Geräte-Management

E-Mails im Container

[10.04.2018] Ob mit dem Diensthandy oder einem privaten Gerät: Mit der App DME können Mitarbeiter der Verwaltung in Hamburg, Schleswig-Holstein und Sachsen-Anhalt von unterwegs aus auf E-Mails, Kalender und Kontakte zugreifen.

Schnell von unterwegs aus E-Mails checken oder nachsehen, wann und wo der nächste Termin ansteht: Wo Arbeit immer unabhängiger wird von Ort und Zeit, wächst auch der Wunsch, kleine Routineaufgaben zwischendurch auf einem Smartphone erledigen zu können, ohne dafür erst einen Computer starten zu müssen. Nicht in jedem Fall ist ein Diensthandy die geeignete Lösung, denn für den Anwender bedeutet das den Einsatz eines zusätzlichen Geräts. Und für Arbeitgeber bringt es Kosten und Verwaltungsaufwand mit sich. Die Lösung: Bring Your Own Device (BYOD). Mitarbeiter nutzen dabei ihr privates Gerät für dienstliche Aufgaben. Die Herausforderung besteht darin, dienstliche Daten zuverlässig von privaten zu trennen und vor unberechtigtem Zugriff sowie Schad-Software zu schützen.

Drei Länder mit DME

In den Bundesländern Hamburg, Schleswig-Holstein und Sachsen-Anhalt setzt der IT-Dienstleister Dataport die so genannte Container-Lösung DME (Dynamic Mobile Exchange) ein, eine in sich geschlossene App, die von anderen Anwendungen konsequent isoliert auf dem mobilen Endgerät eines Beschäftigten arbeitet. DME hat im Jahr 2012 eine Blackberry-Infrastruktur für die drei Länder abgelöst und läuft inzwischen auf insgesamt etwa 4.200 Geräten. Hersteller der App ist das dänische Unternehmen Excitor, das 2015 von der japanischen Soliton-Gruppe übernommen wurde.
Zentrale Funktionen von DME, wie es in Hamburg, Schleswig-Holstein und Sachsen-Anhalt eingesetzt wird, sind die Bearbeitung von E-Mails, Kalender, Aufgaben und Kontakten. Die App läuft auf den Geräten der Mitarbeiter jederzeit im Hintergrund, synchronisiert die Daten aber erst, nachdem der Anwender sich angemeldet hat. Auf Wunsch informiert die App über neue Nachrichten im Postfach. Anwender können, zum Beispiel bei Abwesenheit, automatische Antworten definieren. Außerdem können sie E-Mail-Anhänge herunterladen und diese in einem integrierten Viewer und Editor lesen und bearbeiten. Um eine Vermischung privater und dienstlicher Daten zu unterbinden, lassen sich die Dateien dabei nur innerhalb der App speichern. Nicht möglich ist in der aktuellen Version die Bearbeitung eines Postfachs durch Dritte, zum Beispiel durch einen Vertreter, oder die Arbeit mit einem Funktionspostfach.

Anbindung an Verzeichnisdienst

Über DME ist der Benutzer an das Active Directory (AD), den zentralen Verzeichnisdienst der Behörden, angebunden, auf das er online jederzeit Zugriff hat. Direkt auf dem Smartphone werden nur die persönlichen Kontakte des jeweiligen Anwenders gespeichert. Nicht möglich ist es, ein komplettes Adressbuch, etwa das gesamte Behördentelefonbuch von Hamburg, herunterzuladen und zu synchronisieren. In eingeschränktem Umfang können die Nutzer das Verhalten der App selbst steuern, indem sie beispielsweise einstellen, zu welchen Tageszeiten und in welchen Abständen DME Daten synchronisieren soll. Neben diesen derzeit genutzten Basisfunktionen verfügt DME seitens des Herstellers über die technischen Voraussetzungen, kleine, in die App integrierte Web-Anwendungen mit HTML5 zu entwickeln. So könnte zum Beispiel der Nachrichtenkanal aus dem Firmen-Intranet auf dem Smartphone

dargestellt oder Zugriff auf ein Dokumenten-Management-System wie SharePoint ermöglicht werden.

Lizensierte Sicherheit

DME wird für mobile Geräte mit Android- oder iOS-Betriebssystem angeboten. Um die App auf einem privaten Smartphone nutzen zu können, beantragt der Anwender über die IT-Leitstelle seiner Behörde die Freischaltung und lädt sie aus dem Google Play Store oder dem iTunes Store herunter. Zusätzlich müssen Nutzer von Android-Smartphones sich verpflichten, die Sicherheits-App Sophos zu installieren. Zwar verwenden die meisten Privatanwender bereits kostenlose Anwendungen wie AntiVir oder McAfee. Diese sind jedoch in der Regel nicht für den dienstlichen Gebrauch lizenziert, sodass der Einsatz auf einem Gerät, auf dem DME dienstlich genutzt wird, einen Lizenzbruch darstellt. Es besteht das Risiko, dass Hersteller von Sicherheits-Software auslesen, ob professionell genutzte Apps auf einem Endgerät installiert sind, und gegebenenfalls Klage erheben. Dataport stellt deshalb zusammen mit DME eine Sicherheits-Software zur Verfügung, die für den dienstlichen Gebrauch lizenziert ist und erwirbt die erforderliche Anzahl an Lizenzen für alle Anwender zentral.

Verschlüsselter Transport

Entscheidend beim Einsatz einer BYOD-Lösung ist die Sicherheit der dienstlichen Daten, zum einen auf dem Gerät, zum anderen beim Transport zwischen Gerät und Rechenzentrum. DME speichert dienstliche Daten daher in einem eigenen verschlüsselten Container, in dem sie physisch von anderen getrennt sind. In einem virtuellen Container könnten die Daten immer noch an verschiedenen Orten abgelegt werden. Da der Funktionsumfang von DME Copy and Paste verbietet, wird der Austausch von privaten und dienstlichen Daten zusätzlich unterdrückt. Auf diese Weise landen keine Firmeninformationen bei Facebook oder Twitter.
Außerdem ist nicht nur der Container selbst auf dem Gerät verschlüsselt, sondern auch der Transport vom Server zum Smartphone und zurück. Der Schlüssel, um auf die Daten zuzugreifen, ist das AD-Passwort des Anwenders. Die Passwortrichtlinie von Dataport bestimmt also mit über die Komplexität des Schlüssels und somit über die Sicherheit von DME. Als weiteres Sicherheits-Feature prüft DME beim Start, ob der Anwender sich auf seinem Android-Smartphone durch Rooting beziehungsweise auf seinem Apple-Gerät durch Jailbreak erweiterte Administratoren-Rechte verschafft hat. Ist das der Fall, startet DME gar nicht. Gleiches gilt zum Beispiel für Fairphones, die dem Nutzer grundsätzlich volle Zugriffsrechte gewähren. Diese Funktionalität ist insbesondere deshalb wichtig, weil Dataport die privaten Geräte der Anwender nicht zentral administrieren kann und sicher sein muss, dass Einstellungen an der App nicht verändert werden.

Angepasste Konfiguration

Dataport stellt DME bei Bedarf weiteren interessierten Kunden zur Verfügung. Funktionsumfang und Konfiguration der App werden dabei an die Benutzergruppe und die jeweiligen IT-Richtlinien des Kunden angepasst. Dabei muss sich jeder Kunde individuell mit den eigenen Datenschützern, IT-Sicherheitsexperten und dem Personalrat abstimmen. Dataport setzt die Anforderungen unter Berücksichtigung seiner Sicherheitsvorgaben um und betreibt die mandantenspezifischen DME-Lösungen zentral im eigenen Rechenzentrum.

()

Dieser Beitrag ist in der Ausgabe April 2018 von Kommune21 erschienen. Hier können Sie ein Exemplar

bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Infrastruktur, Geräte-Management