Wieso James Bond nicht auf Tinder wäre: Dating-Apps bleiben für das Diensthandy unsicher

Pressekontakt

Laika Communications GmbH
Tolgahan Kaftan
PR Consultant & Copywriter
tolgahan.kaftan@laika.berlin

- **Dating-Apps & Diensthandy sind kein Traumpaar: Alle von APPVISORY getesteten Dating-Apps weisen grundsätzliche Sicherheitsrisiken auf**
- **Das böse Erwachen nach dem heißen Flirt: happn laut Test am unsichersten, Tinder und Grindr lassen eindeutige Identifizierung von Nutzern zu**

Hannover, 11. Februar 2020: Der Valentinstag steht kurz bevor und landauf, landab glühen die Smartphones noch einmal mehr als sonst beim Swipe für die Liebe auf Tinder, & Co. Doch wie ist es um die sensiblen Daten der Nutzer bestellt, die per Smartphone App nach der großen Liebe fürs Leben oder den Flirt für zwischendurch suchen? Und wie sieht es aus, wenn Mitarbeiter ihre zur Verfügung gestellten Diensthandys nutzen, um Dating-Apps zu installieren?

Aktuelle Tests[1] der App Security Spezialisten von APPVISORY haben ergeben, dass happn, Grindr, Tinder, Parship, Bumble, LoveScout24 und Badoo in puncto Sicherheit klar durchfallen und damit auf betrieblichen Smartphones nichts zu suchen haben.

Liebe ist gefährlich - das Ranking der Getesteten

App	Risk Level (CVSS[2] Score)
happn (Android)	8,8
Grindr (Android)	8,8
Tinder (Android)	8,8
Parship (iOS)	6
Badoo, LoveScout24 & Bumble (iOS)	6

Das traurige Verlierertreppchen geht an happn - der App, die den Standort zweier Personen nutzt, deren Wege sich im realen Leben bereits gekreuzt haben, um auch online die große Liebe herbeizuführen. Was so romantisch klingt, ist in Sachen Datenschutz nur dürftig umgesetzt.

[1] Untersucht wurden die iOS beziehungsweise Android Apps der Anbieter Tinder, Bumble, Happn, parship, LoveScout 24, Badoo und Grindr im Zeitraum der KW 4-5 2020.
[2] Die CVSS Score zeigt die Gefährlichkeit einer App auf einer Skala von 0 (ungefährlich) bis 10 (sehr gefährlich). Siehe auch: https://www.first.org/cvss/calculator/3.0

Und auch die Plattformen, bei denen es weniger romantisch zugeht - Tinder und Grindr - gehen mit den Daten ihrer User sorglos um. Mit der eindeutigen Identifizierung von Nutzern verstoßen sie sogar gegen die DSGVO.

Zufällig Liebe, zufällig nein? happn

Happn verwendet durchgehend transportverschlüsselte Kommunikation, aber sie kommt nicht ohne Analytics-Tracker mit Standort in diversen EU- und Nicht-EU-Ländern aus.

Deutlich skeptischer kann man die Einbindung eines externen Firewall-Dienstes namens „Cloudflare" sehen. Cloudflare ist zwar eine Art mobile Firewall und damit grundsätzlich eine Sicherheitsfunktion, dennoch verlassen die sensiblen Daten die EU. Aber im Unterschied zu parship, Tinder und Grindr, die auch Cloudflare als Dienst eingebunden haben, weist Happn zumindest in ihren Datenschutzbestimmungen darauf hin. Im umgekehrten Fall wäre es sonst ein klarer Verstoß gegen die EU-DSGVO. Fazit: Es ist eben kein Zufall, wenn es nicht klappt.

Schnelle Liebe, schnelles Risiko? Tinder und Grindr

Die beiden beliebten Dating-Apps Tinder und Grindr unterscheiden sich in der Transportverschlüsselung nur dadurch, dass Tinder darauf verzichtet. Beide verwenden Analytics-Tracker mit Standort in diversen EU- und Nicht-EU-Ländern und übertragen die Android-ID, was die eindeutige Identifizierung eines Nutzers erlaubt. Wie happn nutzen Tinder und Grindr Cloudflare, verstoßen aber damit eindeutig gegen die EU-DSGVO, weil sie in ihren Datenschutzbestimmungen nicht auf die Einbindung hinweisen.

Fazit: Liebestöter Deluxe.

Drum prüfe, wer sich ewig bindet, parship nimmt Datensicherheit ernst(er):

Auch wenn die Kommunikation durchgehend verschlüsselt stattfindet, kommt auch parship nicht ohne Analytics-Tracker mit Standort in diversen EU- und Nicht-EU-Ländern aus. Wie happn nutzt auch parship Cloudflare, weist in seiner Datenschutzbestimmung nicht auf die Einbindung hin und verstößt damit eindeutig gegen die EU-DSGVO. Fazit: Nicht alle 11 Minuten verliebt sich ein Datenschützer in parship.

***Es ist, was es ist*, sagen leider auch Badoo, LoveScout24 und Bumble**

Etwas sicherer unterwegs sind Turteltauben mit den Apps Badoo, LoveScout24 und Bumble. Die gute Nachricht ist, dass bei allen dreien die Kommunikation zur jeder Zeit transportverschlüsselt stattfindet. Auffällig

war aber die Nutzung vieler Analytics-Tracker mit dem Standort in den USA, bei Badoo, und in verschiedenen EU- und Nicht-EU-Ländern bei LoveScout24 und Bumble. Bei LoveScout landet ein Tracker sogar in China mit eindeutigem Fingerprint des Gerätes (mittels der UDID und weiteren IDs). Fraglich bleibt auch die Abfrage der Berechtigung für den Kalender bei Badoo, welche mit der Auslieferung von Werbung begründet wird. Fazit: Lieber keinmal, statt dreimal.

APPVISORY Fazit: Dating-Apps sind mit Vorsicht zu genießen und gehören nicht aufs Firmen-Smartphone

Die Themen Datensicherheit und Datenschutz sind zu Recht allgegenwärtig, aber werden synonym verwendet, ohne zu differenzieren. Grundsätzlich garantiert Datenschutz jedem Bürger Schutz vor missbräuchlicher Datenverarbeitung, das Recht auf informationelle Selbstbestimmung und den Schutz der Privatsphäre. Datensicherheit muss dafür Sorge tragen, dass Daten jedweder Art ausreichend gegen Manipulation, Verlust und unberechtigte Kenntnisnahme durch Dritte oder andere Bedrohungen geschützt sind. Da sich die Bewertung für den Laien schwierig gestaltet, kann man sich am CVSS-Score orientieren. Der CVSS-Score gibt in einer Skala von 0 bis 10 aufsteigend Auskunft über die Gefährlichkeit einer App (und anderer IT-Systeme) hinsichtlich Datenschutz und Datensicherheit. „Wenn man sich die Ergebnisse anschaut, sieht man, dass alle getesteten Dating-Apps klar durchgefallen sind. Das liegt in erster Linie daran, dass die App-Anbieter trotz Kenntnis die relevanten Sicherheitslücken und Datenschutzprobleme in ihren Apps bisher nicht behoben haben. Privatanwender sollten demnach selbst entscheiden, wie wichtig Ihnen Ihre persönlichen Daten sind und ob sie deshalb auf Dating per App verzichten wollen. Unternehmen raten wir aktuell dringend dazu, Onlinedating und Firmentelefone zu trennen" erklärt Sebastian Wolters, Gründer und Geschäftsführer von APPVISORY.

Über APPVISORY® by mediaTest digital

APPVISORY ist Europas führende MAM-Software (Mobile Application Management). In Verbindung mit Mobile Device Management Systemen oder Stand-Alone stellt die SaaS-Lösung den Schutz sensibler Unternehmensdaten bei der Nutzung mobiler Endgeräte sicher. Mithilfe von APPVISORY setzen Unternehmen ihre individuellen IT-Sicherheitsrichtlinien sowie Vorgaben laut Bundes-datenschutzgesetz (BDSG) und der neuen EU-Datenschutzgrundverordnung (DSGVO) auf allen Mitarbeitergeräten durch.

Gleichzeitig trägt APPVISORY mit seinem App-Client zur Aufklärung und Sensibilisierung der Anwender bei und fördert die Nutzung von Apps und damit die Digitalisierung und

Mobilisierung von Geschäftsprozessen. mediaTest digital sichert weltweit betrieblich genutzte Smartphones und Tablets von mehreren Hundert Kunden in der Größe von drei bis 50.000 Endgeräten ab.

12 der größten 25 deutschen Unternehmen sowie zahlreiche mittelständische und kleine Unternehmen aus Wirtschaftszweigen wie Banken, Automotive, Energieversorgung oder Behörden zählen heute zu den zufriedenen Kunden. Das in Deutschland ansässige Unternehmen nutzt ausschließlich deutsche Server für das Hosting und die Entwicklung seiner Lösungen. Mehr Informationen zu APPVISORY finden Sie auf www.appvisory.com.