Office 365 auf mobilen Geräten verändert das App- und Device-Management

Immer häufiger wollen Unternehmen ihren Mitarbeitenden möglichst viel von Office 365 auch auf Smartphones und Tablets zur Verfügung stellen. Dies hat zur Folge, dass auch für die Verwaltung von mobilen Apps und Geräten der Einsatz von Microsoft-Diensten aus der Cloud in Betracht gezogen wird.

Firmen wollen zur Steigerung der Produktivität ihren Mitarbeitenden möglichst viele Anwendungen auf Smartphones und Tablets zur Verfügung stellen. Dieser Trend verstärkt sich aus mehreren Gründen weiter. Erstens weil Unternehmen realisieren, dass sie mit dem Bezug von Microsofts Office 365 teilweise für Apps bezahlen, die sie gar nicht nutzen. Ausserdem gibt es für Apps wie etwa die Chat-Anwendung Teams oder den digitalen Notizblock One Note kaum brauchbare Alternativen auf Smartphones. Schliesslich sind Unternehmen grundsätzlich Cloud-Diensten viel aufgeschlossener als noch vor wenigen Jahren. Die Tatsache, dass Microsoft Ende August 2019 in der Schweiz ein eigens Rechenzentrum eröffnet hat und damit auch die Datenhaltung innerhalb der Landesgrenzen gewährleistet wird, dürfte der Cloud-Akzeptanz einen weiteren Schub verleihen.

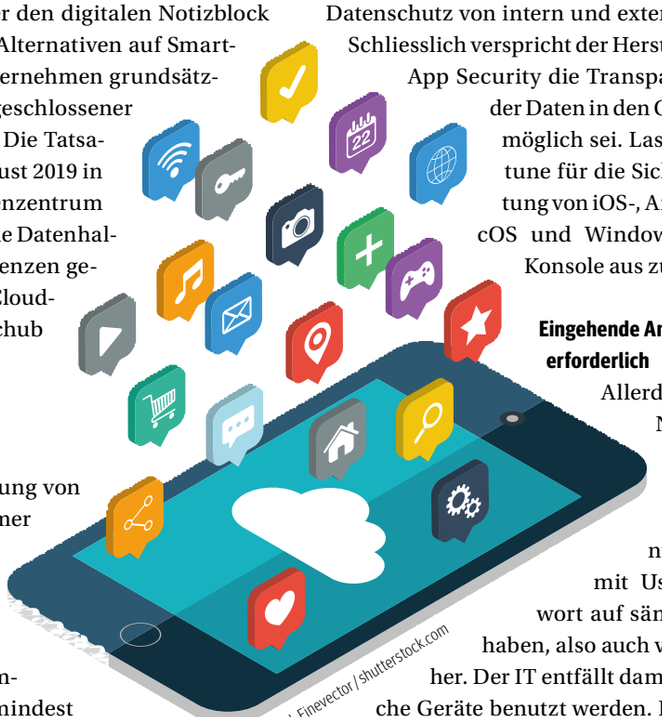

Bild: Finevector / shutterstock.com

Framework für Geräte- und App-Verwaltung

Wenn nun aber die Verwendung von Smartphones und Tablets immer häufiger über eine alleinige Nutzung von E-Mail oder Kalender hinausgeht, kann dies auch beim Management der Apps und Geräte ein Umdenken zur Folge haben. Zumindest ziehen Sicherheitsverantwortliche mittlerweile auch fürs Mobile Device Management (MDM) und Mobile Application Management (MAM) neben den gängigen Herstellern wie Blackberry, Citrix, IBM Maas360, Mobileiron, Sophos oder WMware den Einsatz von Microsoft-Diensten in Betracht – selbstverständlich nicht, ohne zuvor einen Machbarkeitsnachweis erbracht zu haben. Der Hersteller bietet ein dazu Framework zum Schutz von Unternehmensdaten an, das auf eine «Mobile First und Cloud First»-Welt zurechtgeschnitten ist. Es besteht aus fünf Komponenten: Erstens dient Azure Active Directory Premium für die Multi-Faktor-Authentifizierung und Zugriffskontrolle, basierend auf dem Device-Zustand, Benutzerstandort und für ganzheitliche Sicherheitsberichte, Audits und Warnmeldungen. Zweitens soll Advanced Threat Analytics zur Verbesserung von Transparenz sowie zur Prüfung und Kontrolle von Cloud-Anwendungen dienen. Azure Information Protection wiederum ermöglicht dem Hersteller zufolge einen dauerhaften Datenschutz von intern und extern geteilten Dateien. Schliesslich verspricht der Hersteller, dass mit Cloud App Security die Transparenz und Kontrolle der Daten in den Cloud-Anwendungen möglich sei. Last but not least ist Intune für die Sicherung und Verwaltung von iOS-, Android-Geräten, MacOS und Windows10-PCs von einer Konsole aus zuständig.

Eingehende Analyse erforderlich

Allerdings gilt es auch die Nachteile von mobilen Apps aus der Cloud zu bedenken. Etwa, dass Benutzer von überall her mit Username und Passwort auf sämtliche Apps Zugriff haben, also auch von fremden Geräten her. Der IT entfällt damit die Kontrolle, welche Geräte benutzt werden. Deshalb muss unbedingt vor der Einführung eine eingehende Analyse der Situation und eine klare Strategie herausgearbeitet werden. Es gilt zu klären, ob und wie sich das neue System in bestehende On-Premise- oder andere Cloud-Services integrieren lässt und ob die neue Lösung tatsächlich dasselbe leisten kann wie die aktuell im Einsatz befindliche. Hinzu kommt, dass die Konzentration auf einen einzigen Hersteller bedingt, dass die IT-Teams viel enger zusammenarbeiten müssen. Die Unterstützung durch einen externen Mobile-Security-Spezialisten könnte deshalb eine Option sein, weil damit die entsprechenden Skills an einem Ort gebündelt werden.

DER AUTOR

Pascal Meyer
Program Manager, Nomasis

Unternehmen sind Cloud-Diensten viel aufgeschlossener als noch vor wenigen Jahren.