COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/die-4-komponenten-von-sap-mobile-secure,2542392

Mobile Sicherheit

Die 4 Komponenten von SAP Mobile Secure

Datum: 16.07.2013
Autor(en): Andreas Schaffry

Die Anzahl mobiler Anwender in Unternehmen steigt rasant. CIOs stehen vor der Aufgabe, mobile Geräte, Apps und Inhalte umfassend abzusichern sowie mobile Kosten im Griff zu haben. Einen Ansatz dafür bietet das Lösungsportfolio "SAP Mobile Secure".

Benjamin Kunkel, Mobility-Experte bei SAP, ist überzeugt, dass CIOs angesichts der rasant steigenden Anzahl mobiler Anwender unternehmensweit auf allen Ebenen ein mobiles Sicherheitskonzept und die dazu passenden Lösungen brauchen. Foto: SAP

Studien belegen: Die Zukunft der Arbeit ist mobil. Bis 2017 sollen weltweit mehr als 900 Millionen Beschäftigte geschäftliche Aufgaben mobil erledigen, prognostiziert der US-Marktforscher **Forrester Research**[1] in der Studie "Mobile Workforce Adoption Trends 2013". Bereits heute treibt es CIOs bei der Absicherung mobiler Endgeräte, Anwendungen und Dokumente den Angstschweiß auf die Stirn. Die Ursachen dafür sind vielfältig: "Die stetig steigende Zahl der mobilen Anwender in Unternehmen erhöht die Anforderungen an das Enterprise Mobility Management (**EMM**[2])", weiß Benjamin Kunkel, Solution Expert SAP Mobility bei SAP. Zugleich erledigen immer mehr Mitarbeiter Arbeitsaufgaben nach der Devise "Bring your own Device (**ByoD**[3])" mit dem eigenen Smartphone oder Tablet. Oft werden wichtige interne Dokumente ohne Wissen der IT-Abteilung mit privaten Apps bearbeitet und in öffentlichen Cloud-Diensten gespeichert. "Häufig weiß die IT gar nicht, welche Dokumente jenseits des Firmentors genutzt werden - in vielen Fällen völlig ungesichert", sagt Benjamin Kunkel. Nicht zuletzt besteht die Gefahr, dass Kriminelle mobile Devices stehlen oder per Jailbreak knacken, um an geschäftskritische Daten heranzukommen.

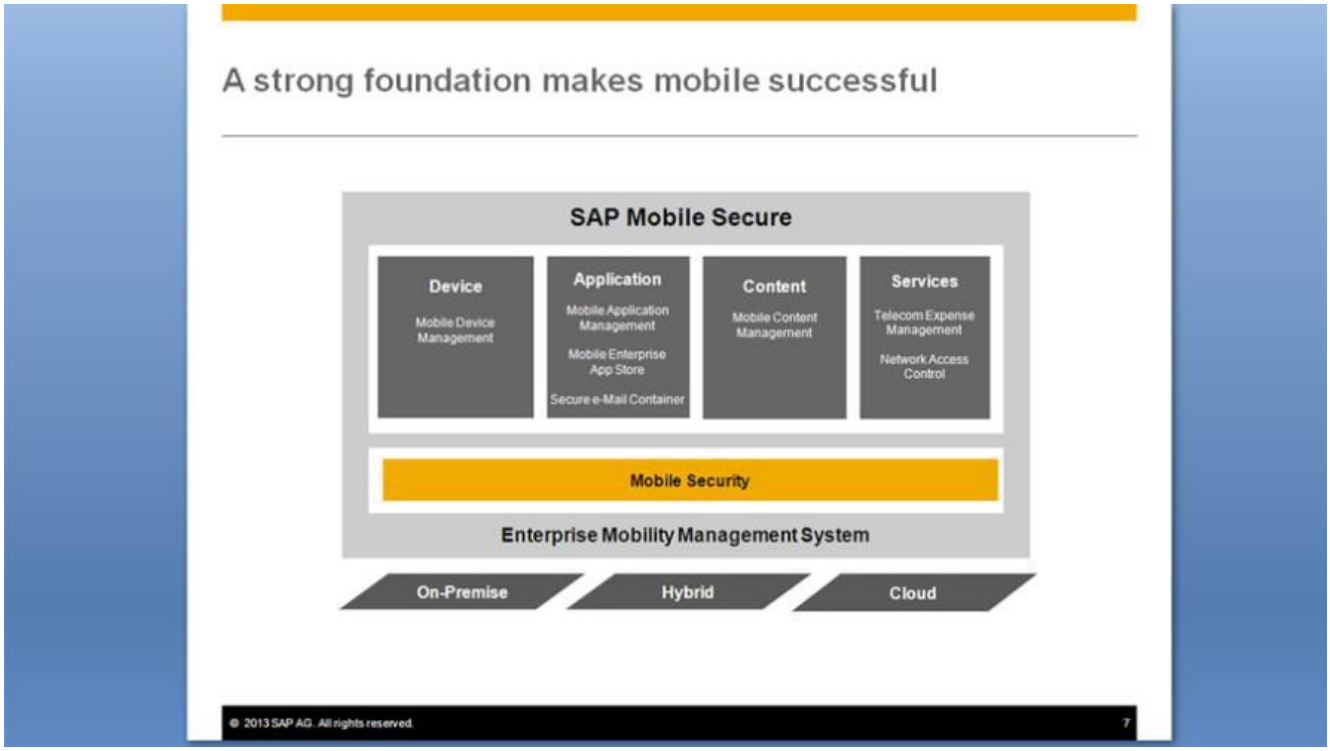
Vier Kernbereiche mobiler Sicherheit

"IT-Verantwortliche stehen daher vor der Aufgabe mobile Sicherheit unternehmensweit auf der Grundlage einer ganzheitlichen Enterprise-Mobility-Management-(EMM)-Strategie umzusetzen, die das gesamte Spektrum mobiler Sicherheit abdeckt", erläutert Benjamin Kunkel. Dazu zählen neben dem "klassischen" Mobile Device Management, das Management mobiler Applikationen, die Verwaltung von Dokumenten und Inhalten sowie mobile Services, wie etwa die Überwachung und Kontrolle der mobilen Kosten. Diese vier Kernbereiche mobiler Sicherheit hat SAP in dem Produktportfolio "SAP Mobile Secure" gebündelt:

1. Gerätesicherheit: In der Mobile-Device-Management (MDM)-Lösung **SAP Afaria**[4] werden unternehmenseigene wie auch private Mobilgeräte mit Android-, iOS- oder Windows-Phone-8-Betriebssystem über ihren gesamten Lebenszyklus von der Bereitstellung bis hin zur Stilllegung verwaltet und abgesichert. IT-Administratoren erkennen in SAP Afaria sofort, ob die unternehmensinternen Sicherheitsrichtlinien für mobile Devices eingehalten werden. Im Ernstfall können sie jedes in der MDM-Lösung verwaltete Gerät sofort sperren, die installierten Apps entfernen und alle gespeicherten Daten, etwa E-Mails, Kalendereinträge oder Notizen, löschen. Dabei können Mitarbeiter Firmengeräte wie auch die eigenen Devices über ein Self Service Portal in der MDM-Lösung anmelden. Im Gegenzug erhalten sie die dort bereitgestellten Apps für ihr Gerät und die jeweiligen Berechtigungen. Sie werden zudem automatisch informiert, wenn im Afaria App Store neue Apps oder Aktualisierungen zu bereits installierten Anwendungen verfügbar sind.

2. App-Sicherheit: Die Absicherung der Applikationen erfolgt mit der "SAP Mobile App Protection by Mocana".

Zusätzliche Schutzhülle für Apps



Mobile Devices, Apps, Dokumente, Kosten: Das Lösungsportfolio "SAP Mobile Secure" deckt alle Bereiche mobiler Sicherheit ab.
Foto: SAP

"Die **App-Wrapping**[5]-Technologien Mocana ziehen um jede iOS- oder Android-App eine zusätzliche Schutzhülle", verdeutlicht Benjamin Kunkel das Prinzip. Dafür werde lediglich das Installationsfile einer App benötigt. Mit der Lösung des Herstellers mobiler Security-Software lassen sich Sicherheitseinstellungen für die unterschiedlichen mobilen Nutzergruppen im Unternehmen individuell definieren, ohne dafür gesonderten Code schreiben zu müssen.

Zum Beispiel kann festgelegt werden, dass eine App nur in einem bestimmten Zeitfenster oder innerhalb des Firmengeländes geöffnet werden darf und keine Daten aus dieser heraus oder in diese hinein kopiert werden können. Zugleich lässt sich in der App einstellen, die Datenübertragung ausschließlich über einen sicheren VPN-Tunnel durchzuführen und nicht per Internet. Die Datenbanken von Apps lassen sich außerdem mit dem Sicherheitsstandard **FIPS**[6] 140-2 zusätzlich verschlüsseln.

Dokumente kontrollieren

3. Dokumentensicherheit: SAP Mobile Documents[7] bietet einen einzigen Zugangspunkt für den Zugriff auf Geschäftsdokumente und -inhalte mit verschiedenen Geräten - ob per Desktop-PC, Notebook, **Tablet-PC**[8] oder Smartphone. Die native App ist passwortgeschützt und lässt sich über Afaria konfigurieren. IT-Administratoren können in SAP Mobile Documents somit Dokumente und Inhalte über zentrale Management- und Sicherheitsrichtlinien kontrollieren.

Sie ermöglicht Mitarbeitern - unabhängig vom Gerätetyp an dem sie gerade arbeiten - den sicheren Austausch von Unternehmensdokumenten für den individuellen wie auch für den Gebrauch im Team. Durch die Verwendung des offenen Content Management Interoperability Standard (**CMIS**[9]) lässt sie sich an CMIS-basierte Enterprise-Content-Management-(**ECM**[10])-Plattformen wie SAP Netweaver Portal Knowledge Management (KM) oder Microsoft Sharepoint anbinden. Zentrale Komponente ist der Mobile Documents Server, der auf dem SAP NetWeaver Application Server (Java) läuft. Er implementiert den Industriestandard CMIS für die App-, Desktop- und Web-Clients sowie Back-End-Systeme und gewährleistet eine sichere Datenübertragung. Die Anwendung ist derzeit für Windows, Apple Mac, das iPad und HTML5-Browser verfügbar.

Die mobilen Kosten im Griff

4. Mobile Services: Im Rahmen des EMM braucht die IT Abteilung zudem eine klare Sicht auf die Kosten der mobilen Kommunikation, um diese genau nachzuvollziehen und zu kontrollieren. Dazu ist es nötig, die Informationen auf mobilen Geräten, wie Gesprächsdauer und Downloadvolumen, mit den entsprechenden Vertragsdaten zu verknüpfen. Vor kurzem hat SAP daher eine Entwicklungskooperation mit dem US-Softwareanbieter **Tangoe**[11] geschlossen. Dessen Telecom-Expense-Management-(TEM)-Lösung und die MDM-Plattform von SAP sollen funktional zusammenwachsen, um das Kosten- und Gerätemanagement zu homogenisieren und Verbrauchsdaten von Devices mit den Vertragsdaten abzugleichen.

Laut SAP können Kunden die SAP Mobile Secure-Anwendungen wahlweise On Premise installieren oder als **Cloud**[12]-Services nutzen. Ebenso möglich sei ein Hybrid-Modell bei dem bestimmte Anwendungen im eigenen Rechenzentrum implementiert und andere On-Demand bezogen werden. Um das Sicherheitsmanagement von Devices, Apps, Dokumenten und mobilen Services für IT-Administratoren zu vereinfachen, will SAP die einzelnen Komponenten des Lösungsportfolios technisch sukzessive über Schnittstellen sehr eng zusammenführen und das Zusammenspiel mit der **SAP Mobile Plattform**[13] weiter ausbauen.

Links im Artikel:

[1] **http://www.forrester.com/2013%2BMobile%2BWorkforce%2BAdoption%2BTrends/fulltext/-/E-RES89442**
[2] **https://www.computerwoche.de/a/sap-kuendigt-neue-afaria-version-an%2C2529831**
[3] **https://www.computerwoche.de/a/byod-prozessqualitaet-rauf-security-risiken-auch%2C2532386**
[4] **https://www.computerwoche.de/a/sap-richtig-mobilisieren%2C2503330**
[5] **https://www.computerwoche.de/a/so-behalten-sie-die-faeden-in-der-hand%2C2516924%2C2**
[6] **http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf**
[7] **https://www.computerwoche.de/a/unterwegs-jederzeit-auf-dokumente-zugreifen%2C2534005**
[8] **https://www.computerwoche.de/k/tablet-pc%2C3453**
[9] **https://www.computerwoche.de/a/emc-ibm-und-microsoft-wollen-neuen-dms-standard-etablieren%2C1873219**
[10] **https://www.computerwoche.de/schwerpunkt/ECM**
[11] **http://www.tangoe.com/News-Events/News/Press-Releases/2013/Tangoe-and-SAP-Sign-Software-Development-Cooperati.aspx**

[12] **https://www.computerwoche.de/schwerpunkt/Cloud-Computing**

[13] **https://www.computerwoche.de/a/bankgeschaefte-per-app-erledigen%2C2535205**
