Ministerie van Financiën

Onderzoeksrapport
Bevindingen onderzoeksopdracht back-up M365 Belastingdienst

Definitief

Colofon

Titel	Bevindingen onderzoeksopdracht back-up M365 Belastingdienst
Uitgebracht aan	Persoonsgegevens
Datum	6 juli 2026
Kenmerk	2026-0000286953
Referentienummer	2026-FIN-006

Inlichtingen
Auditdienst Rijk
Persoonsgegevens

Inhoud

Samenvatting—5

1 Inleiding—7
1.1 Aanleiding onderzoek en opdrachtgever—7
1.2 Doelstelling en onderzoeksvragen—8
1.3 Afbakening—8
1.4 Leeswijzer—9

2 Bevindingen—10
2.1 Bevindingen bij onderzoeksvraag I: stelsel van maatregelen voor dagelijkse M365-back-up naar on-premises datacenter Belastingdienst—10
2.1.1 Beschrijving M365-omgeving Belastingdienst—10
2.1.2 Beschrijving ontwikkelproject back-up M365 en pilot—11
2.1.3 Back-upvoorziening M365 Belastingdienst in ontwikkeling—11
2.1.4 Afwijking beveiligingsbeleid: inspectie van geëncrypte M365-back-updatastromen technisch niet mogelijk—13
2.1.5 Exitscenario M365: versterking inzicht aannames en afhankelijkheden noodzakelijk—13
2.2 Bevindingen bij onderzoeksvraag II: volledig meenemen van alle relevante gebruikersdata M365 in back-up—14
2.2.1 Gebruik van M365-diensten op hoofdlijnen in beeld; eisen en uitgangspunten back-up nog niet in samenhang expliciet vastgesteld door stuurgroep—14
2.2.2 Configuratie M365-gebruikers in scope voor back-up complex en nog niet gedocumenteerd—15
2.2.3 Belastingdienst zelf verantwoordelijk voor onderhoud maatwerkscripts voor back-up—15
2.3 Bevindingen bij onderzoeksvraag III: inhoudelijk en aantoonbaar overeenkomen van back-up met brondata—16
2.3.1 Nog geen end-to-endcontrole om volledigheid van M365-back-up vast te stellen—16
2.3.2 Verschillende softwarefouten onderkend in de back-up oplossing op het gebied van back-up en herstel—16
2.4 Bevindingen bij onderzoeksvraag IV: afronding back-up M365 binnen het afgesproken tijdvenster—17
2.4.1 Geen formele juridische borging dat het back-upproces blijft werken zoals ingericht—17
2.4.2 Nog niet aangetoond dat de back-up oplossing, de back-up binnen het gekozen tijdvenster kan uitvoeren voor de gehele Belastingdienstpopulatie—18
2.5 Bevindingen bij onderzoeksvraag V: bruikbaarheid back-up bij ongeplande exit M365—18
2.5.1 Back-up M365-data on-premises opgeslagen, maar heeft karakter black box; in exitscenario is ondersteuning door leveranciers niet gegarandeerd—18
2.5.2 Testen herstel individuele objecten planmatig aangepakt, maar nog niet afgerond—19

3 Verantwoording onderzoek—20
3.1 Werkzaamheden—20
3.2 Referentiekader—20
3.3 Gehanteerde standaard en kwaliteitsborging—20

3.4 Verspreiding rapport—21

4 Ondertekening—22

Bijlage I Managementreactie—23

Samenvatting

Belastingdienst, Douane en Toeslagen: nieuwe werkplek gebruikt public cloud
De Belastingdienst, Douane en Toeslagen zijn van plan om hun kantoorautomatiseringsomgeving te migreren naar Microsoft 365 (M365) in de public cloud, terwijl primaire systemen in het eigen datacenter blijven draaien. Dit gebeurt binnen een context waarin recent veel aandacht is ontstaan voor de risico's van de sterke afhankelijkheid van grote, niet-Europese IT-leveranciers, vooral rond publiccloudgebruik door overheidsorganisaties.

Conform het Rijksbreed Cloudbeleid 2022 is een exitstrategie ontwikkeld, die voorziet in dagelijkse back-ups van M365-data naar het on-premises datacenter van de Belastingdienst, zodat gebruikersdata altijd beschikbaar blijft buiten de cloud. Momenteel wordt deze back-upvoorziening ontwikkeld en getest. Persoonsgegevens Persoonsgegevens heeft de Auditdienst Rijk gevraagd onderzoek te doen naar de inrichting en aandachtspunten van deze back-upvoorziening.

Aanpak van het onderzoek
De doelstelling van het onderzoek is om inzicht te bieden in het stelsel van maatregelen voor de dagelijkse back-up van M365-gebruikersdata naar het on-premises datacenter van de Belastingdienst. We hebben de doelstelling uitgewerkt in vijf onderzoeksvragen, waarbij het kwaliteitscriterium 'integriteit' centraal staat. We vatten integriteit in dit onderzoek op als het waarborgen dat alle relevante gebruikersdata volledig wordt meegenomen in de back-up, dat deze data aantoonbaar overeenkomt met de brondata in M365 zonder ongeautoriseerde of onbedoelde wijzigingen en dat de data tijdig en bruikbaar beschikbaar is voor herstel of het faciliteren van een alternatieve werkplekoplossing.

Voor de uitvoering van het onderzoek hebben we relevante documentatie opgevraagd en geanalyseerd, interviews gehouden met direct betrokken medewerkers en door waarneming ter plaatse inzicht gekregen in de werking van het M365-back-upsysteem en het bijbehorende stelsel van maatregelen. De bevindingen in dit onderzoek geven de stand van maart 2026 weer.

Stand van zaken back-up M365
Medio januari 2026 is de Belastingdienst een project gestart voor de ontwikkeling van een back-upvoorziening voor de M365-omgeving. Hiervoor wordt een geïntegreerde back-up oplossing van een leverancier uit de Verenigde Staten ingezet. Dit is een back-upoplossing die al eerder via een aanbesteding is geselecteerd voor het maken van back-ups binnen het eigen datacenter van de Belastingdienst.
Het project kent een gefaseerde aanpak: momenteel staat het testen van het herstel van individuele gebruikersdata centraal, zoals mailboxen. Sommige onderdelen, zoals het terugzetten van OneDrive-data en SharePoint-sitegegevens, zijn technisch nog niet volledig mogelijk of moeten nog worden getest.
De M365-pilot met circa 6000 gebruikers biedt praktijkervaring met het dagelijkse back-upproces. Omdat het project nog niet is afgerond, zijn de onderzoeksbevindingen deels gebaseerd op tussentijdse resultaten. Waar relevant is dit expliciet vermeld. Bevindingen die rechtstreeks het gevolg zijn van de status van het project zijn niet in deze samenvatting opgenomen.

Belangrijkste bevindingen en aanbevelingen
Ons onderzoek leverde meerdere bevindingen op over het stelsel van maatregelen voor de dagelijkse back-up van M365-gebruikersdata, waarbij we ook aanbevelingen hebben geformuleerd. De vier belangrijkste bevindingen vatten we hierna samen.

1. Versterking inzicht aannames en afhankelijkheden noodzakelijk
Het exitplan waarvan de back-up van M365-gebruikersdata als maatregel deel uitmaakt, is gebaseerd op een scenario waarbij de M365-dienstverlening plotseling wordt onderbroken, bijvoorbeeld door geopolitieke ontwikkelingen en/of sancties. De ADR acht de kans in een dergelijke situatie significant dat ook de dienstverlening van andere leveranciers zal stoppen. Het scenario gaat niet in op de gevolgen hiervan, terwijl de Belastingdienst impliciet wel aannames doet op dit gebied.

Aanbeveling: Maak de aannames en uitgangspunten in het scenario en het exitplan expliciet en tref waar mogelijk aanvullende beheersmaatregelen. Maak verder de restrisico's inzichtelijk en laat deze op een passend managementniveau accepteren.

2. Ondersteuning on-premises back-upoplossing M365 geen zekerheid
De M365-back-upoplossing is in het datacenter van de Belastingdienst geplaatst. De beheerders van de Belastingdienst hebben geen inzicht in de interne werking van de oplossing en deze functioneert daarmee als een 'black box'. Herstel van data is alleen mogelijk via de standaardinterfaces van de oplossing. Als deze interfaces uitvallen, is de Belastingdienst afhankelijk van de ondersteuning door externe leveranciers. In een exitscenario is het echter onzeker of deze ondersteuning beschikbaar blijft, waardoor herstel van data mogelijk niet kan plaatsvinden.

Aanbeveling: Voer een expliciete risicoanalyse uit voor het exitscenario waarbij er rekening mee wordt gehouden dat de ondersteuning voor de back-upoplossing door de leveranciers bijvoorbeeld als gevolg van een sanctie niet meer beschikbaar is. Overweeg om periodiek gebruikersdata te herstellen in een direct toegankelijk format en deze data in deze vorm te bewaren.

3. Verschillende softwarefouten onderkend in back-upoplossing voor M365
De Belastingdienst heeft bij het testen van de back-upoplossing een aantal softwarefouten gevonden die deels invloed hebben op de volledigheid van de back-up en herstel. Zelf heeft de Belastingdienst de indruk in Nederland de 'launching customer' te zijn voor de back-upoplossing op het gebied van het on-premises herstel van M365-data en hiervoor zelfs wereldwijd een van de eerste te zijn. Hierdoor bestaat een verhoogd risico dat de Belastingdienst bij uitbreiding naar meer M365-gebruikers tegen nieuwe softwarefouten of andere functionele problemen aanloopt, wat kan leiden tot niet herstelbare back-ups.

Aanbeveling: Blijf gedurende het toevoegen van M365-gebruikers intensief en systematisch de back-upoplossing testen. Richt hierbij extra aandacht op randgevallen en nieuwe gebruikssituaties, zodat eventuele softwarefouten tijdig worden gedetecteerd en kunnen worden opgelost.

4. Nog geen end-to-endcontrole voor vaststellen volledigheid back-up
De Belastingdienst heeft in het kader van de M365-pilot een dagelijkse back-up van M365-gebruikersdata ingericht. Een dashboard geeft inzicht in de uitvoering en status van de dagelijkse M365-back-up. De back-upbeheerders monitoren de back-up op basis van het dashboard en rapporteren afwijkingen. Een end-to-endcontrole waarmee kan worden vastgesteld of de M365-back-ups volledig zijn ontbreekt nog. Hierdoor bestaat het risico dat afwijkingen pas bij herstel aan het licht komen.

Aanbeveling: Versterk mede op basis van een risicoafweging de end-to-endcontrole en voer periodiek deze volledigheidscontrole uit.

1 Inleiding

1.1 Aanleiding onderzoek en opdrachtgever

Mede door recente geopolitieke ontwikkelingen is er veel politieke en maatschappelijke aandacht voor de risico's van een significante afhankelijkheid van grote IT-leveranciers van buiten de EU. Dit geldt ook voor het gebruik van de public cloud door overheidsorganisaties. Binnen deze context zijn de Belastingdienst, de Douane en Toeslagen voornemens om met hun kantoorautomatiseringsomgeving (digitale werkplek) op korte termijn over te stappen naar de public cloud met Microsoft 365 (M365). Dit publiccloudgebaseerde platform biedt onder meer een geïntegreerde suite aan productiviteitsdiensten, zoals e-mail, tekstverwerking, spreadsheets, samenwerkingstools en centrale bestandsopslag. Met deze migratie komt de (digitale) werkplek in een public cloud, terwijl de primaire systemen van de Belastingdienst in het eigen datacenter blijven draaien. Ook bij gebruik van Europese datacenters voor M365 blijft Microsoft als leverancier uiteindelijk onder de Amerikaanse wet- en regelgeving vallen.

Achtergrond is dat de Belastingdienst sinds 2021 werkt aan de vervanging van de werkplek binnen de eigen organisatie, de Douane en Toeslagen. De overstap naar M365 voor kantoorautomatisering was na een afweging van alternatieven vanaf het begin als toekomstbeeld voorzien. In oktober 2025 is in een Kamerbrief nader toegelicht dat Belastingdienst, Douane en Toeslagen (verder: de Belastingdienst) gezamenlijk besloten hebben om daadwerkelijk over te stappen op M365. In deze brief is als motivatie gegeven dat enkel M365 op korte termijn kan voldoen aan de eisen rond functionaliteit, veiligheid, continuïteit en efficiëntie, dit in tegenstelling tot alternatieven.

De Belastingdienst heeft een exitstrategie opgesteld voor M365 in lijn met het Rijksbreed Cloudbeleid 2022 voor het gebruik van public cloud. Deze strategie beschrijft hoe de kantoorautomatiseringsomgeving indien nodig zo gecontroleerd mogelijk kan worden gemigreerd naar een alternatieve omgeving. De strategie maakt onderscheid tussen een geplande exit (zoals door het regulier aflopen van een contract) en een ongeplande exit (door onvoorziene omstandigheden). Als belangrijke beheersmaatregel voor een ongeplande exit moet de organisatie dagelijks een back-up van de M365-data maken, die wordt opgeslagen in het on-premises datacenter van de Belastingdienst. Het doel is om altijd een actuele kopie van de gebruikersdata beschikbaar te hebben buiten de cloudomgeving. Hoewel dat een snel herstel van de werkplekdienstverlening niet garandeert, vormt deze back-up wel een essentiële basis om een alternatieve werkplekvoorziening te vullen met gebruikersdata.

Eerder startte de Belastingdienst een pilot waarbij enkele duizenden medewerkers van de Belastingdienst de nieuwe werkplek met M365 gebruiken. De back-upvoorziening, waarmee dagelijks een back-up wordt gemaakt van de gebruikersdata in M365 naar het on-premises datacenter van de Belastingdienst, wordt momenteel ontwikkeld en getest. Als deze voorziening naar behoren functioneert, dan is de Belastingdienst van plan om M365 gefaseerd uit te rollen naar de resterende werkplekken.

Persoonsgegevens heeft de Auditdienst Rijk gevraagd onderzoek te doen naar de inrichting en eventuele aandachtspunten van de back-upvoorziening als essentieel onderdeel van de exitstrategie. De uitkomsten van dit onderzoek worden meegenomen in het besluit over verdere uitrol.

1.2 Doelstelling en onderzoeksvragen

De doelstelling is om inzicht te bieden in het stelsel van maatregelen voor de dagelijkse back-up van M365-gebruikersdata naar het on-premises datacenter van de Belastingdienst met als referentie het kwaliteitscriterium integriteit. Aan deze doelstelling hebben we invulling gegeven door de volgende vragen te beantwoorden:

1. Hoe ziet het stelsel van maatregelen voor de dagelijkse M365-back-up naar het on-premises datacenter van Belastingdienst er op hoofdlijnen uit?

Welke bevindingen heeft de ADR ten aanzien van:

2. het volledig meenemen van alle relevante gebruikersdata van alle door Belastingdienst gebruikte M365-diensten in de dagelijkse back-up;
3. het inhoudelijk en aantoonbaar overeenkomen van de data vastgelegd in de back-up in het datacenter van de Belastingdienst met de brondata in M365 zonder ongeautoriseerde of onbedoelde wijzigingen;
4. de uitvoering en afronding van de back-up binnen het afgesproken tijdvenster waarbij alle gebruikersdata wordt meegenomen die op het moment van het begin van het tijdvenster aanwezig is;
5. de bruikbaarheid van de back-up voor het voorzien van een alternatieve werkplekoplossing van gebruikersdata in het geval een ongeplande exit van M365 plaatsvindt?

Waar mogelijk hebben we bevindingen voorzien van een risico-inschatting en handelingsperspectief.

1.3 Afbakening

Het object van onderzoek betreft het stelsel van maatregelen dat de Belastingdienst heeft ingericht voor de dagelijkse back-up van gebruikersdata uit de door de organisatie gebruikte M365-omgeving naar het on-premises datacenter van de Belastingdienst. Het onderzoek geeft de stand van maart 2026 weer. Onder gebruikersdata wordt alle data verstaan die gebruikers in M365 hebben gegenereerd, gedeeld of ontvangen en die volgens de interne definitie tot de back-upscope behoort. Dit omvat primaire data zoals e-mails, documenten en spreadsheets, evenals relevante metadata die nodig is voor herstel en functionaliteit in een alternatieve werkomgeving.

Het onderzoek richt zich op de borging van de integriteit van de gebruikersdata door organisatorische, technische en waar relevant contractuele maatregelen. Hierbij verstaan we onder integriteit:

1. Volledigheid: alle relevante gebruikersdata (zowel individueel als gedeeld) uit de M365-services gaat mee in de back-up.
2. Juistheid, bruikbaarheid en toegankelijkheid: de geback-upte gebruikersdata komt aantoonbaar overeen met de brondata in M365 zonder ongeautoriseerde of onbedoelde wijzigingen. De data kan functioneel worden gebruikt voor herstel en het faciliteren van een alternatieve werkplekoplossing.
3. Tijdigheid: aan het einde van ieder dagelijks back-upvenster is alle gebruikersdata die aan het begin van dat venster in M365 aanwezig was, succesvol en volledig naar het on-premises datacenter van de Belastingdienst gekopieerd.

Onderwerpen die niet expliciet zijn genoemd, vallen niet in de scope van dit onderzoek. In het bijzonder zijn uitgesloten:

- back-up- en recoveryprocessen binnen M365 zelf;
- business continuity management;
- langjarige archivering van gebruikersdata;
- het wijzigingsbeheerproces voor M365 en de back-up;
- logging en monitoring;
- naleving van wet- en regelgeving op onderwerpen als Archiefwet, AVG, NIS2, BIO 2.0 en inkoop.

1.4 Leeswijzer

In hoofdstuk 2 geven we een overzicht van de bevindingen per onderzoeksvraag. In hoofdstuk 3 gaan we op hoofdlijnen in op de werkzaamheden die we voor dit onderzoek uitgevoerd hebben, op de standaard voor onderzoek en voor welke doelgroep we dit rapport hebben opgesteld. Bijlage I bevat de managementreactie op het rapport.

2 Bevindingen

2.1 Bevindingen bij onderzoeksvraag I: stelsel van maatregelen voor dagelijkse M365-back-up naar on-premises datacenter Belastingdienst

Onderzoeksvraag I is: 'Hoe ziet het stelsel van maatregelen voor de dagelijkse M365-back-up naar het on-premises datacenter van Belastingdienst er op hoofdlijnen uit?'.

Het stelsel van maatregelen omvat zowel technische oplossingen, zoals het back-upsysteem, als bijbehorende organisatorische en procedurele maatregelen. Deze zijn uitgewerkt als onderdeel van de onderstaande onderwerpen:

- de M365-omgeving die de Belastingdienst heeft ingericht en of deze in technische zin gereed is voor uitrol binnen de Belastingdienst, Douane en Toeslagen;
- beschrijving van het ontwikkelproject voor de back-up M365 en de pilot M365;
- de back-upvoorziening die in het on-premises datacenter van Belastingdienst wordt ingericht om gebruikersdata uit de M365-omgeving veilig te stellen;
- afwijking beveiligingsbeleid voor geëncrypte M365-back-updatastromen;
- het exitscenario voor de M365-omgeving dat de aanleiding vormt voor de inrichting van de M365-back-up.

2.1.1 Beschrijving M365-omgeving Belastingdienst

De Belastingdienst, Douane en Toeslagen (verder: de Belastingdienst) doorlopen een transitie waarbij de oude Digitale Werkplek Belastingdienst (DWB) stapsgewijs wordt vervangen door de Digitale Brug Overheidsdiensten (DBO) werkplek voor alle medewerkers van de Belastingdienst. Deze DBO is ontwikkeld om te gebruiken in combinatie met Microsoft 365 (M365). In de basis is M365 een 'Software as a Service'-voorziening die draait in de public cloud van Microsoft. Per medewerker heeft de Belastingdienst de meest uitgebreide M365-licentie. In de basis gebruikt de Belastingdienst binnen deze licentie de volgende M365-functionaliteit voor de werkplek:

- kantoorautomatisering (M365 Apps for enterprise, zoals Word en Excel);
- e-mail (Exchange Online);
- documentopslag (OneDrive for Business);
- digitaal samenwerken (Microsoft MS-Teams en SharePoint Online).

In overleg kunnen onderdelen van de Belastingdienst aanvullende functionaliteit activeren die onderdeel uitmaakt van de beschikbare licenties, zoals Power BI. Medewerkers hebben toegang tot de M365-functionaliteit via, onder meer, een laptop die is ingericht met Windows 11 of een Macbook.

Centraal maakt de Belastingdienst in ieder geval gebruik van de volgende mogelijkheden binnen M365:

- functionaliteit gericht op de beheersing van de informatiehuishouding van de Belastingdienst, met als doel om op termijn de naleving van relevante wet- en regelgeving op onder meer het gebied van archiefbeheer te borgen;
- de borging van de beschikbaarheid van gebruikersdata (zoals documenten) in de dagelijkse operatie. Hiervoor zijn onder meer standaardbewaartermijnen en retentie ingesteld. Van bestanden worden meerdere versies bewaard en door de eindgebruiker verwijderde informatie blijft beschikbaar;

- toepassing van vertrouwelijkheidslabels op documenten en e-mails, onder meer als basis voor het treffen van extra maatregelen gericht op de vertrouwelijkheid van deze documenten.

Ook gebruikt de Belastingdienst diverse beveiligingsoplossingen die voor hun functioneren afhankelijk zijn van Azure (public cloud Microsoft) en/of M365.

2.1.2 *Beschrijving ontwikkelproject back-up M365 en pilot*

Medio januari 2026 is de Belastingdienst in projectvorm gestart met de bouw van een back-upvoorziening voor de M365-omgeving. Dit project valt onder het programma dat de Belastingdienst al enkele jaren heeft lopen voor de ontwikkeling van de nieuwe werkplek inclusief de overgang naar M365 als geheel. Als basis gebruikt de Belastingdienst een back-upsysteem dat eerder is geselecteerd via een aanbesteding en dat ook voor andere back-updoeleinden al wordt ingezet. Het betreft een geïntegreerde back-up oplossing van een leverancier uit de Verenigde Staten (verder: back-up oplossing), die onder meer functionaliteit biedt voor back-up en recovery van gebruikersdata uit M365. Binnen het programma is gekozen voor een gefaseerde aanpak van het M365-back-upvraagstuk. Het huidige project richt zich op het realiseren van de back-up en het aantonen dat de data juist en volledig is opgeslagen voor individuele gebruikers en in principe is te herstellen. Op het moment van onderzoek was het project nog in uitvoering en was bijvoorbeeld nog niet alle beheerdocumentatie opgesteld. In een vervolgproject zal de focus liggen op het gelijktijdig herstel van data voor alle gebruikers vanuit een back-up, het herstel van werkplekfunctionaliteit buiten M365 en de ontwikkeling van het bijbehorende draaiboek.

De M365-omgeving wordt al sinds enige tijd beproefd in pilotvorm door circa 6000 gebruikers. Als onderdeel van deze pilot wordt binnen het project proefgedraaid met de dagelijkse M365-back-up.

2.1.3 *Back-upvoorziening M365 Belastingdienst in ontwikkeling*

Zoals we in § 2.1.2 aangaven, is de Belastingdienst gestart met het inrichten van een aanvullende back-upvoorziening, ter ondersteuning van de cloud-exitstrategie. Deze back-upvoorziening dient als aanvulling op de bestaande maatregelen binnen de M365-omgeving voor het borgen van de beschikbaarheid van gebruikersdata. Het doel van deze voorziening is om de gebruikersdata uit de M365-omgeving dagelijks fysiek (on-premises) op te slaan in het eigen datacenter van de Belastingdienst.

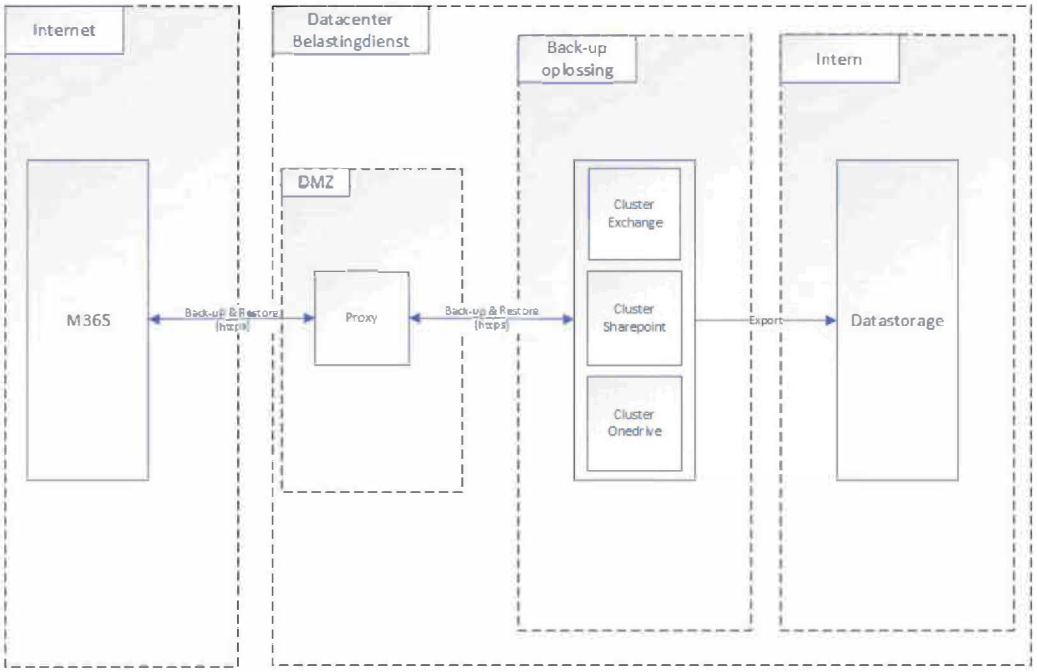
In juridische zin is de voorziening gelaagd opgebouwd. De Belastingdienst heeft voor de back-up oplossing een contract met een Nederlandse leverancier voor het leveren van de hardware en met een technologiebedrijf uit de Verenigde Staten voor het leveren van technisch beheer. Vervolgens heeft dit technologiebedrijf een contract met de leverancier van de geïntegreerde back-up oplossing die ook uit de Verenigde Staten afkomstig is. Het hoofdkantoor van beide leveranciers is gevestigd in de Verenigde Staten. In de praktijk leveren de leveranciers de ondersteuning voor de back-up oplossing op locatie van het datacenter van de Belastingdienst.

Figuur 1 is een schematische weergave van de M365-back-upvoorziening van de Belastingdienst. Van links naar rechts wordt op enkele onderdelen een toelichting gegeven:

1. Tussen de M365-omgeving (bereikbaar via internet) en de on-premises omgeving (het datacenter) van de Belastingdienst loopt een datastroom voor de back-up. De back-up oplossing en de interne datastorage waarop gebruikersdata kan worden hersteld, bevinden zich in het datacenter van de Belastingdienst.
2. In technische zin bestaat de datastroom voor de back-up uit drie delen die corresponderen met de M365-functionaliteit voor de werkplek die de Belastingdienst in de basis gebruikt. Deze datastromen zijn versleuteld en

lopen via internet via een regulier koppelvlak (DMZ / Proxy) van de Belastingdienst naar de back-up oplossing.

3. Om capaciteitsredenen is per datastroom een instantie (cluster) van de back-up oplossing ingericht. Startpunt is de eenmalige uitvoering van een volledige back-up gevolgd door een dagelijkse incrementele back-up die is gericht op de gewijzigde gebruikersdata van de afgelopen 24 uur.
4. De Belastingdienst maakt separaat een back-up van de identiteits- en toegangsinformatie uit M365 (via Entra ID) voor het eventueel herstellen van eigenaarschap en toegangsrechten van gebruikersdata.
5. Herstel van gebruikersdata vindt plaats door deze vanuit de back-up oplossing te plaatsen op de interne datastorage van de Belastingdienst. Deze functionaliteit is momenteel volop in ontwikkeling. Op het moment van onderzoek werd het herstellen van bijvoorbeeld een individuele mailbox getest. Software om het format van een herstelde mailbox om te zetten naar een format dat bruikbaar is voor het doelsysteem werd op het moment van onderzoek nog aangeschaft.



Figuur 1 Schematische weergave back-upvoorziening M365

2.1.4 *Afwijking beveiligingsbeleid: inspectie van geëncrypte M365-back-updatastromen technisch niet mogelijk*

Zoals we in § 2.1.3 aangaven, lopen er voor de M365-back-up drie geëncrypte datastromen. Volgens het beveiligingsbeleid van de Belastingdienst moeten geëncrypte datastromen vanaf het internet (in dit geval vanuit M365 / Microsoft cloud) bij binnenkomst in het datacenter worden geïnspecteerd. Om technische redenen kan deze inspectie voor deze datastromen niet worden uitgevoerd, omdat de encryptie niet kan worden onderbroken. Persoonsgegevens heeft voor deze werkwijze tijdelijk ontheffing verleend tot en met 31 mei 2026.

Risico

Het risico is dat dit probleem uiteindelijk technisch niet kan worden opgelost en dat de enige optie is om de afwijking van het beveiligingsbeleid van de Belastingdienst te accepteren.

Aanbeveling

Onderzoek en evalueer alternatieve beveiligingsmaatregelen die het risico van de niet-geïnspecteerde geëncrypte datastromen kunnen mitigeren. Draag vervolgens zorg voor implementatie van deze maatregelen in combinatie met een periodieke evaluatie van het resterende risico en de effectiviteit van de maatregelen. Leg de gemaakte keuzes en eventuele afwijkingen van het beveiligingsbeleid duidelijk vast en stem de uitkomsten tijdig af met P-gv. en relevante stakeholders.

2.1.5 *Exitscenario M365: versterking inzicht aannames en afhankelijkheden noodzakelijk*

Op grond van het Rijksbreed Cloudbeleid 2022 en de achterliggende kaders heeft de Belastingdienst een analyse gemaakt van twee exitscenario's voor zijn M365-gebruik. In het eerste scenario vindt een direct vertrek plaats uit M365 door een crisis en/of door plotselinge (geopolitieke) ontwikkelingen. Een voorbeeld is het instellen van sancties door de Verenigde Staten waardoor Microsoft de M365-dienstverlening moet staken. De M365-omgeving inclusief de gebruikersdata van de Belastingdienst die hierin is opgenomen, is in dit geval met onmiddellijke ingang voor langere tijd of permanent niet meer toegankelijk. Het tweede scenario betreft een regulier afscheid van de M365-omgeving door beëindiging van het contract. Volgens de Belastingdienst is voor een dergelijk geval contractueel vastgelegd dat de Belastingdienst negen maanden de tijd heeft om de gebruikersdata vanuit de M365-omgeving over te brengen naar een alternatieve omgeving. In deze paragraaf wordt het tweede scenario verder buiten beschouwing gelaten.

Een belangrijk onderdeel van het exitplan dat hoort bij het eerste scenario is het on-premises beschikbaar maken van de M365-gebruikersdata in het eigen datacenter van de Belastingdienst, zoals al beschreven in § 2.1.3. Andere onderdelen van het exitplan zijn nog in ontwikkeling en betreffen bijvoorbeeld (in ieder geval voor de komende drie jaar) het opnieuw in gebruik nemen van bestaande diensten die zijn gebaseerd op de oude werkplek van de Belastingdienst, zoals HCL Notes en de on-premises Microsoft Office en SharePoint-software. De M365-gebruikersdata wordt bij een exit weer hersteld in de on-premises Belastingdienst-omgeving. Ook is voorzien dat de gebruikte on-premises mail gateway het mogelijk maakt om de e-mail van de Belastingdienst snel weer in het eigen datacenter te laten bezorgen in plaats van in de M365-omgeving.

De ADR signaleert dat het eerste exitscenario beknopt is uitgewerkt door alleen het stopzetten van de M365-dienstverlening in beschouwing te nemen. De ADR schat in dat in een dergelijke situatie de kans significant is dat ook de dienstverlening van andere leveranciers die vallen onder wet- en regelgeving uit de Verenigde Staten zal worden stopgezet. Het scenario gaat niet in op de gevolgen hiervan, terwijl er impliciet wel aannames worden gedaan op dit gebied. Twee concrete voorbeelden zijn:

- Bij een volledig herstel van alle M365-gebruikersdata uit de back-up in de on-premises Belastingdienst-omgeving kunnen onverwacht problemen optreden. In dit geval is er mogelijk geen ondersteuning meer beschikbaar

van de betrokken leveranciers, waardoor herstel niet mogelijk blijkt (zie ook § 2.5.1).

- De beveiligingsoplossingen die de Belastingdienst gebruikt, worden geleverd door Microsoft of andere leveranciers uit de Verenigde Staten. Deze oplossingen zijn óf publiccloudgebaseerd, óf in het datacenter van de Belastingdienst geplaatst maar voor de veilige werking afhankelijk van zeer regelmatig bijgewerkte dreigingsinformatie (zoals virusdefinities) die door een leverancier uit de Verenigde Staten wordt verstrekt. De kans is dan ook aanzienlijk dat deze oplossingen bij het optreden van het scenario direct of op zeer korte termijn onbruikbaar worden. Gevolg is enerzijds dat herstel van M365-gebruikersdata risicovol wordt: eerder niet gedetecteerde dreigingen kunnen altijd in de te herstellen gebruikersdata aanwezig zijn. Anderzijds is het voor een verantwoord functieherstel van de e-mail van de Belastingdienst voor communicatie met de buitenwereld van belang, dat er minimaal een detectieoplossing voorzien van actuele dreigingsinformatie (zoals een virusscanner) wordt toegepast.

Risico
Door het niet expliciteren van aannames en uitgangspunten in het scenario houdt de Belastingdienst onvoldoende rekening met de mogelijkheid dat noodzakelijke randvoorwaarden niet kunnen worden ingevuld en herstel van de dienstverlening en de veilige toegang tot gebruikersdata niet mogelijk blijkt bij een exit.

Aanbeveling
Maak de aannames en uitgangspunten in het scenario en het exitplan expliciet en tref waar mogelijk aanvullende beheersmaatregelen. Maak verder de restrisico's inzichtelijk en laat deze op een passend managementniveau accepteren.

2.2 Bevindingen bij onderzoeksvraag II: volledig meenemen van alle relevante gebruikersdata M365 in back-up

Onderzoeksvraag II is: 'Welke bevindingen heeft ADR ten aanzien van het volledig meenemen van alle relevante gebruikersdata van alle door Belastingdienst gebruikte M365-diensten in de dagelijkse back-up?' Voor het beantwoorden van deze vraag zijn interviews gehouden met architecten, een back-upspecialist, een M365-specialist, lijnmanagers en een programmamanager. Op basis van de interviews en ontvangen documentatie zijn wij gekomen tot de bevindingen in de volgende paragrafen.

2.2.1 Gebruik van M365-diensten op hoofdlijnen in beeld; eisen en uitgangspunten back-up nog niet in samenhang expliciet vastgesteld door stuurgroep

In opdracht van de stuurgroep heeft het verantwoordelijke projectteam een addendum voor de M365-back-up opgesteld op de M365-solutionarchitectuur. Hierin staat onder meer een beschrijving van de M365-diensten die de Belastingdienst in de basis gebruikt en in scope zijn voor de back-up (zie ook § 2.1.1). Ook gaat het addendum in op de M365-gebruikers in relatie tot de back-up en wordt de back-upoplossing technisch en procesmatig nader uitgewerkt op basis van kaders, uitgangspunten en eisen. Op een aantal punten worden belangrijke keuzes gemaakt: zo is bijvoorbeeld de oorspronkelijke eis uit de beschrijving van de exitstrategie M365 om een real-time back-upvoorziening in te richten in de uitwerking een dagelijkse back-up geworden. Een belangrijke afweging hierbij is de vraag hoeveel data de Belastingdienst bereid is te verliezen (Recovery Point Objective). Het addendum heeft het karakter van een werkdocument en wordt in diverse gremia binnen de Belastingdienst besproken. De Belastingdienst heeft aangegeven dat hij van plan is om het addendum door de stuurgroep vast te laten stellen zodra het volledig is bijgewerkt.

Risico
Zonder formele vaststelling van het addendum door de stuurgroep bestaat het risico dat de gestelde eisen en uitgangspunten voor de M365-back-up onvoldoende overeenkomen met de feitelijke behoefte van de Belastingdienst. Hierdoor kan het

voorkomen dat te veel of te weinig beheersmaatregelen worden getroffen en de M365-gebruikersdata niet adequaat wordt beschermd, met als gevolg dat er in een exitscenario onvoorzien dataverlies optreedt.

Aanbeveling
Leg de vereisten voor de M365-back-up volledig vast in het addendum op de M365-solutionarchitectuur en laat deze formeel vaststellen door de stuurgroep.

2.2.2 *Configuratie M365-gebruikers in scope voor back-up complex en nog niet gedocumenteerd*

Een uitgangspunt voor de volledigheid van de M365-back-up is dat alle gebruikers die bekend zijn in M365 in de back-up moeten worden meegenomen. Dit betreft zowel actieve als inactieve gebruikers. Actieve gebruikers maken op dat moment daadwerkelijk gebruik van M365. Inactieve gebruikers hebben nog wel een account maar maken geen gebruik meer van M365 (bijvoorbeeld oud-medewerkers). De Belastingdienst wil ook van inactieve gebruikers de M365-gebruikersdata in de back-up meenemen. Bevindingen op dit gebied zijn:

1. Het beheer van gebruikers die in de back-up oplossing zijn geconfigureerd om te worden meegenomen in de back-up is complex. De betrokken back-upbeheerders hebben het beheermechanisme voor gebruikers tijdens een waarneming ter plaatse helder uitgelegd aan de ADR, maar het mechanisme is nog niet gedocumenteerd. Het betreft binnen het project nog werk in uitvoering.
2. De configuratie van inactieve gebruikers voor opname in de back-up levert nog problemen op.
3. Voor beheer van gebruikers in de back-up oplossing wordt gebruikgemaakt van niet formeel door de leverancier ondersteunde scripts, zie § 2.2.3.

Risico
Doordat het beheermechanisme voor configuratie van de gebruikers in scope voor de M365-back-up nog niet is gedocumenteerd en er nog problemen zijn met back-up van inactieve gebruikers, bestaat het risico dat niet alle relevante gebruikersdata wordt meegenomen in de back-up, waardoor data verloren kan gaan.

Aanbeveling
Los de problemen met het configureren van inactieve gebruikers op en documenteer het beheermechanisme voor het meenemen van zowel actieve als inactieve gebruikers in de M365-back-up, zodat dit proces transparant en reproduceerbaar is.

2.2.3 *Belastingdienst zelf verantwoordelijk voor onderhoud maatwerkscripts voor back-up*

Voor verschillende onderdelen van het back-up- en herstelproces voor M365 maakt de Belastingdienst gebruik van zelf aangepaste maatwerkscripts. Deze scripts zijn gebaseerd op voorbeelden uit de Github-repository van de leverancier, maar de Belastingdienst heeft ze afgestemd op de eigen eisen en de omgeving. De leverancier van de back-up oplossing biedt geen ondersteuning voor deze scripts en het aanpassen en onderhouden ervan is daarmee de verantwoordelijkheid van de Belastingdienst zelf. Het gaat onder andere om een script voor het beheer van gebruikers in de back-up oplossing die in de M365-back-up moeten worden meegenomen, een script voor het maken van een back-up van gebruikersdata uit EntraID (benodigd voor herstel van autorisaties in SharePoint) en een script voor herstel van data uit de back-up.

Risico
Het M365-back-up- en herstelproces wordt verstoord als de maatwerkscripts niet meer aansluiten op M365 of de back-up oplossing door bijvoorbeeld technische ontwikkelingen.

Aanbeveling
Beschouw als Belastingdienst de ontwikkelde scripts expliciet als maatwerk en richt hiervoor een bijpassend proces voor onderhoud in.

2.3 Bevindingen bij onderzoeksvraag III: inhoudelijk en aantoonbaar overeenkomen van back-up met brondata

Onderzoeksvraag III is: 'Welke bevindingen heeft de ADR ten aanzien van het inhoudelijk en aantoonbaar overeenkomen van de data vastgelegd in de back-up in het datacenter van de Belastingdienst met de brondata in M365 zonder ongeautoriseerde of onbedoelde wijzigingen?' Voor het beantwoorden van deze vraag zijn interviews gehouden met architecten, een back-upspecialist, een M365-specialist, lijnmanagers en een programmamanager. Op basis van de interviews en ontvangen documentatie zijn wij gekomen tot de bevindingen in de volgende paragrafen.

2.3.1 Nog geen end-to-endcontrole om volledigheid van M365-back-up vast te stellen

De Belastingdienst heeft mede in het kader van de M365-pilot een dagelijkse M365-back-up geconfigureerd in de back-up oplossing. De uitvoering en status van deze back-ups zijn inzichtelijk via het dashboard van de back-up oplossing. Dit dashboard rapporteert gesignaleerde afwijkingen, bijvoorbeeld als een actieve gebruiker binnen M365 niet kan worden gevonden en er daardoor geen back-up van diens mailbox kan worden gemaakt. De betrokken back-upbeheerders geven aan het dashboard dagelijks te monitoren als onderdeel van de projectfase van de M365-back-up en waar nodig actie te ondernemen naar aanleiding van de gesignaleerde afwijkingen. Op dit moment ontbreekt voor de M365-back-up echter nog een end-to-endcontrole, bijvoorbeeld op het aantal gebruikers, mailboxen, bestanden of hoeveelheid data. Dit betekent dat er geen zekerheid is of de gemaakte back-up in aantallen of volumes volledig overeenkomt met M365 en de back-up oplossing. Hierdoor kan niet volledig worden aangetoond dat de M365-back-up volledig is.

Risico

Zonder het uitvoeren van een end-to-endcontrole is er geen zekerheid dat de back-up compleet, juist en identiek aan de bron is. Eventuele afwijkingen zullen pas (te laat) bij herstel aan het licht komen.

Aanbeveling

Versterk mede op basis van een risicoafweging de end-to-endcontrole en voer periodiek deze volledigheidscontrole uit.

2.3.2 Verschillende softwarefouten onderkend in de back-up oplossing op het gebied van back-up en herstel

De Belastingdienst heeft bij het testen van de back-up oplossing een aantal softwarefouten gevonden die deels invloed hebben op de volledigheid van de back-up. Zo stopt de back-up van een individuele mailbox als hierin een corrupt bestand aanwezig is. Een andere softwarefout is dat een lege map in een OneDrive ervoor zorgt dat herstel van de data uit de betreffende OneDrive niet mogelijk is. Beide fouten zijn aangemeld bij de leverancier van de geïntegreerde back-up oplossing, maar zijn nog niet opgelost. Over deze punten heeft de Belastingdienst aan de ADR laten weten:

1. de leverancier van de back-up oplossing verricht naar inschatting van de Belastingdienst alle mogelijke inspanning om problemen snel en adequaat op te lossen.
2. In de markt is het gebruikelijker dat dataherstel wordt uitgevoerd naar een andere M365-tenant, terwijl herstel naar lokale opslag buiten M365 minder vaak voorkomt en deze functionaliteit in de praktijk nog weinig is beproefd.
3. In vervolg op het voorgaande punt heeft de Belastingdienst zelf de indruk in Nederland de 'launching customer' te zijn voor de back-up oplossing op het gebied van het on-premises herstel van M365-data en hiervoor zelfs wereldwijd een van de eerste te zijn.

Risico

De functionaliteit in de back-up oplossing voor het on-premises herstellen van M365-data is nog geen bewezen technologie. Hierdoor bestaat een verhoogd risico

dat de Belastingdienst bij uitbreiding naar meer M365-gebruikers tegen nieuwe softwarefouten of andere functionele problemen aanloopt, wat kan leiden tot niet-herstelbare back-ups.

Aanbeveling
Blijf de back-up oplossing gedurende het toevoegen van M365-gebruikers intensief en systematisch testen. Richt hierbij extra aandacht op randgevallen en nieuwe gebruikssituaties, zodat tijdig eventuele softwarefouten worden gedetecteerd en kunnen worden opgelost.

2.4 Bevindingen bij onderzoeksvraag IV: afronding back-up M365 binnen het afgesproken tijdvenster

Onderzoeksvraag IV is: 'Welke bevindingen heeft de ADR ten aanzien van de uitvoering en afronding van de back-up binnen het afgesproken tijdvenster waarbij alle gebruikersdata wordt meegenomen die op het moment van het begin van het tijdvenster aanwezig is?' Voor het beantwoorden van deze vraag zijn interviews gehouden met architecten, een back-upspecialist, een M365-specialist, lijnmanagers en een programmamanager. Op basis van de interviews en ontvangen documentatie zijn wij gekomen tot de bevindingen in de volgende paragrafen.

2.4.1 Geen formele juridische borging dat het back-upproces blijft werken zoals ingericht

Voor het maken van de dagelijkse M365-back-up maakt de back-up oplossing gebruik van de standaard programmatische interface (API) van M365 (M365 API). Deze API wordt door alle M365-klanten binnen een regio gebruikt en kent dynamische gebruikslimieten. Wanneer deze limieten worden overschreden, past Microsoft throttling toe: het afremmen van het API-verkeer om te voorkomen dat één organisatie, zoals de Belastingdienst, disproportioneel veel capaciteit benut en andere gebruikers mogelijk hinder daarvan ondervinden. Dit zou ertoe kunnen leiden dat de M365-back-up aanzienlijk langer duurt dan gebruikelijk of zelfs mislukt.
In het contract tussen Belastingdienst en Microsoft zijn op dit onderwerp geen afspraken gemaakt. In de praktijk is de Belastingdienst met het maken van de M365-back-up nog niet tegen limieten aangelopen. Inschatting van de Belastingdienst is dat throttling vooral plaatsvindt als veel partijen gelijktijdig gebruikmaken van M365 en Microsoft de bandbreedte over klanten moet verdelen. In de praktijk heeft de Belastingdienst doorgaans de mogelijkheid om op rustige momenten extra data te verwerken via de M365 API voor de back-up.
De ADR schat in dat het risico op throttling toeneemt in uitzonderlijke situaties, bijvoorbeeld als een exitscenario aanstaande is en veel gebruikers tegelijkertijd hun data uit M365 willen veiligstellen of bij uitval van complete Microsoft-datacenters in de regio. In dergelijke gevallen zullen de limieten waarschijnlijk aanzienlijk lager liggen, terwijl juist op die momenten het slagen van de back-up van cruciaal belang is.
Daarnaast vindt de back-up van M365-gebruikersdata plaats over het internet. Hierdoor is het proces ook gevoelig voor externe verstoringen, zoals een DDoS-aanval op de internetkoppeling van de Belastingdienst of de M365 API. Een dergelijke aanval kan de uitvoering van de back-up nadelig beïnvloeden.

Risico
De tijdigheid van de uitvoering van het back-upproces wordt aangetast, doordat er een verstoring optreedt. Met Microsoft zijn geen formele afspraken gemaakt over API-limieten en throttling om de back-up uit te voeren zoals gepland in zowel normale als uitzonderlijke omstandigheden, bijvoorbeeld kort voor het optreden van het exitscenario. Daarnaast is het back-upproces mogelijk kwetsbaar voor externe verstoringen, zoals een DDoS-aanval op de internetkoppeling van de Belastingdienst. Opgemerkt wordt dat door het gebruik van een incrementele back-upstrategie (zie ook § 2.1.3) bij een verstoring alleen de gewijzigde gebruikersdata van de afgelopen 24 uur wordt geraakt.

Aanbeveling

Documenteer de risicoafweging voor het niet hebben van formele afspraken en richt aanvullende beheersmaatregelen in gebaseerd op het risico. Neem in deze analyse ook de mogelijke impact van externe verstoringen, zoals DDoS-aanvallen, mee.

2.4.2 *Nog niet aangetoond dat de back-up oplossing, de back-up binnen het gekozen tijdvenster kan uitvoeren voor de gehele Belastingdienstpopulatie*

De Belastingdienst voert de M365-back-up buiten kantooruren uit. Het is noodzakelijk dat de back-up vóór de start van de volgende werkdag is afgerond. In de huidige pilot blijkt dat het proces voor het maken van een incrementele back-up voor enkele duizenden gebruikers circa twee uur duurt. Wanneer deze tijdsduur lineair wordt geëxtrapoleerd naar het volledige aantal beoogde M365-gebruikers van de Belastingdienst, dan zou het uitvoeren van de back-up te lang duren.

Op basis van de best practices van de leverancier van de back-up oplossing is de verwachting dat de M365-back-up parallel kan worden uitgevoerd, waarbij per groep van enkele duizenden gebruikers de back-up gelijktijdig verloopt. Hierdoor kan de totale back-uptijd voor alle beoogde gebruikers binnen acceptabele grenzen blijven. Het testen van deze parallelle uitvoering op basis van verschillende gebruikersgroepen moet echter nog in de praktijk plaatsvinden en de goede werking moet nog worden aangetoond. Dit kan pas worden uitgevoerd naarmate meer medewerkers van de Belastingdienst daadwerkelijk gebruikmaken van M365.

In een interview met de betrokken back-upbeheerders hebben wij gezien dat monitoring plaatsvindt op onder meer de looptijd van de M365-back-up.

Risico

De M365-back-up wordt niet binnen het beschikbare tijdvenster afgerond, waardoor M365-gebruikersdata niet tijdig wordt veilig gesteld.

Aanbeveling

Zet de huidige monitoringsactiviteiten voor de M365-back-up voort en tref waar noodzakelijk aanvullende beheersmaatregelen.

2.5 Bevindingen bij onderzoeksvraag V: bruikbaarheid back-up bij ongeplande exit M365

Onderzoeksvraag V is: 'Welke bevindingen heeft de ADR ten aanzien van de bruikbaarheid van de back-up voor het voorzien van een alternatieve werkplekoplossing van gebruikersdata in het geval een ongeplande exit van M365 plaatsvindt?'

De context voor de beantwoording van deze onderzoeksvraag is dat de focus van de Belastingdienst op dit moment ligt op het inrichten van een aantoonbaar volledige en juiste on-premises back-upvoorziening van de gebruikersdata uit M365. Zoals we ook al in § 2.1 beschreven, is het een bewuste keuze van de Belastingdienst om een vervolg op het huidige project te richten op herstel van werkplekfunctionaliteit inclusief restore van M365-gebruikersdata in een alternatieve werkplekomgeving. Binnen deze context signaleren wij de bevindingen in de volgende paragrafen.

2.5.1 *Back-up M365-data on-premises opgeslagen, maar heeft karakter black box; in exitscenario is ondersteuning door leveranciers niet gegarandeerd*

De back-up van de gebruikersdata uit M365 wordt on-premises opgeslagen op de back-up oplossing in het datacenter van de Belastingdienst. De beheerders van de Belastingdienst hebben geen inzicht in de interne werking van de back-up oplossing en dit functioneert daarmee als een 'black box'. Dit betekent ook dat er geen inzicht is in het interne dataformat waarin de back-ups van de gebruikersdata zijn opgeslagen.
Toegang tot én herstel van de gebruikersdata vindt plaats via de grafische gebruikersinterface of de standaard programmatische interface (API) van de back-up oplossing. Als deze interfaces niet functioneren op het moment dat dataherstel

noodzakelijk is, dan heeft de Belastingdienst geen toegang tot de back-up van gebruikersdata, ook al staat deze in het eigen datacenter. Op dit moment kan de Belastingdienst in een dergelijk geval ondersteuning vragen van de betreffende leveranciers maar in het exitscenario is niet gegarandeerd dat deze ondersteuning nog beschikbaar is.

Risico
In een noodsituatie is de Belastingdienst afhankelijk van het goed functioneren van de herstelfunctionaliteit van de back-up oplossing voor gebruikersdata. Als deze functionaliteit niet beschikbaar is en ondersteuning door de leveranciers ontbreekt, kan de Belastingdienst in het exitscenario de gebruikersdata niet herstellen uit de back-up.

Aanbeveling
Voer een expliciete risicoanalyse uit voor het exitscenario waarbij er rekening mee wordt gehouden dat de leveranciers de back-upoplossing niet meer kunnen ondersteunen, bijvoorbeeld door een sanctie. Als mitigerende maatregel geven wij in overweging om periodiek (bijvoorbeeld wekelijks) een restore uit te voeren van de gebruikersdata in het datacenter van de Belastingdienst in een direct toegankelijk format en deze data in deze vorm te bewaren. Hiermee wordt enerzijds het herstelproces getest en anderzijds is daarmee altijd een actuele en direct toegankelijk kopie van de gebruikersdata beschikbaar.

2.5.2 Testen herstel individuele objecten planmatig aangepakt, maar nog niet afgerond

Momenteel richt het project zich op het testen van het herstel van individuele objecten uit de M365-back-up, zoals een mailbox. Hiervoor is een testplan opgesteld dat de Belastingdienst stapsgewijs doorloopt. Er staan nog enkele testbevindingen open en niet alle activiteiten zijn al uitgevoerd. Zoals in § 2.3.2 is toegelicht, is het herstellen van OneDrive-data nog niet mogelijk door een probleem met het terugzetten van lege mappen. Ook is herstel van de combinatie van SharePoint-sitegegevens en toegangsgegevens uit EntraID wel als testactiviteit benoemd, maar nog niet uitgevoerd.

De ADR constateert dat de Belastingdienst het herstel van individuele objecten uit de M365-back-up planmatig test, maar dat deze werkzaamheden ten tijde van het onderzoek nog niet waren afgerond. Het doel van een vervolg op het huidige project is het integraal (in bulk) herstellen van gebruikersdata, maar daarvoor is op dit moment nog geen testplan opgesteld.

Omdat het testen van het herstel van individuele objecten uit de M365-back-up binnen het project wel in beeld is, maar de werkzaamheden nog niet zijn afgerond, formuleren we voor dit onderdeel geen risico's of aanbevelingen.

3 Verantwoording onderzoek

3.1 Werkzaamheden

Dit onderzoek is uitgevoerd in maart 2026 conform onze opdrachtbevestiging met referentie 2026-82492. Wij merken op dat het onderzoek is uitgevoerd, terwijl het project back-up M365 nog niet was afgerond. Dit betekent dat wij in een aantal gevallen tussentijdse resultaten en producten hebben onderzocht. Waar dit relevant is, hebben wij dit vermeld in onze onderzoeksresultaten.

Voor de beantwoording van de onderzoeksvragen 2 t/m 5 hebben wij een referentiekader opgesteld, inclusief een overzicht van op te vragen documentatie. In § 3.2 staat een beschrijving van het referentiekader op hoofdlijnen. De ontvangen documentatie is geanalyseerd aan de hand van het referentiekader. Hierin staan ook de uitkomsten van de interviews die wij hebben gehouden met betrokken medewerkers van de Belastingdienst en de resultaten van waarneming ter plaatse, waarmee wij inzicht hebben gekregen in de werking van het M365-back-upsysteem en het bijbehorende stelsel van maatregelen. De eerste onderzoeksvraag heeft een meer beschrijvend karakter en is rechtstreeks beantwoord op basis van de in deze paragraaf genoemde werkzaamheden.

De volgende medewerkers zijn geïnterviewd:

Persoonsgegevens

3.2 Referentiekader

De eerste onderzoeksvraag heeft een verkennend en inventariserend karakter en hiervoor is als algemene kwaliteitseis gehanteerd dat het stelsel van maatregelen door de Belastingdienst is uitgewerkt in termen van organisatie, processen en procedures, en technische maatregelen.

Het referentiekader voor de onderzoeksvragen 2 t/m 5 is gerealiseerd op basis van de detaillering van de respectievelijke onderzoeksvragen, de uitwerking van het kwaliteitscriterium integriteit zoals beschreven in § 1.3, de belangrijkste risico's die hiermee samenhangen en de beheersdoelstellingen waarmee deze risico's kunnen worden gemitigeerd.

3.3 Gehanteerde standaard en kwaliteitsborging

Deze opdracht is uitgevoerd in overeenstemming met de Internationale Standaarden voor de Beroepsuitoefening van Internal Auditing. Dit onderzoek verschaft geen zekerheid in de vorm van een oordeel of conclusie, omdat het een onderzoeksopdracht betreft en geen controle-, beoordelings- of andere assurance-opdracht. Als hier wel sprake van was geweest, dan zouden we wellicht andere zaken hebben geconstateerd en gerapporteerd.

De opdracht is uitgevoerd conform de algemene uitgangspunten voor de uitoefening van de interne auditfunctie bij de rijksdienst. Daarbij hoort ook een stelsel van kwaliteitsborging. Een onderdeel daarvan is dat er een onafhankelijke kwaliteitstoetsing heeft plaatsgevonden op deze onderzoeksopdracht.

3.4 Verspreiding rapport

De ADR is de interne auditdienst van het Rijk. Dit rapport is primair bestemd voor de opdrachtgever met wie wij deze opdracht zijn overeengekomen. Voor de openbaarmaking van ADR-rapporten door het opdrachtgevende ministerie gelden de voorschriften uit de Wet open overheid. De minister van Financiën stuurt elk halfjaar een overzicht van de rapporten die de ADR heeft uitgebracht naar de Tweede Kamer.

4 Ondertekening

Den Haag, 6 juli 2026

Persoonsgegevens

Auditdienst Rijk

Bijlage I Managementreactie

Belastingdienst

Belastingdienst

Auditdienst Rijk

Persoonsgegevens

Concerndirectie Informatie-voorziening en Databeheersing
CIO Office

Contactpersoon

Persoonsgegevens

Datum
7 juli 2026

Betreft: Managementreactie onderzoeksopdracht ADR naar back-up en recoveryvoorziening voor Microsoft 365 in de public cloud

Geachte Persoonsgegevens

De Belastingdienst heeft de Auditdienst Rijk (ADR) verzocht om onderzoek te verrichten naar de inrichting en eventuele aandachtspunten van de zogenoemde back-upvoorziening welke specifiek was ingericht voor de uitrol van M365 met betrekking tot de kantoorautomatisering voor de Belastingdienst, Douane en Dienst Toeslagen. Het onderzoek is uitgevoerd in een periode waarin de back-upvoorziening nog niet was afgerond. De ADR benoemt ook in haar onderzoeksrapport dat onderzoeksresultaten deels gebaseerd zijn op tijdelijke resultaten. De Belastingdienst heeft kennisgenomen van dit onderzoeksrapport en dankt de ADR voor de aangedragen bevindingen en aanbevelingen.

Aangezien de Belastingdienst eerst het on-premises scenario gaat uitlopen, zal de context en daarmee de opzet van de backup-voorziening wezenlijk veranderen. De waardevolle aandachtspunten van de ADR worden door de Belastingdienst meegenomen in het vervolg van het traject.

Met vriendelijke groet,

Persoonsgegevens

Auditdienst Rijk
Postbus 20201
2500 EE Den Haag
Persoonsgegevens