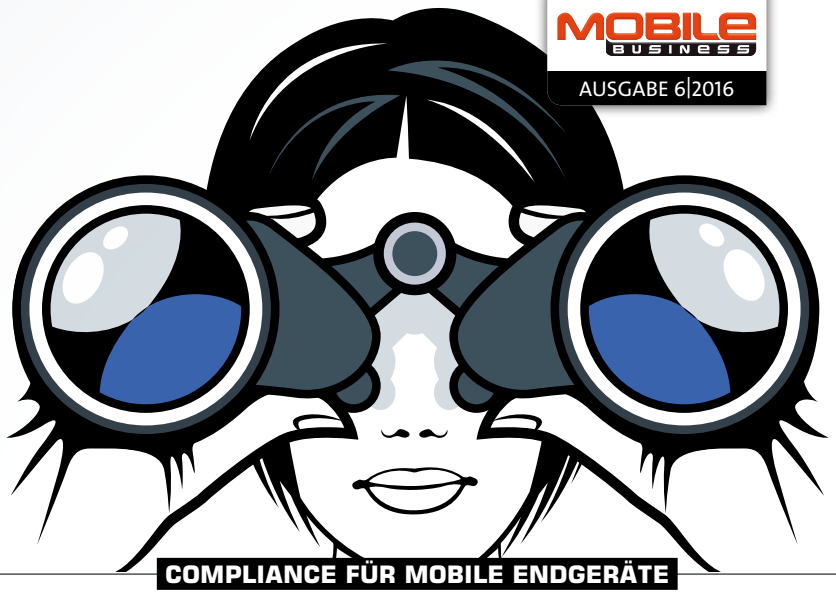
AUSZUG AUS...
MOBILE BUSINESS
AUSGABE 6|2016

ALLE GERÄTE IM BLICK



COMPLIANCE FÜR MOBILE ENDGERÄTE

Ein integriertes Mobile Device Management optimiert bei der Sedus Stoll AG den ***UMGANG MIT MOBILEN ENDGERÄTEN.*** Zusätzliche Compliance-Richtlinien sorgen zudem für entsprechende Datensicherheit.

Mobile Endgeräte gehören zum beruflichen Alltag und werden von Mitarbeitern entsprechend eingefordert – diese Erfahrung musste auch die IT-Abteilung der Sedus Stoll AG machen. Die Mitarbeiter fragten zunehmend nach einer Integration von Mobilgeräten ins Unternehmensnetzwerk und dem Zugriff auf geschäftliche E-Mails. Um die Geräte sicher in die IT einbinden und verwalten zu können, setzt der Komplettanbieter für Büroeinrichtungen eine Software zum Mobile Device Management (MDM) ein.

Eric Michael, Leiter IT-Infrastruktur, und seine Kollegen entschieden sich dazu, den Mitarbeitern Geräte zur Verfügung zu stellen, die beruflich und privat genutzt werden dürfen. Die Verwaltung der 250 mobilen Endgeräte, davon 150 iPads für den Vertrieb, bedeutete für die IT-Verantwortlichen jedoch einen erheblichen Verwaltungsaufwand. Bis Anfang 2011 war noch der Lotus Notes Traveler im Einsatz, mit dem die Postfächer manuell auf den jeweiligen Endgeräten eingebunden werden konnten. „Für uns war das viel Aufwand. Es war zwar möglich, diese Aufgabe an IT-versierte Nutzer auszulagern. Wenn etwas nicht funktionierte, gab es aber keine Möglichkeit, dem Nutzer vernünftige Hilfestellungen aus der Ferne zu geben“, erläutert Michael.

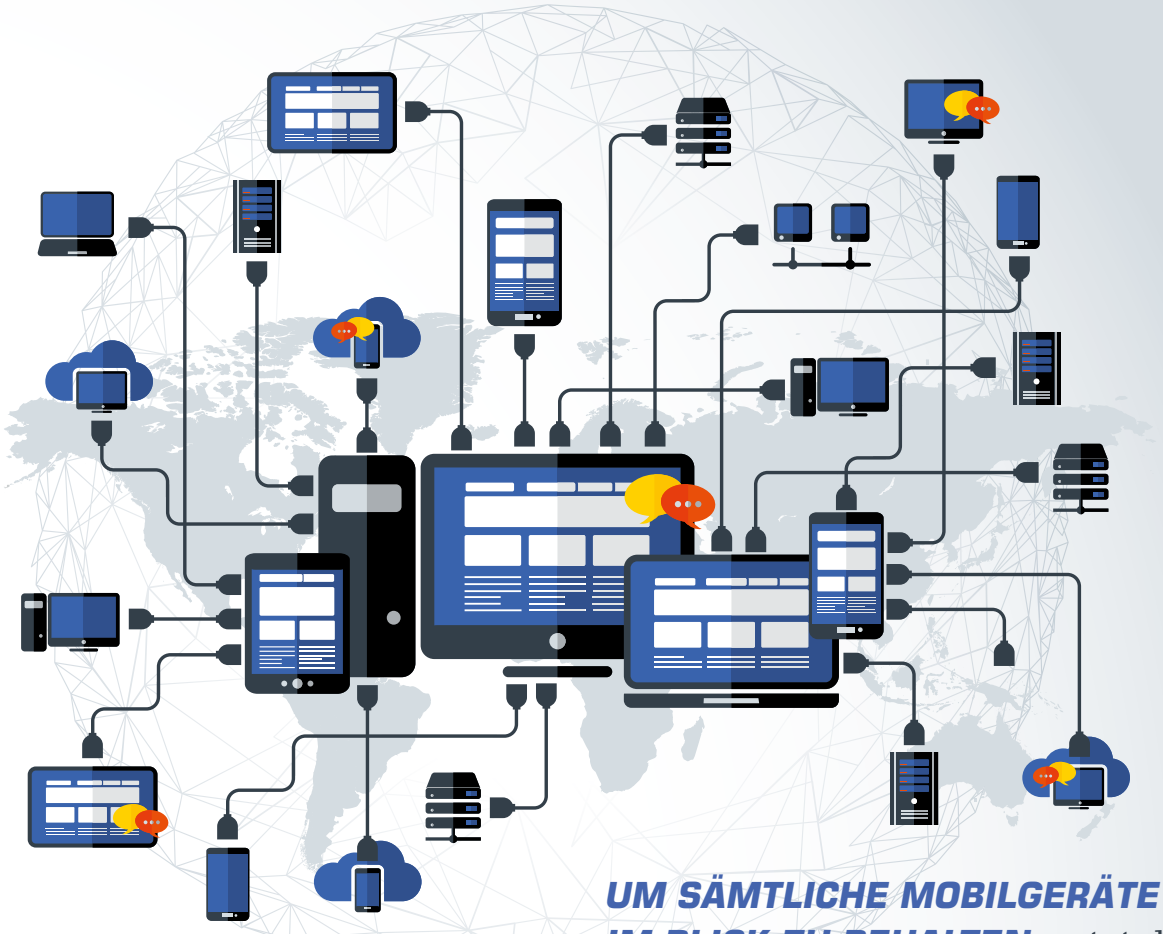
Vor diesem Hintergrund kam der Wunsch nach einem zuverlässigen und funktionsfähigen Mobile Device Management auf. Die Entscheidung fiel 2011 zunächst auf die Lösung eines großen Herstellers. Nach kurzer Zeit zeigte sich jedoch, dass diese zu komplex in der Handhabung war. Aus diesem Grund musste sich die IT-Abteilung nach einer Alternative umsehen. Die Wahl fiel dann auf Baramundi Mobile Devices, welche im April 2015 die bestehende MDM-Software ablöste.

Bereits seit dem Jahr 2012 befindet sich die Client-Management-Software des Herstellers im unternehmensweiten Einsatz. Die Entscheidung für die Management Suite begründet Michael mit der einfachen Bedienung, dem modularen Aufbau und der einheitlichen Oberfläche über alle Funktionalitäten hinweg. „Mit fünf Mitarbeitern am Standort sind wir eine kleine Truppe und realisieren in dieser Aufstellung Helpdesk, Network-Support, Serverbetreuung und Applikationsbetreuung für die gesamte Gruppe der Sedus Stoll AG. Dafür müssen wir nicht viele verschiedene Standalone-Lösungen einsetzen und können darüber unsere IT-Landschaft zentral verwalten und absichern.

Schnelle Integration

Auch ohne Vorkenntnisse können IT-Verantwortliche schnell produktiv mit der MDM-Lösung arbeiten. „Der Schulungsaufwand ist bei dieser Funktionalität nahezu bei null. Sie können jedem Mitarbeiter innerhalb von 15 Minuten erklären, wie er ein mobiles Endgerät aufnehmen soll und wie er bestimmte Profile verteilen kann“, so der IT-Infrastrukturleiter. Auch die Implementierung lief problemlos ab und hat in Summe eine Stunde Zeit benötigt.

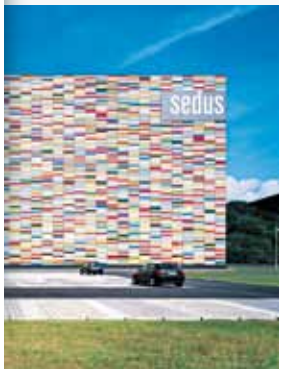
Im täglichen Geschäft wird die Software u.a. für die Aufnahme neuer Geräte in das Unternehmensnetzwerk verwendet. Hierfür wird ein QR-Code erzeugt, der dem betreffenden Mitarbeiter ➔



UM SÄMTLICHE MOBILGERÄTE IM BLICK ZU BEHALTEN, setzt die Sedus Stoll AG auf eine Mobile-Device-Management-Software.

SEDUS STOLL AG

Branche: Büroeinrichtungen und Arbeitsplatzkonzepte
Hauptsitz: Waldshut-Tiengen (zwei produzierende Werke, acht europäische Tochtergesellschaften)
Mitarbeiter: 829
www.sedus.de



zugesendet wird. Indem der Anwender den QR-Code mit seinem Gerät scannt, wird dieses in die Verwaltung der Lösung eingebunden. Dazu muss die App „Baramundi Mobile Agent" auf dem Gerät installiert werden. „Unsere Standardprofile verteilen wir für E-Mail-Accounts, WLAN-Profil und Security. Das bedeutet, dass jedes neu hinzugefügte Gerät automatisch Firmen-WLAN, Exchange-Accounts und die Passwortanforderung erhält", fügt Michael hinzu.

Voller Überblick

Um für die nötige Sicherheit zu sorgen, haben die IT-Verantwortlichen verbindliche Compliance-Richtlinien für die Nutzung mobiler Geräte für das gesamte Unternehmen festgelegt. Werden Jailbreaks oder auch unerwünschte Apps von den Endanwendern installiert, wird die IT-Abteilung direkt informiert und kann den Nutzer anschreiben oder eine automatisierte Aktion wie das Löschen von Profilen oder Remote Wipe ausführen lassen. „Die Tatsache, dass wir über alle Geräte und die darauf installierten Applikationen hinweg den vollständigen Überblick wahren können, entspricht unseren Sicherheitsanforderungen. Da es sich bei dem Software-Hersteller um ein deutsches Unternehmen handelt, ist auch die Lösung nach deutscher Datenschutzrechtsprechung ausgerichtet. Das gibt uns die notwendige Rechtssicherheit", sagt der IT-Leiter.

„Durch das Mobile Device Management haben wir unsere bestehende Client-Management-Lösung um eine sinnvolle Funktionalität ergänzt. Wir haben jetzt den vollen Überblick über alle mobilen Endgeräte, konnten unsere IT-Sicherheit damit steigern und sparen bei der Verwaltung unserer Clients Zeit. Hier bewährt sich einmal mehr der integrative und modulare Ansatz der Lösung", resümiert Eric Michael.

ARMIN LEINFELDER.