheid van benodigde kennis binnen de organisatie. ICT-uitbestedingen worden op een te laag niveau in de organisaties uitgevoerd. De verantwoordelijkheid, kennis en awareness over ICT, beheer en risico's in de gedigitaliseerde overheidsorganisaties zijn nog onvoldoende op alle managementniveaus. Daarnaast is geconstateerd dat overheidsorganisaties te weinig (contractuele) terugvalopties hebben ingericht om een crisissituatie en/of acute uitval van hun ICT-diensten op te vangen. Overheidsorganisaties monitoren op operationeel niveau de risico's van uitbestede ICT-dienstverlening. De strategische risico's van ICT-leveranciers en ICT-dienstverlening worden te weinig gewogen.

Handelingsperspectief en vervolgstappen
Ik herken het bovenstaande geschetste beeld en omarm de aanbevelingen in het rapport. Gezien de benoemde bevindingen en aanbevelingen is actie van de individuele overheidsorganisaties en van de overheid als geheel acuut en noodzakelijk om de digitale autonomie te versterken en de weerbaarheid ten aanzien van de continuïteit van primaire overheidsprocessen en de daarbij behorende ICT-dienstverlening te verbeteren.

Burgers moeten kunnen rekenen op een betrouwbare overheid. Weerbaarder worden is niet alleen een informatieveiligheid-uitdaging: business continuïteit is een verantwoordelijkheid van álle (top)managers en bewindspersonen.

Het rapport raakt aan een aantal bredere onderwerpen op het gebied van de nationale veiligheid en digitale onafhankelijkheid. Dit sluit aan bij de al bestaande Nationale Veiligheidsstrategie[2] over het vergroten van de digitale weerbaarheid van Nederland. Actielijn 7 gaat met name over het digitaal weerbaarder maken van het bedrijfsleven, hierdoor kan de leveringszekerheid worden vergroot. Het verbeteren van de digitale weerbaarheid van de (Rijks)overheid zelf, is tot dusver onderbelicht gebleven. Daarnaast is er nog een bredere ontwikkeling gaande genaamd "Whole of Society". Hierbij wordt aangegeven dat de samenleving zich voor moet bereiden op crises en eventuele deelname aan een gewapend conflict. Ook hier geldt dat de (Rijks)overheid digitaal kwetsbaar is. Tevens sluit deze ontwikkeling aan bij de Weerbaarheidsopgave van de departementen, pijler 1 'het beschermen en versterken van vitale en andere belangrijke processen in de maatschappij' en pijler 3 'de Nederlandse democratie en rechtstaat blijven overeind'.

Wat wetgeving betreft wordt met de voorziene inwerkingtreding van de Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet (Cbw) eind 2025 een wettelijk fundament gelegd tot het verhogen van de weerbaarheid van onze vitale infrastructuur. Tegelijkertijd vragen het huidige dreigingslandschap en de weerbaarheidsopgave om een versnelling. Mede gezien de huidige geopolitieke ontwikkelingen vind ik het noodzakelijk om prioritering aan te brengen in de veelheid van aanbevelingen. Allereerst is het van belang om enkele overheidsbrede risicogebieden te benoemen. Binnen deze gebieden is het, gegeven het nationale veiligheidsbelang, noodzakelijk om overheidsbreed gezamenlijk dezelfde koers te varen met als doel continuïteit van belangrijke overheidsprocessen. Hoogste prioriteit krijgen de aanbevelingen die hoogrisico en vitale processen raken.

De Interdepartementale Commissie Bedrijfsvoering Rijk (ICBR) draagt zorg voor de bemensing van acties en geeft sturing aan de uitvoering van de aanbevelingen. De Taskforce Continuïteit ICT dienstverlening, bestaande uit adviseurs van verschillende organisaties, draagt zorg voor de coördinatie en uitvoering van de acties. In deze Taskforce wordt kortcyclisch gewerkt om vaart te houden in de benodigde activiteiten en de benodigde resultaten te realiseren. De reikwijdte van de acties is in beginsel de rijksoverheid en waar mogelijk kunnen andere overheidslagen aanhaken. Voor een aantal specifieke acties wordt verbreding via een plateauplanning uitgewerkt.

Vanuit mijn coördinerende overheidsbrede verantwoordelijkheid geef ik prioriteit aan de volgende activiteiten:

- Opzetten van een Center of Excellence, als motor voor de uitvoering van activiteiten en voor bundeling en bijeenbrengen van, kennis en kunde ter ondersteuning en facilitering van overheidsorganisaties. Het Center of Excellence zal samengesteld worden uit medewerkers met diverse expertises (IV-expertise, inkoop, juridisch, etc.).
- Inrichten van centrale monitoring van leveranciers voor het proactief volgen van marktontwikkelingen van ICT-diensten en ICT-leveranciers om proactief te kunnen handelen bij dreigende acute en langdurige uitval van ICT-diensten.
- Verkennen van voorafgaande toetsing van risicovolle ICT-uitbestedingen.

[2] *Kamerstuk 30 821, nr.178.*

- Opzetten van een overheidsbrede IT-sourcingstrategie die ons in staat stelt staat om risico gebaseerd, verantwoord en uniform beslissingen te nemen over wat we inkopen en wie we contracteren. Gestart wordt met het herijken van de sourcingstrategie voor de Rijksoverheid. Andere overheidslagen sluiten aan via een plateauplanning.
- Ontwikkelen van overheidsbrede terugvalfaciliteiten voor noodsituaties. Hiervoor worden business cases uitgewerkt. De daadwerkelijke uitvoering is enkel mogelijk met forse investeringen.
- Toetsing op de nakoming van toegepaste kaders, risicomanagement en effectiviteit van mitigerende maatregelen voor digitale weerbaarheid van overheidsprocessen.
- Het zorgdragen voor de continuïteit van de (vitale) overheidsprocessen voor burgers, bedrijven en samenleving is een verantwoordelijk die veel verder strekt dan de IV-verantwoordelijkheid binnen een organisatie. Inzet op versterking van continuïteitsmanagement, digitaal bewustzijn en leiderschap acht ik tevens van belang.

Bovenstaande acties worden nader uitgewerkt onder meer door het opstellen van plannen van aanpak en business cases. Daarna zal de financiering voor de daadwerkelijke realisatie in besluitvorming worden gebracht.

Voor de overige uit te voeren acties om de basis op orde te krijgen sluit ik aan bij de voorgestelde aanpak met de routekaart uit het rapport als handvat voor het op te stellen *Plan om de weerbaarheid van de Nederlandse overheid ten aanzien van ICT-dienstverlening te vergroten*. Daarnaast krijgen enkele activiteiten een plek in de Nederlandse Digitaliseringsstrategie[3]. Tevens streef ik naar versterking van al lopende ontwikkelingen.

Met de bestaande toezichthouders, de Algemene Rekenkamer, de Autoriteit Persoonsgegevens en het Adviescollege ICT-Toetsing, ga ik nader in gesprek om effectief toezicht op dit gehele proces en de uitvoering te borgen.

Ik herhaal uit het rapport: “Een verhoogde digitale weerbaarheid draagt bij aan de maatschappelijke weerbaarheid.”.
Gezien de geconstateerde urgentie is actie noodzakelijk om de weerbaarheid van de Nederlandse overheid te vergroten, om daarmee ook ontwrichtende situaties in onze samenleving te voorkomen. Het is een gezamenlijke actie van het kabinet om deze verandering te realiseren.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

[3] Kamerstuk 26643, nr.1366

DG Digitalisering & Overheidsorganisatie
Taskforce CID

F. Rijkaart

Onze referentie
2025-0000542953