LfDI Baden-Württemberg **26.2.2021**

Kursorische, technisch-organisatorische Prüfung von Microsoft Office 365 im Rahmen des Pilotprojekts des Kultusministeriums zur Nutzung von Microsoft Office 365 an Schulen

Bei der kursorischen technisch-organisatorischen Prüfung von Microsoft Office 365 einschließlich Microsoft Teams in der Konfiguration des Pilotprojekts des Kultusministeriums Baden-Württemberg sind eine Reihe von möglichen Mängeln aufgefallen. Die folgende Übersicht fasst die wichtigsten zusammen.

Für die Tests standen mehrere Accounts unter der Domain bw.schule zur Verfügung. Die Tests wurden im Februar 2021 durchgeführt.

1. Umfangreiche, intransparente Datenflüsse

Bereits bei einfachen kursorischen Tests im Pilotbetrieb konnten wir Verbindungen zu über 250 verschiedenen Hosts feststellen, deren Zweck nicht in jedem Fall ersichtlich ist. Nur 50 (unter 20 %) davon sind in *Anhang 1 Verarbeitungen O365.xlsx* zur Datenschutzfolgenabschätzung (DSFA) des Kultusministeriums, die mit Hilfe von Microsoft erstellt wurde, aufgeführt.

Während die Funktionalität einiger Hosts aus der DSFA hervorgeht oder teilweise auch selbsterklärend ist, ist bei einem Großteil die Funktion und Erforderlichkeit nicht deutlich erkennbar, z.B. bei:

- web.vortex.data.microsoft.com
- sfeur.loki.delve.office.com
- lpcres.delve.office.com
- upload.fp.measure.office.com
- augmentation.osi.office.net
- api.flightproxy.teams.microsoft.com
- webdir1e.online.lync.com
- ogma.osi.office.net
- account.activedirectory.windowsazure.com
- login.windows.net
- graph.windows.net

Eine Bewertung ist erst möglich, wenn die Zwecke der einzelnen Übermittlungen und der anschließenden weiteren Verarbeitungen geklärt sind.

2. Verarbeitungen zu eigenen Zwecken von Microsoft

Nach wie vor ist unklar, welche Verarbeitungen Microsoft zu eigenen Zwecken oder eigenen Geschäftsinteressen durchführt, auf welche Rechtsgrundlagen diese sich stützen und auf welche Datentransfers diese aufbauen. Welche Daten werden dazu wie und wo erhoben, übermittelt und verarbeitet? Handelt es sich dabei um Telemetrie-, Diagnose-oder anders genannte Daten, z.B. um von Microsoft so genannte „Dienstgenerierte Daten“? (vgl. auch den vorherigen und folgenden Punkt)

3. Telemetrie-, Diagnose- oder anders genannte Daten

Bei der Nutzung von Microsoft 365 werden laut Microsoft zahlreiche Telemetrie-, Diagnose- und anders genannte Daten (z.B. „Dienstgenerierte Daten“ oder „Wesentliche Dienste“) erhoben und von Microsoft verarbeitet. Einige wenige dieser Daten werden von Microsoft dokumentiert, vgl. z.B.:

- https://docs.microsoft.com/de-de/deployoffice/privacy/required-diagnostic-data
- https://docs.microsoft.com/de-de/deployoffice/privacy/optional-diagnostic-data
- https://docs.microsoft.com/de-de/deployoffice/privacy/essential-services.

Eine vollständige Dokumentation aller verarbeiteten Daten, Datenflüsse und Ereignisse, eine vollständige Beschreibung der Verarbeitungen, Verantwortlichkeiten und Rechtsgrundlagen ist uns nicht bekannt.

Bereits im Oktober 2020 haben wir dem Kultusministerium und Microsoft beispielhafte 26 Datenflüsse sowie ein Musterdokument übermittelt, das für die Dokumentation aller Ereignisse herangezogen werden kann.

Bei der kursorischen Prüfung von MS 365 in Konfiguration des Pilotbetriebs haben wir sehr umfangreiche Datenflüsse festgestellt, die wir dieser Kategorie zugeordnet haben. Darunter fallen nach unserem Verständnis Datenflüsse u.a. (aber nicht nur) an die folgenden Endpunkte:

- https://browser.events.data.microsoft.com/OneCollector/1.0/
- https://browser.pipe.aria.microsoft.com/Collector/3.0/
- https://iamtelemetrycollector.microsoft.com/v1/Telemetry
- https://mobile.pipe.aria.microsoft.com/Collector/3.0/
- https://teams.events.data.microsoft.com/Collector/3.0/
- https://web.vortex.data.microsoft.com/collect/v1

Eine vollständige Dokumentation aller Endpunkte aber auch aller Übermittlungen personenbezogener Daten durch die Server (z.B. vom Tenant zu weiteren Microsoft-Servern) liegt uns nicht vor. Die obige Übersicht bezieht sich daher nur auf die Übermittlungen, die auf Client-Seite im Rahmen des Pilotsprojekt sichtbar waren.

Insgesamt haben wir bei der kursorischen Prüfung im Pilotprojekt bei insgesamt rund fünf Stunden Nutzung über 20000 Ereignisse (darunter über 900 verschiedene Ereignis-Arten) festgestellt. Für die überwiegende Anzahl ist uns keine Dokumentation bekannt. Viele liegen in einem unüblichen Binärformat vor, so dass nicht genau ersichtlich ist, welche und wie viele Daten übermittelt werden. Die Ereignisse enthalten nach unserer Untersuchung neben z.B. Nutzer- und Geräte-IDs sehr detaillierte Informationen über das Nutzungsverhalten der Nutzenden, z.B. wann wer welche Tasten(kombination) drückt, welche Funktion wie nutzt, wie schnell tippt oder wohin klickt.

Eine Rechtsgrundlage (vgl. Artikel 6 Absatz 1 sowie u.U. Artikel 9 Absatz 2 DS-GVO) für diese umfassende Beobachtung, Aufzeichnung und Auswertung des vollständigen Nutzer- und Geräteverhaltens sowie für die Übermittlung an und die eigennützige Weiterverarbeitung dieser Daten durch Microsoft ist nicht erkennbar. Ebenso erschließt sich nicht, warum dies für die Zwecke der Schulen (Bereitstellung einer E-Mail-Funktion und eines persönlichen Arbeitsplatzes mit Online-Speicherdienst) zwingend erforderlich sein sollte. Es ist fraglich, ob personenbezogene Daten ausschließlich auf rechtmäßige Weise verarbeitet werden (vgl. Artikel 5 Absatz 1 DS-GVO).

4. „Microsoft-Authenticator-App“ enthält Datentransfers zu Werbedienstleister

Nutzer müssen einen zweiten Faktor zur Authentisierung angeben. Dazu wird sehr prominent auf die Microsoft-Authenticator-App hingewiesen, eine weitere Möglichkeit ist die Hinterlegung einer Telefonnummer.

Die MS-Authenticator-App begrüßt den Nutzer mit dem Hinweis „Microsoft respektiert Ihre Privatsphäre“, hat zu diesem Zeitpunkt aber bereits zahlreiche Übermittlungen personenbezogener Daten einschließlich Geräte-IDs an Microsoft, an die Adjust GmbH (einem Dienstleister aus dem Bereich der Adtech-Industrie) sowie an Google durchgeführt. Dazu werden die Hosts app.adjust.com, mobile.pipe.aria.microsoft.com, in.appcenter.ms und firebaseinstallations.googleapis.com kontaktiert.

Für diese aber auch für zahlreiche darauf bei der weiteren Nutzung der App stattfindende Übermittlungen ist für uns keine Rechtsgrundlage ersichtlich.

Laut Datenschutz-Folgenabschätzung des Kultusministeriums sollte die Nutzung der Microsoft-Authenticator-App desktiviert sein und stattdessen FreeOTP verwendet

werden. Warum werden Nutzende zur Installation der Microsoft-Authenticator-App gedrängt, ist dies eine Fehlkonfiguration seitens des Kultusministeriums (wenn ja: welche?) oder ein Fehler seitens Microsoft?

5. Einholung gesonderter Einwilligungen in die Datenschutzerklärung von Microsoft

Die digitale Bildungsplattform Baden-Württemberg ist ein Projekt des Landes Baden-Württemberg. Bei der Komponente des Arbeitsplatzes mit Office 365 wird an einigen Stellen bei der Nutzung allerdings eine Einwilligung der Nutzer in die Datenschutzerklärung von Microsoft, und/oder die Zustimmung zu Allgemeinen Geschäftsbedingungen, „Nutzungsbedingungen“ oder einen „Microsoft-Servicevertrag“ verlangt oder auf diese mit dem Hinweis verwiesen, dass diese gelten würden.

Es stellt sich die Frage der Freiwilligkeit (was wären die Folgen einer Nichtabgabe der Erklärung durch den Nutzer?), und damit der Wirksamkeit solcher Einwilligungs- und Zustimmungserklärungen. Des weiteren stellt sich die Frage, was nun gelten soll: Sollen die bei Nutzung eingeholten Erklärungen die Bedingungen, die zwischen KM/Schulen und Microsoft vereinbart wurden, verdrängen? Gehen damit einseitige Erklärungen seitens Microsoft vor? Hier droht es zu einem Wirrwarr an Regelungsregimen zu kommen, die in ihrem Verhältnis untereinander unklar sind. Die Notwendigkeit derartiger Erklärungen des Nutzers gegenüber Microsoft können wir bislang nicht erkennen, eine unmittelbare vertragliche Beziehung zwischen Microsoft und dem Nutzer dürfte insoweit nicht bestehen.

Zudem wird die Art der Einholung den Anforderungen an die Informiertheit der Nutzer und an Fairness und Transparenz der Verarbeitung nicht gerecht.

Dieser Fall tritt beispielsweise auf, wenn Nutzer Feedback zur digitalen Bildungsplattform Baden-Württemberg geben wollen, beim Einfügen von Emojis in E-Mails, bei der Übersetzungsfunktion, bei einigen Funktionen von MS Teams wie z.B. Edu Class Notebook, Edu Staff Notebook, Wiki usw.

Teilweise wird sogar eine Einwilligung in „Cookies zu Werbezwecken und Ihr Erlebnis auf unseren Websites zu verbessern“ eingefordert, zum Beispiel bei der Nutzung der Hilfefunktion und der Dokumentation von Microsoft, auf die Nutzende bei der normalen Arbeit mit dem Produkt immer wieder gelenkt werden.

6. Nutzung mit den mobilen Apps möglich und Übermittlung von Zugangsdaten bzw. E-Mail-Zugangsdaten an Microsoft

Die Nutzung der mobilen Apps (Android, iOS) soll laut Dokumentation des Kultusministeriums in der Datenschutz-Folgenabschätzung unterbunden sein. Die DSFA untersucht nicht die spezifischen Risiken durch die Mobilen- oder Desktop-Anwendungen für die Interessen oder Grundrechte und Grundfreiheiten betroffener Personen. Daher sollen im Rahmen der digitalen Bildungsplattform (derzeit im Pilotbetrieb) ausschließlich die Web-Anwendungen (z.B. Outlook Online, Word Online) zum Einsatz kommen und durch Konfiguration innerhalb Microsoft 365 die Nutzung alle anderen im Zusammenhang mit der Bildungsplattform unterbunden werden.

Bei der Prüfung konnten wir feststellen, dass die Anmeldung und Nutzung mit den uns zur Verfügung stehenden Test-Accounts mit z.B. mit den Android-Apps

- „Microsoft Outlook“
- „Microsoft Office: Word, Excel, PowerPoint und mehr“
- „Microsoft Word“
- „Microsoft Excel“
- „Microsoft OneDrive“

möglich ist. Bei der Nutzung finden u.U. zahlreiche weitere Verarbeitungen statt, die genauer untersucht werden müssten.

Bei der Prüfung von „Microsoft Outlook“ für Android konnten wir feststellen, dass diese App nicht nur mit Microsoft 365 Konten genutzt werden kann, sondern auch als normaler E-Mail-Client mit beliebigen E-Mail-Diensteanbietern oder von einer Institution selbst betriebenen Servern z.B. via IMAP/SMTP oder ActiveSync (Exchange).

Nutzende erwarten, dass E-Mail-Clients bzw. -Apps eine direkte Verbindung zum jeweiligen E-Mail-Server aufbauen, ohne die Zugangsdaten oder Kommunikationsinhalte an den Hersteller des Clients zu übermitteln. Bei der Nutzung von „Microsoft Outlook“ unter Android finden Verbindungen dabei aber nicht wie üblich direkt zwischen Client bzw. App und Server, sondern ausschließlich über Microsoft-Server statt. Dafür speichert Microsoft die Zugangsdaten zu dem E-Mail-Konto (einschließlich des Passworts) auf eigenen Servern, verarbeitet alle ein- und ausgehenden E-Mails auf eigenen Servern und hat damit vollständigen Einblick sowohl in Inhalts- als auch in alle Metadaten der Kommunikation, obwohl dies für die Funktionalität eines E-Mail-Clients nicht notwendig ist.

Passwörter dürfen aus Sicherheitsgründen ausschließlich bei den betroffenen Nutzern gespeichert werden, eine Offenbarung und Speicherung der Zugangsdaten an einen

Anbieter wie Microsoft verstößt bei vielen Organisationen gegen deren Sicherheitsrichtlinien.

Wie aufgezeigt ist die Nutzung der mobilen Anwendungen im Rahmen des Pilotprojekts möglich, obwohl laut KM eine andere Konfiguration vorliegt. Ist dies eine Fehlkonfiguration seitens des Kultusministeriums (wenn ja: welche?) oder ein Fehler seitens Microsoft?

7. Teams Desktop-Anwendung trotz Deaktivierung nutzbar

Auch die Nutzung der Desktop-Anwendungen ist laut Dokumentation seitens des KM vollständig deaktiviert und ausdrücklich ausgeschlossen, es sollen demnach ausschließlich die Browser-Versionen zum Einsatz kommen. Dennoch werden Nutzende immer wieder auf die Desktop-Version hingewiesen oder zur Nutzung gedrängt, der Download startet teilweise automatisch. Bei einem Test mit der Teams Desktop App war deren Nutzung mit den uns zur Verfügung stehenden Testaccounts problemlos möglich. Mit anderen Desktop-Anwendungen haben wir das nicht getestet.

Warum können Desktop-Anwendungen mit den Accounts des Pilotbetriebs der digitalen Bildungsplattform genutzt werden, ist dies eine Fehlkonfiguration seitens des Kultusministeriums (wenn ja: welche?) oder ein Fehler seitens Microsoft?

8. Einladung externer Teilnehmer zu Videokonferenzen

Bei der Prüfung war es nicht ohne Aufwand möglich, externe Teilnehmer zu Videokonferenzen ohne Angabe von deren E-Mail-Adresse einzuladen. Eine übliche Funktion ist die Einladung per Link, die einladende Personen auf einem beliebigen Weg versenden können, ohne dem Anbieter des Dienstes Daten über die Teilnehmer preiszugeben.

Welche Verarbeitungen finden mit diesen Einladungs-E-Mails, Metadaten, E-Mail-Adressen oder davon abgeleiteten Werten (wie Hashes) statt? Wo und wie lange werden diese gespeichert, finden Drittstaatentransfers statt?

Welche personenbezogenen Daten oder Telemetrie-, Diagnose- und anders genannte Daten werden von den Teilnehmern erfasst, an Dritte oder Unterauftragsverarbeiter übermittelt oder mit weiteren Informationen (wie z.B. beliebigen Anmeldedaten, Benutzerkennungen und Geräte-IDs) verknüpft?

9. Funktionen wie Diktat und Übersetzung

Laut den Gesprächen mit dem Kultusministerium sollten Funktionen wie Diktat und Übersetzung deaktiviert sein, da bei diesen Funktionen ein Drittstaatentransfer vorkommen oder die verarbeiteten Daten von Microsoft zu eigenen Zwecken verarbeitet, gespeichert und analysiert werden können.

Diese Funktionen konnten allerdings im Testzeitraum in der Version von Microsoft 365 des Pilotprojekts genutzt werden. Ist dies eine Fehlkonfiguration seitens des Kultusministeriums (wenn ja: welche?) oder ein Fehler seitens Microsoft?

Welche Verarbeitungen finden dabei statt, wo finden die Verarbeitungen statt, finden Drittstaatentransfers statt, finden Verarbeitungen zu eigenen Geschäftsinteressen Microsofts statt, wie lange werden verarbeitete Daten (sowohl Quell- als auch Zieldaten oder Zwischenschritte) gespeichert? Findet eine Anonymisierung oder Pseudonymisierung statt? Werden die Daten (z.B. Texte, Audio-Aufzeichnungen) für die Verbesserung des Dienstes genutzt, werden sie von Menschen oder maschinell zur Qualitätskontrolle, Dienstverbesserung oder anderen Zwecken herangezogen? Werden Daten an Auftragsverarbeiter oder Dritte übermittelt?

10. Zahlreiche Drittstaatentransfers

Bei kursorischen Tests im Rahmen der Bildungsplattform sind sehr zahlreiche Drittstaatentransfers – im Wesentlichen in die USA – aufgefallen. Im Abstand weniger Sekunden finden solche Übermittlungen statt, zumeist handelt es sich dabei um Telemetrie- und Diagnosedaten.

Laut der Datenschutzfolgenabschätzung des Kultusministeriums laufen Anmeldeprozesse über Server in Drittstaaten. Die kursorische Prüfung im Pilotbetrieb ergab, dass solche Anmeldungen nicht nur bei einem Login-Vorgang sondern automatisch bei der normalen Nutzung innerhalb des Dienstes in sehr kurzen Abständen (oft innerhalb von wenigen Minuten oder gar kürzer) erfolgen und von Microsoft mitsamt des Standorts des Nutzers und weiteren Angaben verarbeitet und für einen langen Zeitraum gespeichert werden. Eine Erforderlichkeit dafür und für die damit einhergehenden Drittstaatentransfers ist nicht ersichtlich.

11. Gewährleistung der Betroffenenrechte

Bereits vor dem Pilotbetrieb wurde über den Dienstleister des Kultusministeriums eine Auskunft nach Artikel 15 DS-GVO durchgeführt („Data Subjects Rights Request“). Die

gelieferten Daten erhielten nur einen Bruchteil der verarbeiteten bzw. an Microsoft zur weiteren Verarbeitung übermittelten Daten. Wie unterstützt Microsoft die Schulen bzw. das Kultusministerium bei deren Verpflichtungen nach Kapitel 3 DS-GVO (insbesondere Artikel 15 und evtl. 20 DS-GVO) und wie kommt Microsoft seinen eigenen Verpflichtungen nach Kapitel 3 DS-GVO nach, soweit Microsoft Daten in eigener Verantwortung verarbeitet?

12. Vertraulichkeit der Kommunikation

Es ist unklar, welche Metadaten bei der Kommunikation per E-Mail, Chat oder Videokonferenz wo und wie lange gespeichert und anderweitig verarbeitet werden. Ebenso ist unklar, welche Daten zur Spam- und Malwarebekämpfung verarbeitet und wo hin übermittelt werden. So stellt sich die Frage, ob z.B. E-Mails oder Teile davon, Dokumente und andere Anhänge (auch z.B. von externen Nutzern übermittelte) von Microsoft, Unterauftragsverarbeitern oder Dritten abseits der reinen Übermittlung verarbeitet werden und z.B. in einen Pool an Informationen über potentielle Gefahren einfließen. Ähnliche Fragen stellen sich bei der Audio- und Videokommunikation.

Während der Prüfung war es zwar möglich, als „vertraulich“ deklarierte E-Mails an Empfänger außerhalb des Systems zu versenden. Nach der Anmeldeprozedur konnten die Empfänger die übermittelten Nachrichten allerdings nicht lesen. Wahrscheinlich handelt es sich dabei um einen Fehler.

Dennoch ist fraglich, ob mit der gewählten Methode wirklich eine vertrauliche E-Mail-Kommunikation möglich ist. Es handelt sich nicht um eine Ende-zu-Ende-Verschlüsselung.

Auch ist nicht ersichtlich, dass die Anforderungen aus der Orientierungshilfe „Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail“ des Arbeitskreises Technische und organisatorische Datenschutzfragen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder sowie die Technische Richtlinie „Sicherer E-Mail-Transport“ des Bundesamts für Sicherheit in der Informationstechnik (BSI TR-03108) eingehalten werden.