Samenvatting DPIA Windows 10 Enterprise v.1809 and preview v. 1903

11 juni 2019

De inkoopafdeling van het Rijk die verantwoordelijk is voor de aanschaf van Microsoft producten en diensten, SLM Microsoft Rijk, heeft een gegevensbeschermingseffectbeoordeling (Data Protection Impact Assessment, hierna: DPIA) uit laten voeren op de verwerking van gegevens over het gebruik van de grootzakelijke versie van Windows 10. Het DPIA rapport beschrijft de dataprotectierisico's voor betrokkenen door de verzameling van gegevens over het individuele gebruik van Windows 10 Enterprise versie 1809. Dit is de versie van het besturingssysteem die Microsoft in de herfst van 2018 heeft gelanceerd. De DPIA biedt ook een vooruitblik op versie 1903 die eind mei 2019 is gelanceerd. De DPIA is uitgevoerd door Privacy Company.

Onderwerp van de DPIA: telemetriegegevens op het niveau Beveiliging en Tijdlijn

De DPIA beschrijft de verschillen in dataprotectierisico's voor betrokkenen voor twee verschillende telemetrie-instellingen: Beveiliging en geblokkeerd door de firewall. Technisch gezien verzamelt Microsoft Corporation systematisch diagnostische gegevens over het individuele gebruik van de Windows 10 software (niet beperkt tot de Enterprise versie). Via de ingebouwde telemetrie-client verzamelt Microsoft automatisch telemetriegegevens op het apparaat, en verzendt die regelmatig naar haar cloudservers in de Verenigde Staten.

Systeembeheerders kunnen de dataverzameling minimaliseren door het telemetrieniveau op Beveiliging te zetten (Security), of door het telemetrieverkeer naar bekende eindpunten in het Microsoft netwerk te blokkeren.

De risico's van gegevensverwerking op de niveaus Basis en Volledig zijn niet onderzocht, omdat uit de openbare documentatie van Microsoft blijkt dat het bedrijf op die niveaus vertrouwelijke en gevoelige persoonsgegevens kan verzamelen.

Doorgaans slaan overheidsorganisaties de bestanden die ze maken met Office op in overheidsdatacentra, *on-premises*. De DPIA analyseert ook de dataprotectierisico's van nieuwe hybride netwerken, waarbij gegevens worden opgeslagen in Microsoft's cloudopslagdiensten *SharePoint Online* en *OneDrive for Business*. Dit rapport beschrijft ook de nieuwe Windows Tijdlijn (Timeline) functionaliteit. Hiermee kunnen gebruikers hun activiteiten bewaren in de Microsoft cloud om hun werk voort te kunnen zetten op andere apparaten.

Geen hoge dataprotectierisico's

Het gebruik van het Windows 10 besturingssysteem op de werkcomputer kan risico's met zich brengen op inbreuk op de persoonlijke levenssfeer van ambtenaren. Dit omdat Microsoft systematisch gegevens verzamelt over het gebruik van haar software en online diensten (diagnostische gegevens). Dit zijn doorgaans persoonsgegevens.l

Op grond van een technische analyse van het telemetriegegevensverkeer concludeert dit rapport dat Microsoft via de telemetrie op het Beveiligingsniveau weinig persoonsgegevens verwerkt, en geen persoonsgegevens van gevoelige aard. Daarom zijn er géén hoge dataprotectierisico's als het telemetrieniveau op Beveiliging wordt gezet, of het telemetrieverkeer wordt geblokkeerd.

Dit rapport identificeert vier lage dataprotectierisico's die veroorzaakt worden door de verwerking van diagnostische gegevens op Beveiligingsniveau over het gebruik van Windows 10 Enterprise. Hierbij is het uitgangspunt dat beheerders het gebruik van Windows Tijdlijn centraal blokkeren.

De (lage) risico's zijn:

1. Gebrek aan doelbinding en een rechtmatige grondslag voor de verwerking van de diagnostische persoonsgegevens;
2. Gebrek aan controle over derde partijen/verwerkers en toezicht via audits op de feitelijke gegevensverwerking;

3. De doorgifte van diagnostische persoonsgegevens naar de Verenigde Staten, terwijl er twee rechtszaken lopen bij het Europees Hof van Justitie over de adequaatheid van dataprotectiewaarborgen;
4. De lange bewaartermijn van de diagnostische persoonsgegevens.

Naleving van de AVG en paraplu-DPIA

De Windows 10 Enterprise software wordt op grote schaal gebruikt door verschillende overheidsorganisaties en bestuursorganen in Nederland, zoals de ministeries, de rechtspraak, de politie en de belastingdienst. Naar schatting 300.000 ambtenaren werken dagelijks met het besturingssysteem, vaak in combinatie met Microsoft Office software.

SLM Microsoft Rijk voert onderhandelingen met Microsoft namens de Rijksoverheid, maar de individuele overheidsorganisaties kopen de licenties en bepalen de instellingen en de omvang van de diagnostische gegevensverwerking door Microsoft Corporation in de Verenigde Staten. Deze paraplu-DPIA is richtinggevend en corrigerend, en bedoeld om de organisaties te ondersteunen bij het uitvoeren van eigen DPIA's, maar kan de specifieke risico-inschattingen niet invullen die de organisaties zelf moeten maken. Deze inschattingen zijn afhankelijk van de specifieke manier waarop ze de software aanbieden, de mate van vertrouwelijkheid van het werk, en de soorten persoonsgegevens die ze verwerken.

Diagnostische gegevens Windows 10 Enterprise

Microsoft heeft uitgelegd dat ze circa 1.200 soorten gebeurtenissen verzamelt via de Windows 10 telemetrie. Deze gegevens worden geanalyseerd door tien teams met Microsoft technici. De verzameling van telemetriegegevens is dynamisch. De technici van Microsoft kunnen nieuwe soorten informatie toevoegen aan de telemetrie gegevensstroom zonder voorafgaande kennisgeving aan gebruikers. De verzameling van Windows 10 telemetriegegevens staat los van, en is onafhankelijk van, de telemetriegegevens die door Microsoft Office worden verzameld. De gegevens worden ook naar verschillende netwerkeindpunten van Microsoft verstuurd.

Behalve de telemetriegegevens verzamelt Microsoft ook diagnostische gegevens over het gebruik van haar diensten op haar eigen cloudservers, als gebruikers bestanden openen of opslaan via SharePoint Online en OneDrive (in systeem-gegenereerde logbestanden). Deze gegevensverzameling is onzichtbaar voor de eindgebruikers.

Microsoft legt terecht uit dat diagnostische gegevens niet verward moeten worden met de functionele gegevens die noodzakelijkerwijs over internet verstuurd moeten worden om een gevraagde dienst te kunnen leveren. Bijvoorbeeld, een lokale weer- of nieuwsapp die om de locatie van een gebruiker vraagt. In dat geval zijn de locatiegegevens functionele gegevens. Met de term diagnostische gegevens wordt daarom bedoeld: de opslag door Microsoft op individueel niveau van technische metagegevens over het individuele gebruik van de Windows 10 Enterprise software, en de daarmee verbonden online diensten zoals SharePoint Online.

Technische analyse van de telemetriegegevens

De DPIA bevat een analyse van de inhoud van telemetriegegevens, zoals die zijn verzameld in de in het testlab van SSC-I, een IT-leverancier die deel uitmaakt van de Dienst Justitiële Inrichtingen. SSC-I heeft dit testlab ingericht in opdracht van het ministerie van Justitie en Veiligheid. Met behulp van de Data Viewer Tool in Windows 10, en het onderscheppen van het verkeer met Fiddler, is het uitgaande telemetrieverkeer opgeslagen gedurende het uitvoeren van een aantal precies uitgewerkte test scenario's. Het uitgaande verkeer is nog drie dagen erna vastgelegd, omdat Microsoft de telemetriegegevens in *batches* naar zichzelf verstuurt. De testscenario's zijn een weergave van de meest voorkomende taken in Windows door een gemiddelde ambtenaar en bevatten ook het gebruik van Windows Tijdlijn.

Persoonsgegevens

Op het telemetrieniveau Beveiliging verzamelt Microsoft een beperkte hoeveelheid gegevens over het individuele gebruik van de Windows 10 software door een ambtenaar. De verzamelde

telemetriegegevens bevatten een aantal unieke identifiers. Die identifiers stellen Microsoft in staat om gegevens over een individuele gebruiker door de tijd heen te combineren. Microsoft beschikt over de technische middelen om een individuele gebruiker te identificeren. Daarom zijn de verzamelde telemetriegegevens persoonsgegevens als bedoeld in artikel 4(1) van de AVG.

Gedurende dit onderzoek zijn er op het Beveiligingsniveau geen inhoudelijke gegevens (uit de inhoud van bestanden of emails) waargenomen in de telemetriegegevens.

Microsoft als verantwoordelijke voor de gegevensverwerking

Microsoft beschouwt zichzelf als (onafhankelijke) verwerkingsverantwoordelijke voor de gegevensverwerking via Windows 10 Enterprise. Microsoft beschouwt zichzelf (volgens de Online Service Terms) alleen als verwerker voor de diensten Windows Analytics en de specifieke online beveiligingsdienst Windows Defender Advanced Threat Protection.

Microsoft neemt hiermee een ander juridisch standpunt in over haar rol dan ten aanzien van de online diensten zoals Azure en Office 365. Bij die online diensten beschouwt Microsoft zichzelf wel als verwerker. Op de gegevensverwerking in Windows 10 is geen van de juridische privacywaarborgen van toepassing die vastgelegd zijn in de mantelovereenkomst tussen Microsoft en het Rijk. In plaats daarvan gelden alleen de algemene, op consumenten gerichte, verzekeringen uit de algemene privacyverklaring.

Uit een feitelijke analyse van de rollen blijkt dat het wenselijk is dat Microsoft zich – ook bij Windows 10 Enterprise – als verwerker gedraagt. Maar dat is bij de huidige werkwijze niet het geval. Omdat Microsoft de doelen bepaalt, en de overheidsorganisaties Microsoft in staat stellen voor die doelen gegevens te verwerken, zijn ze gezamenlijke verwerkingsverantwoordelijken voor de verwerking van diagnostische gegevens. Die feitelijke verhouding is niet geformaliseerd in een gezamenlijke verantwoordelijken-overeenkomst.

Gebrek aan doelbinding en grondslag

In haar technische documentatie noemt Microsoft specifieke doelen voor de verwerking van diagnostische gegevens over het individuele gebruik van de Windows 10 software. Maar deze informatie is niet juridisch bindend. Op grond van de overeenkomst met afnemers kan Microsoft de diagnostische gegevens verwerken voor bijna alle, zeer algemene, doelen uit haar algemene privacyverklaring. De 16 relevante doelen behelzen het gebruik van persoonsgegevens voor gepersonaliseerde advertenties in Windows 10 en in apps, om commerciële aanbiedingen te doen, en om de contactgegevens van klanten te gebruiken voor wervingsdoelen via email, SMS, post en telefoon.

De verwerking van de diagnostische gegevens voor zoveel brede en onafgebakende doelen, is in strijd met het doelbindingsbeginsel. Een organisatie mag alleen persoonsgegevens verwerken als zij er een grondslag voor heeft. De mogelijke grondslagen staan in artikel 6 van de AVG. Als (enige of gezamenlijke) verantwoordelijke kan Microsoft geen geslaagd beroep doen op toestemming van werknemers als bedoeld in de AVG in verband met de afhankelijke positie van werknemers, terwijl toestemming wel vereist is op grond van artikel 11.7a van de Telecommunicatiewet voor het ophalen van gegevens via internet via de ingebouwde software als die verwerking niet strikt noodzakelijk is.

Als (gezamenlijke) verwerkingsverantwoordelijken (of als gegevensverwerker) mogen Microsoft en de overheidsorganisaties op het Beveiligingsniveau een beperkt aantal diagnostische gegevens verwerken om te bepalen welke security updates nodig zijn, om problemen op te kunnen lossen met de verzending van de telemetriegegevens, om kwaadaardige software te kunnen herkennen en verwijderen en voor de Windows Defender antivirus en apparaatbescherming.

Als de verwerkingen beperkt zouden zijn tot deze gerechtvaardigde doelen, zou Microsoft een geslaagd beroep kunnen doen op de noodzaak voor de behartiging van haar gerechtvaardigd belang of dat van de overheidsorganisatie. In sommige gevallen zou Microsoft dan ook een

geslaagd beroep kunnen doen op de noodzaak voor de naleving van de overeenkomst van de werknemer met de overheidsorganisatie.

Conclusies

Als overheidsorganisaties de aanbeveling volgen van SLM Microsoft Rijk om Windows 10 Enterprise alleen te gebruiken met de telemetrie ingesteld op het laagste niveau Beveiliging (of het telemetrieverkeer geblokkeerd), and als ze centraal voorkomen dat gebruikers hun activiteiten kunnen synchroniseren via Windows Tijdlijn, zijn er geen hoge dataprotectierisico's die voortvloeien uit de diagnostische gegevensverzameling in Windows 10 Enterprise.

Dit rapport beschrijft contractuele, technische en organisatorische maatregelen die Microsoft en de overheidsorganisaties kunnen treffen om de resterende lage risico's helemaal weg te nemen.

Microsoft heeft op 21 mei 2019 een nieuwe versie van Windows 10 Enterprise gelanceerd, versie 1903. Deze versie maakt het mogelijk voor systeembeheerders op de Windows Update for Business functionaliteit te gebruiken als het telemetrieniveau op Beveiliging staat. In vorige Windows 10 versies was deze functionaliteit alleen beschikbaar bij telemetrieniveau Basis of hoger.

SLM Microsoft Rijk levert significante inhoudelijke input aan Microsoft voor het ontwerp van een structurele oplossing voor Windows 10 Enterprise klanten voor versie 1809 en latere versies. Microsoft geeft aan dat deze oplossing overheidsorganisaties in staat zal stellen om de AVG op een makkelijkere manier na te leven bij het gebruik van telemetrieniveaus Basis en hoger. Aan deze oplossing wordt gewerkt. Microsoft verwacht later dit jaar een aankondiging hierover te kunnen doen.