PRODATIS®

The eBusiness Solution Company.

Office 365: ein technisches Datenschutz-Update

Es wird viel über die Übertragung der Diagnosedaten von Office 365 an Microsoft diskutiert. Mittlerweile gibt es Möglichkeiten, diese Datenübertragung zu deaktivieren. Wir zeigen Ihnen, was sich alles abschalten lässt – und was Sie auch abschalten sollten. Zusätzlich stellen wir die Analytics-Analysedienste vor.

Im 9. Tätigkeitsbericht 2019 trifft das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) in Kapitel 3.4 „Windows 10 und Telemetriedaten" die Aussage, bei Windows 10 Enterprise Version 1909 lasse sich die Übermittlung der sogenannten Telemetriedaten an Microsoft komplett ausschalten (siehe https://ogy.de/baylda-tb-2019, S. 22). Das BayLDA gibt jedoch keine genauen Hinweise auf die ebenfalls dort zitierten „von Microsoft offiziell zur Verfügung gestellten Informationen und Tools". Der Umkehrschluss ergibt, dass Nutzer die Übermittlung von Messdaten in Windows Home/Professional und Education nicht komplett ausschalten können.

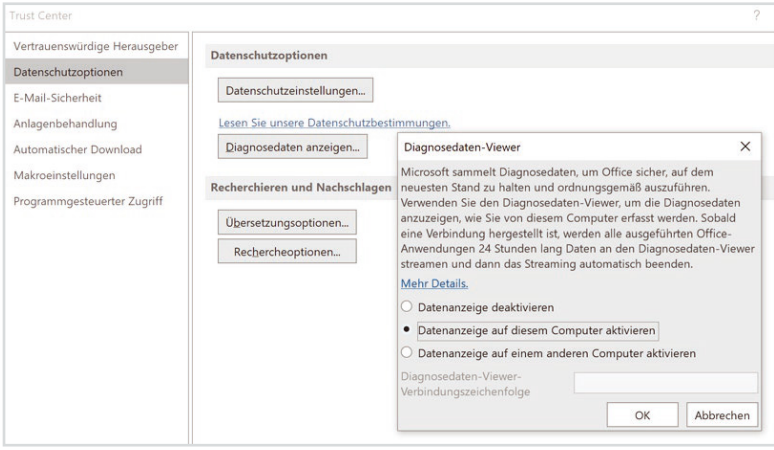

Abbildung 1: So lassen sich die Diagnosedaten für Microsoft Office 365 aktivieren

Diagnosedaten anzeigen lassen

Bei Microsoft Office 365 ist die Situation besser. Hier gibt es die Möglichkeit, die Übermittlung der Telemetriedaten komplett zu deaktivieren. Ein erster Schritt in diese Richtung ist, sich zunächst die Diagnosedaten anzeigen zu lassen.

Um Office-365-Diagnosedaten zu sammeln, gehen Sie in eine beliebige Office-Anwendung und wählen „Da-

tei“ → „Optionen“ → „Trust Center“ → „Einstellungen für das Trust Center“ → „Datenschutzoptionen“ aus. Unter „Diagnosedaten anzeigen“ schalten Sie die Option „Datenanzeige auf diesem Computer aktivieren“ ein (Abbildung 1). Sie können dann in der Diagnosedatenanzeige sehen, welche Daten an Microsoft übertragen wurden, und die Wirksamkeit von Einstellungen direkt überprüfen. Um auch Windows-10-Diagnosedaten zu bekommen, suchen Sie in der Anwendung „Microsoft Store“ nach „Diagnostic Data Viewer“. Dann wechseln Sie in das Startmenü und wählen „Einstellungen“ → „Datenschutz“ → „Diagnose & Feedback“ aus. Dort stellen Sie den Schalter unter „Diagnosedaten anzeigen“ auf „ein“. So werden die Diagnosedaten auch lokal gespeichert.

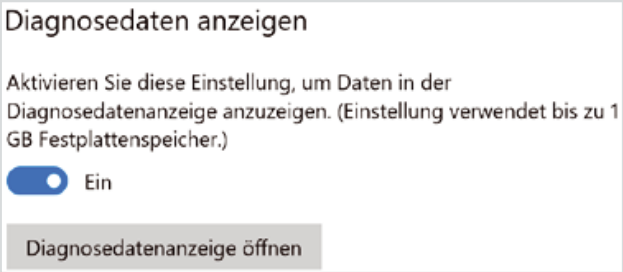

Abbildung 2: Diagnosedaten für Windows 10 aktivieren

Empfehlungen zu Telemetrie-Einstellungen unter Office 365

Um in Office 365 Telemetrie-Einstellungen vornehmen zu können mit dem Ziel, die Menge der übertragenen Daten reduzieren, muss mindestens die Microsoft-Oce-365-Version 1905 installiert sein.

Umfang der Telemetrie-Datenübertragung

Für den Umfang der Telemetrie-Datenübertragung in Microsoft Office 365 gibt es drei Levels: ■

- keine Telemetriedaten senden (3) ■
- optionale Daten senden (2)■
- erforderliche Daten senden (1)

Diese Einstellungen lassen sich über Gruppenrichtlinien oder Registry-Einstellungen vornehmen. Dabei wird in der Registry der Parameter „SendTelemetry“ nutzerspezisch entsprechend dem Wert in der Klammer gesetzt. Wir empfehlen, den Wert auf „3“ („weder noch“ bzw. „keine Daten“) zu setzen.

Verbundene Dienste

Darüber hinaus sollte die IT vier weitere Einstellungen zu den verbundenen Diensten (Controller Connected Experiences) setzen (Tabelle 1).

Das ist aber nicht immer „nebenwirkungsfrei“. Auf dem Rechner des Autors führt der Wert „DisconnectedState=2“ zu Problemen mit dem Zugriff auf Office-Dateien auf WebDAV-Freigaben (konkret beim Verschlüsselungsprogramm Cryptomator). Insofern muss die IT in der jeweiligen IT-Umgebung des Unternehmens oder der Behörde testen, ob Nebenwirkungen auftreten.

PRAXIS TIPP: Sorgen Sie als DSB dafür, dass der Verantwortliche die Beschäftigten deutlich darauf hinweist, dass sie die mobilen Office-365-Apps für iOS und Android nicht einsetzen dürfen. Das Gleiche gilt für die Office-365-Web-Apps, da sich bei ihnen die Übertragung von Diagnosedaten noch nicht abstellen lässt.

Customer Experience Improvement Program

Auch das „Customer Experience Improvement Program (CEIP)“ sollte die IT deaktivieren. Dazu muss sie einen Registry-Eintrag „CEIPEnable“ erstellen und auf null setzen (siehe Listing 1). Gleichzeitig gilt es, zwei Aufgaben zu deaktivieren. Dazu startet man die „Aufgabenplanung“, sucht unter „Aufgabenplanungsbibliothek“ → „Microsoft“ → „Windows“ → „Customer Experience Improvement Program“ nach den beiden Aufgaben „Consolidator“ und „UsbCeip“ und deaktiviert sie über das Kontextmenü. Diese beiden Programme sammeln und übertragen regelmäßig die Daten zum CEIP.

LinkedIn-Integration

Dann ist empfehlenswert, die LinkedIn-Integration für Office 365 auszuschalten. Dazu wählt man in der Administrationsoberfläche von Office 365 („Das neue Admin Center“ aktivieren) das „Azure Active Directory Admin

Richtlinieneinstellung	Registrierungseinstellung	Werte
Umfang der von Office 365 an Microsoft gesendeten Diagnosedaten	SendTelemetry	1 = erforderlich 2 = optional 3 = weder noch
verbundene Dienste, die Inhalte analysieren, in Office 365 erlauben	UserContentDisabled	1 = aktiviert 2 = deaktivier
verbundene Dienste, die Online-Inhalte herunterladen, in Office 365 erlauben	DownloadContentDisabled	1 = aktiviert 2 = deaktiviert
zusätzliche optionale verbundene Dienste in Office 365 erlauben	ControllerConnectedServicesEnabled	1 = aktiviert 2 = deaktivier
verbundene Dienste in Office 365 zulassen	DisconnectedState	1 = aktiviert 2 = deaktivier

Tabelle 1: Einstellungen zum Datenschutz für Microsoft Office 365

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\Common\Privacy]
"DisconnectedState"=dword:00000002
"UserContentDisabled"=dword:00000002
"DownloadContentDisabled"=dword:00000002
"ControllerConnectedServicesEnabled"=dword:00000002

[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\common\clienttelemetry]"SendTeleme-
try"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SQMClient]"CEIPEnable"=dword:00000000
```

Listing 1: Die Registry-Einstellungen, um die Telemetrie (Tabelle 1) und den CEIP-Client zu deaktivieren, als Input-Datei für den Registry-Editor.

Center“ aus und dann unter „Benutzer“ die „Benutzereinstellungen“. Dort dann unter LinkedIn-Kontoverbindungen den „Nein“-Button auswählen. Diese Funktionalität ist für deutsche Kunden derzeit anscheinend per Default deaktiviert. Ob das tat-sächlich so ist, sollte die IT aber überprüfen.

Analytics-Analysen

Neben den bisher angesprochenen datenschutzrelevanten Funktionalitäten hat Microsoft Anfang 2020 begonnen, die Analytics-Analysen breiter zur Verfügung zu stellen. Seit Kurzem stehen einige der Funktionen auch in den Business-Lizenzen zur Verfügung, nicht nur in den Enterprise-Lizenzen.

Microsoft MyAnalytics

Den Analysedienst „MyAnalytics“ gibt es in der Office-365-Version E5 schon länger. Mittlerweile ist er auch in Microsoft 365 und allen Office-365-Business-Paketen mit E-Mail-Hosting (Exchange Online) enthal-

ten. Microsoft wirbt damit, dass die Mitarbeiter durch die Einblicke in die persönliche Arbeitsweise mit Microsoft 365 produktiver werden. Unter anderem analysiert das Tool, wie viel Zeit ein Mitarbeiter damit verbringt, E-Mails zu lesen und zu schreiben, und zwar sowohl innerhalb als auch außerhalb der Dienstzeit. Außerdem wertet MyAnalytics aus, mit welchen Kollegen man die Zeit in Besprechungen verbringt.

Man kann sich wöchentlich E-Mails zusenden lassen, die das Zeitverhalten aufbereitet darbieten. Diese E-Mails enthalten auch personenbezogene Daten Dritter. So nennt die Analyse die Top-Kommunikationspartner namentlich. MyAnalytics ist daher datenschutzrechtlich kritisch. Das Tool verarbeitet zwar überwiegend eigene Daten. Doch es geht auch darum, Daten Dritter auszuwerten: Mit wem verbringe ich Zeit in Besprechungen? Außerdem ist der Einsatz von MyAnalytics mitbestimmt.

Beschäftigte können die Einstellungen selbst über das Portal https://myanalytics.microsoft.com verwalten. Das ist für Freiberufler und kleinste Unternehmen ein gangbarer Weg. In Unter-nehmen können die Administratoren für alle Beschäftigten MyAnalytics konfigurieren – und am besten deaktivieren. Wer im Microsoft-365-Admin-Center (neue Version) angemeldet ist, kann über das „Zahnrad" die Einstellungen einblenden und dann nach einem Klick auf den Link „Einstellungen" (direkt unter der Überschrift „MyAnalytics") zu den Feature-Einstellungen wechseln. Abbildung 3 zeigt, wie sich MyAnalytics vollständig abschalten lässt.

Microsoft Workplace Analytics

Microsoft wirbt für Workplace Analytics mit dem Satz: „Nutzen Sie das volle Potenzial Ihrer Daten durch Einblicke in die tägliche Nutzung von Office 365." Dahinter steckt eine Auswertung der Zusammenarbeit der Beschäftigten mit Office 365. Das Analysetool wertet ähnlich wie MyAnalytics gemeinsame Kalendereinträge und die Nutzung der Office-Programme aus.

Workplace Analytics ermittelt z.B. die Stunden, die ein Beschäftigter durchschnittlich in Besprechungen verbringt, die Anzahl von Terminen und wie stark Mitarbeiter per E-Mail oder durch gemeinsame Meetings interagieren. Workplace Analytics wertet allerdings die Daten in der Software aus. Bei einem Termin geht es also um die eingetragene Dauer des Termins und nicht um die tatsächliche Dauer.

Abbildung 3: Microsoft MyAnalytics bitte komplett deaktivieren! Zusätzlich lässt sich unter „MyAnalytics" das Plug-in „Insights" installieren. Dieses Plug-in für Outlook sollte jedoch nicht installiert werden, da es weitere Daten für die Analytics-Analyse sammelt.

ACHTUNG: Da die Auswertungen zu MyAnalytics auf dem Exchange-Server stattfinden, ist eine Konfiguration auf dem Klienten (z.B. durch Gruppenrichtlinien) nicht möglich. Microsoft stellt unter https://ogy.de/myanalytics eine Anleitung zur Verfügung, wie sich die Einstellungen über PowerShell-Befehle deaktivieren lassen.

Das Arbeitsverhalten und die Zusammenarbeit von Teams und einzelnen Beschäftigten auszuwerten und zu vergleichen, soll die Produktivität und Effizienz des

Unternehmens steigern. Diese Auswertung ist jedoch nur sinnvoll, wenn die Mitarbeiter die Kalendereinträge einheitlich nutzen. Der eine Mitarbeiter trägt nur echte Termine ein, der andere Platzhalter, um Zeiten für die ungestörte Arbeit zu blockieren. Beide Verhalten sind legitim, aber nicht vergleichbar.

Abbildung 4: Ein (nicht personenbezogener) Ausschnitt aus einer MyAnalytics-Mail. Die E-Mail enthält auch Namen und E-Mail-Adressen von Kommunikationspartnern und Mitarbeitern

ONLINE-TIPP

- Zusammenfassung der Datenerfassung in Office: https://privacy.microsoft.com/de-de/data-collecti-on-Office■
- Datenschutz-Folgenabschät-zung zu Microsoft Office und Windows-Software: https://ogy.de/dpia-ms-office

Die Empfehlung: Wir bewegen uns hier im Bereich der Mitbestimmung. Verantwortliche sollten das Thema daher zuerst mit den Personalvertretungsgremien diskutieren. Ob das Werkzeug den versprochenen Nutzen bringt, sehen zudem viele Experten kritisch.

Quelle:
www.datenschutz-praxis.de

Alle Screenshots:
Prof. R. Gerling

Konfigurationsempfehlungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Herbst 2019 Empfehlungen zur sicheren Konfiguration von Microsoft-Office-Produkten herausgebracht (siehe https://ogy.de/bsi-empfehlungen-ms-office). In insgesamt sieben PDF-Dateien mit einer übergreifenden Richtlinie und Einzeldokumenten zu Access, Excel, Outlook, Power-Point, Visio und Word gibt das BSI detaillierte Einstellungsempfehlungen zu den Versionen 2013, 2016 und 2019. Insgesamt handelt es sich um 457 Einzeleinstellungen, die sich per Gruppenrichtlinie vornehmen lassen. Viele dieser Einstellungen sind per Microsoft-Default nicht konfiguriert. Das BSI empfiehlt, diese Einstellungen trotzdem auf einen festen Wert zu setzen, falls sich die Default-Werte einmal ändern.