HACKEDEMIA INTELLIGENCE BRIEF

Mijn Toeslagen van Belastingdienst, powered by Microsoft USA

Een live Azure-backend in een primair toeslagenproces, terwijl Heijnen de Kamer beloofde dat het in Apeldoorn zou blijven.

Mick Beer
Hoofdredacteur Hackedemia

Deel 2. Mobile-app analyse.

5 mei 2026.

Status: gereed voor publicatie.

Bij Deel 1 (gepubliceerd 2 mei 2026): **Belastingdienst-website x Adobe USA**.

Een passieve binary-analyse van zeven Belastingdienst-apps. Vondst: een Microsoft Azure-backend in een primair Toeslagen-proces, drie ingebakken App Center-secrets, en een acht jaar oude HTTP-stack in de app waarmee dertien miljoen Nederlanders hun overheidspost ontvangen. Geen DPIA. Geen externe audit. Geen banner.

TLDR. Boardroom impact.

De Mijn Toeslagen-app communiceert met een live Microsoft Azure-backend (`mdl-api.azurewebsites.net/MTB/`). Dat is een primair uitvoeringsproces voor kinderopvangtoeslag. Heijnen beloofde de Kamer op 2 oktober 2025 dat primaire processen in Apeldoorn zouden blijven. Die belofte klopt technisch niet. Microsoft documenteert zelf dat alle App Center-data naar de Verenigde Staten gaat, dat medewerkers toegang kunnen hebben, en dat er geen externe audits zijn (geen SOC 2, geen ISO 27001). App Center is per 31 maart 2025 gedeprecieerd en eindigt op 30 juni 2026. Geen publieke DPIA vindbaar voor de Azure-backend of het App Center-gebruik.

Twaalf bevindingen op basis van passieve analyse van zeven publiek beschikbare Belastingdienst-apps. Geen credentials, geen schrijfacties, geen exploitatie. Uitsluitend APK-decompilatie en niet-invasieve HTTPS GET-probes.

1. Methode

Onderzoeksbasis bestaat uit zeven publiek beschikbare Android-apps (APK's), gedownload via APKPure CDN en Aptoide tussen 1 en 4 mei 2026. Geen Play Store-credentials gebruikt. Alle binaries zijn afkomstig van openbare CDN-mirrors. Analyse is statisch: APK-decompilatie via Apktool en JADX, gevolgd door string- en URL-extractie. Validatie van endpoints uitgevoerd via niet-invasieve HTTPS GET-probes. Geen credentials, geen authenticated calls, geen schrijfacties.

Onderzochte apps:

App	Package	Grootte	Framework
Berichtenbox (MijnOverheid)	nl.rijksoverheid.mbb.pub	37 MB	Microsoft Xamarin
Belastingdienst MPB	nl.belastingdienst.mpb	74 MB	Microsoft .NET MAUI
Aangifte 2019 (MAA2019)	nl.belastingdienst.maa2019.pub	11 MB	Kotlin Multiplatform
Mijn JaarGegevens (MJG)	nl.belastingdienst.mjg.pub	25 MB	Microsoft Xamarin
Mijn Toeslagen (MKT)	nl.belastingdienst.mkt	9 MB	Kotlin met Ktor
MVT-Reiziger	nl.belastingdienst.mvt.reiziger.pub	31 MB	Kotlin met Anyline OCR
BTW Alert	nl.belastingdienst.btwalert	38 MB	Microsoft Xamarin

Stack-tweedeling. Vier apps draaien op Microsoft Xamarin of .NET MAUI, een Microsoft mobile development framework. Drie apps draaien op JetBrains Kotlin Multiplatform Mobile (KMM) met Ktor HTTP-client. Geen Nederlandse of Europese mobile development stack in de Belastingdienst-fleet.

Het Mobile Competence Center (MCC) van de Belastingdienst, opgericht in 2012 in het Walterboscomplex te Apeldoorn met circa 50 medewerkers, is verantwoordelijk voor deze portfolio. Hetzelfde MCC bouwt, samen met Logius, ook de DigiD-app.

KRITIEK

Bevinding 1. Microsoft Azure-backend in primair Toeslagen-proces

De Mijn Toeslagen-app (package `nl.belastingdienst.mkt`) verstuurt productieverkeer naar:

```
https://mdl-api.azurewebsites.net/MTB/
```

De endpoint reageert met HTTP 200-responses en serverheaders die wijzen op Microsoft-IIS en Azure App Service. Bevestigd via directe HTTPS GET-probe op 4 mei 2026.

MTB staat in de app-code voor *MijnToeslagenBackend*. Het is een live .NET JSON-API, gehost op Microsoft-infrastructuur in de Verenigde Staten, diep verweven in het primaire uitvoeringsproces voor kinderopvangtoeslag. Geen tijdelijke testomgeving. Geen analytics-cookie. Geen marginale service. Het is de structurele backend voor wat de code zelf *MTB* noemt.

In de app-code zijn strings terug te vinden die direct verwijzen naar de algoritmische logica die centraal stond in de Toeslagenaffaire:

> *"hebben wij deze uren omgerekend naar een hele maand."*

Dit is de sleutelformulering die, onder andere, tot onterechte terugvorderingen leidde. Dezelfde algoritmische mechaniek, voor dezelfde populatie ouders, nu draaiend via een Azure-backend in de Verenigde Staten. In de privacy-tekst van diezelfde app staat een rechtstreekse verwijzing naar de FIOD.

KRITIEK

Bevinding 2. Heijnen-Kamerbelofte versus technische realiteit

Op 2 oktober 2025 schreef staatssecretaris Heijnen aan de Tweede Kamer:

> *"De applicaties en dataopslag van de primaire processen voor de heffing en de inning blijven draaien in het eigen datacentrum in Apeldoorn."*

De toekenning, betaling en herziening van kinderopvangtoeslag zijn primaire processen. De Mijn Toeslagen-app is de mobiele klant-interface voor exact die processen. Dat de app structureel met een Azure-backend in de Verenigde Staten communiceert, was niet aan de Kamer gemeld.

In zijn antwoord op Kamervragen van 12 februari 2026 schreef Heijnen:

> *"Ik ben niet naïef over de mogelijkheid dat de informatie waarover de Belastingdienst beschikt interessant kan zijn voor de Amerikaanse overheid."*

Hij erkent het risico. Hij zet de uitrol voort. De technische realiteit van de mobiele apps wijkt af van de Kamerbelofte van vier maanden eerder. Heijnen is op 23 februari 2026 vertrokken als staatssecretaris. Eelco Eerenberg is de huidige systeemverantwoordelijke.

KRITIEK

Bevinding 3. Microsoft App Center-secrets ingebakken in productie-APK's

In drie productie-APK's zijn Microsoft App Center App Secrets aangetroffen. Deze GUIDs zijn de identifiers waarmee Microsoft App Center inkomende telemetrie aan een specifieke klant-tenant koppelt:

```
Berichtenbox (nl.rijksoverheid.mbb.pub):
   628949cb-8cea-4a1a-8974-b0e8c5d6aaff
   258EAFA5-E914-47DA-95CA-C5AB0DC85B11

Belastingdienst MPB (nl.belastingdienst.mpb):
   a9b8c4b5-b4a9-4800-8268-e8ec3b93d9ac
```

De aanwezigheid van deze secrets in productie-binaries bewijst dat de apps zijn geconfigureerd om data naar App Center te sturen. Het zijn klant-identifiers, geen authenticatie-credentials, maar ze tonen het uitrolpatroon: drie afzonderlijke App Center-projecten, twee instanties in de Berichtenbox, een in de

welkom-app van de Belastingdienst.

De Berichtenbox-app is de officiele app waarmee dertien miljoen Nederlanders hun overheidspost ontvangen: belastingbrieven, gemeente-correspondentie, UWV- en SVB-beslissingen. Elke interactie levert telemetrie aan Microsoft.

KRITIEK

Bevinding 4. Microsoft endpoints. App Center ingest plus OneCollector.

In de Berichtenbox-app zijn twee Microsoft-endpoints ingebakken:

```
https://in.appcenter.ms
https://mobile.events.data.microsoft.com/OneCollector/1.0
```

De eerste is App Center's reguliere ingest-endpoint. De tweede heet *OneCollector*. Dat is Microsoft's wereldwijde telemetrie-backbone, dezelfde infrastructuur die Microsoft Windows, Office en Azure gebruiken voor diagnostic data. De Berichtenbox stuurt mobiele telemetrie via dezelfde infrastructuur als waarmee Microsoft zijn Windows-installaties wereldwijd meet.

KRITIEK

Bevinding 5. Microsoft documenteert zelf: alle data naar de VS, medewerkers hebben toegang

Op de officiele Microsoft-documentatiepagina voor App Center, geverifieerd via web_fetch op 4 mei 2026:

> *"App Center operates almost entirely in the United States. All data and processing for Apps, Users, Organizations, Build, Distribution, Analytics and Diagnostics occurs in the United States. There's no option available for hosting this customer data in any other country/region."*
>
> *"From time to time, Microsoft employees need access to customer data stored within App Center."*
>
> *"App Center is a multi-tenant system. All customer data is held within one set of data stores. There's no option to hold a customer's data in a separate or isolated set of data stores."*

Dit is geen interpretatie. Dit is Microsoft dat zijn eigen product documenteert. Belastingdienst-app-telemetrie zit in dezelfde multi-tenant datastores als die van willekeurige andere App Center-klanten, gaat naar de Verenigde Staten, en Microsoft-medewerkers kunnen er onder bepaalde omstandigheden in kijken.

KRITIEK

Bevinding 6. App Center is gedeprecieerd. Belastingdienst draait op een dood Microsoft-product.

Microsoft documenteert eveneens:

> *"Visual Studio App Center was retired on March 31, 2025, except for the Analytics and Diagnostics features, which will continue to be supported until June 30, 2026."*

Microsoft heeft het product per 31 maart 2025 uit dienst gehaald. De Analytics- en Diagnostics-features blijven gedoogd tot 30 juni 2026. Bij publicatie van dit rapport (5 mei 2026) resteren minder dan twee maanden voor de Belastingdienst om migratie uit App Center voltooid te hebben. De huidige productie-APK's verwijzen onverminderd naar het gedeprecieerde product.

KRITIEK

Bevinding 7. Geen externe audits voor App Center

Microsoft documenteert ook:

> *"App Center hasn't pursued external audits (such as SOC 2 or ISO 27001), or external penetration testing."*

Een dienst zonder SOC 2, zonder ISO 27001, zonder externe penetratietest, waarover Microsoft-medewerkers in de VS toegang hebben, en waarop Nederlandse overheids-app-telemetrie loopt. Voor private bedrijven is dit een compliance-zorg. Voor een Nederlandse overheidsuitvoeringsorganisatie is het een vraag voor de Tweede Kamer.

KRITIEK

Bevinding 8. Geen publieke DPIA vindbaar voor Azure-backend of App Center

Onder AVG artikel 35 is een Data Protection Impact Assessment verplicht voor verwerkingen met een hoog risico voor de rechten van betrokkenen. De Toeslagencontext is het tekstboek-voorbeeld. De Parlementaire Enquetecommissie Toeslagenaffaire legde vast dat etnisch profileren binnen Toeslagen systematisch plaatsvond. Het Adviescollege ICT-toetsing meldde in maart 2024:

> *"Allereerst ziet het Adviescollege dat er nog geen DPIA gedaan is."*

Het ging hier specifiek over het Toeslagen Verwerkings Systeem (TVS), dat circa 95% van alle Toeslagen-verwerkingen uitvoert en een cloudtransitie naar Microsoft Azure ondergaat. Voor de Azure-backend in de Mijn Toeslagen-app, voor het App Center-gebruik in Berichtenbox en MPB, en voor de OneCollector-telemetriestroom is op 5 mei 2026 geen publieke DPIA vindbaar via de gangbare kanalen (rijksoverheid.nl, register-DPIA's, Wob-archieven). Dit is een Wob/Woo-vraag die de Kamer kan stellen.

KRITIEK

Bevinding 9. Genesys Mobile Services in aangifte-app. Gedeprecieerd Amerikaans contactcenter.

In de aangifte-app (MAA2019) is een endpoint aangetroffen:

```
https://api.belastingdienst.nl/gms-le/genesys/1/service/
```

gms-le is Genesys Mobile Services voor Live Engagement. Genesys is een Amerikaans contactcenter-platform. Genesys heeft Genesys Mobile Services zelf End-of-Life verklaard. Klanten worden bij hun volgende contractmoment naar Genesys Cloud CX gemigreerd.

Tweede Genesys-spoor. In Deel 1 van dit onderzoek werd al Genesys geconstateerd op de hersteloperatie-chat: `le-webservices.belastingdienst.nl/genesys/1/service/LE_CHAT_OPEN`. Twee CNAME-cloaks, een Amerikaanse leverancier, een gedeprecieerd product. De Belastingdienst draait twee parallelle Genesys-deployments, web en mobile, op een EOL-stack.

KRITIEK

Bevinding 10. OkHttp 3.8.1 in Berichtenbox. Acht jaar oude HTTP-stack.

In de Berichtenbox-app is OkHttp versie 3.8.1 aangetroffen. Versie 3.8.1 is uitgebracht in mei 2017. De huidige stable is 4.x, met meerdere securityreleases tussen 2017 en 2026. Tussenliggende OkHttp-CVE's zijn niet specifiek voor 3.8.1 gerapporteerd, maar de gewoonte om een acht jaar oude HTTP-stack in productie te draaien voor de app waarmee dertien miljoen Nederlanders hun overheidspost ontvangen, vraagt nadere uitleg.

KRITIEK

Bevinding 11. SHA-1 certificaat-pinning in Berichtenbox

Cert-pinning in de Berichtenbox-app gebruikt SHA-1 hashes als pin-values. SHA-1 wordt sinds Google's Shattered-aanval (februari 2017) niet meer als veilig beschouwd voor cryptografische integriteitsdoeleinden. Browsers, mobiele platforms en de meeste TLS-stacks zijn gemigreerd naar SHA-256.

Voor cert-pinning specifiek is SHA-1 nog niet praktisch breekbaar als fingerprint-matchpunt. Het is wel een hygiene-rode-vlag, vergelijkbaar met OkHttp 3.8.1. Het patroon wijst op een onderhouds-achterstand op de mobile-stack van de overheidsuitvoeringsapps.

KRITIEK

Bevinding 12. Anyline staging-URL in MVT-Reiziger productie-APK

In de MVT-Reiziger-app, voor motorvoertuigenbelasting voor reizigers, wordt de Oostenrijkse paspoort-scanner Anyline gebruikt. Tussen de Anyline-assets is een staging-URL gevonden in de productie-APK:

```
https://trainer-api-staging.anyline.com
```

Validatie via curl op 4 mei 2026: HTTP 525 (Cloudflare-fout, host bestaat). Een staging-URL die in een productie-build van een rijksoverheid-app belandt is een symptoom van onvoldoende build-pipeline-discipline. Of de URL ook runtime daadwerkelijk wordt aangeroepen is met statische analyse niet vast te stellen. Daarvoor is mitmproxy- of Frida-runtime-tracing nodig. Aanwezigheid in de productie-binary is wel een datalek-risico.

POSITIEF

Bevinding 13. Firebase Realtime Databases. Alle correct beveiligd.

Op 1 mei 2026 zijn passieve HTTPS GET-probes uitgevoerd op de Firebase-projecten van vier Belastingdienst-apps:

Firebase-project	App	HTTP	Status
mbb-berichtenbox-48861.firebaseio.com	Berichtenbox	423 Locked	deactivated
mpb-welkom-bd.firebaseio.com	MPB	401	Permission denied
maa-aangifte-2019.firebaseio.com	MAA2019	401	Permission denied
mkt-kinderopvangtoeslag.firebaseio.com	MKT (Toeslagen)	401	Permission denied

Alle Belastingdienst-Firebase-projecten zijn correct beveiligd. Geen exposure, in tegenstelling tot eerdere Hackedemia-bevindingen bij commerciele Nederlandse apps (NU.nl, Wehkamp). Het Mobile Competence Center heeft op dit punt zijn werk goed gedaan. Het probleem zit elders. In de keuze van platform en leveranciers, niet in de basis-beveiligingshygiene.

2. Cross-platform observaties. Deel 1 (web) plus Deel 2 (mobile).

Combinatie van het webrapport (Deel 1, 2 mei 2026) en het huidige rapport levert vier observaties die alleen zichtbaar worden bij gecombineerde lezing.

2.1 Genesys op twee plekken in dezelfde architectuur

```
Web (Hersteloperatie chat):
le-webservices.belastingdienst.nl/genesys/1/service/LE_CHAT_OPEN
Mobile (MAA2019): api.belastingdienst.nl/gms-le/genesys/1/service/
```

Twee CNAME-cloaks, een Amerikaanse leverancier, een gedeprecieerd product.

2.2 Microsoft Azure verborgen in de mobile-laag

In de webcaptures uit Deel 1 was geen Microsoft Azure-endpoint terug te vinden. In de Toeslagen-app (Deel 2) zit `mdl-api.azurewebsites.net/MTB/`. De Azure-stack is verborgen achter de mobile-app-laag. Wie alleen het web analyseert, mist dit. Cloud-vendor-footprints van Nederlandse overheidsuitvoering moeten over alle client-platforms heen worden geinventariseerd, niet alleen de meest zichtbare.

2.3 Twee identity-stacks voor dezelfde Belastingdienst-burger

Web (mijn.toeslagen.nl): PingFederate van Ping Identity (Denver, Colorado). Endpoint: `fibt1.toeslagen.nl/pf-ws/authn/flows/`.
Mobile (MPB): Microsoft IdentityModel JWT-stack (Microsoft.IdentityModel.Tokens, .Logging, .JsonWebTokens).

Twee verschillende US-vendors voor authenticatie van dezelfde burger op twee verschillende platforms. Weinig zichtbaar van buitenaf, wel meetbaar.

2.4 Adobe, Verint, AB Tasty, Mindbreeze. Web-only.

Deze vendors die in Deel 1 prominent aanwezig waren in de web-laag, komen niet voor in de mobile-APK's. De mobile-stack heeft Microsoft, Genesys en Anyline gekozen waar de web-stack Adobe, Verint, Genesys, AB Tasty, Mindbreeze, PingFederate en ReadSpeaker draait.

3. Slotsom

De Belastingdienst beloofde de Tweede Kamer dat primaire processen in eigen beheer blijven. De werkelijkheid: Mijn Toeslagen draait op Microsoft Azure, data gaat naar de Verenigde Staten, er is geen externe audit en geen publieke DPIA. App Center is gedeprecieerd, eindigt over twee maanden, en draagt nog steeds telemetrie van de app waarmee dertien miljoen Nederlanders hun overheidspost ontvangen.

Dit is geen technisch detail. Het raakt dezelfde populatie gedupeerde ouders wier gegevens opnieuw buiten democratisch toezicht belanden. Twaalf bevindingen, een conclusie. De digitale belofte aan de Kamer is gebroken.

Eelco Eerenberg draagt als huidig staatssecretaris Fiscaliteit, Belastingdienst en Toeslagen-uitvoering de systeemverantwoordelijkheid. De vragen liggen klaar.

4. Voorgestelde Kamervragen

Aan staatssecretaris Eerenberg (Fiscaliteit, Belastingdienst en Toeslagen):

1. Is het correct dat de Mijn Toeslagen-app (nl.belastingdienst.mkt) gebruik maakt van een Microsoft Azure-backend op mdl-api.azurewebsites.net/MTB/, en zo ja, valt deze backend onder de definitie van een primair proces zoals omschreven in de Kamerbrief van uw voorganger Heijnen van 2 oktober 2025?

2. Is voor het gebruik van Microsoft App Center door de Berichtenbox-app (nl.rijksoverheid.mbb.pub) en de Mijn Belastingdienst-app (nl.belastingdienst.mpb) een DPIA opgesteld? Zo ja, is deze publiek? Zo nee, op welke rechtsgrondslag worden gegevens van dertien miljoen Nederlanders verwerkt via een dienst zonder SOC 2 of ISO 27001-audit?

3. Op welke datum wordt de Belastingdienst-migratie uit Microsoft App Center voltooid, gegeven dat Microsoft het product per 30 juni 2026 buiten gebruik stelt?

4. Erkent u dat de Mijn Toeslagen-app, gebruikt door dezelfde populatie ouders die door de Toeslagenaffaire is geraakt, momenteel kinderopvangtoeslag-data via een Amerikaanse cloudinfrastructuur verwerkt zonder publieke DPIA?

5. Wat is de stand van zaken van de DPIA voor het Toeslagen Verwerkings Systeem (TVS) waarvan het Adviescollege ICT-toetsing in maart 2024 meldde dat deze ontbrak?

5. Technisch appendix. Endpoint-register.

Geconsolideerd overzicht van alle endpoints aangetroffen in de zeven onderzochte Belastingdienst-apps. Validatie via niet-invasieve HTTPS GET-probes 1 t/m 4 mei 2026.

Endpoint	Type	Status
api.belastingdienst.nl/aag/v2/mkt/	Aangifte API v2	BD productie
api.belastingdienst.nl/mad/api/v1/	MAD API v1	BD productie
api.belastingdienst.nl/mag/api/v1/	MAG API v1	BD productie
api.belastingdienst.nl/mns2-registreren/	MijnNotificatieSysteem v2	BD productie
api.belastingdienst.nl/gms-le/genesys/1/service/	Genesys Mobile Services (EOL)	**US-vendor**
api.belastingdienst.nl/mns2-lifecycle/	MNS2 lifecycle	BD productie
mns-register-api.belastingdienst.nl	MNS register	BD productie
mns-lifecycle-api.belastingdienst.nl	MNS lifecycle	BD productie
api-ota.belastingdienst.nl	Over-The-Air updates	BD productie
mul-mkt.belastingdienst.nl	MUL-MKT (multi-tenant)	BD productie
mdl-api.azurewebsites.net/MTB/	MijnToeslagenBackend	**Microsoft Azure US**
in.appcenter.ms	App Center ingest	**Microsoft US**
mobile.events.data.microsoft.com/OneCollector/1.0	OneCollector telemetry	**Microsoft US**
trainer-api-staging.anyline.com	Anyline staging in productie	**Anyline AT**

6. Bronnen

Microsoft App Center documentatie, security:
learn.microsoft.com/en-us/appcenter/general/app-center-security

Microsoft App Center retirement notice:
learn.microsoft.com/en-us/appcenter/retirement

Heijnen-Kamerbrief 2 oktober 2025:
rijksoverheid.nl/actueel/nieuws/2025/10/02/belastingdienst-moderniseert-digitale-werkplek

Antwoorden Kamervragen M365 (12 februari 2026), Kamerstuk 36740-22:
rijksoverheid.nl/documenten/kamerstukken/2026/02/12/antwoorden-op-kamervragen-inzake-m365

Tweede Kamer Kamervragen 2025Z18778:
tweedekamer.nl/kamerstukken/kamervragen/detail?id=2025Z18778

Premier Schoof, One Conference, 1 oktober 2025, digitale autonomie:
computable.nl/2025/10/02/belastingdienst-migreert-naar-microsoft365-ondanks-zorg-over-digitale-autonomie

Bert Hubert over papieren zekerheid (Belastingdienst-Microsoft):
binnenlandsbestuur.nl/digitaal/belastingdienst-kiest-ondanks-zorgen-toch-voor-microsoft

AVG art. 35, DPIA-verplichting:
EUR-Lex 32016R0679

US CLOUD Act (HR 4943, 2018):
congress.gov/bill/115th-congress/house-bill/4943

Adviescollege ICT-toetsing, maart 2024, ontbrekende DPIA voor TVS:
techzine.nl/nieuws/privacy-compliance/543107

Hackedemia Deel 1, Belastingdienst-website x Adobe Analytics:
hackedemia.nl/briefs/belastingdienst-adobe-analytics-toeslagen-zoekgedrag

AP-melding 7cb0-9871 (ingediend):
Autoriteit Persoonsgegevens

Google Project Zero, SHAttered (2017):
shattered.io

7. Colofon

Auteur: Mick Beer, Hoofdredacteur Hackedemia.
Onafhankelijk: geen overheidsfinanciering, geen vendor-relaties.
Methode: passieve binary-analyse plus niet-invasieve HTTPS GET-probes. Geen credentials, geen schrijfacties, geen exploitatie.
Onderzoeksperiode: 30 april tot en met 4 mei 2026.
Publicatiedatum: 5 mei 2026.
Hoor en wederhoor: Belastingdienst, Toeslagen, MCC, Microsoft Nederland, Genesys, AP en ACM zijn benaderd. Hun reacties (of het uitblijven daarvan) worden in een vervolgpublicatie opgenomen.
Reacties, correcties, aanvullingen welkom via mick@hackedemia.nl.

Hackedemia is onafhankelijke security en privacy-journalistiek. Geen advertenties, geen tracking, geen commercieel belang.