PRESSEMITTEILUNG

Pressekontakt

Sebastian Wolters | CEO

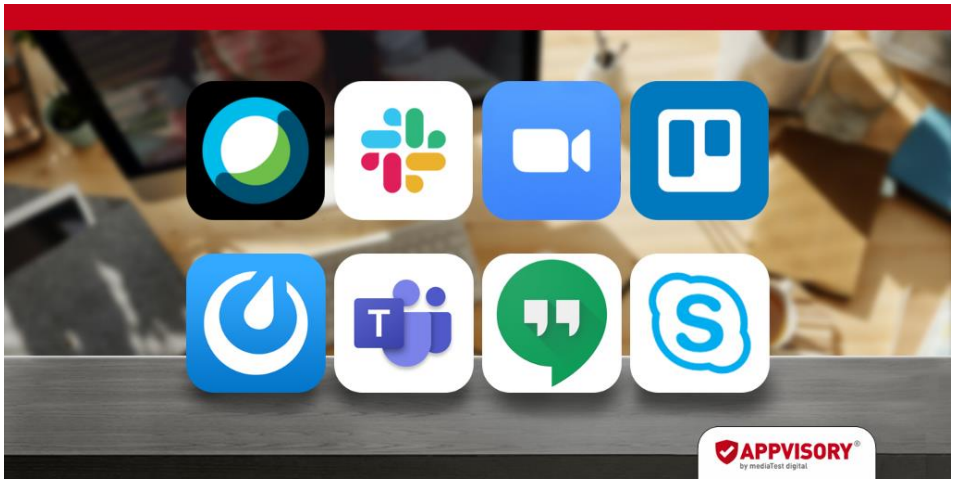
press@appvisory.com
Telefon +49 (0)511 35 39 94-20
Fax +49 (0)511 35 39 94-12

Datum: 16. April 2020

So (un)sicher sind Teamwork-Apps und Video-Konferenzen von Zoom, Slack, Google & Co.

- **Video-Konferenz & Kollaborationstools sind aktuell im Homeoffice unverzichtbar, aber mit Vorsicht zu genießen: Alle von APPVISORY getesteten Software-Apps weisen grundsätzliche Sicherheitsrisiken auf**
- **Nicht aus allen Wolken fallen: cloudbasierter Videokonferenz- und Kollaborationsdienst Cisco WebEx Meetings laut Test am unsichersten, Zoom Cloud lässt eindeutige Identifizierung von Nutzern zu**
- **APPVISORY stellt kostenlosen Guide für ein sicheres Homeoffice zur Verfügung**

Für Unternehmen sind sie Glück im Unglück: Videokonferenz- und Kollaborationstools - halten sie doch damit Mitarbeiter und Menschen in der aktuellen Krise zusammen. Doch wie ist es um die sensiblen Daten der Nutzer bestellt, die per Smartphone App der nächsten Videokonferenz beiwohnen? Und wie sieht es mit der Sicherheit aus, wenn Mitarbeiter über Slack oder Trello ihren Workflow mit ihren Kollegen abstimmen?



Aktuelle Tests[1] der App Security Spezialisten von APPVISORY haben ergeben, dass Cisco WebEx Meetings, Zoom Cloud Meetings, Slack, Trello, Mattermost, Skype for Business, Microsoft Teams und Google Hangouts in puncto Sicherheit

[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.

noch nachbessern müssen und zumindest auf betrieblichen Smartphones nur mit Vorsicht zu genießen sind.

Zusammenarbeit mit Augenmaß - das Ranking der Getesteten von unsicher bis sicher

Cisco WebEx Meetings (Android)	Risk Level (CVSS Score[2]):	8,8
Zoom Cloud Meetings(Android)	Risk Level:	7,5
Slack (Android)	Risk Level:	7,5
Trello (Android)	Risk Level:	7,5
Mattermost (iOS)	Risk Level:	6.0
Skype for Business (iOS)	Risk Level:	6,0
Microsoft Teams (iOS)	Risk Level:	6,0
Google Hangouts (iOS)	Risk Level:	6,0

Beim Thema Sicherheit ist Cisco WebEx Meetings trauriger Verlierer - dem mächtigen Tool, das zwar Online-Kollaboration und Kommunikation vereint, mangelt es nicht nur an ausreichender Verschlüsselung, sondern auch an einer sicheren Implementierung von Webview.

Und auch die beliebte Videokonferenz-Anwendung Zoom Cloud Meetings hat zwar jüngst nach Medienkritik nachgebessert, wie bei der unzulässigen Weiterleitung von Informationen an Facebook, doch ist auch hier die Verschlüsselung noch unzureichend für den Einsatz in Unternehmen.

Cisco WebEx Meetings, Zoom Cloud Meetings - Hausaufgaben nicht gemacht

Beide Anwendungen haben keine durchgehende und ausreichende Verschlüsselung. Zwar verhindert Zoom mittlerweile das Mitlesen verschlüsselter Verbindungen. Verbessern muss Zoom die Sicherung von Daten auf externen Speichern, da es anderen Apps auf dem Gerät ermöglicht die Inhalte mitzulesen. Die unsichere Verwendung von Webview ist eine kritische Sicherheitslücke bei Cisco WebEx Meetings. Im Test zeigte sich auch, dass die Weitergabe von Daten an Drittanbieter leider nicht ausgeschlossen werden kann. Für Zoom ist der zusätzliche Einsatz einer MTD (Mobile Threat Defense) - Lösung empfehlenswert.
Fazit: Aus dem Haus, aus dem Sinn. Eine interessant open-source-basierte Alternative bietet sich mit Jitsi Meet, hierzu folgt ein Testbericht in Kürze.

Slack und Trello - durch die Hintertür

Die beiden bekannten Kollaborationstools Slack und Trello haben das gleiche Problem. Sie erstellen und schreiben sensible Daten in temporäre Dateien, was ein erhöhtes Sicherheitsrisiko darstellt. Slack erlaubt zwar ein kurzzeitiges Mitschneiden des Datenverkehrs für statistische Analysen, aber das Mitlesen einer verschlüsselten Verbindung ist nicht möglich. Trello hingegen überträgt Metadaten an mehrere Tracking-Dienste inklusive Gerätemodell, Betriebs-system, Netzbetreiber und Werbe-Id. Für Slack ist der zusätzliche Einsatz einer MTD (Mobile Threat Defense) -Lösung ratsam.
Fazit: Kein Heimspiel.

[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

Skype for Business und Google Hangouts haben ordentlich nachgebessert

Gerade bei Verstößen gegen Datenschutz und Datensicherheit haben beide Tools deutlich nachgebessert. Jedoch verwenden die Videokonferenz-Anwendungen Skype for Business und Google Hangouts unsichere Schnittstellen (APIs). Im aktuellen Test sind sie leider auch anfällig für sogenannte Man-In-The-Middle-Attacken (MITM). Dazu kommt, dass Skype Metadaten an Microsoft überträgt und Hangouts den Gerätenamen (häufig der Vorname des Besitzers) an Google sendet.
Fazit: Wer im Glashaus sitzt, sollte nicht mit Daten werfen.

Mattermost und Microsoft Teams - klein vs. groß

Das datenschutzkonforme open-source-basierte Kollaborationstool Mattermost baut nur eine Verbindung zur selbst-gehosteten Instanz auf. Wenn die Ressourcen und Kenntnisse zum Erstellen und Betreuen von Mattermost auf einem eigenen Server vorhanden sind, ist der Kommunikationsservice klar Alternativen vorzuziehen. Im Gegensatz zu Microsoft Teams, das Metadaten an Dritte überträgt und auch bei der Verschlüsselung noch Schwächen zeigt. Für beide Anwendungen ist der zusätzliche Einsatz einer MTD (Mobile Threat Defense) -Lösung empfehlenswert.
Fazit: Mattermost bei vorhandener Expertise.

APPVISORY stellt kostenlosen Guide für das sichere Homeoffice zur Verfügung

Die im Test aufgedeckten Sicherheitsrisiken müssen Unternehmen jedoch nicht einfach so hinnehmen. Um Firmen bei ihrer rasanten Umstellung auf Homeoffice in Zeiten von Corona sicher zu begleiten, hat das Team von APPVISORY in Zusammenarbeit mit der BFI, der Beratungsgesellschaft für Informationstechnologie, eine Anleitung für Unternehmen erstellt. Der Ratgeber hilft dabei, eine sichere und ortsunabhängige Arbeitsumgebung für eigene Mitarbeiter einzurichten.
Da aber die im Test vorgestellten Anwendungen bei weitem nicht alle auf dem Markt abdecken, möchte APPVISORY in der Krisenzeit auch einen Beitrag leisten Unternehmen dabei zu unterstützen schneller und vor allem sicherer zu digitalisieren. Deshalb bietet APPVISORY seinen Dienst für 90 Tage unverbindlich und kostenlos an.

APPVISORY Fazit: Videokonferenz- und Kollaborationstools sind zwar aktuell unverzichtbar, aber mit Vorsicht anzuwenden

APPVISORY zieht Bilanz. Zwar sind die Themen Datensicherheit und Datenschutz zu Recht allgegenwärtig, aber sie werden 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, 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 Videokonferenz- und Kollaborationstools unbedingt nachbessern müssen. Die App-Anbieter haben trotz Kenntnis die relevanten Sicherheitslücken und Datenschutzprobleme in ihren Apps bisher nicht behoben. Privatanwender dürfen zwar selbst entscheiden, wie wichtig ihnen ihre persönlichen Daten sind, aber bei der Zusammenarbeit mit Kollegen müssen andere Richtlinien gelten. Unternehmen raten wir aktuell dringend dazu, Videokonferenz- und Kollaborationstools für das Firmentelefon genau anzuschauen bzw. prüfen zu lassen oder im Zweifelsfall zumindest als lokale Instanz selbst zu hosten (wie z.B. bei Mattermost möglich). Nicht zuletzt deshalb haben wir uns entschlossen, APPVISORY neuen Interessenten für drei Monate kostenlos zur Verfügung zu stellen, um in dieser hochdynamischen Zeit die nötige Sicherheit nicht vernachlässigen zu müssen und die bitter nötige Digitalisierung der Arbeitsplätze und Workflows schnell und unkompliziert zu unterstützen" 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-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.