Tückische Tinder-Techtelmechtel: Ernste Sicherheitslücken bei Dating-Apps

Moskau/Ingolstadt, 4. Januar 2018

Ob sexuelle Vorlieben, Nacktfotos oder schlicht Passwörter – Nutzer von Dating-Apps geben bei der Partnersuche oft sehr vertrauliche Daten preis. Doch wie sicher gehen die Apps mit diesen Daten um? Um diese Frage zu beantworten, hat Kaspersky Lab neun beliebte Dating-Apps – darunter Tinder – auf Sicherheits- und Datenschutz-Schwachstellen überprüft [1]. Das Ergebnis ist ernüchternd: über Dating-Apps lässt sich häufig die hinter einem Account stehende reale Person entlarven; auch können User über Dating-Apps einfach lokalisiert, verschlüsselte Kommunikation abgefangen und Sicherheitsvorkehrungen umgangen werden.

Laut Bitkom kennen 88 Prozent der deutschen Internet-Nutzer einen Dienst zur Partnersuche [2]. Die steigende Popularität von Dating-Apps bringt jedoch ernstzunehmende Sicherheits- und Datenschutzprobleme mit sich. Das Problem: die meisten Dienste verlangen diverse persönliche Informationen der Nutzer.

Laut der Kaspersky-Analyse bergen Dating-Apps folgende Schwachstellen:

- bei 60 Prozent der Tinder-Nutzer konnten der vollständige Namen sowie weitere Konten in Sozialen Netzwerken nachvollzogen werden;
- sechs der untersuchten Apps boten Dritten die Möglichkeit, den Standort der Nutzer zu bestimmen;
- bei fünf Apps lassen sich Daten auch innerhalb der verschlüsselten Verbindung abfangen – sie sind also anfällig für Spionage oder Manipulation der Kommunikation (Man-in-the-Middle-Attacken);
- bei acht Apps war es möglich, Token-basierte Authentifizierungsmethoden zu umgehen – der Grund: mithilfe von Superuser-Rechten werden von den Apps zu viele Informationen zur Verfügung gestellt.

„Unsere Analyse zeigt, dass sich Nutzer von Dating-Apps um Cybersicherheit kümmern sollten, da viele dieser Dienste nicht gegen verschiedene Arten von Angriffen geschützt sind“, sagt Roman Unuchek, Sicherheitsexperte bei Kaspersky Lab. „Auch bringen sich die Nutzer selbst in Gefahr, indem sie sensible persönliche Informationen in ihren Profilen, wie zum Beispiel ihren Ausbildungs- oder Arbeitsort, weitergeben. Mit diesen Informationen können Eindringlinge die tatsächlichen Konten von Opfern auf Facebook oder LinkedIn leicht finden. Es eröffnet auch Möglichkeiten zum Stalking – um Nutzer zu belästigen und ihre Bewegungen im wirklichen Leben zu verfolgen. Daher sollte auch beim Online-Dating auf Privatsphäre, Sicherheit und Datenschutz geachtet werden.“

Spionagefalle Dating-App trotz Token?

Die Experten von Kaspersky Lab zeigen in ihrer Analyse, dass auch Token-basierte Authentifizierungsmethoden, zum Beispiel bei Neuregistrierungen, unsicher sind. Ein Token wird auf Anfrage von einem Server erstellt, um den Nutzer eindeutig zu identifizieren und verlangt normalerweise den Zugriff auf ein Facebook-Konto. Mit dieser Methode erhalten Anwendungen alle notwendigen Daten, um den Nutzer auf seinen Servern authentifizieren zu können. Tokens werden laut der Kaspersky-Analyse jedoch häufig gespeichert oder unsicher verwendet und können daher leicht gestohlen werden. Die Folge: Eindringlinge können auch ohne Anmelde- und Kennwortdetails vorübergehend Zugriff auf Konten von Opfern erhalten.

Auch speichern die meisten der untersuchten Apps den Nachrichtenverlauf im selben Ordner, in dem sich auch der Token befindet. Sobald der Angreifer Superuser-Rechte erhalten hat, erhält er Zugriff auf die Korrespondenz. Solche Angriffe sind besonders für Nutzer von Android-Geräten gefährlich, insbesondere wenn auf den Geräten noch veraltete Software mit ungepatchten Sicherheitslücken läuft, über die Angreifer Root-Zugriff auf das Gerät und so Zugang zu privaten Informationen erhalten.

Kaspersky Lab rät Online-Datern zu folgenden Sicherheitsmaßnahmen:

- unzureichend geschützte öffentliche WLAN-Netze meiden,
- über eine VPN-Verbindung eine sichere Verbindung herstellen,
- keine sensiblen Informationen wie Ausbildung oder Arbeitsplatz teilen
- und eine Cybersicherheitslösung wie Kaspersky Security Cloud [3] auch auf Smartphone und Co. einsetzen.

Die komplette Analyse „Dangerous liasons“ ist auf https://securelist.com/dangerous-liaisons/82803/ verfügbar.

[1] https://securelist.com/dangerous-liaisons/82803/ und https://www.kaspersky.de/blog/dating-apps-threats/15111/

[2] https://www.bitkom.org/Presse/Presseinformation/Vorurteile-gegenueber-Online-Dating-verschwinden.html

[3] https://www.kaspersky.de/security-cloud

Nützliche Links:

- Kaspersky-Blog „Dangerous liaisons”: https://securelist.com/dangerous-liaisons/82803/
- Kaspersky-Blog „Sind Online-Dating-Apps” tatsächlich sicher?”: https://www.kaspersky.de/blog/dating-apps-threats/15111/
- Kaspersky-Blog „Trottel in der App Falle: Die wundervolle Welt der Tinder Bots“: https://www.kaspersky.de/blog/tinder-bots/10100/
- Kaspersky Security Cloud: https://www.kaspersky.de/security-cloud

Über Kaspersky Lab

Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 2017 sein 20-jähriges Firmenjubiläum feiert. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Next Generation Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen Einrichtungen sowie Privatanwendern weltweit. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexen und aufkommenden Cyberbedrohungen. Mehr als 400 Millionen Nutzer und 270.000 Unternehmenskunden werden von den Technologien von Kaspersky Lab geschützt.

Weitere Informationen zu Kaspersky Lab finden Sie unter http://www.kaspersky.com/de/. Kurzinformationen erhalten Sie zudem über www.twitter.com/Kaspersky_DACH und www.facebook.com/Kaspersky.Lab.DACH. Aktuelles zu Viren, Spyware, Spam sowie Informationen zu weiteren IT-Sicherheitsproblemen und -Trends sind unter https://de.securelist.com/ und auf dem Kaspersky-Blog auf http://blog.kaspersky.de/ abrufbar.

Redaktionskontakt:

Berkeley Kommunikation GmbH
Florian Schafroth
florian.schafroth@berkeley.global
Tel.: +49-89-7472-62-43
Fax: +49-89-7472-62-17
Landwehrstraße 61
80336 München

Kaspersky Labs GmbH
Stefan Rojacher
stefan.rojacher@kaspersky.com
Tel.: +49-841-98-189-325
Fax: +49-841-98-189-100
Despag-Straße 3
85055 Ingolstadt
