Datenschutzhinweis der Deutsche Telekom Security GmbH („Telekom“) für die Nutzung der Mobile Protect Pro App (MPP)

Allgemeines

Der Schutz Ihrer persönlichen Daten hat für die Deutsche Telekom Security GmbH einen hohen Stellenwert. Es ist uns wichtig, Sie darüber zu informieren, welche persönlichen Daten erfasst werden, wie diese verwendet werden und welche Gestaltungsmöglichkeiten Sie dabei haben.

Welche Daten werden erfasst, wie werden sie verwendet und wie lange werden sie gespeichert?

a) Bei der Erbringung der Leistungen:
In den Privacy Settings der MPP Konsole kann der Administrator definieren, welche Daten von der Anwendung erhoben werden sollen. Folgende Daten können erhoben werden. Per Konfiguration kann der Kunden Administrator einstellen, ob diese Daten erhoben werden. Da ein Angriff lokal auf dem Endgerät durch die z9 Engine erkannt wird, sind nur sehr wenig Daten zur Identifizierung und sicheren Kommunikation des Endgerätes mit der MPP Konsole notwendig. Die Daten aller Handlungsverläufe, die sowohl in der MPP App als auch in der zConsole durchgeführt werden, werden für 30 Tage gespeichert und anschließend gelöscht. Threatdaten werden für 30 Tage gespeichert und anschließend gelöscht.

b) **Beim Einloggen (Starten der App):**
- Bis einschließlich der Version 4.7 Zugangsdaten (Benutzername/E-Mail und Passwort) – ab Version 4.8.xx eindeutiger Token
- Hashwert des Gerätes (MD5 der IMEI oder der Seriennummer), bei iOS (MD5 der IMEI)
- Betriebssystem des Gerätes

c) **Geräteinformation nach dem Anmelden (Android):**
- Eindeutiger Push Token der App auf dem Gerät, um Nachrichten von der Konsole zu verifizieren
- Lokation: GPS Längen- und Breitengrade – auf den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS Daten ermittelt. (optional einstellbar)
- Netzwerk: MAC- und IP Address, BSSID, SSID
- Gerät: Betriebssystem, Betriebssystem Version, Model, IMEI, Jailbroken, Entwickler Option
- Liste installierter Apps
- Verbindungsstatus (WLAN oder 3G)
- Benutzer Informationen: Benutzername /E-Mail (aus der Konsole ermittelt)

d) **Geräteinformation nach dem Anmelden (iOS):**
- Eindeutiger Push Token der App auf dem Gerät, um Nachrichten von der Konsole zu verifizieren
- Lokation: GPS Längen- und Breitengrade – auf den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS Daten ermittelt. (optional einstellbar)
- Netzwerk: MAC- und, IP Address BSSID, SSID
- Gerät: Betriebssystem, Betriebssystem Version, IMEI, SNO (wenn verfügbar)
- Liste installierter Apps (nur verfügbar, wenn ein MDM angebunden ist)
- Verbindungsstatus (WLAN oder 3G) (optional einstellbar)
- Benutzer Informationen: Benutzername/E-Mail (aus der Konsole ermittelt)

e) **Bei der Synchronisation mit einem MDM:**
- Hashwert der lokalen z9 Engine (Anomalieerkennungssoftware) und Schadsoftware Datenbank
- Lokation: GPS Längen- und Breitengrade – je nach den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS Daten ermittelt. (optional einstellbar)
- Netzwerk: Router BSSID und SSID
- Gerät: IP und MAC Adresse des Gerätes
- App Forensik: Aktive Apps auf dem Gerät (Android, iOS)
- Verbindungsstatus (WLAN oder 3G)

f) Bei der Entdeckung eines Angriffsext oder Video Chat:
- Zeit des Ereignisses
- Angriffsbezeichnung
- Lokation: GPS Längen- und Breitengrade – auf den durch den Administrator eingestellten Privacy Definitionen werden Straße, Stadt, Bundesland (Region, Zeitzone, Ländercode, Kontinent) aus den GPS Daten ermittelt. (optional einstellbar)
- Erkennung der App (Binärcode, Hashwert)
- Netzwerk: Mac und IP Adresse, Router BSSID und SSID, Benachbarte WLAN Netzwerke (BSSID / SSID), Netzwerkstatistiken (bestehende TCP / UDP Verbindungen zum Zeitpunkt des Angriffs inclusive IP und Port Adresse), ARP Tabelle aller lokalen Hosts im WLAN, die mit dem Gerät kommunizieren sowie Informationen zur Basisstation
- Gerät: Betriebssystem, Betriebssystem Version, Gerätemodel, IMEI, aktive APP (Android), Verbindungsstatus (WLAN oder 3G), ARP Tabelle des Gerätes (vor und nach dem Angriff), Liste von (zum Zeitpunkt des Angriffes) aktiven Prozessen, im Fall von Angriffen auf das Filesystem der vollqualifizierte Datei-/Ordnerpfad die auf dem Gerät geändert wurden.
- App Forensik: Auf dem Gerät installiert Apps, Paketname der entdeckten Schadsoftware/App
- Nur iOS: Im Fall von Angriffen auf das Profil, werden alle Profile Informationen an die Konsole übermittelt.

Darüber hinaus gehende personenbezogene Daten, wie z. B. Ihr Name, Ihre Anschrift oder Telefonnummer, werden von der APP nicht erfasst.

Berechtigungen

Um die App auf Ihrem Gerät nutzen zu können, muss die App auf verschiedene Funktionen und Daten Ihres Endgeräts zugreifen können. Dazu ist es erforderlich, dass Sie bestimmte Berechtigungen erteilen (Art. 6 Abs. 1 a DSGVO).
Die Berechtigungskategorien sind von den verschiedenen Herstellern unterschiedlich programmiert. So werden z. B. bei Android Einzelberechtigungen zu Berechtigungskategorien zusammengefasst und Sie können auch nur der Berechtigungskategorie insgesamt zustimmen.
Soweit Sie Berechtigungen erteilt haben, nutzen wir diese nur im nachfolgend beschriebenen Umfang (siehe auch die vorangegangenen Abschnitte):

Standortdaten

Sofern von Ihrem Administrator der MPP zConsole eingestellt (siehe oben), benötigt die App Informationen zu Ihrem aktuellen Standort, um die Lokation wo ein Angriff auf Ihr mobiles Endgerät stattgefunden hat, zu bestimmen (z.B. maliziöse WLANs).

Internetkommunikation
Um ggf. Angriffe auf Ihr mobiles Endgeräte auf der MPP zConsole Ihres Administrators anzuzeigen, benötigt die App Internet Zugang über W-LAN oder Mobilfunk.

Sendet die App Push-Benachrichtigungen?

Push-Benachrichtigungen sind Nachrichten, die von der App auf Ihr Gerät gesendet und dort priorisiert dargestellt werden. Diese App kann Push-Benachrichtigungen verwenden, um Ihnen entdeckte Schwachstellen und Angriffe auf Ihrem mobilen Endgerät anzuzeigen, wenn es von Ihrem Administrator auf der MPP zConsole so eingestellt ist. Diese App verwendet Push-Benachrichtigungen im Auslieferungszustand, sofern Sie bei der App-Installation oder bei der ersten Nutzung eingewilligt haben (Art. 6 Abs. 1 a DSGVO).

Wird mein Nutzungsverhalten ausgewertet, z. B. für Werbung oder Tracking?

Nein, in der MPP App werden keine Tools / Cookies zur Auswertung des Nutzungsverhaltens eingesetzt. (bezogen auf MPP App).

Nein, in der zConsole werden ausschließlich Tools / Cookies, die für den Betrieb der zConsole erforderlich sind, eingesetzt. Diese sind Folgende: (bezogen auf MPP zConsole

Erforderliche Tools
Diese Tools/ Cookies sind notwendig, damit die MPP zConsole (Management Konsole) einwandfrei funktioniert. Es handelt sich um technisch notwendige Tools/ Cookies. Rechtsgrundlage für diese Tools/ Cookies ist Art. 6 Abs. 1 b DSGVO **(s. Anhang)**.

Wird das Auditlog gespeichert? Wenn ja, wie lange wird das Auditlog gespeichert? *(bezogen auf MPP zConsole)*

Das Auditlog speichert Handlungsverläufe, die sowohl in der MPP App als auch in der zConsole durchgeführt werden. Dazu gehören z.B. das Einloggen in die MPP App oder die Durchführung von Änderungen in der zConsole. Diese Informationen sind nur für den Administrator sichtbar. Die Daten werden für 30 Tage gespeichert und anschließend gelöscht.

Wo finde ich die Informationen, die für mich wichtig sind?

Dieser Datenschutzhinweis gibt einen Überblick über die Punkte, die für die Verarbeitung Ihrer Daten in dieser App durch die Telekom gelten.
Weitere Informationen, auch zum Datenschutz in speziellen Produkten, erhalten Sie auf https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/datenschutz und unter http://www.telekom.de/datenschutzhinweise.

Wer ist verantwortlich für die Datenverarbeitung? Wer ist mein Ansprechpartner, wenn ich Fragen zum Datenschutz bei der Telekom habe?

Datenverantwortliche ist die Deutsche Telekom Security GmbH, Bonner Talweg 100, 53113 Bonn. Bei Fragen können Sie sich an unseren Kundenservice wenden oder an unseren Datenschutzbeauftragten, Herrn Dr. Claus D. Ulmer, Friedrich-Ebert-Allee 140, 53113 Bonn, datenschutz@telekom.de.

Welche Rechte habe ich?

Sie haben das Recht,

a) **Auskunft** zu verlangen zu Kategorien der verarbeiteten Daten, Verarbeitungszwecken, etwaigen Empfängern der Daten, der geplanten Speicherdauer (Art. 15 DSGVO);
b) die **Berichtigung** bzw. Ergänzung unrichtiger bzw. unvollständiger Daten zu verlangen (Art. 16 DSGVO);
c) eine erteilte Einwilligung jederzeit mit Wirkung für die Zukunft zu **widerrufen** (Art. 7 Abs. 3 DSGVO);
d) einer Datenverarbeitung, die aufgrund eines berechtigten Interesses erfolgen soll, aus Gründen zu **widersprechen,** die sich aus Ihrer besonderen Situation ergeben (Art 21 Abs. 1 DSGVO);
e) in bestimmten Fällen im Rahmen des Art. 17 DSGVO die **Löschung** von Daten zu verlangen - insbesondere soweit die Daten für den vorgesehenen Zweck nicht mehr erforderlich sind bzw. unrechtmäßig verarbeitet werden, oder Sie Ihre Einwilligung gemäß oben (c) widerrufen oder einen Widerspruch gemäß oben (d) erklärt haben;
f) unter bestimmten Voraussetzungen die **Einschränkung** von Daten zu verlangen, soweit eine Löschung nicht möglich bzw. die Löschpflicht streitig ist (Art. 18 DSGVO);
g) auf **Datenübertragbarkeit,** d.h. Sie können Ihre Daten, die Sie uns bereitgestellt haben, in einem gängigen maschinenlesbaren Format wie z.B. CSV erhalten und ggf. an andere übermitteln (Art. 20 DSGVO;)
h) sich bei der zuständigen **Aufsichtsbehörde** über die Datenverarbeitung zu **beschweren** (für Telekommunikationsverträge: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit; im Übrigen: Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen).

An wen gibt die Telekom meine Daten weiter?

An Auftragsverarbeiter, das sind Unternehmen, die wir im gesetzlich vorgesehenen Rahmen mit der Verarbeitung von Daten beauftragen, Art. 28 DSGVO (Dienstleister, Erfüllungsgehilfen). Die Telekom bleibt auch in dem Fall weiterhin für den Schutz Ihrer Daten verantwortlich. Wir beauftragen Unternehmen insbesondere in folgenden Bereichen: IT, Vertrieb, Marketing, Finanzen, Beratung, Kundenservice, Personalwesen, Logistik und Druck.

An Kooperationspartner, die in eigener Verantwortung Leistungen für Sie bzw. im Zusammenhang mit Ihrem Telekom Vertrag erbringen. Dies ist der Fall, wenn Sie Leistungen solcher Partner bei uns beauftragen oder wenn Sie in die Einbindung des Partners einwilligen oder wenn wir den Partner aufgrund einer gesetzlichen Erlaubnis einbinden.

Aufgrund gesetzlicher Verpflichtung: In bestimmten Fällen sind wir gesetzlich verpflichtet, bestimmte Daten an die anfragende staatliche Stelle zu übermitteln. Beispiel: Nach Vorlage eines Gerichtsbeschlusses sind wir gemäß § 101 Urheberrechtsgesetz verpflichtet, Inhabern von Urheber- und Leistungsschutzrechten Auskunft über Kunden zu geben, die urheberrechtlich geschützte Werke in Internet-Tauschbörsen angeboten haben sollen.

Wo werden meine Daten verarbeitet?

Ihre Daten werden nur in Deutschland gespeichert und verarbeitet.

Wie sicher sind die Daten gespeichert?

Zum Schutz Ihrer Daten vor unberechtigtem Zugriff und Missbrauch haben wir umfangreiche technische und betriebliche Sicherheitsvorkehrungen nach deutschem Recht (DSGVO) getroffen

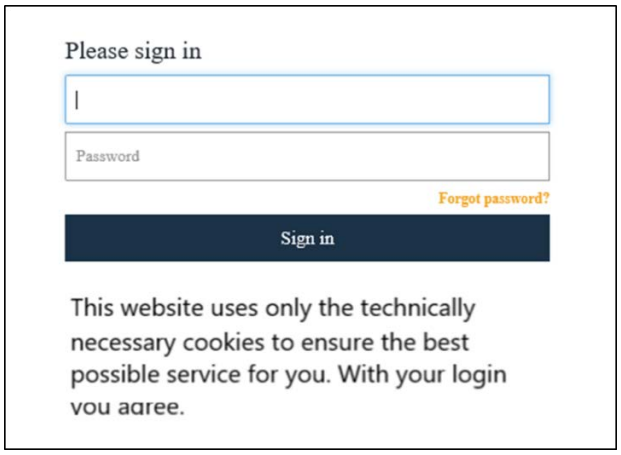
Werde ich über Änderungen dieser Datenschutzhinweise informiert?

Sollten wir die vorliegenden Datenschutzhinweise ändern müssen, werden wir Sie (Kunden-Administratoren) im Rahmen von Software-Updates auf die entsprechenden Änderungen hinweisen.

Ihre Datenschutz-Einstellungen

Die MPP zConsole verwendet ausschließlich technisch notwendige Tools / Cookies. Mit dem LogIn akzeptieren Sie die Verwendung der technisch notwendigen Tools / Cookies.

Stand der Datenschutzhinweise 18.06.2020



Anhang:

Wird mein Nutzungsverhalten ausgewertet, z. B. für Werbung oder Tracking?

Erforderliche Tools

Firma	Name	Beschreibung (Funktion)	Eingebunden als
Zimperium	csrftoken	Dieses Cookie ist mit der Django-Webentwicklungsplattform für Python verknüpft. Es soll eine Website vor bestimmten Softwareangriffen auf Webformulare schützen.	Auftragsverarbeiter
Zimperium	zcookie	Sitzungstoken Sitzungstoken sind Daten, die in der Netzwerkkommunikation (häufig über HTTP) verwendet werden, um eine Sitzung zu identifizieren. Zudem wird es verwendet, um mehrere zusammengehörige Anfragen eines Benutzers zu erkennen und einer Sitzung zuzuordnen.	Auftragsverarbeiter
Zimperium	zcookie panel	Sitzungstoken für zpanel zPanel ist das Adminstrations-Tool, mit dem wir alle Kunden in einer Umgebung (VPC) verwalten.	Auftragsverarbeiter
Zimperium	zme	Systemtoken, Erstanbieter-Token zme wird verwendet, um die Client-Website über den Kunden (system_token) zu informieren, der dem Benutzer zugeordnet ist. Sie gelten auch als Erstanbieter-Cookies. Diese werden von der vom Benutzer besuchten Website gesetzt.	Auftragsverarbeiter