Ministerie van Justitie en Veiligheid

Directie Informatievoorziening en Inkoop

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
Henrique Barnard

T 070 370 79 11

Datum
1 november 2022

Projectnaam
Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS Rijk

CIO Rijk, CIO-beraad, CTO-raad, deelnemers SLM MIcrosoft, Google Cloud en Amazon Web Services, geinteresseerden

memo

Toelichting op de getroffen maatregelen in Office365 for the Web and mobile Office apps (DPIA juni 2020)

SLM Rijk (Strategisch Leveranciersmanagement Rijk) heeft onderzoek laten doen naar het gebruik van 'Office for the Web and mobile Office apps'. Dit traject is gestart met een Data Protection Impact Assessment (DPIA) in 2020.[1] Met de DPIA is de verwerking van diagnostische gegevens onderzocht. Er is geen onderzoek gedaan naar verwerking van functionele- of inhoudelijke gegevens van gebruikers (zoals tekst, foto´s of video´s).

Microsoft heeft diverse maatregelen getroffen om de geconstateerde risico's in de DPIA weg te nemen. Deze maatregelen zijn (ook technisch) gecontroleerd. Hieronder volgt daarvan een overzicht. Een samenvatting van de diensten, de DPIA, de risico´s en de overeengekomen maatregelen is al gepubliceerd.[2]

In de DPIA is geconstateerd dat er zes hoge- en drie lage risico's waren ten aanzien van Office for the Web and the mobile Office apps.

Na afronding van de DPIA heeft SLM Rijk de bevindingen met Microsoft gedeeld. SLM Rijk en Microsoft zijn vervolgens in gesprek gegaan over maatregelen die de zes hoge risico's kunnen mitigeren. Daarbij is overeenstemming bereikt over de maatregelen die Microsoft zou doorvoeren.

In de periode na het afronden van de DPIA is de voortgang van de overeengekomen mitigerende maatregelen gemonitord en beoordeeld.

Getroffen maatregelen Microsoft

Zoals hierboven aangegeven zijn SLM Rijk en Microsoft in 2020 maatregelen overeengekomen om de zes hoge risico's te mitigeren. Van belang daarbij is dat

[1] Data protection impact assessment Office 365 for the Web and mobile Office apps, 30 June 2020, URL: https://www.rijksoverheid.nl/documenten/rapporten/2020/06/30/data-protection-impact-assessment-office-365-for-the-web-and-mobile-office-apps.

[2] Zie: https://open.overheid.nl/repository/ronl-4d806ca8-3adf-468f-a6d2-56c2a020c0fa/1/pdf/Samenvatting%20DPIA%20Office%20Web%20en%20Mobiele%20apps%2030%20juni%202020.pdf.

sommige maatregelen snel konden worden doorgevoerd. Andere maatregelen vereisten meer tijd om te implementeren.

De geconstateerde risico's en de daarbij overeengekomen maatregelen waren als volgt:

Nr.	Hoge risico's	Overeengekomen maatregelen Microsoft
1	Gebrek aan doelbinding voor de diagnostische gegevens van mobiele Office apps en Office for the Web	Alleen optreden als verwerker voor de mobiele Office apps en Office for the Web (met uitzondering van de Controller ConnectedExperiences en de legitieme zakelijke doeleinden van Microsoft), niet als verantwoordelijke, en de gegevens alleen verwerken voorde drie geautoriseerde doeleinden.
		Alleen gebruikmaken van geautoriseerde subverwerkers in de Online Services. Als Microsoft subverwerkers wil inschakelen, moeten deze worden goedgekeurd in overeenstemming met het privacy amendement van de Rijksoverheid.
		Stoppen met het verzenden van persoonsgegevens naar derde partijen, tenzij dit een geautoriseerde subverwerker is of het verkeer is goedgekeurd in verband met een ingeschakelde Controller Connected Experience of een ingeschakelde Add-in.
		Ervoor zorgen dat alle Controller Connected Experiences centraal kunnen worden uitgeschakeld door beheerders.
2	Gebrek aan transparantie diagnostische gegevens Office for the Web, de mobiele Office apps, Connected Experiences en de Connected Cloud Services	Volledige en begrijpelijke documentatie publiceren over de verwerking van diagnostische gegevens van de mobiele Office apps, Office for the Web, alle Connected Experiences en de Connected Cloud Services.
		Beschikbaar stellen van data viewing mogelijkheden voor verkeer van de mobiele OneDrive, Outlook en Teams apps.
3	Gebrek aan controle over het telemetrieniveau in Office for the Web en de mobiele Outlook,Teams en OneDrive apps	Alleen optreden als verwerker voor de mobiele Office apps en Office for the Web en de gegevens alleen verwerken voor de drie geautoriseerde doeleinden.
		Implementeren van telemetrie keuzemogelijkheden voor beheerders voor de mobiele OneDrive, Outlook en Teams apps
		Technische maatregelen treffen om ervoor te zorgen dat de verzameling van diagnostische gegevens via telemetrie via Office for the Web tot het noodzakelijke minimum wordt beperkt.
4	Gebrek aan controle doorgifte persoonsgegevens via Office for the Web aan derden	Geen integratie van diensten in de Online Services die persoonsgegevens doorgeven aan derden via Office for the Web, tenzij de derde partij een geautoriseerde subverwerker is of (onderdeel is van) een ingeschakelde Controller Connected Experience.
		Ervoor zorgen dat de in de DPIA geïdentificeerde derde partijen uit de diensten worden verwijderd, als subverwerkers worden geautoriseerd of (onderdeel worden van) een Controller Connected Experience.

Nr.	Hoge risico's	Overeengekomen maatregelen Microsoft
5	Gebrek aan controle: doorgifte van persoonsgegevens van mobiele Office apps aan derden	Geen integratie van diensten in de Online Services die persoonsgegevens doorgeven aan derden via de mobiele Office apps, tenzij de derde partij een geautoriseerde subverwerker of (onderdeel is van) een ingeschakelde Controller Connected Experience.
		Er voor zorgen dat de in de DPIA geïdentificeerde derde partijen uit de diensten worden verwijderd, als subverwerkers worden geautoriseerd of (onderdeel van) een Controller Connected Experience worden.
6	Geen inzage voor betrokkenen	De inzagerechten van betrokkenen respecteren. Wanneer ze verwerker is, door het huidige DSAR-programma uit te breiden met alle gegevens die via de Connected Experiences, Azure AD en mobiele Office apps zijn verzameld, met uitzondering van de Required Service Data.
		De inzagerechten van betrokkenen honoreren voor de persoonsgegevens die Microsoft als verantwoordelijke verzamelt.

In augustus 2020 is geconstateerd dat aan de volgende mitigerende maatregelen tegemoet is gekomen door Microsoft.

1. Nadere informatie geven over de in het DPIA-rapport genoemde derden en de classificatie van deze partijen als subverwerker (indien Microsoft een verwerker is) of als Controller Connected Experience, een Non-Microsoft Product of een Add-In (indien Microsoft de verwerkingsverantwoordelijke is).

2. Uitrollen van controles waarmee de systeembeheerder, naar keuze van de klant, het gebruik van optionele/Controller Connected Experiences voor de mobiele toepassingen Excel, OneDrive, Outlook, PowerPoint, Teams en Word kan beperken of uitschakelen.

3. Uitrollen van controles om de verzameling door Microsoft van diagnostische gegevens van de mobiele toepassingen Excel, OneDrive, Outlook, PowerPoint, Teams en Word te beperken (keuze voor telemetriebeperking voor beheerders), plus ervoor zorgen dat alle diagnostische gegevens die worden verzameld vanuit Office for the Web worden beperkt tot (het minimumniveau van) de vereiste Servicegegevens.

4. De aanwezigheid voorkomen van bepaalde inhoud (bestands-, pad-, gebruikersnamen) in de (strikt noodzakelijke) telemetriegegevens wanneer delen van Office for the Web worden gebruikt, tenzij de verwerking onvermijdelijk is om de gevraagde functionaliteit van een dienst te leveren, concreet, om samenwerking mogelijk te maken aan bestanden in OneDrive.

In april 2021 heeft een vervolgonderzoek plaatsgevonden en is in een technisch onderzoek geconstateerd dat Microsoft *grotendeels* tegemoet is gekomen aan alle overige overeengekomen mitigerende maatregelen.

De aanwezigheid van een Controller Connected Experience in de Outlook Web app en de aanwezigheid van namen en e-mailadressen in de telemetriegegevens die verzonden worden door de Android OneDrive, iOS OneDrive en Word Online applicaties waren wel nog twee punten van zorg. Deze punten zijn uitgediept en nader besproken met Microsoft.

In juli 2022 is er opnieuw een technische verificatie gedaan en is gekeken naar de nog openstaande punten. De vraagstelling en de uitkomsten daarvan zijn in onderstaande tabel opgenomen. Hieruit blijkt dat Microsoft in drie van vijf (zie nr. 1, 3, en 5) gevallen het verkeer naar derden heeft stopgezet. In de situaties genoemd onder 2 en 4 kunnen systeembeheerders van overheidsorganisaties het verkeer effectief centraal blokkeren voor alle gebruikers met PowerShell-opdrachten.

Nr.	Vraag	Antwoord
1	Is Microsoft gestopt met het versturen van verkeer naar derden via thumbnails in de Teams store (getest op Windows)?	Ja
2	Heeft Microsoft de toegang tot Bing in SharePoint Online (toegankelijk via een browser) geblokkeerd, of kan een beheerder dergelijk verkeer effectief blokkeren?	Nee, maar systeembeheerders kunnen dit verkeer uitschakelen met PowerShell-opdrachten
3	Heeft Microsoft de toegang tot Bing en Giphy in de Outlook Web App (bij gebruik van Expressions) geblokkeerd, of kan een admin dergelijk verkeer effectief blokkeren?	Ja
4	Heeft Microsoft de toegang tot locatiegegevens (waarbij Microsoft optreedt als zelfstandige verantwoordelijke) in Calendar for the Web geblokkeerd, of kan een beheerder dergelijk verkeer effectief blokkeren?	Nee, maar Microsoft heeft in oktober 2022 een PowerShell-opdracht gegeven waarmee systeembeheerders dit verkeer centraal kunnen blokkeren.
5	Is Microsoft gestopt met het versturen van gegevens naar Cloudflare als een gebruiker de privacy-instellingen van Teams op een iOS-apparaat raadpleegt?	Ja

De werking van de twee Powershell-opdrachten is (technisch) getest en de maatregelen blijken effectief om te voorkomen dat Microsoft persoonsgegevens van klanten voor eigen doelen zou mogen verwerken.

Conclusie en implementatieadvies

Microsoft is tegemoet gekomen aan de overeengekomen mitigerende maatregelen ten aanzien van de geconstateerde hoge privacyrisico´s.

Microsoft heeft twee risico's ondervangen door PowerShell-opdrachten ter beschikking te stellen. Dit vergt weliswaar iets meer werk dan de dataminimalisatie-instellingen in het dashboard waar SLM Rijk op aanstuurde, maar met de opdrachten kunnen systeembeheerders de risico's wel verlagen.

Een algemeen en belangrijk aandachtspunt blijft de rechten van betrokkenen onder de AVG, waaronder het recht op inzage. Meer specifiek gaat het om inzage in de categorie telemetriegegevens die Microsoft ´Required Service Data´ noemt. SLM blijft hierover in gesprek met Microsoft om dit op het noodzakelijke niveau te brengen.

Overige aanbevelingen voor overheidsorganisaties

1. Schakel de Controller Connected Experiences uit.

2. Stel de telemetrieverzameling van de mobiele Office apps in op het laagste niveau.

3. Gebruik als beheerder regelmatig de Data Viewer Tool om de telemetrie te bekijken die vanuit de mobiele Office apps wordt verzonden.

4. Stel intern een bewaartermijnenbeleid op, maak het bekend en dwing naleving af / ruim verouderde gegevens op, dit vanwege de risico's van doorgifte naar de VS.

5. Test regelmatig nieuwe versies van de mobiele Office apps en beveel gebruikers aan om de nieuwste versies te installeren.

6. Stel bij gebruik van de Connected Cloud Services (Teams, OneDrive en SharePoint) een beleid op om te voorkomen dat bestandsnamen en bestandspaden persoonsgegevens bevatten.

7. Informeer medewerkers over de inzagemogelijkheden via Microsoft's Data Subject Access Request tool en de auditlogs.[3]

Met vriendelijke groet,

Team Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services

[3] https://open.overheid.nl/repository/ronl-4d806ca8-3adf-468f-a6d2-56c2a020c0fa/1/pdf/Samenvatting%20DPIA%20Office%20Web%20en%20Mobiele%20apps%2030%20juni%202020.pdf.