IT-ADMINISTRATOR.DE

08/2013

iadministrator

Das Magazin für professionelle System- und Netzwerkadministration

Sonderdruck für baramundi software AG

Wissen

Zentrale Verwaltung von mobilen Geräten und Desktop-Clients

Zentrale Verwaltung von mobilen Geräten und Desktop-Clients

Dompteur im Geräte-Zoo

von Armin Leinfelder

Administratoren stoßen auf zahlreiche Hürden, wenn es gilt, mobile Endgeräte ebenso sicher und zuverlässig zu verwalten wie PCs oder Notebooks. Auch die Anzahl der unterschiedlichen Gerätetypen und OS-Versionen ist groß. Und das Risiko, dass eines der kleinen Geräte mit vertraulichen Daten an Bord verloren geht, ist wesentlich höher als bei Notebooks. Wie kombinierte Client Lifecycle- und Mobile Device Management-Suiten helfen, den Überblick zu behalten, zeigt dieser Beitrag.

Im klassischen Client-Management ist der Administrator noch der wahre Herrscher über die Endgeräte. Durch das Setzen entsprechender Richtlinien und vor allem durch das Vorenthalten von Administrationsrechten gegenüber dem Endanwender können tiefere Eingriffe wie Programminstallationen bereits sehr einfach verhindert werden. Doch auf den populären Smartphones und Tablets sieht die Situation zunächst anders aus. Der Besitzer des Geräts ist in der Regel sein eigener Administrator. Er bestimmt selbst, welche Apps er installiert oder deinstalliert. Somit kann das Unternehmen zwar auf organisatorischer Ebene Richtlinien aufstellen, was der Mitarbeiter installieren darf und was nicht. Präventive Maßnahmen auf technischer Ebene sind jedoch nur in besonderen Konstellationen möglich.

Angesichts von Trends wie Bring Your Own Device (BYOD), wo Benutzer ihr privates Gerät auch für berufliche Zwecke nutzen, wird auch künftig das Managen von Mobilgeräten anders aussehen, als es heute auf dem firmeneigenen Windows-Client der Fall sein mag. Denn BYOD-Benutzer waren zuvor bereits Admin auf ihrem Gerät und wollen das in aller Regel auch bleiben, wenn das Gerät für die Arbeit genutzt wird. Aber auch in Unternehmen ohne BYOD gibt es gute Gründe, weshalb der User selbst Admin-Rechte hat. So sehen Consumer-Geräte auf iOS oder Android-Basis oft nur einen Benutzer vor und der ist dann eben auch Administrator. Ferner bekommen Mitarbeiter im Außendienst oft mehr Rechte zugestanden als Personal im Büro, zu deren regelmäßigen Arbeitszeiten auch Administratoren erreichbar sind.

Client- und Mobile Device Management

Hat sich die IT-Abteilung bislang mit dem Management von Windows-Clients und Servern beschäftigt, so besteht inzwischen auch Bedarf, mobile Geräte mit den damit verbundenen Plattformen wie iOS, Android oder Windows Phone 8 zu verwalten. Aber es sind nicht nur die neuen Plattformen, die Veränderungen für die IT-Administration bringen. Auch etablierte Desktop-Systeme wie Windows entwickeln sich in Richtung Mobilität, was gerade an den Modern-UI-Apps von Windows 8 zu erkennen ist. Es überrascht daher nicht, dass laut Marktstudien derzeit das Mobile Device Management zu den wichtigsten IT-Themen zählt.

Nun stellt sich der IT-Verantwortliche natürlich die Frage, mit welchen Tools er den Mobilgeräten als IT-Administrator am besten begegnen kann. Meist nutzen Administratoren klassische Client-Lifecycle-Management (CLM)-Systeme für das Verwalten von Rechnern. Ausgehend davon lassen sich zunächst drei Klassen von Mobile Device Management (MDM)- Tools unterscheiden: Dedizierte MDM-Produkte, kombinierte CLM-MDM-Werkzeuge und integrierte CLM-MDM-Lösungen. Dedizierte MDM-Produkte sind junge Lösungen, die sich ausschließlich auf das Management mobiler Geräte spezialisieren und dabei die Verwaltung von Desktop-Betriebssystemen nicht abdecken. Diese Tools bieten meist eine Vielzahl von Features und berücksichtigen alle populären Mobilplattformen. Der Leistungsumfang orientiert sich an den Möglichkeiten, die der Plattformhersteller zum Management seiner Geräte vorsieht.

Durch die ausschließliche Fokussierung auf Mobilgeräte muss der Administrator zur Verwaltung von klassischen Clients eine andere Lösung nutzen und steht damit vor dem Problem, zwei Tools pflegen und bedienen zu müssen, um alle Geräte der Mitarbeiter zu verwalten. Obgleich sich für beide Bereiche sicherlich Tools finden lassen, deren Bedienung – isoliert betrachtet – komfortabel und optimal erscheint, so ist es gerade der permanente Wechsel zwischen zwei Werkzeugen, der die Komplexität erhöht. Unterschiedliche Bedienkonzepte und Benutzerschnittstellen sowie redundante Daten in beiden Systemen zu denselben Mitarbeitern erschweren IT-Verantwortlichen die Arbeit und bieten keinen Gesamtüberblick. Auch die Beziehung zu mehreren Softwareanbietern schafft zusätzlichen Aufwand.

Bild 1: Kombinierte Management Suites wie von baramundi verschaffen dem Administrator einen Gesamtüberblick

Zwei Welten wachsen zusammen

Kombinierte CLM-MDM-Produkte bieten einen ersten Lösungsansatz. Hierbei ergänzt ein klassischer CLM-Hersteller fehlende MDM-Funktionalitäten durch Hinzufügen von MDM-Komponenten unabhängiger Hersteller und schnürt daraus ein neues Paket. Dabei sollte der Kunde ein genaues Augenmerk darauf richten, wie tief diese Integration erfolgt ist. Handelt es sich nur um eine kommerzielle Integration, also verkauft der CLM-Anbieter auch die MDM-Komponente, oder wurde in eine technische Integration investiert? Bei letzterem – was sicherlich die attraktivere Lösung für den Anwender ist – sollte dann evaluiert werden, wie homogen sich die Kombination bedienen lässt. Gibt es eine gemeinsame Benutzerschnittstelle, oder weiterhin zwei? Ist das Bedienkonzept homogen oder verschieden? Werden dieselben Stammdaten gemeinsam geteilt oder sind gewisse Daten doppelt zu erfassen?

Integrierte CLM-MDM-Produkte stellen damit eine elegante Alternative für ein gemeinsames Management klassischer Clients und Mobilgeräte dar. Mit "integriert" im engeren Sinne sind all jene Lösungen gemeint, bei denen ein – meist erfahrener – CLM-Hersteller seinen Funktionsumfang von der Verwaltung klassischer Clients und Server auf das Management mobiler Geräte ausgedehnt hat. Der Vorteil einer solchen Suite liegt auf der Hand: Beide Teile stammen von einem Hersteller und die Administration erfolgt durch ein einziges Produkt. Dadurch lassen sich Bedienkonzepte und Benutzeroberflächen wesentlich homogener bereitstellen. Der Pflegeaufwand für eine zweite Management-Lösung entfällt und einheitliche Sicherheitsstandards lassen sich in einem ganzheitlichen System leichter durchsetzen. Ferner können Trends von Desktop- und Mobil-Plattformen gemeinsam betrachtet werden, um auch in Zukunft eine stimmige Administration zu ermöglichen.

Plattformübergreifendes Arbeiten

Nutzer tendieren dazu, ihre Arbeit auf mehreren Geräten parallel oder sequentiell zu bearbeiten. So beginnt ein Anwender möglicherweise unterwegs eine Recherche oder eine E-Mail auf seinem Mobilgerät und setzt seine Arbeit daran nach seiner Ankunft im Büro oder zuhause auf dem Desktop-PC fort. Wenn somit verschiedene Geräte ein und denselben Fall bearbeiten, dann sollten auch auf all diesen Geräten nach Möglichkeit dieselben Programme, Dateien und Rechte zur Verfügung stehen. Natürlich sind auch die Sicherheitsrichtlinien für diesen Prozess ganzheitlich zu betrachten. Für IT-Verantwortliche bedeutet dies, dass sie wahrscheinlich die gleichen administrativen Tätigkeiten für alle involvierten Plattformen durchführen und für Konsistenz sorgen müssen.

Was sind nun die typischen Administrationsaufgaben und -Funktionen, die heute mit einem MDM-Produkt automatisiert werden können? Hier bieten die großen Plattformen wie iOS, Android und Windows Phone im Detail unterschiedliche Möglichkeiten, die bei der Einführung einer MDM-Lösung anhand der jeweiligen Feature-Matrix genau hinterfragt werden sollten. Ferner erweitern verschiedene Gerätehersteller – beispielsweise Samsung mit den Lösungen SAFE und KNOX – die Plattformmöglichkeiten von Android durch zusätzliche Funktionalitäten und APIs, auf die MDM-Tools zugreifen können. An dieser Stelle sollen daher als Zusammenfassung nur die gängigsten Funktionen vorgestellt werden.

Anforderung an Management-Suites

Bevor eine Management-Suite ein Mobilgerät verwalten kann, muss dieses erst ins Unternehmensnetz integriert werden – das Gerät muss dem System bekannt gemacht werden. Die Rede ist dabei vom sogenannten Enrollment. Dabei wird auf der Serverseite eine Referenz zum Endgerät erzeugt und das Gerät lernt seinen Management-Server kennen. Auf dem Device kann dazu eine Agent-App nötig sein, oder es werden die Bordmittel der Mobilplattform genutzt. Der Austausch der dazu notwendigen Daten kann über verschiedene Arten erfolgen, beispielsweise per E-Mail an den Smartphone-Nutzer oder durch Scannen eines QR-Codes mit der Kamera des Mobilgeräts.

Nach dem Enrollment stehen Funktionen zur Inventarisierung, Konfiguration von Einstellungen, der Verteilung von Apps bis hin zum Remote Wipe – dem Löschen der Daten auf einem verlorenen Gerät aus der Ferne – zur Verfügung. Wesentliche Funktionen sind dabei:

- Sperren und Entsperren
- Vollständiges Löschen von Gerät und Speicherkarten
- Geräteverschlüsselung aktivieren
- Erkennen von Manipulationen der Firmware (Jailbreaks, Rooting)
- Compliance Dashboards, Regeln und automatisierte Reaktionen
- Hardware-Informationen
- Installierte Apps, Profile und Zertifikate
- SIM-Karten-Informationen
- Roaming-Status
- Sicherheitseinstellungen
- Software-Verteilung und -Konfiguration

- Installation und Deinstallation von Apps
- Konfiguration von WLAN und VPN
- Einrichtung von Exchange-Konten
- Deaktivieren der Kamera

Um die oben genannten Einstellungen gleichzeitig auf viele Endgeräte anzuwenden, bieten geeignete Lösungen eine Parametrisierung der Werte an. Am Beispiel der E-Mailkonfiguration bedeutet dies, dass der Servername zwar für alle Benutzer derselbe ist, jedoch die E-Mailadresse für jeden Einzelnen individuell gefüllt wird. Zum Definitionszeitpunkt parametrisiert der Administrator daher diesen Wert durch eine entsprechende Variable im Management-System.

Self Service ist ein weiterer Trend, dem eine MDM-Lösung dadurch gerecht werden kann, indem der Administrator versierten Benutzern gewisse Funktionen zur Selbstbedienung bereitstellt. Das kann eine Auswahl von Apps sein, die der Endanwender in einer Kiosk-App zum Installieren angeboten bekommt. Im Gegensatz zum schier unüberschaubaren Angebot der Appstores kann das Unternehmen den Anwendern darin nützliche Apps vorschlagen oder auch festlegen, dass der Anwender ausschließlich die dort gelisteten Apps installieren darf. Aber auch andere Features wie Compliance-Checks können dem Endbenutzer per App zur Verfügung gestellt werden. Beides ermöglicht dem Anwender schnelle Lösungen und spart Administratoren routinemäßige Auskünfte, Unterstützung und die damit verbundene Zeit.

Datenschutz und Compliance nicht vergessen

Ein besonderes Augenmerk sollten Anwender auf das Thema Datenschutz richten – nicht alle angebotenen Lösungen entsprechen den deutschen und europäischen Vorgaben. Kann der Administrator beispielsweise ohne weitere Absicherung die Bewegung des Benutzers per Geo-Location überwachen? Wird beim Löschen zwischen privaten (BYOD) und Firmengeräten unterschieden? Oder lässt eine Nutzungsauswertung (Application Usage Tracking) etwa Rückschlüsse auf die Arbeitsweise von Mitarbeitern zu? Diese und weitere Fragen sollten im Unternehmen auf organisatorischer Ebene geklärt und in Form von Betriebsvereinbarungen oder IT-Richtlinien fixiert werden. Dabei sind neben IT-Experten die entsprechenden Rollen im Unternehmen wie Datenschutzbeauftragter, Betriebsrat und gegebenenfalls juristische Berater zu konsultieren. Stehen die Datenschutzregeln erst mal fest, dann sind die in Frage kommenden Management-Lösungen dahingehend zu evaluieren, wie gut sie diese Regeln befolgen und deren Einhaltung sicherstellen können.

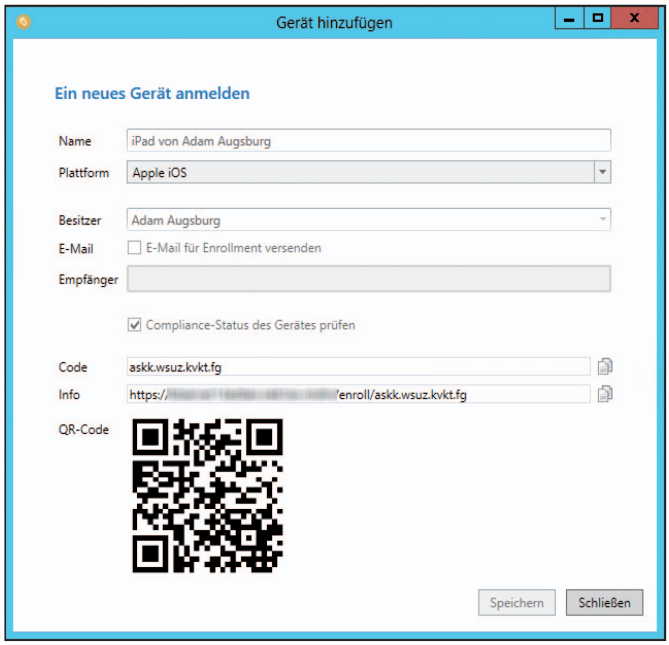

Bild 2: Beim Enrollment werden mobile Devices an die Management Suite gebunden und von dieser fortan überwacht

Um die Compliance von Endgeräten, also die Einhaltung von Unternehmens-IT-Richtlinien, stets sicherstellen zu können, sind geeignete Tools mit entsprechenden Übersichten von Vorteil. Der Grundgedanke ist hierbei, dass der Administrator in Übereinstimmung mit den Unternehmensrichtlinien die technischen Regeln festlegt und deren Einhaltung kontinuierlich überprüft. Bei Regelverstößen kann der Administrator dann gezielt reagieren oder gar Automatismen hinterlegen, die nach Erkennen eines Compliance-Verstoßes umgehend eine vorkonfigurierte Aktivität ausführen. Die Compliance-Überwachung nutzt dabei Grundfunktionalitäten der MDM-Lösung und bietet darüber hinaus Dashboards zur Visualisierung und konfigurierbare Regelwerke.

Ausgehend von aggregierten Diagrammen, anhand derer sich der IT-Verantwortliche eine schnelle Übersicht über alle Geräte verschaffen kann, ist per Drill-Down das Navigieren zum betroffenen Gerät möglich. Je nach Bedarf kann der Administrator dann den betroffenen Mitarbeiter ansprechen und beispielsweise um die Deinstallation unerlaubter Apps bitten oder aber unmittelbar Profile entziehen, die Zugriff auf das Unternehmensnetz gewähren. Auch das komplette Löschen des Geräts per Remote Wipe wäre möglich, wobei derartige Eingriffe eher Ereignissen wie dem Geräteverlust vorbehalten sind.

Fazit

Die Nutzung mobiler Geräte macht das Leben der Mitarbeiter leichter und effizienter. In den nächsten Jahren werden sich die Plattformen rasant weiterentwickeln und damit neue Anforderungen an Management-Tools stellen. Das Leben des Administrators wird durch den wachsenden Geräte-Zoo aber erst einmal schwieriger. Somit liegt der Bedarf an Mobile Device Management-Lösungen auf der Hand. Doch bietet der Markt hierzu bereits eine breite Auswahl an Lösungsansätzen.

Betrachten wir die Geräteformen nicht isoliert voneinander, sondern gemeinsam, so erscheint es nur konsequent, auch Administrationslösungen zu suchen, die sowohl Client- als auch Mobile Device-Management bieten. Mobile Geräte werden im Arbeitsleben die herkömmlichen Plattformen so schnell nicht komplett ersetzen können. Daher sind auch zukünftig Lösungen gefragt, die beide Welten verbinden. *(dr)*

Armin Leinfelder ist Produktmanager bei der baramundi software AG.