Nationales Testinstitut für Cybersicherheit

Technische Sicherheitsanalyse Mobile App “TikTok”

Begutachtung der Sicherheitsrisiken aus Schweizer Perspektive

v1.0 / 3c4514bd
18.04.2023 07:12

Document ID	NTC-20230223-1-de
Subject	Technische Sicherheitsanalyse Mobile App “TikTok”
Version	v1.0 / 3c4514bd
Date	18.04.2023 07:12
Classification	Öffentlich
Authors	Tobias Castagna, Sven Fassbender, Dilip Many, Raphael M. Reischuk, Fabio Zuber
Responsible	Dr. Raphael M. Reischuk

Management Summary

Ausgangslage und Hintergrund

In den letzten Jahren haben mehrere Länder auf mögliche Sicherheitsrisiken in Zusammenhang mit der Verwendung der "TikTok"-App des chinesischen Anbieters *ByteDance* hingewiesen. In den letzten Monaten wurde in diversen Ländern über ein mögliches Verbot der App diskutiert und dieses zum Teil umgesetzt. Aktuelle Beispiele sind die EU-Kommission und die UK-Regierung, welche im Frühjahr 2023 wegen Sicherheitsbedenken beschlossen haben, die App auf Dienstgeräten zu verbieten.

Schweizer Behörden und Unternehmen sind mit der gleichen Fragestellung konfrontiert. Um den Entscheidungsprozess mit unabhängigen Informationen zu unterstützen, hat das Nationale Testinstitut für Cybersicherheit NTC auf Anregung und in Absprache mit dem Nationalen Zentrum für Cybersicherheit NCSC die TikTok App untersucht.

Der vorliegende Bericht gibt eine Einschätzung betreffend mögliche Risiken bei der Benutzung der TikTok-App auf verwalteten Mobilgeräten, welche bei Mitarbeitenden von Schweizer Unternehmen und Behörden im Einsatz sind. Der Bericht fokussiert auf technische Aspekte rund um den Schutz der individuellen Privatsphäre, der Vermeidung von Überwachung und Spionage bei der Nutzung von TikTok auf Android- und iOS-Mobilgeräten. Andere Aspekte wie beispielsweise Schutz vor Manipulation, Zensur oder politischer Meinungsmache wurden bewusst nicht berücksichtigt.

Die zur Verfügung stehende Zeit und Ressourcen wurden prioritär genutzt, um kritische und praxisrelevante Risiken zu analysieren. Weiterführende detaillierte Analysen, beispielsweise durch Reverse Engineering oder Langzeitverhaltensbeobachtungen, wurden bislang nicht durchgeführt. Zudem wurde auf möglichst realitätsnahe Testbedingungen geachtet, ohne besondere Schutzmassnahmen, wie sie beispielsweise durch restriktiv konfigurierte Mobile Device Management (MDM) Lösungen möglich wären.

Zusammenfassende Einschätzung

Das beobachtete Verhalten der TikTok-App entspricht grundsätzlich den Erwartungen an eine Social-Media-App. Die App beantragt jedoch weitreichende und potenziell problematische Systemberechtigungen, die für die Benutzerüberwachung missbraucht werden könnten. Beispiele dafür sind der Zugriff auf das Mikrofon, die Kamera und die Ortungsdienste. Diese Berechtigungen können mehrheitlich durch die typischen Funktionalitäten einer Social-Media-App erklärt werden. Beispielsweise werden Mikrofon und Kamera benötigt, um Videos aufzuzeichnen – eine der Hauptfunktionalitäten der TikTok-App. Dennoch werden auffallend häufig Positionsdaten an die ByteDance Backend-Server gesendet: Sofern die Berechtigung erteilt wurde, erfolgt dies unter iOS bei jedem Start der App. Positiv aufgefallen ist, dass Berechtigungen in der Regel erst dann angefragt werden, wenn sie tatsächlich für eine durch die Benutzenden aufgerufene Funktion benötigt werden. Zudem ist es möglich, die App zu verwenden, auch wenn Berechtigungen nicht gewährt oder entzogen werden.

Abgesehen von den prinzipiellen Risiken im Zusammenhang mit den angeforderten Berechtigungen bestehen weitere konzeptionelle Risiken. So sind die über die App versandten Nachrichten nicht Ende-zu-Ende verschlüsselt. Daher kann beispielsweise ByteDance, als Betreiber der TikTok Infrastruktur, die Nachrichten prinzipiell einsehen und modifizieren. Dieses Risiko dürfte für Privatpersonen höher sein als für Unternehmen und Behörden, da im geschäftlichen Kontext in der Regel andere Kanäle für den Austausch sensitiver Daten verwendet werden.

Bei der Überprüfung konnten keine Hinweise auf eine Benutzerüberwachung festgestellt werden. Unter Berücksichtigung der Tatsache, dass nur die Anwesenheit von Schwachstellen bewiesen werden kann, aber nicht deren Abwesenheit, kann folglich dennoch keine pauschale Unbedenklichkeitserklärung gegeben werden. So ist beispielsweise eine Überwachung der Nutzer durch die App aufgrund der weitreichenden Berechtigungen grundsätzlich technisch realisierbar. Die App könnte bereits heute versteckte Überwachungsfunktionen beinhalten, die nur unter bestimmten Bedingungen ausgelöst werden (z.B. an bestimmten Orten oder zu bestimmten Uhrzeiten). Zudem liessen sich versteckte Funktionen durch die häufigen Updates nahezu unbemerkt nachrüsten. Dies gilt grundsätzlich für jede Anwendung und insbesondere für solche mit weitreichenden Berechtigungen.

Des Weiteren wurde festgestellt, dass ein kleiner Teil der Kommunikation mit den TikTok-Backend-Server zusätzlich verschlüsselt wird. Der genaue Inhalt dieser Kommunikation ist unbekannt und es ist daher unklar, welche Informationen über diesen Kanal möglicherweise abfliessen.

Zusammenfassend wird empfohlen, den Einsatz der TikTok-App, insbesondere im geschäftlichen und behördlichen Kontext, kritisch zu hinterfragen. Dies gilt prinzipiell auch für andere Apps, die mit weitreichenden Berechtigungen ausgestattet sind und im geschäftlichen und behördlichen Kontext von begrenztem Nutzen sind. Werden derlei Apps zugelassen, sollten durch technische und organisatorische Massnahmen sichergestellt werden, dass nur die unbedingt erforderlichen Berechtigungen gewährt werden und dass der Einsatz auf das erforderliche Minimum beschränkt wird.

Weitere Details zu den identifizierten Risiken und den dazugehörigen Massnahmenempfehlungen sind in Abschnitt 3 ab Seite 10 aufgeführt.

Rahmenbedingungen

Die Untersuchung wurde auf Anregung und in Absprache mit dem NCSC durchgeführt. Da es sich um ein Initiativprojekt mit Finanzierung und Durchführung durch das NTC handelt, wurden die Ziele, der Umfang und die Rahmenbedingungen durch das NTC definiert.

Die Untersuchung hat im Zeitraum vom 23. Februar bis zum 24. März 2023 stattgefunden und wurde durch ein Kernteam von drei Testexperten durchgeführt, welche selektiv und nach Bedarf durch weitere Spezialisten aus dem NTC-Kompetenznetzwerk unterstützt wurden. Insgesamt wurden etwa 300 Arbeitsstunden in die Untersuchung investiert.

Bei der Analyse wurde auf möglichst realitätsnahe Testbedingungen geachtet, ohne besondere Schutzmassnahmen, wie sie beispielsweise durch restriktiv konfigurierte Mobile Device Management (MDM) Lösungen möglich wären. Weitere Details bezüglich Umfang und Einschränkungen sind in Abschnitt 1 ab Seite 5 aufgeführt.

Änderungen

Version	Datum	Änderungen	Interne ID
1.0	2023-04-18, 08:00	Ausgangsdokument	3c4514bd

Inhaltsübersicht

1 Umfang und Einschränkungen der Sicherheitsanalyse **5**

1.1 Umfang der Analyse im Überblick 5

1.2 Umfang der Analyse im Detail 6

2 Befundliste **8**

3 Befunde im Detail **10**

3.1 Kommunikation mit dem Backend 10

3.2 Mobile App 17

4 Testfälle **34**

4.1 Netzwerk-Kommunikation 34

4.2 Privatsphäre und Datenschutz 35

1 Umfang und Einschränkungen der Sicherheitsanalyse

In diesem Abschnitt wird der Umfang der durchgeführten Sicherheitsanalyse beschrieben. Dabei wird auch auf die selbst auferlegten sowie die technischen und ressourcenbedingten Einschränkungen eingegangen. Es folgt eine Übersicht über die wichtigsten Punkte, gefolgt von einer detaillierten Erläuterung.

1.1 Umfang der Analyse im Überblick

Bei der Überprüfung wurde der Fokus auf Risiken für die individuelle Privatsphäre sowie auf Überwachung und Spionage gesetzt. Weiterführende detaillierte Analysen, beispielsweise durch Reverse Engineering oder Langzeitverhaltensbeobachtungen wurden nicht durchgeführt.

Die bei der Analyse berücksichtigten Test-Cases sind in Abschnitt 4 ab Seite 34 aufgelistet. Die folgende Auflistung beschreibt den groben Umfang der Analyse:

- Kommunikation zwischen den mobilen Apps und dem TikTok Backend
- Angefragte Berechtigungen der Apps und Zugriff auf Sensoren wie Kamera, Mikrofon und GPS

Folgende Bereiche und Aspekte wurden in dieser Analyse bewusst **nicht** untersucht:

- Die öffentliche Webseite von TikTok sowie andere nicht aufgeführte Plattformen
- Die Wirksamkeit der von den Betriebssystemen angebotenen Schutzfunktionen, insbesondere die Beschränkung der Rechte einer App
- Eine allfällige Weitergabe der Personendaten an ByteDance-Partner und Dritte
- Prozesse und Algorithmen zur Moderation und Zensur der geteilten und angezeigten Inhalte
- Psychologische Faktoren wie Einflüsse auf Selbstdarstellung, Erfolgsdruck, Konzentrationsspanne, etc.

Das folgende Diagramm zeigt eine schematische Übersicht all jener Komponenten, die Teil der vorliegenden Sicherheitsanalyse sind.

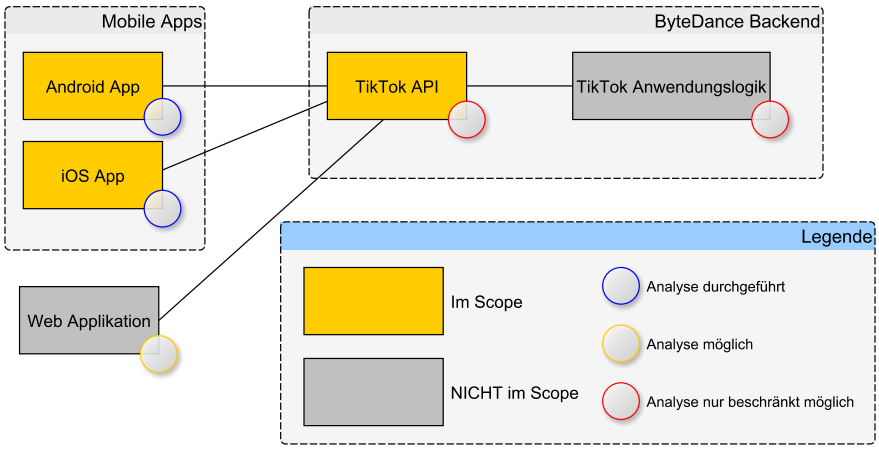

Abbildung 1: Übersicht der Komponenten von TikTok aus Sicht NTC.

1.2 Umfang der Analyse im Detail

Die zur Verfügung stehende Zeit und Ressourcen wurden genutzt, um kritische und praxisrelevante Risiken zu analysieren. Weiterführende detaillierte Analysen, beispielsweise durch Reverse Engineering oder Langzeitverhaltensbeobachtungen, waren in der zur Verfügung stehenden Zeit nicht möglich und wurden nicht durchgeführt. Solche weitreichenden Untersuchungen könnten unter Umständen allfällige ausgeklügelte Überwachungstechniken aufzeigen, sofern vorhanden. Es ist allerdings wichtig festzuhalten, dass nur die Anwesenheit von Schwachstellen bewiesen werden kann, nicht jedoch deren Abwesenheit. Dies gilt gleichermassen für umfangreichere Tests. Zudem könnten Überwachungsfunktionen durch die häufig stattfindenden Updates der App nachträglich eingebaut oder nur unter bestimmten Bedingungen ausgelöst werden (z.B. an gewissen Orten oder zu gewissen Uhrzeiten).

Es ist generell nicht bekannt, was mit den versandten Daten und Metadaten aufseiten ByteDance unternommen wird. Es ist unmöglich, dies ohne weitgehende Kooperation des Anbieters zu prüfen. Daher kann über die Nutzung der Daten und Metadaten keine Aussage gemacht werden.

Die Wirksamkeit der von den Betriebssystemen angebotenen Schutzfunktionen, insbesondere die Beschränkung der Rechte einer App, wurden nicht untersucht. Bei der Beurteilung wird davon ausgegangen, dass diese vollständig wirksam sind.

Bei der Überprüfung wurde der Fokus auf Risiken für die individuelle Privatsphäre sowie auf Überwachung und Spionage bei der Nutzung der TikTok-App auf Android- und iOS-Mobilgeräten im geschäftlichen und behördlichen Kontext gelegt. Die TikTok-Webseite sowie andere Plattformen wie beispielsweise Android TV wurden nicht berücksichtigt. Ebenfalls wurde nicht auf gesellschaftliche Risiken wie Zensur, Meinungsmanipulation durch Algorithmen, Auswirkungen auf die Psyche von Jugendlichen oder Ähnliches eingegangen.

Die physischen Standorte der Backend-Server wurden nicht genauer betrachtet, da dies kein

massgebendes Kriterium ist, um eine Aussage darüber zu treffen, an wen die Daten schlussendliche gesandt werden, resp. wer darauf Zugriff hat. Relevant scheint jedoch die Erwähnung, dass es sich bei dem Datenverarbeiter, ByteDance, um ein Unternehmen unter chinesischen Gesetzgebung handelt.

Bei der Untersuchung wurde auf eine möglichst realitätsnahe Testumgebung geachtet. Dennoch kann diese nicht hundertprozentig der Realität entsprechen. Es kann zudem nicht ausgeschlossen werden, dass bestimmte (problematische oder unproblematische) Funktionalitäten nur unter bestimmten Bedingungen genutzt oder ausgelöst werden könnten. Eine Nachbildung aller Eventualitäten ist nicht möglich.

Um eine bessere Analyse des Netzwerkverkehrs zu ermöglichen, erfolgte sämtliche Kommunikation über WLAN. Die Geräte waren nicht mit SIM-Karte ausgerüstet und konnten nicht über das Mobilfunknetz kommunizieren.

Für die Untersuchung wurden primär Android- und iOS-Mobilgeräte im Originalzustand verwendet. Um gewisse Testfälle abzubilden, welche tiefgreifende Systemberechtigungen voraussetzen, wurde vereinzelt auf iOS-Geräte mit Jailbreak zurückgegriffen.

Sämtliche Tests wurden auf der zu Beginn der Untersuchung aktuellsten Version der TikTok-App durchgeführt:

- Android: `28.3.3`
- iOS: `28.2.0` und `28.4.0` (Bei einer Neuinstallation während des Tests konnte nur die aktuellste Version aus dem App Store installiert werden. Dies wird so von Apple forciert.)

Es sei an dieser Stelle explizit darauf hingewiesen, dass es sich bei der Überprüfung um eine Momentaufnahme handelt. Allfällige Anpassungen an der App, welche vor- oder nachträglich vorgenommen werden, können nicht erfasst werden. Gleiches gilt für allfällige App-Varianten, welche in anderen Ländern oder Sprachregionen zum Einsatz kommen.

Wie im Management Summary beschrieben, spielen die Berechtigungen der App eine wichtige Rolle bei der Risikoeinschätzung. Bei der Analyse wird die Annahme getroffen, dass die durch das Android- und iOS-Betriebssystem durchgesetzten Berechtigungen wie erwartet greifen und nicht umgangen werden können. Diese Annahme kann gemacht werden, da die Berechtigungssysteme auf Android und iOS grundsätzlich als robust und wirkungsvoll gelten. Diese Annahme wurde jedoch in dieser Untersuchung nicht überprüft und ist nicht uneingeschränkt gültig. Beispielsweise könnten durch nicht behobene Schwachstellen im Betriebssystem oder auf manipulierten Mobilgeräten ("Rooting" auf Android und "Jailbreak" auf iOS) die Berechtigungssysteme umgangen werden.

2 Befundliste

Im Folgenden werden alle Befunde aufgeführt und in eine von vier Kategorien gruppiert: Befunde hoher Priorität, Befunde mittlerer Priorität, Befunde niedriger Priorität und Informationen und Anomalien. Alle Befunde werden im Detail in Abschnitt 3 behandelt.

Hohe Risiken (H)

Befunde in dieser Kategorie entsprechen schweren Schwachstellen und sollten sofort analysiert und korrigiert werden. Angreifer können die Schwachstellen möglicherweise direkt ausnutzen und schweren Schaden anrichten.

NTCF-182 H FB01 Übermittlung von Kontakt-Hash-Werten 10
NTCF-184 H FB04 Fehlende Ende-zu-Ende-Verschlüsselung von Direktnachrichten . 15
NTCF-186 H FI02 Verwendung der Ortungsdienste bei jedem Start der App 21

Befunde in dieser Kategorie können viele oder alle Benutzende des Systems betreffen. Die Schwachstellen können mit ausreichenden Berechtigungen leicht ausnutzbar sein und sind eher leicht zu erkennen. Die Schwachstellen können über das öffentliche Internet oder durch physischen Zugriff auf ein System ausnutzbar sein. Diese Schwachstellen stellen eine realistische Bedrohung durch Amateure dar und sollten vor dem Go-Live behoben werden.

Mittlere Risiken (M)

Befunde in dieser Kategorie sollten mittelfristig analysiert und korrigiert werden. Angreifer können die Schwachstellen möglicherweise ausnutzen und Schaden mittleren Ausmasses anrichten.

NTCF-188 M FI04 Ermittlung des Geräte-Status 26
NTCF-190 M FI06 Multi-Faktor-Authentisierung wird nicht erzwungen 31

Befunde in dieser Kategorie betreffen wenige bis viele Benutzende des Systems. Die Schwachstellen sind möglicherweise schwieriger auszunutzen, und es kann aufwendiger sein, sie zu entdecken. Die Schwachstellen können über das Internet oder durch physischen Zugriff auf ein System ausnutzbar sein. Diese Schwachstellen stellen somit eine realistische Bedrohung durch fortgeschrittene Angreifer dar und sollten innerhalb kurzer Zeit behoben werden.

Geringe Risiken (L)

Befunde in dieser Kategorie sollten mittelfristig analysiert und auf Behebung überprüft werden. Angreifer können möglicherweise keinen unmittelbaren Schaden anrichten, aber sie können sich zumindest einen Vorteil verschaffen.

NTCF-183 L FB03 Verschlüsselte Inhalte in HTTP-Headern 13
NTCF-185 L FI01 Abfrage installierter Apps 17
NTCF-187 L FI03 Regelmässige Anfragen im Hintergrund 24
NTCF-189 L FI05 Verwendung eines integrierten Browsers 29

Befunde in dieser Kategorie betreffen eine kleine Anzahl von Benutzenden oder haben keine unmittelbaren Auswirkungen auf Benutzerdaten. Die Schwachstellen sind eher kompliziert auszunutzen oder erfordern umfangreiche Berechtigungen. Die Ausnutzung dieser Schwachstellen erfordert möglicherweise Kenntnisse der internen Infrastruktur oder einen tiefen Zugriff auf die Systeme. Diese Schwachstellen können als "Defense-in-Depth"-Kontrollen verstanden werden, die die Gesamthärtung des Systems verbessern würden.

3 Befunde im Detail

In diesem Abschnitt werden alle Befunde im Detail präsentiert. So beschreibt Abschnitt 3.1 (Seite 10 ff.) die Erkenntnisse bezüglich der Kommunikation mit dem Backend. Abschnitt 3.2 (Seite 17 ff.) beschreibt die Befunde zu den mobile Apps unter iOS und Android.

3.1 Kommunikation mit dem Backend

Dieses Kapitel beschreibt die Erkenntnisse bezüglich der Kommunikation mit dem Backend.

Befund NTCF-182 H (Übermittlung von Kontakt-Hash-Werten): **Die TikTok mobile App übermittelt Hash-Werte von vorhandenen Kontakten. ByteDance nutzt diese Informationen, um Verbindungen zwischen den Benutzenden herzustellen.** FB01 [20230308]

Hintergrund

Die TikTok-App übermittelt an ein ByteDance Backend die Hash-Werte aller Kontakte aus dem Adressbuch, für die eine mobile Nummer eingetragen ist. Diese Information wird von ByteDance genutzt, um den Benutzenden bekannte Kontakte innerhalb des TikTok-Systems als Freunde vorzuschlagen. Zwar werden die Kontaktinformationen nicht im Klartext zugänglich gemacht, jedoch muss angenommen werden, dass ByteDance in der Lage ist, die Informationen aus den Hash-Werten zu rekonstruieren. Da es insbesondere eine begrenzte Anzahl an möglichen enumerierbaren Rufnummern gibt[1], können diese mit grosser Wahrscheinlichkeit anhand der Hash-Werte rekonstruiert werden.

Diese Information ist für das Unternehmen ByteDance von grossem Wert, da Rufnummern in der Regel einem bestimmten Individuum zugeordnet werden können. Erteilen die Benutzenden der TikTok-App die Berechtigung, auf Kontakte zuzugreifen, so werden diese Informationen unmittelbar an ByteDance übermittelt. Dies erfolgt ohne die Zustimmung der Betroffenen.

Nachweis

Die folgende HTTP-Anfrage eines iOS-Gerätes zeigt exemplarisch die Übermittlung eines Kontaktes an ein ByteDance Backend:

[1] Theoretisch möglich können bis zu 250 Milliarden Nummern weltweit existieren; effektiv existieren jedoch wohl eher zehn Milliarden. Quelle: https://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use.

```
POST /aweme/v1/upload/hashcontacts/?version_code=[...] HTTP/2
Host: api16-normal-useast1a.tiktokv.com
[...]

need_unregistered_user=1&people_contact_list=%5B%7B%22contact%22%3A%2255282
     c18206b9beb9998f5eaa15b85c9388463965678af5209e2cc3a3ff5b947%22%2C%22phone_list%22%3A%5B%7B
     %22name%22%3A%2255282c18206b9beb9998f5eaa15b85c9388463965678af5209e2cc3a3ff5b947%22%2C%22
     hashed_phone%22%3A%221c1127746328b46401d4a1a8e296d09e2b1888e993e371a0a73cd21e5290675c%22%2
     C%22region_code%22%3A%223d914f9348c9cc0ff8a79716700b9fcd4d2f3e711608004eb8f138bcba7f14d9
     %22%7D%5D%7D%5D&scene=1&sync_only=1
```

Der Inhalt der oben aufgeführten HTTP-Anfrage ist kodiert. Zur besseren Lesbarkeit wird der Inhalt im Folgenden dekodiert dargestellt:

```
[
  {
    "contact": "55282c18206b9beb9998f5eaa15b85c9388463965678af5209e2cc3a3ff5b947",
    "phone_list": [
      {
        "name": "55282c18206b9beb9998f5eaa15b85c9388463965678af5209e2cc3a3ff5b947",
        "hashed_phone": "1c1127746328b46401d4a1a8e296d09e2b1888e993e371a0a73cd21e5290675c",
        "region_code": "3d914f9348c9cc0ff8a79716700b9fcd4d2f3e711608004eb8f138bcba7f14d9"
      }
    ]
  }
]
```

Vorbedingungen

Damit die TikTok-App auf die Kontakte zugreifen kann, müssen die Benutzenden der App diese Berechtigung erteilen. Nach erfolgter Anmeldung in der TikTok-App wird diese Berechtigung von der App angefragt. Sobald die Berechtigung erteilt wurde, werden die lokalen Kontakte in Hash-Werten an das ByteDance Backend übermittelt.

Auswirkungen

Die Kenntnis darüber, welche Kontakte die TikTok-Benutzenden haben, erlaubt es dem Unternehmen ByteDance, unterschiedlichste Rückschlüsse zu ziehen. Da Rufnummern in der Regel eindeutig einem Individuum zugeordnet werden können, ist diese Information als sensibel zu betrachten. Da weder die Benutzenden noch ByteDance die betroffenen Personen über das Teilen der Informationen informieren, muss davon ausgegangen werden, dass das beobachtete Verhalten gegen den Grundsatz der Transparenz (Art. 4 Abs. 4 DSG) sowie gegen den Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG) verstossen. Die getroffenen technischen Massnahmen – namentlich das Ableiten von Hash-Werten – bietet keinen ausreichenden Schutz für die Vertraulichkeit dieser Informationen.

Im zeitlichen Rahmen der Untersuchung war es nicht möglich, das eingesetzte Hash-Verfahren mittels Reverse-Engineering zu ermitteln. ByteDance muss jedoch in der Lage sein, die Hash-Werte zu interpretieren, ansonsten ist eine Zuordnung zu anderen TikTok-Usern nicht möglich. Daher ist davon auszugehen, dass ein deterministisches Hash-Verfahren eingesetzt wird, welches bei jeder Operation basierend auf der gleichen Eingabe den gleichen Hash-Wert erzeugt.

Dies konnte experimentell bestätigt werden, indem zwei unterschiedliche Kontakte mit der gleichen Rufnummer angelegt wurden. Die anschliessend übermittelten Hash-Werte unterschieden sich nur im Namen, nicht aber in der Rufnummer.


```
[
  {
    "contact": "55282c18206b9beb9998f5eaa15b85c9388463965678af5209e2cc3a3ff5b947",
    "phone_list": [
      {
        "name": "55282c18206b9beb9998f5eaa15b85c9388463965678af5209e2cc3a3ff5b947",
        "hashed_phone": "1c1127746328b46401d4a1a8e296d09e2b1888e993e371a0a73cd21e5290675c",
        "region_code": "3d914f9348c9cc0ff8a79716700b9fcd4d2f3e711608004eb8f138bcba7f14d9"
      }
    ]
  },
  {
    "contact": "8c41d3623e50d6a373040e51e1ce710eeb57b798676870cdf13ea3b1306c1da0",
    "phone_list": [
      {
        "name": "8c41d3623e50d6a373040e51e1ce710eeb57b798676870cdf13ea3b1306c1da0",
        "hashed_phone": "1c1127746328b46401d4a1a8e296d09e2b1888e993e371a0a73cd21e5290675c",
        "region_code": "3d914f9348c9cc0ff8a79716700b9fcd4d2f3e711608004eb8f138bcba7f14d9"
      }
    ]
  }
]
```


Da ByteDance den eingesetzten Hash-Algorithmus und allfällige Salt-Werte kennt, ist das Unternehmen in der Lage, aus den Hash-Werten die zugehörige Rufnummer abzuleiten, z.B. via vorberechneter Tabellen. Die gleiche Aussage trifft auch auf die anderen Hash-Werte zu.

Empfehlungen

Es wird empfohlen, der TikTok-App keinen Zugriff auf die Kontakte zu gewähren.

Befund NTCF-183 L (Verschlüsselte Inhalte in HTTP-Headern): **Die TikTok-App versendet mittels verschlüsselten HTTP-Headern lokale Inhalte an das ByteDance Backend.** FB03 [20230308]

Hintergrund

Die TikTok-App versendet Inhalte mittels nicht standardisierter HTTP-Header an ein ByteDance Backend. Der Inhalt dieser HTTP-Header ist offenbar teilweise verschlüsselt. Unklar ist jedoch, welche Inhalte hier verschlüsselt werden. Insbesondere der *X-Argus*-Header kann eine Länge von bis zu 600 Zeichen haben und wird in jedem API-Call übermittelt. Es können somit grössere Datenmengen in diesem Header enthalten sein, deren Ursprung unklar ist.

Die Untersuchung der in diesen Headern übermittelten Daten war in der zur Verfügung stehenden Zeit nicht abschliessend möglich.

Nachweis

Der folgende Auszug zeigt exemplarisch den *X-Argus*-Header:

```
POST /v3/conversation/get_read_index?aid=1233&device_platform=iphone&version_code=2840 HTTP/2
Host: api16-normal-useast1a.tiktokv.com
X-Argus: [...]
X-Gorgon: [...]
X-Khronos: 1678352403
X-Ladon: [...]
```

Nachforschungen haben gezeigt, dass einige Informationen zu der Verschlüsselung sowie mutmasslich entschlüsselte Inhalte bereits öffentlich dokumentiert wurden. Beispielsweise wurde in folgendem Github-Repository[2] festgehalten, wie die Daten verschlüsselt werden. Ausserdem ist dokumentiert, dass es sich bei den verschlüsselten Daten um Daten im `protobuf` Format handelt. Der in diesem Repository entschlüsselte `protobuf`, enthält keine Informationen, welche auf sensible Inhalte hindeuten.

Das NTC prüft zur Zeit weitere Schritte zur genaueren Überprüfung des Headers und ist mit dem Autor des Repositories in Kontakt.

Vorbedingungen

Das Senden von Inhalten mittels HTTP-Headern ist ohne weitere Voraussetzungen möglich, solange die App Zugriff auf das Internet hat. Da dies für ihr korrektes Funktionieren notwendig ist, kann von einem Internetzugang ausgegangen werden.

[2] https://github.com/xtekky/TikTok-X-Argus

Auswirkungen

Obwohl die verschlüsselten Daten nicht näher untersucht wurden, lassen sich einige Mutmassungen darüber anstellen. Es wird nicht davon ausgegangen, dass in den HTTP-Headern Daten enthalten sind, welche z.B. über die Kamera, das Mikrofon oder die Medien-Bibliothek gesammelt wurden. Ein Zugriff auf diese Schnittstellen des Betriebssystems ist nur nach Genehmigung des Nutzenden möglich. Zudem ist ein momentan aktiver Zugriff über eine *Sensor Benachrichtigung* (grüner Punkt oben rechts unter Android, farbiger Punkt oben rechts unter iOS) erkennbar und wird unter iOS zusätzlich im *App-Datenschutzbericht* protokolliert (sofern dieser aktiviert ist). Missbräuchliche Zugriffe auf solche Schnittstellen konnten im Rahmen der Untersuchung nicht festgestellt werden.

Möglich wäre jedoch grundsätzlich die Übermittlung jeglicher Daten, auf die die App Zugriff hat – z.B. eine Liste der aktuell auf dem Betriebssystem installierten Apps (siehe Befund NTCF 185) oder des beim Start festgestellten Standorts (siehe Befund NTCF 186).

Da die verschlüsselten Inhalte in der zur Verfügung stehenden Zeit nicht entschlüsselt oder mittels Reverse-Engineering sichtbar gemacht werden konnten, kann nur eine eingeschränkte Aussage über die möglichen Auswirkungen getroffen werden. Grundsätzlich wird Verschlüsselung nur dann eingesetzt, wenn die Vertraulichkeit einer Information geschützt werden soll. Gleichzeitig macht der Einsatz von Verschlüsselung jedoch auch die damit versehenen Inhalte unkenntlich. Dies erschwert Sicherheitsforschern, festzustellen, welche Daten übermittelt werden.

Ob die hier eingesetzte Verschlüsselung dem legitimen Schutz sensitiver Informationen oder dem Verschleiern der Natur der übermittelten Daten dient, kann nicht beurteilt werden.

Empfehlungen

Es wird empfohlen, eine tiefergehende Überprüfung durchzuführen. Diese sollte zum Ziel haben, die an das ByteDance Backend übermittelten verschlüsselten Inhalte sichtbar zu machen.

Befund NTCF-184 H (Fehlende Ende-zu-Ende-Verschlüsselung von Direktnachrichten): **Die TikTok-App verschlüsselt die Direktnachrichten zwischen Nutzenden nicht Ende-zu-Ende. Der Betreiber der Infrastruktur sowie der Betreiber des Dienstes kann die Inhalte der Direktnachrichten einsehen.** iOS Android FB04 [20230308]

Hintergrund

Beim Versenden einer Direktnachricht muss diese von der TikTok-App zuerst an die Server von ByteDance übermittelt werden, welche sie dann wiederum an den jeweiligen Empfänger zustellen. Dabei verwendet ByteDance die Infrastruktur des Unternehmens *Akamai Technologies*. Da die versendeten Direktnachrichten dabei nicht durch eine zusätzliche Schicht Verschlüsselung (die sogenannte Ende-zu-Ende-Verschlüsselung) geschützt sind, könnten sowohl *Akamai Technologies* als auch ByteDance, sowie eventuell weitere an der Datenübertragung beteiligte Infrastrukturbetreiber deren Inhalt mitlesen.

Nachweis

Der folgende Ausschnitt zeigt die gesendete Direktnachricht *Hey* im nur über HTTPS transportverschlüsselten HTTP-Body der Anfrage:

```
1 POST /v1/message/send?aid=1233&device_platform=iphone&version_code=2840 HTTP/2
2 Host: api16-normal-useast1a.tiktokv.com
3 [...]
4
5 [...]
6 {"aweType":0,"text":"Hey"}
7 [...]
```

Vorbedingungen

Da die Verbindung zwischen der App und den Servern von *Akamai Technologies* bzw. ByteDance durch HTTPS verschlüsselt ist, kann die fehlende Ende-zu-Ende-Verschlüsselung nur von diesen Infrastrukturbetreiber ausgenützt werden, um die Nachrichten zu lesen.

Auswirkungen

Sowohl der Betreiber der Infrastruktur (*Akamai Technologies*) als auch der Empfänger der Information (ByteDance) kann die Inhalte der Direktnachrichten einsehen. Es besteht die Möglichkeit, dass sich die Nutzenden der App nicht über diesen Umstand im Klaren sind. Somit könnten Nutzende die App verwenden, um potenziell sensible Informationen per Direktnachricht an andere Nutzende zu versenden. Da die Vertraulichkeit der Nachrichten gegenüber den eben genannten Parteien nicht gewährleistet ist, können je nach Inhalt der Direktnachrichten entsprechende Schäden entstehen.

Empfehlungen

Es wird empfohlen, die Funktion zum Versenden von Direktnachrichten innerhalb der TikTok-App nur für nicht sensible Inhalte zu verwenden.

3.2 Mobile App

In diesem Kapitel werden Erkenntnisse, welche den Aufbau der mobilen Apps betreffen, festgehalten.

Befund NTCF-185 L (Abfrage installierter Apps): **Die TikTok-App für iOS prüft bei der Ausführung, ob bestimmte andere Apps auf dem Mobiltelefon installiert sind. Der Herausgeber der App kann diese Information vielfältig nutzen. Es besteht derzeit keine Evidenz darüber, dass die gesammelten Daten an die Backend-Server gesendet werden.** iOS FI01 [20230308]

Hintergrund

Die TikTok-App für iOS prüft bei der Ausführung, ob bestimmte Apps auf dem Mobiltelefon installiert sind. Das beobachtete Verhalten kann damit zusammenhängen, dass die TikTok-App mehr oder weniger Buttons (z.B. zum Teilen von Inhalten) anzeigt, je nachdem, welche anderen Apps installiert sind. Da diese Information im ungünstigsten Fall potenziell sensible Informationen über den Nutzer preisgeben kann (z.B. Zugehörigkeit zu einer bestimmten Ethnie oder Religion), ist diese Abfrage als bedenklich einzustufen.

Zum jetzigen Zeitpunkt ist jedoch unklar, ob die Informationen an die Backend-Server gesendet und von ByteDance ausgewertet werden. Aus diesem Grund wird der Befund in diesem Dokument als geringes Risiko eingestuft.

Nachweis

Der folgende Auszug aus der `Info.plist`-Datei der TikTok-App zeigt die zum Zeitpunkt der Untersuchung aktuelle Liste der Drittanbieter-Apps, welche von der TikTok-App ermittelt werden können:

```
<key>LSApplicationQueriesSchemes</key>
  <array>
    <string>akulaku</string>
    <string>gojek</string>
    <string>tngdwallet</string>
    <string>tg</string>
    <string>viber</string>
    <string>fbapi</string>
    <string>fb-messenger-api</string>
    <string>fbauth2</string>
    <string>fbshareextension</string>
    <string>kakao61f447fe9723aa9c0b67a52eeb998e77</string>
    <string>kakaokompassauth</string>
    <string>storykompassauth</string>
    <string>kakaolink</string>
    <string>kakaotalk-5.9.7</string>
    <string>storylink</string>
    <string>line</string>
    <string>instagram</string>
    <string>instagram-stories</string>
    <string>lineauth</string>
    <string>line3rdp.com.zhiliaoapp.musically</string>
    <string>whatsapp</string>
    <string>fb-messenger-platform-20150714</string>
    <string>zalo</string>
    <string>twitter</string>
    <string>twitterauth</string>
    <string>bandapp</string>
    <string>snapchat</string>
    <string>kakaostory</string>
    <string>navercafe</string>
    <string>naverblog</string>
    <string>vkauthorize</string>
    <string>vk</string>
    <string>vk-share</string>
    <string>fb-messenger-share-api</string>
    <string>fb-messenger</string>
    <string>itms-beta</string>
    <string>comgooglemaps</string>
    <string>resso</string>
    <string>ttmusic</string>
    <string>mobilelegends</string>
    <string>snssdk1233</string>
    <string>ascendmoney</string>
    <string>boostapp</string>
    <string>momo</string>
    <string>capcut</string>
    <string>capcut840</string>
    <string>reddit</string>
    <string>scbeasy</string>
    <string>lemon8opensdk</string>
    <string>tiktoknow</string>
    <string>lark</string>
    <string>https</string>
    <string>http</string>
  </array>
```

Tatsächlich wurde während der Verwendung der TikTok-App auf dem Gerät des NTC-Analysten das Vorhandensein der folgenden Drittanbieter-Apps ermittelt:

```
canOpenURL: capcut://
canOpenURL: tiktoknow://
canOpenURL: kakaostory://
canOpenURL: zalo://
canOpenURL: whatsapp://
canOpenURL: navercafe://
canOpenURL: viber://
canOpenURL: bandapp://
canOpenURL: instagram://app
canOpenURL: twitter://
canOpenURL: naverblog://
canOpenURL: line://
canOpenURL: snapchat://
canOpenURL: tg://
canOpenURL: instagram-stories://share
canOpenURL: vkauthorize://authorize
canOpenURL: kakaolink://
canOpenURL: fb-messenger-share-api:/
canOpenURL: reddit://
canOpenURL: fbapi://
```

Zur dynamischen Analyse des Verhaltens der TikTok-App wurde das folgende Frida-Skript verwendet:

```
/*
$ frida -U -f com.zhiliaoapp.musically -l tiktok.js
*/
Interceptor.attach(ObjC.classes.UIApplication["-␣canOpenURL:"].implementation, {
onEnter: function (args) {
    console.log('canOpenURL:' , ObjC.Object(args[2]).toString());
},
onLeave: function (retval) {
}
});
```

Unter Android wird die Berechtigung `android.permission.get_tasks` implizit bei der Installation der TikTok-App erteilt. Diese kann genutzt werden, um auszulesen, welche Prozesse momentan laufen. Aus Zeitgründen wurde dies unter Android nicht näher untersucht.

Vorbedingungen

Die Vorbedingungen für die Möglichkeit zur Abfrage der Drittanbieter-Apps schafft ByteDance mit den Einträgen in der `Info.plist`-Datei. Diese wird unter anderem im Rahmen des Apple App Store-Reviews geprüft. Scheinbar bestehen beim Betreiber des App Stores keine Bedenken, dass die eingeräumten Berechtigungen von ByteDance missbraucht werden könnten.

Auswirkungen

Eine solche Abfrage kann Rückschlüsse auf die Benutzenden betreffende, sensible Informationen erlauben. Wird eine bestimmte App beispielsweise hauptsächlich von Menschen genutzt, welche einer bestimmten Ethnie oder Religion angehören, kann die Kenntnis darüber, ob die App installiert ist, dem Unternehmen ByteDance entsprechende Rückschlüsse erlauben.

Eine Übermittlung der Informationen über installierte Drittanbieter-Apps an ein ByteDance Ba-

ckend wurde im Rahmen der Untersuchung nicht festgestellt. Es kann jedoch nicht ausgeschlossen werden, dass diese Informationen in codierten oder verschlüsselten Inhalten der HTTP-Anfragen enthalten sind (siehe Befund NTCF 183).

Werden diese Informationen tatsächlich nur lokal auf dem Mobiltelefon verwendet, so ist das Verhalten der TikTok-App unbedenklich. Problematisch wird es erst, wenn die Informationen an ein ByteDance Backend übermittelt werden. Dies konnte jedoch im Rahmen dieser Untersuchung nicht ausgeschlossen werden.

Empfehlungen

Benutzende haben in der Praxis keine Möglichkeit, dieses Verhalten der TikTok-App zu unterbinden. Eine tiefergehende Prüfung, ob die Informationen an ein ByteDance Backend übermittelt werden, wird empfohlen.

Befund NTCF-186 H (Verwendung der Ortungsdienste bei jedem Start der App): **Die TikTok-iOS-App verwendet bei jedem Start der App die Ortungsdienste und sendet den genauen Standort des Mobiltelefons an ein ByteDance Backend. Der Herausgeber der App kann diese Information vielfältig nutzen.** iOS FI02 [20230308]

Hintergrund

Die TikTok-App übermittelt auf iOS bei jedem Start den geografischen Längen- und Breitengrad der Benutzenden an ein ByteDance Backend. Diese Preisgabe von sensiblen Informationen an das Unternehmen ByteDance scheint für den Verwendungszweck der TikTok-App nicht notwendig und setzt somit die Benutzenden einem Risiko aus, geografisch geortet zu werden.

Unter Android konnte beim Start der App keine Kommunikation des aktuellen Standortes an ein ByteDance Backend festgestellt werden.

Nachweis

Die folgende HTTP-Anfrage zeigt die Übertragung des geografischen Längen- und Breitengrades an ByteDance zum Zeitpunkt des App-Starts:

```
POST /tiktok/location/submit-v2/?app_id=1233&sdk_version=2.2.6&version_code=28.4.0&language=en
    &app_name=musical_ly&app_version=28.4.0&op_region=CH&residence=CH&device_id
    =7207398165421950470&channel=App%20Store&mcc_mnc=&tz_offset=3600&account_region=ch&
    sys_region=CH&aid=1233&locale=en&screen_width=640&uoo=1&openudid=
    ec168dab9cc9d038a6999641c617545c292650c0&cdid=A6F8EFE2-4C1A-412C-9DBB-8DBD131C1212&os_api
    =18&idfv=39656374-6B9F-4DA1-B426-15890ADE37C3&ac=WIFI&os_version=14.3&app_language=en&
    content_language=&tz_name=Europe/Zurich&current_region=CH&device_platform=iphone&
    build_number=284022&device_type=iPhone8,4&iid=7207399044682761990&idfa=9CFE9D17-82B9-42F0
    -8E68-67F83D99A1CF HTTP/2
Host: api16-normal-useast1a.tiktokv.com
[...]

{
  "is_vpn" : false,
  "status" : {
    [...]
    },
    [...]
  },
  "is_proxy" : true,
  "location" : {
    "sys_location" : {
      "locate_type" : 5,
      "encrypted_lat" : "1|705383242|715618705|-1447592911|1|[...]mV2IXi288=",
      "provider" : "iOS",
      "altitude_accuracy" : -1,
      "province" : "ZH",
      "timestamp" : 1678342297,
      "address" : "ZH[...]",
      "encrypted_lng" : "1|713618672|714862390|36977364|1|iy3fSH+Ivv\/[...]\/NLRO9Y=",
      "city" : "[...]",
      "coordinate_system" : "wgs84",
      "accuracy" : 13373.875635070053,
      "altitude" : 0,
      "country" : "Switzerland",
      "district" : "[...]",
      "disable_location_shift" : 0
    }
  },
 [...]
}
```

Vorbedingungen

Um auf die genauen Standortdaten der Benutzenden zugreifen zu können, benötigt die TikTok-App die Berechtigung für den Zugriff auf Ortungsdienste. Diese wird zum ersten Mal angefordert, wenn ein Video zum ersten Mal hochgeladen und das Feld **Location** ausgewählt wird. Benutzende haben sowohl unter iOS als auch unter Android die Möglichkeit, der App entweder einmalig Zugriff auf die Ortungsdienste zu gewähren oder den Zugriff dauerhaft zu erlauben, solange die App verwendet wird. Wählt der Nutzer die Option, die den Zugriff auf die Ortungsdienste während der Nutzung der App erlaubt, sendet die iOS-TikTok-App zukünftig bei jedem Start der App die genaue Position an ein ByteDance Backend. Unter Android wurde dieses Verhalten beim Start der App nicht festgestellt.

Die durch iOS übermittelten geografischen Längen- und Breitengrade werden augenscheinlich verschlüsselt übertragen. Es wird vermutet, dass diese Verschlüsselung einem Ausschluss des Infrastrukturbetreibers dient. Somit sollte der Betreiber der Infrastruktur – in diesem Fall *Akamai Technologies* – nicht in der Lage sein, die exakten geografischen Angaben zu lesen. Jedoch

werden das ermittelte Land, die Region, die Stadt und die Adresse unverschlüsselt übermittelt. Diese Informationen sind somit durch den Betreiber der Infrastruktur einsehbar.

Auswirkungen

Sowohl der Betreiber der Infrastruktur (*Akamai Technologies*) als auch der Empfänger der Information (ByteDance) kennen somit den Standort des TikTok-App-Nutzenden bei Start der App. Diese Information kann im Zusammenhang mit anderen Informationen genutzt werden, um ein Bewegungsprofil einer Person anzulegen.

Empfehlungen

Es wird empfohlen, die Berechtigung für den Zugriff auf die Ortungsdienste nicht zu erteilen. Alternativ kann bei einem Video-Upload bei Bedarf manuell der Standort angegeben werden.

Befund NTCF-187 L (Regelmässige Anfragen im Hintergrund): **Während die App im Hintergrund läuft, schickt sie stündlich HTTP-Anfragen an das Backend. Dies erlaubt eine grobe Ortung anhand der IP-Adresse.** iOS Android FI03 [20230308]

Hintergrund

Apps können auf Mobiltelefonen auch dann Daten versenden, während sie im Hintergrund laufen. Die Berechtigungssysteme von Android und iOS verhindern in so einem Fall jedoch den Zugriff auf GPS-Daten. Da die TikTok-App aber stündlich solche Hintergrund-Nachrichten versendet, ist es für ByteDance trotzdem möglich, eine ungefähre Ortung des Mobiletelefons über die IP-Adresse durchzuführen.

Nachweis

Die folgende HTTP-Anfrage wurde auf einem `Android Mobiltelefon (Samsung A13)` aufgezeichnet, während die TikTok-App im Hintergrund lief. Die Anfrage wird stündlich vom Mobiltelefon an das ByteDance Backend gesendet.

```
POST /tiktok/location/info/?sdk_version=2.3.0-rc.7.2-bugfix&iid=7207781883278345989&device_id
    =7205879119363229190&ac=wifi&channel=googleplay&aid=1233&app_name=musical_ly&version_code
    =280303&version_name=28.3.3&device_platform=android&ab_version=28.3.3&ssmix=a&device_type=
    SM-A137F&device_brand=samsung&language=en&os_api=31&os_version=12&openudid=3
    feac993ea7b747b&manifest_version_code=2022803030&resolution=1080*2208&dpi=450&
    update_version_code=2022803030&_rticket=1678280923393&current_region=GB&app_type=normal&
    sys_region=GB&timezone_name=Europe%2FZurich&residence=GB&app_language=en&ac2=wifi5g&uoo=0&
    op_region=GB&timezone_offset=3600&build_number=28.3.3&host_abi=armeabi-v7a&locale=en&
    region=GB&content_language=en%2C&ts=1678280924&cdid=68b2314c-a9e8-4070-a461-eaf413614ad8
    HTTP/2
Host: api16-normal-useast1a.tiktokv.com
[...]

{
    "upload_source": "bdlocation_background_switch",
    "status": {
        "device_type": 2,
        "is_strict_restricted_mode": false,
        "system_language": "en",
        "locale": "en_GB",
        "location_mode": 1,
        "mcc_mnc": "",
        "permission": 1,
        "system_region": "GB",
        "restricted_mode": 2
    },
    "timestamp": 1678280923,
    "is_vpn": false,
    "is_proxy": true
}
```

Vorbedingungen

Die App muss im Hintergrund laufen, was bedingt, dass die Nutzenden sie nicht vollständig beenden. Zum vollständigen Beenden der App müssen jedoch Schritte ausgeführt werden, die

über das Verlassen der Applikation hinausgehen. Daher kann angenommen werden, dass die TikTok-App bei den meisten ihrer Nutzenden zumindest zeitweise im Hintergrund ausgeführt wird.

Auswirkungen

Sowohl der Betreiber der Infrastruktur (*Akamai Technologies*) als auch der Empfänger der Information (ByteDance) kennen über die IP-Adresse den ungefähren Standort des Endgerätes. Diese Information kann in Verbindung mit anderen Daten dazu verwendet werden, ein Bewegungsprofil einer Person zu erstellen.

Empfehlungen

Es wird empfohlen, die TikTok-App bei Nichtbenutzung vollständig zu beenden.

Befund NTCF-188 M (Ermittlung des Geräte-Status): **Die TikTok-App für iOS ermittelt Informationen über die Betriebsumgebung, welche Rückschlüsse erlauben, ob sich die App in einem *Prüfstand* befindet. Die App und die Backend-Dienste könnten sich in einem solchen Fall anders als gewöhnlich verhalten.** iOS FI04 [20230309]

Hintergrund

Die TikTok-App für iOS sammelt Informationen über die Betriebsumgebung. Diese können Rückschlüsse darüber erlauben, ob die App auf einem Testgerät ausgeführt wird. Solche Methoden können von Herstellern genutzt werden, um den Programmablauf an diese Umgebung anzupassen, z.B. durch Unterdrückung von Verhalten, das geheim gehalten werden soll.

Nachweis

Die TikTok-App prüft das Vorhandensein von `Cydia`, einem inoffiziellen App Store. Cydia kann nur auf Geräten mit Jailbreak ausgeführt werden, wie sie häufig von Sicherheitsforschern eingesetzt werden. Der folgende Auszug zeigt den von der App geprüften Standard-Pfad der App:

```
fileExistsAtPath: /Applications/Cydia.app
```

Die oben aufgeführte Ausgabe wurde mit dem folgenden Frida-Skript zur Laufzeit der App erstellt:

```
/*
$ frida -U -f com.zhiliaoapp.musically -l tiktok.js
*/
Interceptor.attach(ObjC.classes.NSFileManager["-␣fileExistsAtPath:"].implementation, {
onEnter: function (args) {
    console.log('fileExistsAtPath:' , ObjC.Object(args[2]).toString());
},
onLeave: function (retval) {
}
});
```

Entdeckt die TikTok-App einen Jailbreak, z.B. mittels der Cydia-Prüfung, so sendet die App diese Information auch verschlüsselt an ein ByteDance Backend. Der folgende Auszug zeigt den übermittelten Inhalt mit dem Wertepaar `"JBDevice":true` vor der Verschlüsselung:

```
{
  "cell": {
    "mcc": "",
    "mnc": "",
    "ra": ""
  },
  "shortbundleversion": "28.4.0",
  "bundlename": "TikTok",
  "timepassedsincelastlaunch": "195",
  "timestamp": "1678365760.423975",
  "uid": "1678262062308-3965637",
  "platform": "iPhone8,4",
  "fb_anon_id": "XZ64E1EB19-1CE7-4EAD-9DE3-DD2C1641BAA9",
  "counter": "14",
  "prev_session_dur": 191,
  "reinstallCounter": "3",
  "advertiserId": "9CFE9D17-82B9-42F0-8E68-67F83D99A1CF",
  "systemversion": "14.3",
  "iaecounter": "2",
  "lang_code": "en",
  "JBDevice": true,
  "date3": "2023-03-08_085613+0100",
  "deviceData": {
    "cpu_type": "ARM64_V8",
    "cpu_speed": "-1",
    "cpu_64bits": "true",
    "dim": {
      "y_px": 1136,
      "x_px": 640
    },
    "osVersion": "14.3␣(Build␣18C66)",
    "ram_size": "2013",
    "device_model": "iPhone8,4",
    "cpu_count": "2"
  },
  "currentCountrycode": "CH",
  "open_referrer": "",
  "sc_o": "fu",
  "date1": "2023-03-08_085422+0100",
  "systemname": "iOS",
  "ivc": false,
  "localizedmodel": "iPhone",
  "af_events_api": "1",
  "bundleversion": "284022",
  "eventName": "Launched",
  "model": "iPhone",
  "dev_key": "XY8Lpakui8g4kBcposRgxA",
  "currentLanguage": "en-CH",
  "wifi": true,
  "advertiserIdEnabled": true,
  [...]
  "date1_2": "2023-03-08_085422+0100",
  "disk": "5275/15238",
  "sessioncounter": "17",
  "date2": "2023-03-09_134239+0100",
  "firstLaunchDate": "2023-03-08_085613+0100",
  "originalAppsflyerId": "1677740633160-3499600",
  "att_status": 0,
  "platformextension": "ios_native",
  "bundleIdentifier": "com.zhiliaoapp.musically"
}
```


Die Verschlüsselung dieser Inhalte findet mittels `kCCAlgorithmAES128` statt und kann ebenfalls mittels eines Frida-Skripts gehookt und ausgegeben werden. Die verschlüsselten Inhalte werden an die Webadresse `log22-normal-useast1a.tiktokv.com` gesendet.

Weitere Indikatoren für eine Test-Umgebung sind z.B. auch die Verwendung eines Proxy oder eines VPN, welche eine Untersuchung des Netzwerkverkehrs erlauben. Auch diese Informationen werden von der TikTok-App abgefragt und an ein ByteDance Backend übermittelt:

```
POST /tiktok/location/info/?app_id=[...] HTTP/2
Host: api16-normal-useast1a.tiktokv.com
[...]

{
  "status" : {
    "locale" : "en-CH",
    "restricted_mode" : 2,
    "permission" : 60,
    "carrier_region" : "",
    "system_region" : "CH",
    "sim_mccmnc" : {
      "network" : "(null)(null)",
      "primary" : "(null)(null)",
      "secondary" : "(null)(null)"
    },
    "system_language" : "en-CH",
    "network_sim_region" : "",
    "location_mode" : 1,
    "device_type" : 1
  },
  "is_vpn" : false,
  "is_proxy" : true,
  "timestamp" : 1678112554
}
```

Für Android konnte in der zur Verfügung stehenden Zeit nicht getestet werden, ob die App Informationen über Root-Rechte ermittelt oder nicht. Die obige Nachricht an ein ByteDance Backend, ob ein VPN oder Proxy verwendet wird, wurde auch im Netzwerkverkehr der Android-App festgestellt.

Vorbedingungen

Die Abfrage, welche Cydia oder andere für einen Jailbreak typische Dateien erkennt, ist allen Apps erlaubt.

Auswirkungen

Es ist unklar, wofür die oben erwähnten Informationen von ByteDance verwendet werden. Daher kann die Vermutung, dass es sich hierbei um die Erkennung eines Prüfstandes handelt, nicht ausgeschlossen werden. Ist dies der Fall, könnte ein solcher *Prüfstand*-Modus bestimmtes Verhalten der TikTok-App verbergen.

Empfehlungen

Es wird empfohlen, tiefergehende Untersuchungen durchzuführen, um ein abweichendes Verhalten der TikTok-App in *Prüfstand*-Situationen ausschliessen zu können.

Befund NTCF-189 L (Verwendung eines integrierten Browsers): **Die TikTok-App für Android enthält einen integrierten Browser. Dieser liesse sich zur Überwachung und Manipulation von angezeigten Inhalten und Benutzereingaben verwenden. So weit beobachtet, kommt der Browser nur in einem beschränkten Szenario zur Anwendung. Das mögliche Risiko wird daher als gering eingestuft.** Android FI05 [20230327]

Hintergrund

Die TikTok-App für Android verwendet einen integrierten Browser zum Anzeigen von Webinhalten, wenn ein in einem Nutzer-Profil hinterlegter Hyperlink aufgerufen wird.[3] Der Aufruf des Hyperlinks erfolgt via Abfrage an ein ByteDance Backend. Es wird nach dem Laden der Seite die Möglichkeit angeboten, die Seite in einem externen Browser zu öffnen. Hyperlinks lassen sich nur aus dem Nutzer-Profil heraus öffnen. Hyperlinks in Nachrichten an und von Freunden, in Kommentaren zu Videos oder in Videobeschreibungen sind nicht klickbar und lassen sich somit nicht im integrierten Browser aufrufen.

Nachweis

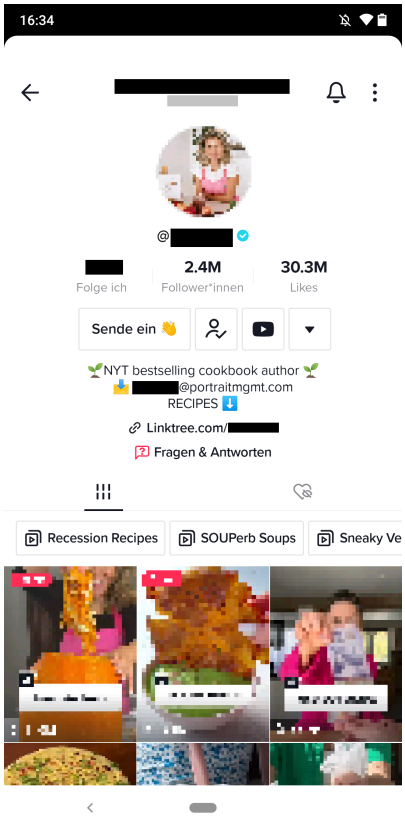

Abbildung 2: Link im Profil (Mitte)

[3] Unter iOS ist dieser Browser nicht integriert.

Die folgende HTTP-Anfrage eines Android-Gerätes zeigt exemplarisch die Übermittlung eines aufgerufenen Links an ein ByteDance Backend:

```
GET /link/?aid=1233&lang=de&scene=bio_url&target=Linktree.com\%2FXXXXXXXX&owner_suid=MS[...]7s
    HTTP/2
Host: web-va.tiktok.com
[...]
```

Die Antwort des Servers dazu lautet:

```
HTTP/2 302 Found
Server: nginx
Content-Type: text/html; charset=utf-8
Content-Length: 52
Location: https://Linktree.com/XXXXXXXX
[...]

<a href="https://Linktree.com/XXXXXXXX">Found</a>.
```

Vorbedingungen

In einem Nutzer-Profil muss ein Hyperlink hinterlegt worden sein.

Auswirkungen

Es kann angenommen werden, dass die Profil-Seite primär beim Entdecken eines neuen Profils besucht wird und danach kaum mehr. Es ist auch nur ein einzelner Link pro Profil vorhanden. Daher wird das Schadenspotential als gering eingeschätzt. Aus diesem Grund wurde nicht untersucht, ob der Browser mit zusätzlichen Funktionen wie z.B. der Übertragung von Benutzereingaben an ByteDance ausgestattet ist.

Im Rahmen des Audits war es nicht möglich, einen Link im eigenen Testprofil zu hinterlegen. Diese Funktion scheint nur für ausgewählte Profile freigeschaltet zu sein.[4] Daher konnte nicht getestet werden, ob beliebige Links gesetzt werden können.

Es gilt zu beachten, dass die TikTok-App bei einem Link-Aufruf mit einem ByteDance Backend kommuniziert und ByteDance daher Kenntnis über den Aufruf hat.

Empfehlungen

Es wird empfohlen, keine Eingaben auf Webseiten zu machen, welche von der TikTok-App aus aufgerufenen wurden. Auch sollten Seiten präventiv, so früh wie möglich, in einem externen Browser aufgerufen werden.

[4] https://linktr.ee/blog/how-to-add-a-linktree-to-your-tiktok-bio/

Befund NTCF-190 M (Multi-Faktor-Authentisierung wird nicht erzwungen): **TikTok gibt Benutzenden die Möglichkeit, sich mittels E-Mail-Adresse und Passwort oder via Telefonnummer zu registrieren. Wenn einer dieser Faktoren kompromittiert ist, kann die Kontrolle über das TikTok-Konto übernommen werden. Zum Schutz vor derlei Attacken, bietet TikTok optional die Möglichkeit, eine Multi-Faktor-Authentisierung zu aktivieren.** FI06 [20230327]

Hintergrund

ByteDance möchte die Registrierung und das Einloggen in das TikTok-Konto so einfach wie möglich gestalten. Aus diesem Grund verzichtet ByteDance auf eine tiefgehende Identitätsprüfung und standardmässig auch auf komplexere MFA-Faktoren. Für Angreifer wäre es potenziell möglich, durch *SIM-Swapping* die Telefonnummer von TikTok-Benutzenden zu übernehmen und so Zugriff auf deren Konten zu erhalten.

Die Aktivierung der von TikTok optional angebotenen "2-Stufen-Verifizierung" (Wortlaut TikTok) schützt vor dieser Art von Angriffen.

Nachweis

TikTok verlangt bei der Registrierung eines Kontos lediglich eine E-Mail-Adresse und ein Passwort oder eine Telefonnummer. Eine Registrierung über andere soziale Medien ist ebenfalls möglich, wurde aber in dieser Untersuchung nicht berücksichtigt.

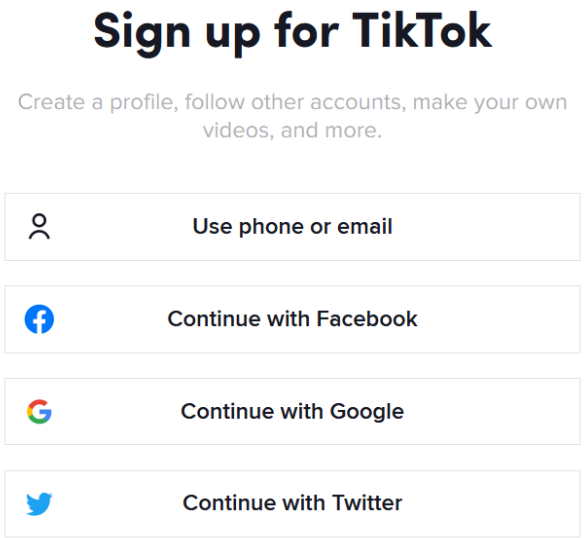

Abbildung 3: Registrierungsmöglichkeiten bei TikTok

Wenn eine Telefonnummer mit einem Konto verknüpft ist, sendet TikTok bei der Anmeldung eine SMS mit einem sechsstelligen Code an die hinterlegte Nummer. Dieser Code reicht aus, um sich

bei dem verknüpften Konto anzumelden.

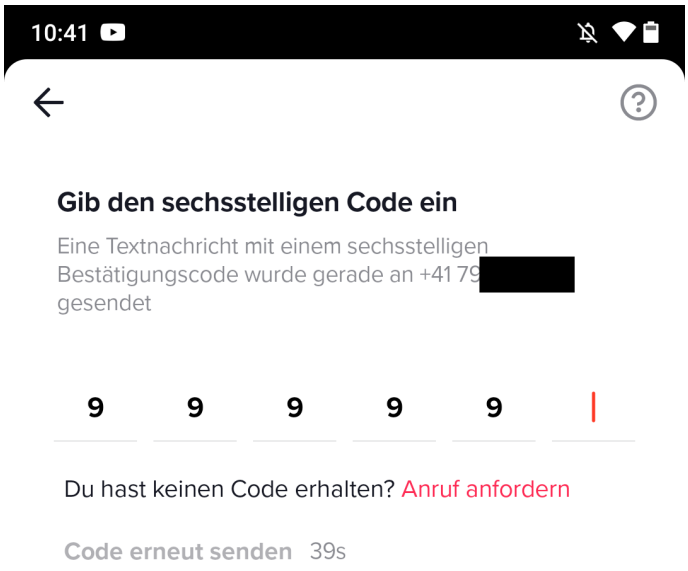

Abbildung 4: Login via SMS in der TikTok-App

Vorbedingungen

Wenn lediglich eine Telefonnummer auf dem Konto registriert ist und keine 2-Stufen-Verifizierung aktiviert ist, besteht die Möglichkeit, das Konto via SIM-Swapping zu übernehmen. Dabei übernehmen Angreifer, z.B. über Social-Engineering-Angriffe beim Mobilfunkprovider die vollständige Kontrolle über die Telefonnummer der betroffenen Person.

Auswirkungen

Wenn die 2-Stufen-Verifizierung nicht explizit aktiviert wird, besteht ein erhöhtes Risiko der Kontenübernahme via SIM-Swapping. Dieses Risiko gilt nicht nur für TikTok, sondern für alle Apps, welche lediglich den Empfang einer SMS-Textnachricht benötigen.

Eine mögliche Konsequenz einer feindlichen Account-Übernahme ist die massenhafte Verbreitung von Falschnachrichten innert kurzer Zeit. Sind behördlich genutzte Accounts davon betroffen, so dürfte die Wirkung gravierender ausfallen. Auch ist denkbar, dass Bots aus anderen Social-Media-Plattformen die Falschinformationen aufgreifen und in eigenen Medien massenhaft teilen und somit möglicherweise weiteren Kreisen zugänglich machen.

Für all jene Accounts mit vielen Followern sei gesagt, dass eine 2-Stufen-Verifizierung durch TikTok erzwungen wird. [5]

[5] https://support.tiktok.com/en/using-tiktok/growing-your-audience/how-to-tell-if-an-account-is-verified-on-tiktok#4

Empfehlungen

Es wird allen Benutzenden empfohlen, in den Konteneinstellungen die Option für 2-Stufen-Verifizierung via Authenticator App zu aktivieren, siehe dazu Tiktok Hilfe: 2-Stufen-Verifizierung aktivieren.

Zudem wird generell die Verwendung von starken und einmaligen Passwörtern empfohlen.

4 Testfälle

In diesem Abschnitt werden alle Testfälle vorgestellt, die während der Sicherheitsanalyse betrachtet wurden. Befunde, die aus einem bestimmten Testfall hervorgehen, sind unter der Kurzbeschreibung des Testfalls verlinkt. Wenn kein Befund verlinkt ist, wurde im Zeitrahmen der Analyse keine relevante Schwachstelle gefunden. Wenn die Testfälle nur für eine Teilmenge der Komponenten gelten, werden die entsprechenden Komponenten explizit aufgeführt.

4.1 Netzwerk-Kommunikation

Die Testfälle zur Kommunikation fokussieren sich auf die Daten, die zwischen der TikTok-App und dem ByteDance Backend ausgetauscht werden, basierend auf einer zu erwartenden Nutzung der TikTok-App durch legitime Benutzende ohne missbräuchliche Absichten.

TF 1 Verschlüsselte Datenübertragung
Wird der Netzwerkverkehr verschlüsselt übertragen?
Risiko: Wird der Netzwerkverkehr nicht verschlüsselt übertragen, so ist es für Angreifer einfach möglich, den Inhalt der Kommunikation mitzulesen oder zu manipulieren.
Befunde: 183, 184

TF 2 Verschlüsselte Datenübertragung mit sicheren Protokollen
Wird der Netzwerkverkehr mittels sicherer Protokolle verschlüsselt?
Risiko: Wird der Netzwerkverkehr mit unsicheren Protokollen übertragen, erleichtert dies den Angreifern, den Inhalt der Kommunikation mitzulesen oder zu manipulieren.

TF 3 Benutzerkonto anlegen und Erstidentifikation
Welche Möglichkeiten für eine Konten-Registrierung werden angeboten? Wie wird die Identität der Benutzenden überprüft?
Risiko: Wird die Identität der Benutzenden nicht ausreichend geprüft, so ist es Angreifern möglich, Konten zu übernehmen oder unter einem fremden Namen zu erstellen. Dadurch können sensible Daten eingesehen oder falsche Informationen verbreitet werden.
Befunde: 190

TF 4 Video erstellen und hochladen
Welche Daten werden erfasst und übertragen, wenn ein Video in der TikTok-App aufgenommen und hochgeladen wird?
Risiko: Werden mehr oder andere Daten erfasst und an ein ByteDance Backend übertragen als von den Benutzenden beabsichtigt, so kann dies ein Hinweis für Benutzerüberwachung sein.
Befunde: 186, 187

TF 5 Private Nachrichten austauchen
Sind die privaten Nachrichten Ende-zu-Ende verschlüsselt?

Risiko: Werden private Nachrichten nicht Ende-zu-Ende verschlüsselt, so ist es für Drittparteien wie die Betreiber des ByteDance Backend möglich, die Nachrichten mitzulesen.
Befunde: 184

TF 6 TikTok-App im Vordergrund
Während die TikTok-App im Vordergrund läuft, ist es ihr möglich, mit bereits erteilten Berechtigungen wie z.B. für die genaue GPS-Ortung Daten zu erheben. Wird diese Möglichkeit übermässig genutzt und Daten an ein ByteDance Backend gesendet?
Risiko: Werden unerwartet Daten an ein ByteDance Backend gesendet, ohne dass ein erkennbarer Nutzen für die Benutzenden besteht, kann dies ein Hinweis auf Benutzerüberwachung sein.
Befunde: 186

TF 7 TikTok-App im Hintergrund
Werden unerwartete Daten an ein ByteDance Backend gesendet, während die TikTok-App im Hintergrund aktiv ist?
Risiko: Eine unerwartete Datenübertragung im Hintergrund kann ein Hinweis auf eine Benutzerüberwachung sein.
Befunde: 187

4.2 Privatsphäre und Datenschutz

Bei den nachfolgend aufgeführten Tests zu Privatsphäre und Datenschutz wurde besonderer Fokus darauf gelegt, wie die TikTok-App mit den Berechtigungen der mobilen Betriebssysteme umgeht. Dabei wurde insbesondere überprüft, welche Berechtigungen wann angefragt werden und ob die erhaltenen Daten an das ByteDance Backend übermittelt werden.

TF 8 Geolocation Tracking
Wird die aktuelle Position des Gerätes erfasst und an das ByteDance Backend übermittelt? Wird die GPS Position zwingend für den Gebrauch der App benötigt?
Risiko: Positionsdaten können verwendet werden, um den aktuellen Standort zu ermitteln oder Bewegungsprofile zu erstellen. Je mehr und genauere Datenpunkte zur Verfügung stehen, desto genauer können die Benutzenden überwacht werden. Bewegungsprofile können Rückschlüsse auf Wohnort, Arbeitsort, Vorlieben und Gewohnheiten etc. ermöglichen.
Befunde: 186, 187

TF 9 Zugriff auf Kontakte
Ist der Zugriff auf die Kontakte zwingend nötig, um die TikTok-App verwenden zu können? Zu welchen Zeitpunkten werden die Kontakte angefragt und übermittelt?
Risiko: Das Sammeln von Kontaktdaten ermöglicht es ByteDance, Nutzerprofile und Beziehungsmuster von unbeteiligten Dritten - also Personen, die TikTok nicht nutzen - zu erstellen.
Befunde: 182

TF 10 Zugriff auf Kalender
Benötigt die TikTok-App Zugriff auf den Kalender der Benutzenden?
Risiko: Kalenderinformationen können sensitive Informationen über den Tagesablauf und die Aktivitäten der Benutzenden enthalten und eignen sich daher gut für die Überwachung. Termine können darüber hinaus wertvolle Zusatzinformationen enthalten, wie z. B. die teilnehmenden Personen, deren Kontaktdaten, Standorte, Aktivitäten usw.

TF 11 Zugriff auf Kamera
Zu welchen Zeitpunkten wird auf die Kamera zugegriffen? Werden die Daten direkt an das ByteDance Backend übertragen?
Risiko: Die Kamera kann dazu benutzt werden, unbemerkt Bilder oder Videos aufzunehmen. Diese Bildinformationen können Aufschluss darüber geben, in welcher Umgebung sich die Benutzenden gerade befinden, welche Personen sich in der Nähe aufhalten oder welche Tätigkeiten ausgeführt werden. Unter Umständen können die Bilder auch als Erpressungsmittel eingesetzt werden.

TF 12 Zugriff auf Mikrofon
Zu welchen Zeitpunkten wird auf das Mikrofon zugegriffen? Werden die Daten direkt an das ByteDance Backend übertragen?
Risiko: Das Mikrofon kann für unbemerkte Tonaufnahmen verwendet werden. Diese Aufnahmen können Aufschluss über die aktuelle Umgebung geben, in der sich die Benutzenden befinden, und den Inhalt von - möglicherweise vertraulichen - Gesprächen offenbaren. Unter Umständen können die Aufnahmen auch als Erpressungsmittel eingesetzt werden.

TF 13 Zugriff auf externen Speicher
Wann wird auf den externen Speicher zugegriffen? Werden nur die ausgewählten Dateien gelesen oder auch auf andere Inhalte?
Component: Android
Risiko: Die App könnte ohne Wissen und ausdrückliche Zustimmung der Benutzenden auf Daten zugreifen und diese lokal verarbeiten oder an das ByteDance Backend übertragen. Dabei kann es sich unter anderem um vertrauliche und personenbezogene Daten handeln.

TF 14 Zugriff auf das lokale Netzwerk
Wird der Zugriff auf das lokale Netzwerk angefragt?
Component: iOS
Risiko: Die Berechtigung erlaubt die Interaktion mit lokalen Netzwerkgeräten, wie z.B. Smart-Home-Geräten. Unter Umständen könnte es möglich sein, solche lokalen Netzwerkgeräte zu steuern oder sensible Informationen auszulesen.

TF 15 Sammeln von Systeminformationen
Werden Informationen zum Mobiltelefon an ein ByteDance Backend gesendet? Werden Informationen über installierte oder ausgeführte Apps gesammelt und an das ByteDance Backend

übertragen?
Risiko: Die Übertragung von Systeminformationen ermöglicht die Erstellung eines Benutzerprofils und die Überwachung der Benutzeraktivitäten. Dies ist insbesondere dann von Bedeutung, wenn Benutzende mehrere Profile (z. B. privat und beruflich) auf demselben Gerät verwenden.
Befunde: 185

TF 16 Datenauszug nach Datenschutzgesetz

Wenn Nutzerinnen und Nutzer von ihrem Auskunftsrecht Gebrauch machen und einen vollständigen Datenauszug anfordern, enthält dieser dann auch nur zweckmässig erhobenen Daten?
Risiko: Die Erhebung und Speicherung von Daten sollte nur in dem Umfang erfolgen, wie es für den jeweiligen Zweck erforderlich ist.

TF 17 Abfrage der Zwischenablage

Greift die TikTok-App ungefragt auf die Zwischenablage zu? Werden die Daten aus der Zwischenablage automatisch an das ByteDance Backend übertragen?
Risiko: Die Zwischenablage kann vertrauliche Inhalte wie Passwörter enthalten.

TF 18 Verwendung eines integrierten Browsers

Verwendet die App einen integrierten Browser? Wenn ja, wozu dient dieser? Verfügt er über besondere Funktionen?
Risiko: Ein integrierter Browser könnte um nahezu beliebige Funktionen erweitert werden. Dies könnte z.B. die Aufzeichnung der angezeigten Inhalte oder der Benutzereingaben ermöglichen. Damit könnten potenziell sensible Daten erfasst und an das ByteDance Backend übertragen werden.
Befunde: 189