Ministerie van Justitie en Veiligheid

von
CIO Rijk, CIO-Rat, CTO-Rat, Teilnehmer SLM
Microsoft, Google und AWS Rijk, interessierte Parteien

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
21 februari 2022

Projectnaam
Strategisch Leveranciersmanagement Microsoft, Google Cloud en AWS Rijk

Ons kenmerk
3867538

memo

DSFA Microsoft Teams, OneDrive und SharePoint online

DSFA-Ergebnisse: sechs geringe Risiken

SLM Rijk[1] hat eine Datenschutz-Folgenabschätzung (DSFA) durchführen lassen zur Datenverarbeitung über Microsoft Teams, OneDrive und SharePoint Online. SLM Rijk hat festgestellt, dass bei der Nutzung dieser Dienste keine hohen Risiken bestehen.

Bei der Transparenz der Telemetriedaten besteht noch Verbesserungsbedarf. Microsoft hat versprochen, den Zugriffsprozess (über die Systemadministratoren) zu verbessern und besser zu erklären, warum viele gesammelte Daten entweder keine personenbezogenen Daten sind oder sofort anonymisiert werden und daher nicht mehr mit einer Person verknüpft werden können Zugriffsanforderer.

Hohes Risiko

Wenn Organisationen Microsoft Teams, SharePoint oder OneDrive Online für die Verarbeitung besonderer personenbezogener Daten verwenden, entsteht ein hohes Risiko. Unternehmen können dieses hohe Risiko für vertrauliche personenbezogene Daten in Dateien auf OneDrive und SharePoint mindern, indem sie ihre eigenen Verschlüsselungsschlüssel mit Microsoft Double Key Encryption verwenden. Microsoft bietet noch keine Ende-zu-Ende-Verschlüsselung für die Streaming-Kommunikation mit mehreren Teilnehmern in Teams an, nur für ungeplante Eins-zu-Eins-Videoanrufe. Microsoft hat bestätigt, dass es E2EE in Teams-Gruppenmeetings und -Chats ermöglichen wird, hat aber noch keinen Zeitplan angekündigt.

Risiken der Übermittlung personenbezogener Daten in die USA

Die Hauptrisiken hängen mit der Tatsache zusammen, dass Microsoft ein US-Unternehmen ist. Dadurch besteht die Möglichkeit, dass amerikanische Ermittlungs- und Geheimdienste Zugriff auf personenbezogene Daten von Nutzern der Dienste verlangen. Das bedeutet, dass bei der Nutzung der Microsoft-Dienste formal eine Übermittlung in ein Land außerhalb der EU ohne angemessenes Schutzniveau der personenbezogenen Daten erfolgt.

Darüber hinaus ist es wichtig zu erwähnen, dass der EDPB (Europäischer Datenschutzausschuss) angekündigt hat, dass er hofft, seine Untersuchung der Nutzung von Cloud-Diensten durch Regierungsbehörden bis Ende dieses Jahres abzuschließen.

Die Chance, dass Ermittlungs- und Geheimdienste den Zugriff verlangen, scheint vor allem theoretisch zu sein. Microsoft hat erklärt, dass es niemals Daten von Mitarbeitern öffentlicher Einrichtungen an Regierungen weitergegeben hat. Also auch nicht an die US-Regierung. Zudem verarbeitet und speichert Microsoft bereits fast alle

[1] SLM Rijk ist das Strategische Beschaffungsmanagement Microsoft des niederländischen Staates

personenbezogenen Daten von Mitarbeitern der niederländischen Regierung ausschließlich in europäischen Rechenzentren, nicht in den USA. Nur die pseudonymen Telemetriedaten werden nun systematisch in die USA gesendet. Bis Ende 2022 wird Microsoft diese personenbezogenen Daten auch automatisch ausschließlich in der EU verarbeiten.

Um die Risiken des Zugriffs auf personenbezogene Daten auf der Grundlage des anwendbaren amerikanischen Rechts abzubilden, hat SLM Rijk die internationale Anwaltskanzlei Greenberg Traurig LLP um Rat zum anwendbaren amerikanischen Recht gebeten. Dieses Wissen wurde in ein Q&A übersetzt, das später veröffentlicht wird.

Datenübermittlungs-Folgenabschätzung (DTIA)
Für jede Art von personenbezogenen Daten, die Microsoft über die drei Dienste verarbeitet, wurden die Risiken einer missbräuchlichen Weiterverarbeitung in einem Datenübermittlungs-Folgenabschätzung (DTIA) dargestellt. Es wurden sieben Arten von personenbezogenen Daten ermittelt, anhand derer eine Berechnung der Wahrscheinlichkeit durchgeführt wird, dass auf die Daten von den amerikanischen Ermittlungs- und Geheimdiensten nach geltendem Recht zugegriffen oder sie angefordert werden:

1. Live-Inhaltsdaten (Teams)
2. Gespeicherte Inhaltsdaten (Teams, OneDrive, SharePoint)
3. Diagnose (Telemetrie) (Teams, OneDrive, SharePoint)
4. Diagnose (Dienstprotokolle) (Teams, OneDrive, SharePoint)
5. Supportdaten (Teams, OneDrive, SharePoint)
6. Sicherheitsdaten (US) (Teams , OneDrive, SharePoint)
7. Kontoinformationen (Azure AD)

Die DTIA basiert auf einem öffentlichen Modell des Schweizer Anwalts David Rosenthal und wurde von Privacy Company angepasst. Dieses Excel wird bald veröffentlicht, damit andere Organisationen die DTIA wiederverwenden können.

Mit freundlichen Grüßen

Teams Strategisches Beschaffungsmanagement Microsoft, Google Cloud und Amazon Web Services