LANline

10,– €

September 2017
28. August

ITP VERLAG

IT ■ Network ■ Datacenter www.lanline.de

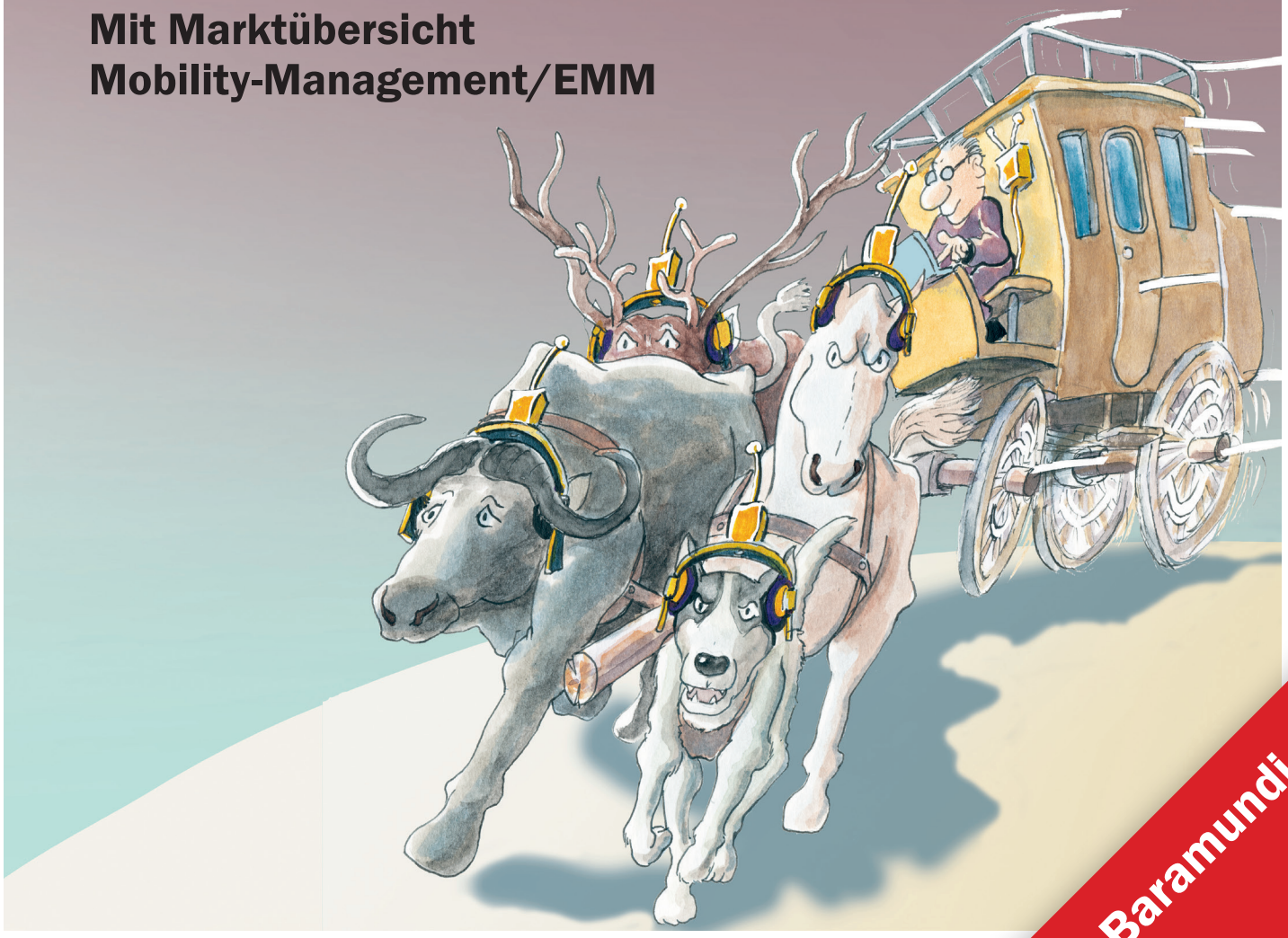
Endpoint-Management

Übergreifende Verwaltung

App-Zugriffe kontrollieren

Mobility und EU-DSGVO

Mit Marktübersicht Mobility-Management/EMM



Ciscos neue Switches und SDN-Funktionen
Das Netzwerk wird lernfähig

Testreihe WS 2016 Teil 2: S2D und Replicas
Plattform für Hyperkonvergenz

Netzwe… und M…
Ma…

Sonderdruck für Baramundi
Mobilgeräte im Griff

September 2017

Umfassendes Mobility-Management

Mobilgeräte im Griff

Längst haben Mobilgeräte den Arbeitsmarkt erobert. Passende Management-Lösungen haben sich vom reinen Mobile-Device-Management (MDM) hin zum Enterprise-Mobility-Management (EMM) entwickelt und verfügen inzwischen über umfangreiche Funktionalität, um Geräte, Apps sowie Daten zu verwalten und abzusichern.

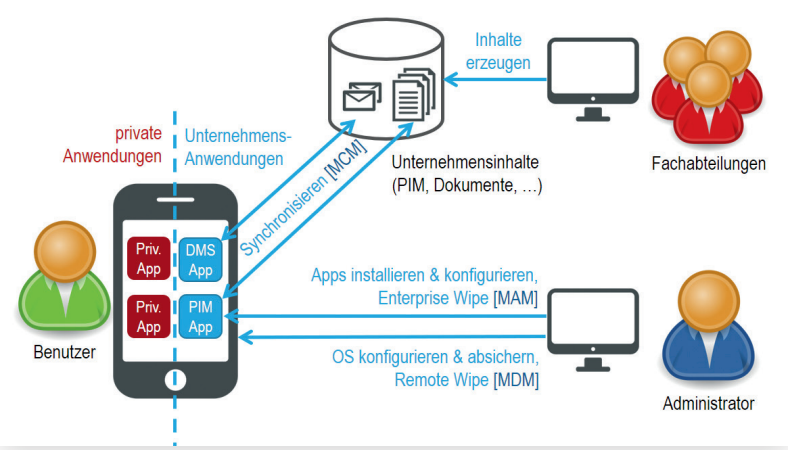
Als vor einigen Jahren mobile Geräte als Arbeitsmittel Einzug in die Unternehmen gefunden haben, stellte das IT-Verantwortliche vor die neue Herausforderung, auch diese Geräte zu managen. Das Verwalten von Desktop-PCs und Servern war bereits Standard und wurde mit entsprechenden Client-Management-Lösungen umgesetzt. Um mobile Geräte ebenfalls verwalten und absichern zu können, kamen MDM-Lösungen ins Spiel. Damit allein ist es jedoch nicht getan. Die IT-Administration muss auch die verwendeten Apps per MAM (Mobile-Application-Management) unter Kontrolle haben. Nur so verhindern Administratoren, dass besonders datenhungrige oder unsichere Apps zum Einsatz kommen.

Mitarbeiter greifen aber mit mobilen Geräten auch auf Unternehmensdaten zu. Zum Schutz des Contents muss die IT-Abteilung klar definieren, wer von wo auf was zugreifen darf. Dazu nutzen Administratoren spezielle MCM-Funtionen (Mobile-Content-Management). Über die Zeit und in Einklang mit den Management-Möglichkeiten der Mobilgeräteplattformen haben die einschlägigen Hersteller die MDM-Werkzeuge weiterentwickelt und um neue Funktionalitäten zum MAM und MCM erweitert. So reicht heute ein einziges Werkzeug aus, um den steigenden Anforderungen Rechnung zu tragen.

Vom Enrollment bis zum Monitoring

Reine MDM-Lösungen ermöglichten es primär, das jeweilige Gerät (Device) zu verwalten. Dazu musste es die IT-Abteilung einmalig in die Management-Lösung aufnehmen. Bereits hier zeigte sich, dass MDM dem Administrator eine enorme Arbeitserleichterung bringt und die Fehlerquote bei der Konfiguration gegenüber der manuellen Einrichtung sinkt.

In umfassenden EMM-Lösungen ist die MDM-Funktionalität natürlich weiter enthalten. Eine elegante Möglichkeit für die Einbindung neuer Geräte (Enrollment) ist ein QR-Code, den die IT-Abteilung per E-Mail an den Nutzer schickt. Dieser kann den Code dann mit seinem Gerät scannen und die Verwaltung des Geräts bestätigen.



Die Mathematik des Mobility-Managements: MDM + MAM + MCM = EMM.

Bild: Baramundi

Ab diesem Zeitpunkt unterliegt das Gerät dem Management der IT-Administration. Ist das Mobilgerät ein Iphone oder Ipad und unterstützt die EMM-Lösung Apples DEP (Device Enrollment Program), kann man die Geräte bereits vor Ausgabe an die Mitarbeiter automatisch in der Management-Lösung erfassen.

Im nächsten Schritt können IT-Administratoren alle im Netzwerk befindlichen Geräte inventarisieren und so Informationen zu Hardware sowie Sicherheitseinstellungen, installierten Apps, Zertifikaten etc. sammeln. Um die Geräte abzusichern, nehmen Administratoren verschiedene Konfigurationen vor. Dazu zählen beispielsweise die Definition eines alphanumerischen Passworts mit einer bestimmten Mindestlänge oder eine automatische Sperre bei Erlöschen des Displays nach einer vorgegebenen Zeit. Gleichzeitig ist es wichtig, diese Einstellungen regelmäßig mit der Management-Lösung zu prüfen.

Mit geeigneten IT-Compliance-Regeln kann die IT auch Jailbreaks oder Rooting erkennen. Solche Eingriffe ins Smartphone-Betriebssystem hebeln dessen Schutzfunktionen aus – das Risiko, sich Schadsoftware einzufangen, steigt damit signifikant an. Zudem ist die Absicherung eines manipulierten Geräts über eine Management-Lösung nur eingeschränkt möglich, da sich dessen Schutzfunktionen umgehen lassen.

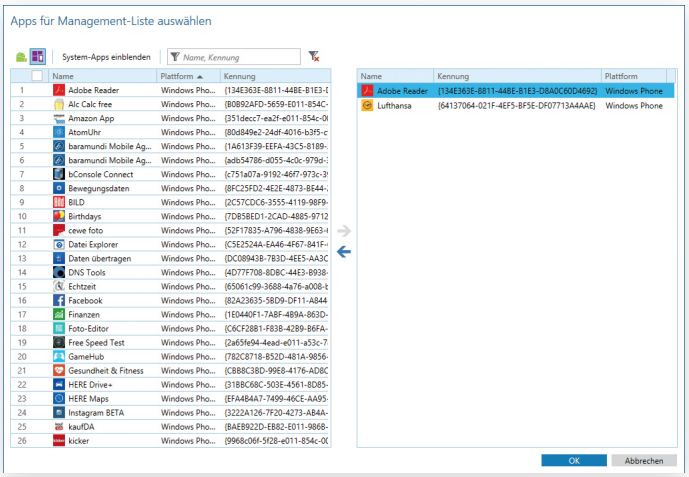
Ebenso wichtig wie das Unterbinden von Firmware-Manipulationen ist das zeitnahe Aktualisieren der Firmware, sobald der Hersteller eine neue Version anbietet. Updates lassen sich ebenfalls über eine EMM-Lösung ausbringen und überwachen. Sie bringen in der Regel nicht nur neue Funktionen, sondern beseitigen regelmäßig auch Schwachstellen.

Management der Apps

IT-Administratoren sollten zudem die verwendeten Apps verwalten. Denn manche

App sind unverhältnismäßig datenhungrig oder die Datenschutzrichtlinien undurchsichtig, sodass sie nicht auf Mobilgeräten im Unternehmen zum Einsatz kommen sollten. Unternehmens-Apps hingegen lassen sich per MAM so konfigurieren, damit sie auf Unternehmensdaten zugreifen zu können.

EMM-Lösungen unterstützen App-Black- und Whitelisting, um die Ausführung gefährlicher Apps zu verhindern und eine Auswahl als vertrauenswürdig eingestufter Apps anzubieten. Per Blacklist kann der Administrator auf kompatiblen Mobilgeräten die Installation und Ausführung ungewünschter Apps unterbinden. Umgekehrt ermöglicht der Whitelisting-Ansatz, explizit erlaubte Apps zu definieren, sodass das EMM-Tool alle nicht gelisteten Apps an der Installation oder Ausführung hindert. Je nach Präferenz kann der Administrator entweder White- oder Blacklisting für ein Endgerät nutzen. Nach der Entscheidung für den Listentyp fügt die EMM-Lösung die gewünschten Apps der Liste hinzu und überträgt sie dann als Profil auf das Mobilgerät.



Die App-Auswahl lässt sich bei EMM-Lösungen mittels Black- oder Whitelisting einschränken. Bild: Baramundi

Unternehmensdaten sicher von Privatem trennen

Besonders der berufliche Einsatz privater Mobilgeräte (Bring Your Own Device, BYOD) stellt Unternehmen vor das Problem, private Daten wie Fotos oder Chats von den geschäftlichen Daten zu trennen, um rechtliche Fallstricke aus dem Weg zu räumen. Die logische Weiterentwicklung der Management-Lösungen bezog sich daher auf das Trennen privater und geschäftlicher Daten, und insbesondere das Absichern und Verwalten von Unternehmensinhalten beim Zugriff per Mobilgerät. Eine häufig gewählte Methode ist ein sogenannter Datencontainer: Ein solcher Container schottet einen Bereich des Smartphones oder Tablets vom restlichen Mobilgerät ab, um bestimmte Dokumente und Daten zu isolieren. Infolgedessen können weder Malware noch System-Ressourcen oder andere (private) Applikationen mit den Daten in diesem sicheren Bereich interagieren. Die sensiblen Daten innerhalb des Containers sind somit geschützt. Hier stehen im Rahmen der EMM-Lösung unterschiedliche Ansätze zur Verfügung: native Trennung auf Betriebssystemebene, native Container des EMM-Herstellers oder aber EMM-Lösungen, die Container-Apps von Drittanbietern unterstützen.

Der Benutzer kann auf seinem Gerät neben den Bordmitteln des Betriebssystems spezielle Container-Apps für PIM (Personal-Information-Management, also E-Mails, Kalender, Kontakte etc.) oder Dokumenten-Management nutzen, die neben der Visualisierung der Inhalte auch die Synchronisation mit Backend-Systemen bewerkstelligen. Derartige Apps liefern je nach Ausprägung auch zusätzliche Sicherheitsfunktionen, um Daten auf den Mobilgeräten zu verschlüsseln und im BYOD-Kontext geschäftliche von privaten Daten getrennt zu halten.

Der Ablauf ist wie folgt: Der Administrator nutzt die EMM-Lösung, um zunächst die Mobilgeräte der Mitarbeiter zu konfigurieren und abzusichern. Dann installiert er die Container-App und konfiguriert sie. Eine solche Konfiguration umfasst beispielsweise die Vorbelegung von Benutzernamen, Verbindungspfade zu Server-Systemen und viele weitere Detaileinstellungen der Apps, die dem Komfort oder der Sicherheit dienen. Im Fall eines Geräteverlusts kann der Administrator im Zusammenspiel mit einer solchen Container-App aus der Ferne gezielt nur die Daten in der App löschen (auch bekannt als „Enterprise Wipe“ oder „Selective Wipe“). Die privaten Daten bleiben dabei unangetastet. Diese Funktion ist eine sehr gute Möglichkeit, BYOD-Konzepte zu implementieren, weil der Administrator dann leichter im Rahmen seiner Befugnisse agieren kann. Die Fachabteilungen, dazu zählt auch der Mobilgerätnutzer, arbeiten weiterhin mit vertrauten Anwendungen, um Inhalte in den Unternehmenslösungen abzulegen. Mit Unternehmenslösungen sind dabei PIM-Systeme wie Microsoft Exchange bis hin zu Dateiablageorte wie Sharepoint, WebDAV und diverse Cloud-Ablagen für Unternehmen gemeint.

Mobility-Risiken beherschen

Egal ob 50 oder 5.000 Mitarbeiter: Unternehmen müssen sich der Herausforderung Mobility stellen. Das Sicherheitsrisiko durch nicht-gemanagte Mobilgeräte und Apps oder unkontrollierten Zugriff auf Unternehmensdaten ist zu groß. Auch aus Sicht der Anwender ist EMM längst kein „Nice to have“ mehr, sondern die Voraussetzung, um effizient und mobil arbeiten zu können. Der erforderliche Funktionsumfang einer EMM-Lösung hängt von der Frage ab, ob Unternehmen Mobilgeräte stellen oder auch die Nutzung privater Smartphones erlauben. Doch nicht immer ist es empfehlenswert, alle verfügbaren EMM-Funktionen zu nutzen. Schränkt man die Nutzer zu stark ein, kann es passieren, dass sie sich Alternativen suchen und damit eine Schatten-IT gefördert wird. Besser ist es, die Anforderungen an Sicherheit und Nutzerfreundlichkeit gegeneinander abzuwägen und daraus passende unternehmenseigene Richtlinien abzuleiten.

Armin Leinfelder/wg

Armin Leinfelder ist Leiter Produkt-Management bei Baramundi, www.baramundi.de.