Ministerie van Justitie en Veiligheid

CIO Rijk, CIO-beraad, CTO-raad, deelnemers SLM MIcrosoft, Google en AWS Rijk, geinteresseerden

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
13 juni 2023

Projectnaam
Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS Rijk

Ons kenmerk
4712670

memo

Toelichting op technisch verificatieonderzoek Microsoft 365 Defender.

Technisch Verificatieonderzoek

SLM Microsoft, Google Cloud en Amazon Web Services (SLM) heeft aan Privacy Company de opdracht gegeven om een technisch verificatieonderzoek te doen naar Microsoft 365 Defender. Een technisch verificatieonderzoek is een onderzoek waarbij (diepgaand) wordt gekeken naar de technische werking van een dienst en of er in overeenstemming met de gemaakte (contractuele) afspraken door een leverancier wordt gehandeld. Eventuele (privacy)risico´s worden daarbij ook geadresseerd.

Microsoft 365 Defender is een beveiligingssuite met diverse diensten om apparaten, gebruikers, e-mail en log-ins te beschermen. De conclusies in het gepubliceerde technische verificatierapport zijn van toepassing op zowel de Enterprise- als de Educatieversie van Microsoft 365.

De volgende diensten vallen binnen de scope van het onderzoek:

- Microsoft Defender for Endpoint (MDE)
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps

Uit het definitieve rapport volgt dat Microsoft 365 Defender goed functioneert. Enkele kanttekeningen worden in het rapport wel gemaakt. Zo bleek uit het onderzoek dat niet alle schadelijke activiteiten, zoals oude spyware, werden herkend en in sommige gevallen het voordeel van de twijfel werd gegeven aan ‘known’ sender domains. Van belang is echter dat dit technisch verificatieonderzoek geen security assessment is en het rapport hier meer context bij geeft.

Verder maakt het rapport onderscheid tussen maatregelen welke(overheids)organisaties zelf kunnen treffen en die waarvoor actie van Microsoft vereist is. Organisaties wordt aangeraden om de aanbevolen maatregelen uit het verificatierapport te raadplegen en de geadviseerde maatregelen door te voeren.[1] Als dit wordt gedaan zijn er geen belemmeringen om Microsoft Defender 365 compliant en veilig te gebruiken.

[1] Deze zijn raadpleegbaar op pagina 6 t/m 8 van het technische verificatierapport.

Daarnaast heeft Microsoft naar aanleiding van gesprekken in april 2023 met SLM en Privacy Company enkele belangrijke verduidelijkingen gemaakt in haar documentatie over de doorgifte van persoonsgegevens naar de VS. Hieronder wordt op dit specifieke punt nader ingegaan.

Internationale doorgifte
Uit de (vertaalde) samenvattende tabel volgen diverse maatregelen voor Microsoft en overheidsorganisaties waaronder het onderstaande doorgifte risico.

Vraag	**Maatregelen Microsoft**	**Maatregelen (overheids)organisaties**
Doorgifte risico	Voltooi de EU Data Boundary zo snel mogelijk voor alle persoonsgegevens. Houd SLM op de hoogte van de voortgang.	Accepteer de risico´s van de overdracht van gepseudonimiseerde serverlogs en telemetriegegevens naar de VS tot het einde van 2023.
		Adviseer beheerders om geen persoonlijke gegevens te uploaden in bijlagen bij support tickets (overdracht naar de VS mogelijk tot eind 2024).
		Overweeg het gebruik van pseudoniemen voor specifieke medewerkers die met geheime gegevens werken en voor systeembeheerders.

De gehele tabel moet worden gelezen in samenhang met de onderliggende documentatie in het rapport. Daaruit volgt ten aanzien van het doorgifterisico dat er een (theoretische) kans bestaat dat Microsoft verplicht is op persoonsgegevens van medewerkers/personen voor veiligheidsdoeleinden over te dragen aan wetgevingsautoriteiten of veiligheidsdiensten. Dit overdrachtsrisico is al grondig geanalyseerd in de Data Transfer Impact Assessment (DTIA) inzake Teams, OneDrive en Sharepoint.[2] Uit dit technische verficatierapport is gebleken dat er geen sprake is van een hoog (doorgifte) risico bij het gebruik van Microsoft 365 Defender.

Als gevolg van de EU Data Boundary[3] wordt Content Data al exclusief in de EU verwerkt, evenals system generated logs. Eind 2023 verwacht Microsoft dat ook alle telemetrie data en geagregeerde data van de server logs, uitsluitend in de EU wordt verwerkt. Daarnaast kunnen naar verwachting eind 2024 alle support tickets van EU Enterprise en onderwijsklanten uitsluitend worden afgehandeld in de EU. Ongeautoriseerde toegang vanuit derde landen kan worden beperkt door personeel te instrueren om geen persoonlijke gegevens in support tickets op te nemen (behalve de naam van de persoon die het ticket indient).

Naast de ontwikkelingen rondom de EU Data Boundary is het van belang dat Microsoft ook andere maatregelen treft inzake internationale doorgifte. Zo pseudonimiseert Microsoft persoonsgegevens die worden verwerkt voor veiligheidsdoeleinden, vecht zij elk verzoek van inlichtingendiensten juridisch aan en publiceert zij tweemaal per jaar transparantierapporten. In deze rapporten is informatie raadpleegbaar over ´Law enforcement requests´.

[2] Deze is raadpleegbaar via: slm-mega.nl.

[3] Meer informatie hierover is raadpleegbaar via: Continuing Data Transfers that apply to all EU Data Boundary services - Microsoft Privacy | Microsoft Learn.

SLM volgt de ontwikkelingen met betrekking tot internationale doorgifte nauwlettend. Ook na 2023 zal SLM het risico van internationale doorgifte afwegen en (her) beoordelen in hoeverre dit rechtmatig kan plaatsvinden. In dit stadium vormt het doorgifte risico, zeker als de aanbevolen maatregelen in het verificatierapport worden toegepast, geen belemmering om Microsoft Defender 365 compliant te gebruiken.

Directie Informatievoorziening en Inkoop

Datum
13 juni 20233

Ons kenmerk
4712670

Conclusie en vervolg
Microsoft Defender 365 biedt een breed scala aan beschermingsmechanismen. Het is dan ook positief dat uit dit technische verificatierapport volgt dat dit product, dat ten goede komt aan de cyberweerbaarheid van organisaties, conform wet- en regelgeving kan worden gebruikt. Geadviseerd wordt wel om de aanbevolen maatregelen uit het rapport te implementeren. SLM blijft de ontwikkelingen bij Microsoft volgen. Ook blijft SLM met Microsoft in gesprek over alle relevante onderwerpen.

Met vriendelijke groet,

Teams Strategisch Leveranciersmanagement Microsoft, Google Cloud en Amazon Web Services