PRESSEMITTEILUNG

Pressekontakt

Sebastian Wolters | CEO

press@appvisory.com
Telefon +49 (0)511 35 39 94-20
Fax +49 (0)511 35 39 94-12

Datum: 19. Mai 2020

Vorsicht bei Langeweile - #WirBleibenZuHause-Apps wie Instagram, TikTok, Disney+ & Co. weisen potenzielle Angriffsmöglichkeiten auf

- **Apps gegen Langeweile sind aktuell unverzichtbar, einige sind jedoch mit Vorsicht zu genießen: sechs der von APPVISORY getesteten Streaming-, Video- und Social-Apps weisen Angriffsmöglichkeiten auf persönliche Daten auf**
- **Die Social-Media Apps Instagram und TikTok sind laut Test am anfälligsten und bergen die Gefahr, dass Kontaktdaten auf externe Server übertragen werden.**
- **Houseparty laut Test am sichersten**

Viele von uns sind derzeit gezwungen, von zu Hause aus zu arbeiten, zu Hause zu bleiben und Kontakt zu anderen einzuschränken. Ganz neue Herausforderungen brechen zeitgleich auf uns herein - beruflich, privat und im sozialen Bereich. Gegen die Langeweile und auch um mit der Familie und Freunden in Kontakt zu bleiben helfen dabei Apps, mit denen die Leichtigkeit und der Spaß in unser Zuhause wieder Einzug halten. Doch wie ist es um die sensiblen Daten der Nutzer bestellt, die per App auf Smartphone oder Tablet die neuesten Videos und Bilder ansehen, streamen, downloaden, liken, hochladen oder teilen? Und wie sieht es mit der Sicherheit aus, wenn Videos, unsere Lieblingsserie oder Kinofilme von Usern über das Handy flimmern?

Aktuelle Tests[1] der App Security Spezialisten von APPVISORY haben ergeben, dass Instagram, TikTok, Disney, Netflix, Amazon Prime Video, YouTube und Houseparty in puncto Sicherheit noch nachbessern müssen und zumindest mit Vorsicht gegen die Langeweile zu genießen sind.

Das Ranking der Getesteten von unsicher bis sicher

Instagram: Version 136.0 (iOS)	Risk Level (CVSS Score[2]):	8,8
TikTok: Version 15.7.0 (iOS)	Risk Level:	7,5
Disney+: Version: 1.4.4 (iOS)	Risk Level:	7,5
Netflix: Version: 12.28.0 (iOS)	Risk Level:	7,5
Amazon Prime Video: Version: 8.3 (iOS)	Risk Level:	6.0
YouTube: Version: 15.16 (iOS)	Risk Level:	6,0
Houseparty: Version: 1.41.1 (iOS)	Risk Level:	6,0

[1] Untersucht wurden die iOS beziehungsweise Android Apps der Anbieter Cisco WebEx Meetings, Zoom Cloud Meetings, Slack, Trello, Mattermost, Skype for Business, Microsoft Teams und Google Hangouts im Zeitraum der KW 14 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

Instagram und TikTok - Ablenkung mit Risiko
Dem Netzwerk aus dem Social-Media-Kosmos mit 15 Millionen Nutzern allein in Deutschland mangelt es an Validierung von Zertifikaten und Hostnamen. Zwar versammelt die App aktive Nutzer, die ihre Bilder und Videos auf Instagram teilen, doch sie kann u.U. auch ohne Validierung Verbindungen zu graph.facebook.com aufbauen, wodurch Daten in die Hände Dritter gelangen könnten.

Und auch bei TikTok, der derzeit angesagtesten App, mangelt es manchen Verbindungen an ausreichender Verschlüsselung, sodass Dritte sich als TikTok ausgeben können, um veränderte Daten in die App zu übertragen. Die sensiblen Kontaktdaten der Nutzer werden u.U. auch auf Server außerhalb der EU übertragen.

Disney+, Netflix, Amazon Prime Video: HD Streaming - highly dangerous?
Alle drei Streaming-Apps bringen in Corona-Zeiten massig Film-Highlights ins Isolations-Wohnzimmer. Im Test zeigte sich, dass die Weitergabe von Daten an Drittanbieter leider nicht ausgeschlossen werden kann, ebenso wäre die eindeutige Identifizierung der Nutzer möglich. Disney+ nutzt Tracking-Dienste von Drittanbietern und benötigt die Mikrofonberechtigung für die Verbindung zu einem Chromecast. Bei Netflix fällt erstmal positiv auf, dass keine Berechtigungen seitens der Nutzer für das Streamen von Inhalten benötigt werden. Allerdings wird für den Kontakt zum Support eine Zustimmung für die Nutzung von Mikrofon und Kamera angefordert, die nicht unbedingt notwendig wäre. Amazon Prime Video nutzt den Google Dienst Crashlytics und übermittelt Metadaten, wie zum Beispiel die Nutzung des Telefonmodells oder die Betriebssystemversion. Metadaten werden häufig zur Identifizierung von Nutzern genutzt, da diese nicht abgeschaltet oder geändert werden können. Hier lauert also eine potenzielle Gefahr.

YouTube - Enjoy the Datenklau
Sie gehört wohl aktuell zu den beliebtesten Apps, um für Unterhaltung Zuhause zu sorgen. Videos oder Musik der Plattform lassen den grauen Alltag ein wenig verblassen. Beim Thema Datensicherheit landet man allerdings auf dem Boden der Tatsachen. Da Google der Eigentümer von YouTube ist, gelten die “Datenschutzrichtlinien” des Internet-Riesen. Google speichert sämtliche Informationen wie Suchanfragen, Login-Informationen, Kontodetails und speichert Standortdaten (falls GPS aktiv ist), welche teilweise weiterverarbeitet werden. Die Security Spezialisten von APPVISORY empfehlen den zusätzlichen Einsatz einer MTD (Mobile Threat Defense) -Lösung. Wer also mit den Datenschutzrichtlinien nicht einverstanden ist, dem bleibt leider nichts anderes übrig, als die App nicht zu installieren und alternativen wie “NewPipe” zu nutzen.

Houseparty - Partylaune, aber mit Bedacht
Die Videochat-App Houseparty ist derzeit ein Supertrend: Hier finden sich Menschen zu Videopartys zusammen, um in Zeiten von Social Distancing in Kontakt zu bleiben. Diese Zeit kann man sich gemeinsam mit diversen Spielen vertreiben – so kann man etwa ein Quiz sowie beliebte Spiele, wie Montagsmaler oder Wer-bin-ich spielen. Die App schneidet im Test zwar am besten ab, aber, wie bei den anderen getesteten Apps, ist der Umgang mit den eigenen Inhalten und persönlichen Daten auch nicht unbedingt mustergültig.

Alle Kontaktdaten werden bei Bestätigung der Datenschutzerklärung auf Servern von Houseparty in den USA gespeichert, daher sollte dieser App der Zugriff aufs Adressbuch verweigert werden. Auch die Nutzung von Analyse- und Tracking-Diensten Dritter stellen ein potenzielles Risiko dar.

APPVISORY Fazit: #WirBleibenZuhause-Apps sind mit Vorsicht zu genießen

APPVISORY zieht Bilanz. Die Corona-Krise hat nicht nur für das Homeoffice einen unglaublichen Schub geleistet, sondern auch für alle jene Apps die ein bisschen Ablenkung versprechen. Die von APPVISORY getesteten Social-Media und Unterhaltungs-Apps stellen zwar bei richtiger Handhabung keine große Gefahr dar, aber die Themen Datensicherheit und Datenschutz bleiben zu Recht allgegenwärtig. Vor allem aber werden sie nach wie vor 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, bietet der CVSS-Score Orientierung. Der CVSS-Score gibt in einer Skala von 0 bis 10 aufsteigend Auskunft über die potentiellen Probleme einer App (und anderer IT-Systeme) hinsichtlich Datenschutz und Datensicherheit.

Aufgrund der Corona-Pandemie sind Instagram, TikTok & Co. so beliebt wie nie zuvor. „Deshalb ist es besonders wichtig, dass sich die jeweiligen Anbieter an die Vorgaben des Gesetzgebers halten. Wer unsere Testergebnisse anschaut, erkennt sofort, dass alle getesteten #WirBleibenZuHause-Apps trotz erheblichen Fortschritts beim Thema Sicherheit noch Verbesserungspotenzial haben, insbesondere Instagram und TikTok. Privatanwender dürfen zwar selbst entscheiden, wie wichtig ihnen ihre persönlichen Daten sind, aber allzu leicht werden die langen Datenschutzrichtlinien weggeklickt und die Nutzer wissen zu wenig über potentielle Risiken. Anwendern raten wir generell dringend dazu, sich die Datenschutzrichtlinien genau anzuschauen und zu prüfen, ob sie mit damit einverstanden sind.” erklärt Sebastian Wolters, Gründer und Geschäftsführer von mediaTest digital.

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-Datenschutz-grundverordnung (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.