2/2013

Kommune21

7,00 € / 13,00 sFr

Bundes-CIO Rogall-Grothe über die Akzeptanz der eID-Funktion des nPA

www.kommune21.de

Kommune21

E-Government, Internet und Informationstechnik

eID-Funktion des neuen Personalausweises

Gründe für schlechte Einschaltquoten

E-Government

- **Verwaltungsmodernisierung:** Was hat das Neue Steuerungsmodell eigentlich bewirkt?

Titel

- **Neuer Personalausweis:** Warum der Durchbruch noch auf sich warten lässt

Informationstechnik

- **Mobile Device Management:** Smartphones und Tablets kontrolliert integrieren

Praxis

- **Wolfsburg:** Bauantrag mit dem Online Antragsmanagement von SAP

Spezial

- **Finanz-Management:** Transparentes Rechnungswesen durch Gesamtabschluss

ISSN 1618-2901 E54570

Kontrolliertes Einbinden

von Thorsten Strauss

Die zunehmende Nutzung mobiler Endgeräte in internen Netzen ist eine Herausforderung für die IT-Sicherheit. Um Smartphones und Tablet-PCs kontrolliert zu integrieren, bieten sich Mobile Device Management (MDM) oder eine Sandbox-Lösung an.

Die Informationstechnologie vollzieht derzeit einen ihrer größten Paradigmenwechsel: Die mobilen Endgeräte sind mittlerweile so klein, handlich und leistungsfähig, dass wir sie immer dabei haben und ständig vernetzt und online sind. Mit den Geräten hat sich auch der Arbeitsalltag verändert. Beschäftigte können über WLAN und Mobilfunkverbindungen fast überall und jederzeit arbeiten und auf Daten zugreifen. Sie bringen ihre privaten Geräte in die Unternehmen und Verwaltungen hinein oder tragen Dienstgeräte zu Außenterminen und in ihr Home Office. Sensible Daten befinden sich folglich nicht mehr nur in der internen, geschützten Infrastruktur, sondern werden auf mobile Endgeräte über- und aus den Organisationen hinausgetragen. Mit der Zeit werden sie mehr und mehr mit privaten Informationen und Anwendungen vermischt.

Smartphones und Tablets ins Behördennetz integrieren.

In eher konservativen Branchen und in der öffentlichen Verwaltung ist es lange Zeit gelungen, sich gegen diesen Trend zu sperren, aber auf Dauer kann er kaum aufgehalten werden: Die Beschäftigten sind aus ihrem privaten Umfeld daran gewöhnt, mit modernsten Geräten zu arbeiten und daher nicht bereit, sich an ihrem Arbeitsplatz mit weniger zufrieden zu geben. Eine Reglementierung von Geräten oder Anwendungen führt zu Unzufriedenheit und schlechter Performance. Im schlimmsten Fall setzen sich die Mitarbeiter darüber hinweg und nehmen eine Regelverletzung in Kauf.

Die treibende Kraft des Trends zu Hightech-Geräten und mobilen Applikationen ist oftmals die mittlere und obere Führungsebene, der ein IT-Leiter nicht einfach verbieten kann, eigene Geräte mitzubringen. Aus dem gleichen Grund stehen – anders als bei früheren, eher schwerfälligen Entwicklungen – die erforderlichen Budgets und Personalressourcen schneller zur Verfügung. Es ist daher zwecklos, sich dem anschwellenden Strom entgegenzustellen. Die beste Strategie ist, eine sichere und managebare Integration der mobilen Geräte zu ermöglichen. Eine intelligente Lösung schaltet die Risiken aus, hält die Kosten im Rahmen und gewährleistet die IT-Sicherheit in der Organisation, ohne die Anwender einzuschränken oder ihre kreative Schaffenskraft zu behindern.

Mobile Device Management (MDM) ist eine Möglichkeit, mobile Endgeräte wie Smartphones und Tablet-PCs sicher in die Verwaltungsinfrastruktur einzubinden: Sie werden zentral gesichert, gesteuert und konfiguriert. Dadurch lassen sich einerseits die Sicherheitsrichtlinien der Organisation auf die Geräte übertragen, andererseits übernimmt das System automatisch bestimmte Aufgaben und erleichtert den IT-Verantwortlichen auf diese Weise die Arbeit. So legt beispielsweise ein integriertes Active Directory neue Mitarbeiter im MDM-System an, ohne dass der IT-Verantwortliche aktiv werden muss. Bei bestimmten Ereignissen, die als gefährlich eingestuft sind, reagiert das System automatisch:

Wenn etwa ein Gerät durch Rooting (Umgehen der Sicherheitsmaßnahmen) oder Jailbreak (inoffizielles Entsperren) kompromittiert ist, kann das Programm die Daten löschen und den IT-Sicherheitsverantwortlichen per E-Mail oder SMS benachrichtigen. Ein Mobile Device Management ist auch in der Lage, Geräte unterschiedlicher Hersteller zu verwalten.

Grundsätzlich gibt es zwei Lösungsansätze, die sich hinsichtlich Sicherheit, Verwaltbarkeit und Anwenderfreundlichkeit unterscheiden: ein Mobile Device Management, das weitestgehend konfiguriert wird, oder eine Sandbox-Lösung. Im ersten Fall werden die vom mobilen Betriebssystem zur Verfügung gestellten Optionen verwendet, um die Geräte zu konfigurieren und die Richtlinien für unterschiedliche Betriebssysteme umzusetzen – ähnlich wie ein Domain Controller verschiedene Windows Clients verwaltet und absichert. Das MDM bietet ein Zugangskontrollsystem zur ActiveSync-Schnittstelle der Organisation und bezieht neben der Berechtigung des Benutzers auch den Gerätestatus (Device Compliance Check) in die Entscheidung ein, ob ein Gerät Zugriff auf Daten wie E-Mail, Kontakte und Kalender erhält. Wenn ein Gerät mit einem Jailbreak versehen ist oder verbotene Apps installiert sind, verweigert das Zugangskontrollsystem diesem den Zugriff. Das Sandbox-System dagegen verschlüsselt die Unternehmensdaten separat in einem Container und trennt sie kryptografisch vom Gerät. Diese Lösung bringt eigene Clients mit, die nur über definierte Wege mit anderen Apps interagieren können. Da die Verantwortlichkeiten klar getrennt sind, müssen Betriebssystem und Hardware nicht eingeschränkt werden: Für die Sandbox ist allein der Support zuständig, für das Gerät ist der Benutzer verantwortlich.

Welche Lösung in einer Verwaltung die passende ist, hängt von den vorhandenen Einsatzszenarien ab. Zunächst wird geklärt, ob die Geräte von Mitarbeitern nur intern oder auch extern genutzt werden, etwa im gesamten Stadtgebiet. Welche Beschäftigten die Geräte nutzen und welche Aufgaben diese wahrnehmen, spielt ebenfalls eine Rolle. Ein drittes Kriterium ist die Art der Daten: Handelt es sich um E-Mails, Datenbanken, öffentlich zugängliche Informationen oder auch vertrauliche Papiere? Werden über Anwendungen Daten auf dem Gerät gespeichert? Entscheidend ist darüber hinaus, ob die Mitarbeiter Geräte nutzen, die der Stadt gehören, oder ob jeder sein eigenes, privates Endgerät für den Dienstzweck verwenden darf. Das Schlagwort lautet hier: Bring Your Own Device (BYOD). Ist letzteres der Fall, müssen klare Regeln für die Trennung von Privat- und Organisationsdaten gelten, etwa wer für welchen Part verantwortlich ist, wie bei einem Hardware-Defekt zu verfahren ist und wer die Kosten trägt. Es muss auch geregelt werden, wie bei Verlust oder Diebstahl reagiert wird und ob die Stadt in diesen Fällen die Daten auf dem privaten Gerät des Mitarbeiters löschen darf.

Besondere Aufmerksamkeit verdient das Thema Apps: Welche Software unbedenklich ist und auf einem Gerät installiert werden darf, hängt davon ab, ob durch die Applikation Kontaktdaten des Unternehmens auf externen Servern landen, was etwa bei Social Apps wie WhatsApp und Facebook der Fall ist. Außerdem sollte geregelt werden, ob nur Programme aus den jeweiligen App Stores oder auch proprietäre Anwendungen genutzt werden dürfen und wie auf Daten der internen Infrastruktur zugegriffen werden darf. Es gibt Lösungen, bei denen eine Middleware als Security Layer dient, die Datenquellen der Infrastruktur sicher anbindet und mobilen Endgeräten zur Verfügung stellt.

Eine mittelgroße Stadt im Regierungsbezirk Düsseldorf hat im Oktober 2011 nach einer Lösung gesucht, um die mobilen Endgeräte der Verwaltung managen und im Notfall aus der Ferne löschen zu können. Aufgrund der geringen Anzahl an Geräten – Smartphones (iOS und Android) und Tablets – kam eine Installation in der eigenen Infrastruktur nicht in Frage, man suchte vielmehr nach einer Cloud-Lösung. Die IT-Berater des Unternehmens RDS schlugen eine Managed Mobility für Mobile Device Management vor, welche die Anforderungen der Stadt erfüllte. Die Vorgaben des Personalrats für den Datenschutz wurden berücksichtigt und ein Mandant eingerichtet, der die Sicherheitsrichtlinien und erforderlichen Konfigurationen enthielt. Das System ist intuitiv nutzbar, die IT-Verantwortlichen konnten nach einer halbtägigen Einweisung mit dem Pilottest starten. Bereits im Dezember wurden die ersten Geräte des produktiven Betriebs in der Umgebung ausgerollt.

Thorsten Strauss ist Leiter Competence Center Mobile & Cloud Solutions bei der RDS Consulting GmbH.