Verwaltung von mobilen Geräten und Apps tendiert Richtung Microsoft.

Der Trend zur vermehrten mobilen Nutzung von Softwareanwendungen auch als Apps auf Smartphones und Tablets hat neben einer verstärkten Nutzung von immer mehr in Microsoft Office 365 vorhandenen Anwendungen zu einem Umdenken in Sachen Verwaltung der Geräte und Applikationen geführt.

VON PASCAL MEYER*

Schon seit geraumer Zeit wollen Unternehmen ihren Mitarbeitenden möglichst viele Anwendungen ihrer Arbeitsumgebung auf mobilen Geräten, also Smartphones und Tablets oder Laptops, zur Verfügung stellen. Dies insbesondere deshalb, weil dadurch Wartezeiten sinnvoll überbrückt oder ganz grundsätzlich Arbeitsabläufe mobil erledigt werden können. Seit wenigen Jahren nun hat sich auch bei vielen Schweizer Unternehmen die Skepsis gegenüber Cloud-Lösungen massiv gelegt. Insbesondere geht heute die Verwendung von Smartphones und Tablets weit häufiger über die alleinige Nutzung von E-Mail, Kalender oder zum Teilen von Informationen hinaus und erstreckt sich bis auf Fachanwendungen und Unternehmens-Apps. Hinzu kommt, dass viele Firmen durch ihre Enterprise-Lizenzierungen von Microsoft Office 365 Anwendungen bezahlen, die sie nicht oder noch nicht nutzen. Mit der verstärkten Verwendung von Microsoft-Lösungen können nun aber einerseits Kosten von Drittanbietern eliminiert und andererseits auch Vereinfachungen in der IT bei der Verwaltung von mobilen Geräten und Apps erzielt werden. Denn mit dieser gestiegenen Akzeptanz gegenüber mobilen Anwendungen auch aus der Cloud einher geht die Einsicht, auch fürs Mobile Device Management (MDM) und Mobile Application Management (MAM) auf Produkte des Softwarekonzerns aus Seattle zurückzugreifen.

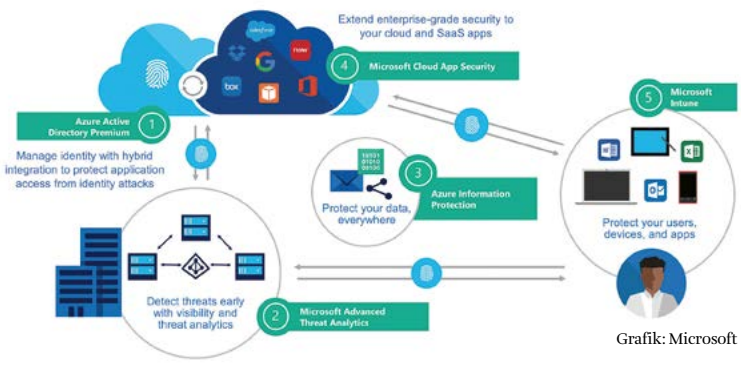
Office 365 + Security. Das macht Sinn, geht es doch bei der übergeordneten Cloud-Strategie von Microsoft nicht nur darum, die Produktivität der Mitarbeitenden, sondern auch die der für die Verwaltung der IT-Infrastruktur Zuständigen zu steigern. Dazu stellt der Hersteller mit EM+S (Enterprise Mobility + Security) ein ganzheitliches Framework zum Schutz von Unternehmensdaten in einer «Mobile First und Cloud First»-Welt» zur Verfügung, und dieses besteht aus folgenden Komponenten:

1. Azure Active Directory Premium für Multi-Faktor-Authentifizierung, Zugriffskontrolle basierend auf dem Device-Zustand, Benutzerstandort sowie ganzheitliche Sicherheitsberichte, Audits und Warnmeldungen
2. Microsoft Advanced Threat Analytics zur Verbesserung von Transparenz, Prüfung und Kontrolle von Cloud-Anwendungen
3. Azure Information Protection für einen dauerhaften Datenschutz von intern und extern geteilten Dateien, einschliesslich der Möglichkeit, Daten zu verfolgen, zu klassifizieren und zu kennzeichnen
4. Microsoft Cloud App Security zur umfassenden Transparenz und Kontrolle der Daten in Cloud-Anwendungen
5. Microsoft Intune zur Vereinfachung der Sicherung und Verwaltung von iOS-, Android- und Windows-PCs von einer Konsole

Produktivität der IT. Mit der Lösung lassen sich erstens Ressourcen schützen, indem Gefahrenstufen für jeden Benutzer und Anmeldeversuch berechnet und Zugangsregeln angewendet werden können, um Missbräuchen bei der Anmeldung Einhalt zu gebieten. Darüber hinaus lassen sich Daten schützen. Die IT erhält nämlich eine bessere Transparenz über Benutzer-, Device- und Datenaktivitäten. So können Dateien bei der Erstellung klassifiziert und bezeichnet sowie deren Verwendung verfolgt und bei Bedarf die Berechtigungen angepasst werden. Schliesslich dient das Zusammenspiel der Komponenten zum Erkennen von Angriffen, bevor sie Schaden verursachen können. So können Angreifer mit Threat-Analysen zur Erkennung von Unregelmässigkeiten identifiziert werden.

Vier-Schritte-Ansatz. Um die Implementierung von mobilen Geräte so einfach wie möglich zu gestalten, empfiehlt sich aus Erfahrung ein Service aus Best Practices, Tools, Ressourcen und auf das Thema spezialisierten Experten. Denn es gibt bei all den genannten Vorteilen auch eine Kehrseite der Medaille: Beispielsweise haben Benutzer von überallher mit Username und Passwort auf sämtliche Apps Zugriff, also auch von fremden Geräten her. Die IT hat damit keine Kontrolle mehr darüber, welche Geräte benutzt werden. Aus diesem Grund sollte vor der Einführung unbedingt eine eingehende Analyse der Situation und eine klare Strategie herausgearbeitet werden. So gilt es beispielsweise zu klären, ob die Lösung das tun kann, was die aktuell im Einsatz befindliche Enterprise-Mobility-

Die Enterprise-Mobility-Lösung von Microsoft wurde für eine «Mobile First und Cloud First»-Welt entwickelt.



Grafik: Microsoft

Management-Plattform leistet, wie sich das neue System in bestehende On-Premise- oder Cloud-Services von Microsoft integrieren lässt und ob es grössere Risiken gibt, die bei dem Vorhaben beachtet werden müssen. Um die Implementierung schliesslich umzusetzen, bedarf es vorab eines seriösen Machbarkeitsnachweises, bevor die entsprechend geplante Migration umgesetzt wird. Erfahrungsgemäss empfiehlt sich dafür ein benutzergesteuerter Wechsel. Dabei wird die Überführung automatisiert und standardisiert. Benutzerprofile des Quellsystems werden weitgehend automatisch ausgelesen, analysiert und in gleichwertige oder vergleichbare Profile des Zielsystems überführt. Dies spart Zeit, vermeidet Fehler und benötigt nur wenig Support. Ein grosser Vorteil ist nämlich beispielsweise die Tatsache, dass der Migrationsprozess nur wenige Minuten dauert und somit die Ausfallzeiten minimiert sind. Der Benutzer bestimmt selbst, wann er die Migration vollziehen will, und ist wieder schneller produktiv.

Fazit. Mit Microsoft EM+S und Intune können Unternehmen mit dem arbeiten, was sie schon im Einsatz haben. Denn sie erhalten ein Set von Lösungen, die so konzipiert sind, dass bereits getätigte Investitionen geschützt werden und damit kostspielige und komplizierte Aufwendungen für Integrationsarbeiten vermieden werden können. Darüber hinaus bietet es eine zukunftssichere Investition, weil die Cloud-Lösung in die lokale Infrastruktur integriert werden kann, skaliert und die Wartung und Up-dates im Hintergrund übernimmt. Die Lösung kann schliesslich weniger finanzielle Aufwände bedeuten als die Kombination aus Einzelprodukten anderer Anbieter. Allerdings hat die Konzentration auf einen Hersteller auch zur Folge, dass die IT-Teams viel enger zusammenarbeiten müssen, da alle auf der gleichen Plattform arbeiten. Hierbei ist die Unterstützung durch einen externen Mobile-Security-Spezialisten eine Option, werden dadurch doch die entsprechenden Skills an einem Ort gebündelt. Schliesslich sollte jede Person in einem Unternehmen künftig in der Lage sein, alle Aufgabe auf einem mobilen Gerät zu erledigen.

*

PASCAL MEYER
ist Program Manager bei Nomasis AG. Als Pionier und Marktführer in der Umsetzung von mobilen IT-Infrastrukturen betreut Nomasis über 200 aktive Kunden aus der Finanzbranche, den öffentlichen Diensten, Industrie, Gesundheitswesen, Handel und Bildung. Seit der Firmengründung im Jahr 2004 hat sich das Unternehmen konsequent auf die Informationssicherheit für den mobilen Mitarbeiter spezialisiert und bringt geschäftsrelevante Daten sicher und einfach auf mobile Geräte wie Smartphones, Tablets und Laptops. **www.nomasis.ch**