

Az. P 6200-282; 6510-1/2

Datum: 02.10.2020

Autor(en):

Kurzprüfung: Office App (Version 16.0.13231.20180 | Android)

Vermerk

Zur Prüfung, welche Daten erhoben und mit welchen Hosts kommuniziert wird, wird die Verknüpfung eines "Geschäfts- oder Schulkonto" durchgeführt.

Für die Prüfung wurden seitens des KM (über BITBW und Datagroup) Testaccounts bereitgestellt. Diese sind in der Konfiguration, wie sie im Realbetrieb zum Einsatz kommen soll, konfiguriert.

Diese Prüfung wurde nicht weiter vertieft, da die Android-App nicht zum Einsatz kommen soll. Sollte die Nutzung wieder in Erwägung gezogen werden, sollte eine weitergehende Analyse stattfinden.

Zusammenfassung:

Unmittelbar nach der Anmeldung versendet die App (Diagnose-)Daten, die personenbeziehbar Informationen beinhalten. Eine Rechtsgrundlage dafür ist nicht erkennbar. Erst nachdem eine Anmeldung erfolgt ist, hat der Nutzer die Möglichkeit der Übermittlung von (Diagnose-)Daten zu widersprechen - bis zu diesem Zeitpunkt sind allerdings schon Daten an Microsoft und den Drittanbieter Google abgeflossen.

Laut einem Bericht (ExodusPrivacy_2020-10-02.png) von Exodus Privacy beinhaltet die App die Code-Signaturen von zwei Trackern:

- Google Firebase Analytics
- HockeyApp

Durch die Einbindung externer (Tracking-)Dienstleister in die App geht ein Anbieter eine Vertrauensbeziehung ein, ohne sich womöglich mit der daraus resultierenden Datenschutz- und Sicherheitsproblematik ausreichend auseinandergesetzt zu haben.

Vorgehen:

Nach Installation der Office-App auf dem Testgerät wird der Netzwerktraffic über die Burp Suite geleitet. Neben der Analyse, mit welchen Hosts die App kommuniziert, erlaubt dieses Vorgehen ebenfalls den Einblick in die übermittelten Daten bzw. Informationen.

Erwartetes Verhalten:

Beim (kollaborativen) Arbeiten bzw. Bearbeiten von Microsoft Office-Dokumenten erfolgen nur notwendige Datenflüsse. Es werden keine Daten an Drittanbieter, Werbe- und Tracking-Dienstleister oder ähnliche übermittelt. Es findet keine Übermittlung von Diagnose-, Telemetrie- oder anders genannten Daten der Nutzer an Microsoft sowie die eigennützige Weiterverarbeitung dieser Daten durch Microsoft im Wege der Beobachtung, Aufzeichnung und Auswertung des Nutzer- und Geräteverhaltens ohne erkennbare Rechtsgrundlage statt.

Festgestelltes Verhalten:

Keine Benutzerinteraktion: Nur Starten der App

Ohne Benutzerinteraktion, unmittelbar nach dem Start, übermittelt die App eindeutige Identifikationsmerkmale an Google, Microsoft und auch Drittanbieter. Die Übermittlung findet ohne die Zustimmung des Nutzers statt - es wird auch kein Hinweisfenster eingeblendet, sondern lediglich ein Verweis auf die Datenschutzerklärung (siehe Screenshots rechts):

14:03        



Ihre Datenschutzoption

Vielen Dank, dass Sie Office verwenden. Wir haben ein paar Aktualisierungen an den Datenschutzeinstellungen vorgenommen, damit Sie sie besser kontrollieren können. Der Administrator Ihrer Organisation gestattet Ihnen die Verwendung mehrerer cloudbasierter Dienste. Sie können entscheiden, ob Sie diese Dienste verwenden.

[Weitere Informationen](#)

Um diese Datenschutzeinstellungen anzupassen, navigieren Sie zu "Datenschutz und Berechtigungen" aus Ihren App-Einstellungen.

Die Bereitstellung dieser optionalen, cloudbasierten Dienste für Sie unterliegt dem Microsoft-Servicevertrag.

[Microsoft-Servicevertrag](#)

SCHLIESSEN

[1] Endpunkt **“gate.hockeyapp.net”**

Dahinter verbirgt sich ein Dienst von Microsoft, der Entwicklern Absturzberichte und Analyse-Tools zur Verfügung stellt. Über den Dienst erfasst Microsoft neben Geräte- und eindeutigen Identifikationsmerkmalen jeden Schritt bzw. Vorgang, den der Nutzer innerhalb der App tätigt. Bspw. die Verknüpfung eines neuen Kontos oder welcher Dialog dem Nutzer eingeblendet wurde (z. B. ShowTurnOffBatteryOptimizationAction).

Unter anderem werden die folgenden Daten übermittelt:

- "ai.device.id": "236b4c02-ce7d-4f66-b201-c560bf35963b"
- "ai.device.model": "moto g(7) power"
- "ai.device.oemName": "motorola", "ai.device.os": "Android"
- "ai.session.id": "5cdf1f97-bcc5-4049-8041-96f9af2f0b2d"
- "ai.user.id": "236b4c02-ce7d-4f66-b201-c560bf35963b"
- [...]
- Event (bspw. ShowTurnOffBatteryOptimizationAction oder FCM registration: Succeeded)

[2] Endpunkt **“firebaseinstallations.googleapis.com”**

Firebase ist eine Entwicklungs-Plattform von Google, die verschiedene Funktionen anbietet. Darunter A/B Testing, Analytics, Crashlytics, usw.

Unter anderem werden die folgenden Daten übermittelt:

- "fid": "cM0oUIFCQCuBcPE7yM_fGa"
- "appId": "1:91905377563:android:b45aadcaa9572c8d"
- "authVersion": "FIS_v2"
- "sdkVersion": "a:16.3.3"
- [...]

Weitere Domains, die während dem (ersten) Start aufgerufen werden:

- **oneclient.sfx.ms**: Lediglich ein GET-Aufruf zum Nachladen einer ts_configuration.jwt-Datei
- **login.microsoftonline.com**: Lediglich ein GET-Aufruf, ohne weitere Inhaltsdaten, der die Authentifizierung einleitet

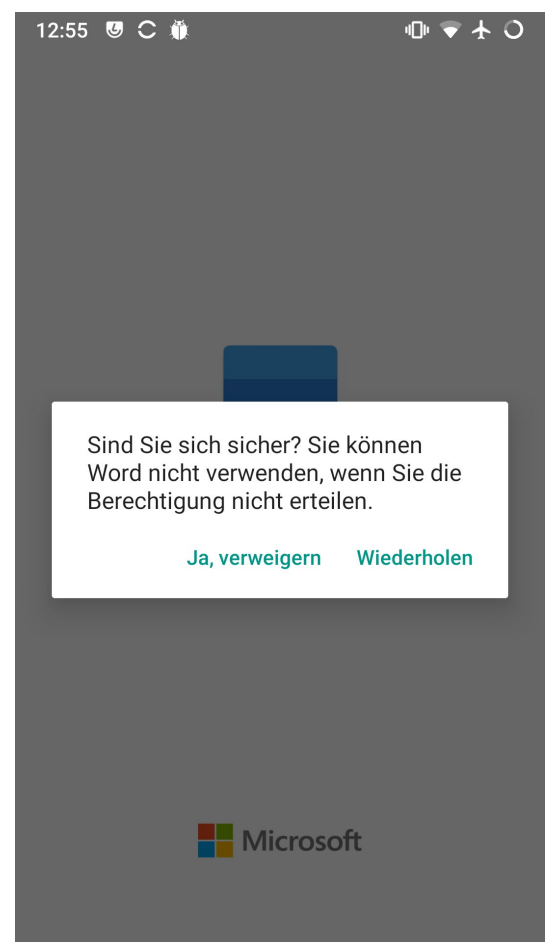
- **android.clients.google.com**: Registrierung der App bei Google Cloud Messaging, zum Erhalt von Push-Nachrichten
- **officecdn.microsoft.com**: Nachladen von Inhaltsdaten
- **ecs.office.com**: Funktion unbekannt
 - Clientid={4042C3C4-297A-3958-86BA-2B90C2B3214}
 - Application=word
 - Platform=android
 - Version=16.0.13231.20130
 - MsoVersion=16.0.13231.20130
 - Audience=Production
 - Build=ship
 - Architecture=droidarm64
 - Language=de-DE
 - OsVersion=9
 - [...]

Datenflüsse während der Nutzung

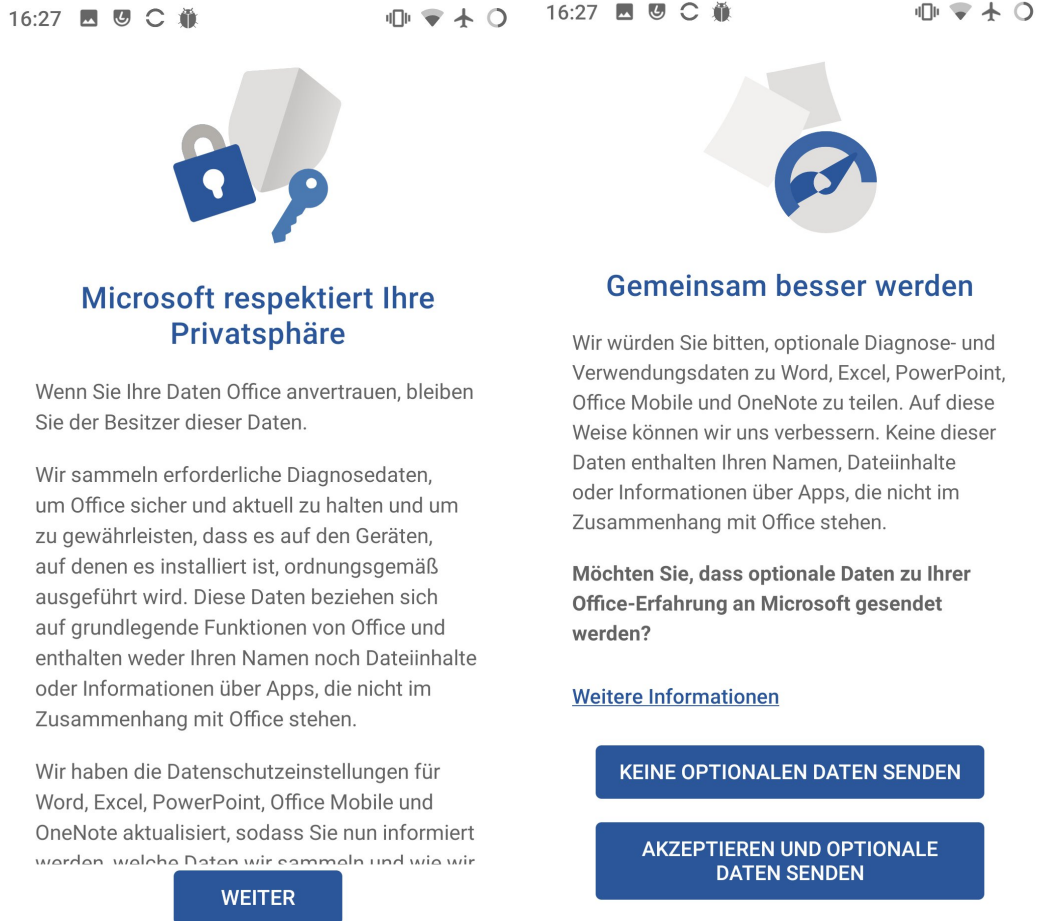
Ohne die Berechtigung auf "Dateien. etc" zuzugreifen beendet sich die App einfach wieder, sofern der Nutzer im Dialog auf "Ja, verweigern" tippt:

Nach der Berechtigungs freigabe und Anmeldung erscheint das folgende Hinweisfenster:

Mit einem Klick auf "Weiter" hat der Nutzer die Möglichkeit die Erfassung von "optionalen" (Telemtrie-) Daten abzustellen - bis zu diesem Zeitpunkt wurden allerdings schon Daten erfasst: Zudem bleibt unklar, was welche nicht-optionale Übermittlung von Daten weiterhin aktiv sind (siehe Screenshots rechts):



Nach der Berechtigungs freigabe und Anmeldung erscheint das folgende Hinweisfenster:



The screenshot shows a mobile notification interface with two columns. The top status bar shows the time 16:27 and various system icons. The left column features an icon of a padlock and a key, with the heading 'Microsoft respektiert Ihre Privatsphäre'. Below this, it explains that data remains the user's property and that diagnostic data is collected to improve Office. A 'WEITER' button is at the bottom. The right column features an icon of a pen and paper, with the heading 'Gemeinsam besser werden'. It asks for optional diagnostic data to be shared to improve Office. A question 'Möchten Sie, dass optionale Daten zu Ihrer Office-Erfahrung an Microsoft gesendet werden?' is followed by a link for 'Weitere Informationen' and two buttons: 'KEINE OPTIONALEN DATEN SENDEN' and 'AKZEPTIEREN UND OPTIONALE DATEN SENDEN'.

Microsoft respektiert Ihre Privatsphäre

Wenn Sie Ihre Daten Office anvertrauen, bleiben Sie der Besitzer dieser Daten.

Wir sammeln erforderliche Diagnosedaten, um Office sicher und aktuell zu halten und um zu gewährleisten, dass es auf den Geräten, auf denen es installiert ist, ordnungsgemäß ausgeführt wird. Diese Daten beziehen sich auf grundlegende Funktionen von Office und enthalten weder Ihren Namen noch Dateiinhalte oder Informationen über Apps, die nicht im Zusammenhang mit Office stehen.

Wir haben die Datenschutzeinstellungen für Word, Excel, PowerPoint, Office Mobile und OneNote aktualisiert, sodass Sie nun informiert werden, welche Daten wir sammeln und wie wir

WEITER

Gemeinsam besser werden

Wir würden Sie bitten, optionale Diagnose- und Verwendungsdaten zu Word, Excel, PowerPoint, Office Mobile und OneNote zu teilen. Auf diese Weise können wir uns verbessern. Keine dieser Daten enthalten Ihren Namen, Dateiinhalte oder Informationen über Apps, die nicht im Zusammenhang mit Office stehen.

Möchten Sie, dass optionale Daten zu Ihrer Office-Erfahrung an Microsoft gesendet werden?

[Weitere Informationen](#)

KEINE OPTIONALEN DATEN SENDEN

AKZEPTIEREN UND OPTIONALE DATEN SENDEN

Mit einem Klick auf „Weiter“ hat der Nutzer die Möglichkeit die Erfassung von „optionalen“ (Telemetrie-) Daten abzustellen - bis zu diesem Zeitpunkt wurden allerdings schon Daten erfasst. Zudem bleibt unklar, welche nicht-optionale Übermittlung von Daten weiterhin stattfindet.