Sichere Alternativen zu riskanten Apps wie Whatsapp, Dropbox und Co.

Bei der Verwaltung mobiler Geräte sehen sich IT-Verantwortliche mit der Frage konfrontiert, wie mit der Nutzung privater Apps und privater Handys umgegangen werden soll. Um zu vermeiden, dass unsichere Apps zum Teilen von Unternehmensdaten verwendet werden, müssen die Geräte mit einem bestmöglichen Anwendererlebnis ins Mobile Device Management eingebunden werden.

Der Autor
Joey Keusch, Key Account Manager, Nomasis

Mittlerweile werden bekanntlich in einer Mehrheit der Unternehmen neben geschäftlichen Smartphones auch private Geräte genutzt. Ausser den gängigen Apps für E-Mail, Kalender oder Unternehmens-Apps für den Zugriff auf Intranets oder Unternehmens-ERPs verwenden aber viele Mitarbeitende ihre Handys auch, um Dokumente mit Arbeitskollegen, Geschäftspartner oder Kunden zu teilen. Dabei benutzen sie leider häufig auch unsichere Werkzeuge wie Dropbox oder Whatsapp. Sie tun dies meistens ganz einfach aus Gewohnheit, weil solche Tools im privaten Umfeld zu den meistgenutzten gehören. Dass die Anwender dabei beim Teilen von vertraulichen Informationen grosse Sicherheitsrisiken eingehen, sind sie sich in den seltensten Fällen wirklich bewusst.

Bewusstsein für Risiken fehlt

Oftmals steht ihnen aber schlicht kein anderes Werkzeug zur Verfügung, und die Nutzung privater Apps ist gar nicht vorgesehen. Sie steht nämlich selten mit den jeweiligen Sicherheitsvorschriften im Einklang. Denn die Verwendung unsicherer Apps kann insbesondere bei unternehmenskritischen Dokumenten nicht im Sinne des Managements sein; sei es, weil es sich hier um Informationen zu geistigem Eigentum oder um andere, einem eingeschränkten Benutzerkreis anvertraute Inhalte handelt. Dabei spielt es keine Rolle, ob Bring your own Device (BYOD) aufgrund der entstehenden Sicherheitsrisiken nicht erlaubt ist. Denn die erwähnten für private Zwecke durchaus nützlichen Apps können auch auf Geschäftshandys und -Tablets heruntergeladen werden. Die grosse Herausforderung stellt also nicht die Herkunft des Geräts, sondern die Vermeidung der Nutzung unerwünschter Anwendungen dar.

Sichere App-Alternativen anbieten

Deshalb ist es unerlässlich, den Nutzern ein bestmögliches Anwendererlebnis zu bieten und je nach Anwendungsfall die passenden Möglichkeiten bereitzustellen, damit sie ohne Barrieren arbeiten können. Eine solche kann beispielsweise das oft nervenaufreibende Einwählen in ein privates virtuelles Netzwerk (VPN) sein. Alternativen sind einfach zu bedienende, sichere Tools für den Datentransfer und die Zusammenarbeit. Mit solchen umfassenden und sicheren EFSS-Lösungen (Enterprise File Sync & Share) können Mitarbeitende jedes gewünschte, kompatible Gerät verwenden, um Dateien sicher mit Kollegen, Kunden, Partnern und Lieferanten nutzen, zu synchronisieren und zu teilen. Dabei verhelfen solche Tools nicht nur den Anwendern zu mehr Produktivität, sondern auch der IT zu umfassenden Kontrollfunktionen über genutzte Unternehmensinhalte. Dazu werden private und vom Unternehmen zur Verfügung gestellte Handys oder Tablets automatisiert in das Netzwerk mit den entsprechenden Sicherheitsmechanismen eingebunden.

Grafik: Chaliya/ shutterstock.com

CIO muss sich der Herausforderung stellen

Die Use Cases müssen ins Unified Endpoint Management (UEM) miteingebunden und in Gruppen aufgeteilt werden, vom administrativen Personal über Mitarbeitende in den Fachabteilungen bis hin zum Management. Dabei muss selbstredend neben den vom Unternehmen zur Verfügung gestellten Geräten auch BYOD in einer intelligenten UEM-Strategie seinen Platz haben. Damit lassen sich nicht nur Sicherheitsprobleme in den Griff kriegen und gesetzliche Auflagen erfüllen, sondern erst noch Kosten sparen.

Der CIO muss sich aber der Herausforderung stellen und im Kampf gegen den sorglosen Umgang mit unsicheren Hilfsmitteln bei den Anwendern das nötige Bewusstsein schaffen und ihren Anforderungen entsprechend benutzerfreundliche Instrumente zur Verfügung stellen.

«Einfache Bedienbarkeit und Sicherheit müssen zentrale Kriterien sein»

Wenn Mitarbeiter ihre eigenen Geräte am Arbeitsplatz verwenden, nutzen sie auch die ihnen bekannten Tools. Den Arbeitgeber stellt dies vor einige Probleme. Welche das sind und was für Alternativen es gibt, weiss Volker Mannel, Senior Sales Engineer bei Acronis. Interview: Coen Kaat

Was ist so gefährlich daran, wenn Mitarbeiter Dropbox und Co. nutzen?
Volker Mannel: Unternehmensdaten, die von Mitarbeitern in die Cloud kopiert werden, sind nicht mehr kontrollierbar und ausserhalb des Firmennetzwerks. Dies sollte auf jeden Fall verhindert werden. Mehrheitlich werden sehr einfache Passwörter benutzt, und Unbefugte haben so einfachen Zugriff auf diese Dienste. Zudem ist die Nutzung von Services wie Dropbox, Whatsapp und anderen üblicherweise für den Heimgebrauch ausgelegt. Firmendaten sind wesentlich sensibler und benötigen einen besseren Schutz vor dem Zugriff durch Dritte. Hinzu kommt, dass bei solchen Diensten in der Regel nicht gewährleistet ist, dass die Unternehmensdaten das Land nicht verlassen. Hingegen bieten Services wie Acronis Files Advanced für die Datenablage im Unternehmensnetzwerk oder Acronis Files Cloud zur Ablage in den Rechenzentren unserer Partner und Serviceprovider eine wesentlich höhere Sicherheit nicht zuletzt dank verschiedener Richtlinien bezüglich Steuerung der Zugriffsberechtigungen.

Gibt es auch eine Möglichkeit, diese bekannten Apps sicher zu verwenden?
Die Datensicherheit von derartigen Apps wird, wenn überhaupt, mit sogenannten Mobile-Device-Management-Lösungen sichergestellt. Plattformen namhafter Hersteller bieten die Möglichkeit, die Kommunikation durch App-Tunnels sicherer zu gestalten oder nur vom Unternehmen zugelassene Apps auf den Geräten auszurollen.

Volker Mannel, Senior Sales Engineer, Acronis.

Wie kann man die Mitarbeiter am besten für diese Problematik sensibilisieren?
Idealerweise stellt man den Mitarbeitern Lösungen zur Verfügung, die es erlauben, die gewünschten Daten jederzeit einfach und mit dem von ihnen bevorzugten Endgeräten abzurufen. Dies verhindert, dass Mitarbeiter eine Schatten-IT betreiben, um im Businessalltag mit Unternehmensdaten umzugehen. Die Lösungen müssen intuitiv bedienbar, sicher und ohne komplizierte Hindernisse sein. Die Usability ist absolut zentral. Aber die Sensibilisierung der Mitarbeiter, idealerweise durch einen internen Datenschutzbeauftragten, spielt eine wesentliche Rolle. Insbesondere gilt es, das Bewusstsein für das Thema Sicherheit zu schärfen, indem Regeln bezüglich Nutzung und Zugriff auf Unternehmensdaten schriftlich festgelegt werden.

Sollten Unternehmen komplett auf Bring your own Device verzichten, wenn sie Herr über ihre Daten bleiben wollen?
Nein. Gerade in diesem Szenario ist es heute wichtig, dass den Nutzern sichere Lösungen zur Verfügung gestellt werden. Nutzer sind es heute gewohnt, verschiedene Apps und Cloud-Dienste zu verwenden, die einfach zu bedienen und immer verfügbar sind. Dies muss das Ziel der Unternehmens-IT sein. BYOD bietet zwar Vorteile, aber auch Nachteile. Diese sollten den individuellen Anforderungen des Unternehmens gegenübergestellt und ausgewertet werden. Wie gesagt, können Mobile-Device-Management-Lösungen helfen, den Zugriff der Geräte sicher zu gestalten. Zudem sollten durch den Datenschutzbeauftragten Richtlinien zur Verwendung von BYOD vorgeben werden.

Woran sollten Unternehmen beim Implementieren einer UEM-Lösung unbedingt denken, damit nachher nichts schiefgeht?
Auf jeden Fall sollte man sich bezüglich der Dienste, die benötigt werden, ein klares Bild der individuellen Bedürfnisse des Unternehmens machen und sich fragen, welche Nutzer heute und in naher Zukunft welche Dienste auf welchem Endgerät erhalten sollen. Selbstverständlich müssen gesetzliche Anforderungen sowie interne Regelungen in die Beurteilung miteinbezogen werden. Bei der Wahl einer Lösung müssen die einfache Bedienbarkeit und die nötigen Sicherheits-Features die zentralen Kriterien sein. Für Letzteres ist in der Regel die IT in der Pflicht, klare und verbindliche Richtlinien zu definieren.