

Link: <https://www.computerwoche.de/a/kommunalverwaltung-nutzt-smartphones,2484318>

Strenge BSI-Sicherheitsrichtlinien

Kommunalverwaltung nutzt Smartphones

Datum: 11.01.2011

Autor(en): Johannes Klostermeier

Die Kommunalverwaltung der Landeshauptstadt Hannover hat 200 Führungskräfte und Verwaltungsmitarbeiter mit Smartphones ausgestattet, damit sie sich unterwegs per Mail und Telefon austauschen können. Eine zentrale Management-Lösung vereinfacht Einführung und Support.

□

Foto:

In der Kommunalverwaltung der niedersächsischen Landeshauptstadt **Hannover**¹ (500.000 Einwohner) arbeiten 10.000 Mitarbeiter, davon haben rund 7000 einen PC-Arbeitsplatz. 200 Führungskräfte und Verwaltungsmitarbeiter aus dem Außendienst sind jetzt mit einem **HTC**² Touch Diamond oder HTC Touch Pro 2 unterwegs, die auf dem Betriebssystem Windows Mobile laufen.

Fallende Gerätepreise führten im Laufe der Jahre dazu, dass ein großer Bestand an PDAs mit heterogenen Betriebssystemen in der Kommunalverwaltung eingesetzt wurde, für die das Betreuungs- und Sicherheitskonzept nicht mehr ausreichte. Daher entschloss sich die Verwaltung im Frühjahr vergangenen Jahres mit einer Mobile Device Management-Lösung der Münchener Firma **Ubitexx**³ (Ubi-Suite Version 3.5) eine zentrale Mobile Device Management-Lösung einzuführen, die PDAs und Smartphones mit sicherem Pushmail nach BSI-Vorgaben austatten sollte.

Bei der Landeshauptstadt Hannover stellt das Rechenzentrum die zentrale IT-Infrastruktur und setzt Richtlinien für den sicheren und effizienten Betrieb von IT-Systemen. Die Betreuung der mobilen Geräte liegt in den Händen der Administration aus den Fachbereichen und Ämtern. Das Rechenzentrum leistet hier Second-Level Support.

Projektleiter Detlev Rackow suchte nach einer Lösung, die das zentrale Erstellen der Konfigurationen im Rechenzentrum und das automatisierte Ausrollen mobiler Geräte durch die Administration in den Fachbereichen, Ämtern und Betrieben ermöglicht. „Um einen pflegeleichten Einsatz zu gewährleisten, musste die Mobile Device Management-Lösung von unseren Administrationskräften ohne Spezialkenntnisse bedient werden können“, sagt Rackow, der gleichzeitig Sicherheitsadministrator der Stadt ist. Da die Einführung neuer Technologien dem Grundschutzkatalog des **BSI**⁴ unterliegen, ist das Projekt bei ihm in den richtigen Händen. Neben der technischen Betreuung interner Sicherheitssysteme leitet er zudem den Bereich Mobile Computing.

Sicherheit nach BSI-Grundschutz gefordert

Rackow: „Eine Herausforderung waren die vom Datenschutzbeauftragten geforderten und vom BSI empfohlenen Sicherheitsmaßnahmen für Smartphones. Danach musste die Datenverschlüsselung auf allen PDAs und Smartphones auch mit älteren Windows Mobile Versionen beim automatisierten Rollout sichergestellt werden.“ Geräteausfälle und das Umgehen der kommunalen Sicherheitseinstellungen auf den mobilen Geräten durch die Benutzer galt es zu verhindern.

Im Frühjahr 2009 erfolgte die Implementierung der Suite. Nach der Installation wurde ein einmonatiger Testlauf durchgeführt. Danach wurden die Benutzer in das System aufgenommen. Für jedes Amt und jeden Fachbereich gibt es eine eigene Benutzergruppe, dort sind auch die Konfigurationen für die Benutzergruppen mit Programmen und Einstellungen hinterlegt. Grundsätzlich enthalten alle Benutzerprofile die Einstellungen für das Windows Exchange Pushmail, ein vereinfachtes GUI und umfassende Sicherheitsfunktionen.

Die Sicherheitspolicies gemäß BSI-Grundschutz und sonstiger BSI-Empfehlungen für Smartphones konnte Rackow damit umsetzen. Per Konfigurationsparameter sind Bluetooth, die Internetrouterfunktion und FM Radio deaktiviert, die Windows Mobile 6.1-eigene Geräteverschlüsselung eingeschaltet und das Installieren sowie Deinstallieren von Software durch den Benutzer gesperrt.

Ebenso sind der Benutzerzugriff auf die Registry und andere sicherheitsrelevante Einstellungen der Systemsteuerung gesperrt. Für die einheitliche Umsetzung der Policy auf allen Smartphones und PDAs sorgt die zentrale Plattform. Zu den Sicherheitsrichtlinien gehört auch, dass der Einsatz mobiler Anwendungen zentral genehmigt werden muss. So ist bei den Führungskräften der Verwaltung Google Maps Mobile beliebt; deswegen wurde es zentral ausgerollt.

Bei der Stadt Hannover erhalten die Mitarbeiter sofort einsatzbereite Smartphones vom Administrator. Er entfernt die PIN-Sperre der SIM-Karte, öffnet im Internet Explorer das Provisioning und gibt den Benutzernamen, das Aktivierungspasswort sowie den Domänen-Namen ein. Das Programm installiert und konfiguriert dann automatisiert Software, Einstellungen und Zertifikate auf dem Smartphone. Der Mitarbeiter gibt das Windows-Kennwort ein und kann danach auf seine E-Mails oder Termine zugreifen. Jeder mobile Mitarbeiter kann das Telefon- und Adressbuch der Kommunalverwaltung auf seinem mobilen Gerät nutzen.

Zeitaufwand hat sich halbiert

Vor der Einführung des Mobile Device Management musste die Administration der Landeshauptstadt jedes mobile Gerät manuell aufsetzen. Die Konfiguration kostete zwischen 30 bis 45 Minuten pro Gerät und führte zu Fehlern. Auch die Parallelinstallation mehrerer Smartphones sparte keine Zeit, und die Fehlerquote stieg. Heute werden neue Smartphones nur noch per Mobilfunknetz (OTA) aufgesetzt. Damit entfallen rund 20 Arbeitsschritte.

Benötigt ein Mitarbeiter ein Smartphone, tragen die Administratoren den User Account in die entsprechende Active Directory-Gruppe ein, das Gerät wird bei der Installation automatisch erfasst. Im Rechenzentrum gibt es deswegen nur noch Arbeit, wenn ein neuer Gerätetyp geprüft und zugelassen wird. „Die PIM-Daten liegen zentral auf dem Server und werden auf den Smartphones verschlüsselt vorgehalten. Die Verschlüsselung könne nur durch den rechtmäßigen Benutzer mittels seiner PIN aufgelöst werden.“ Geht ein Gerät verloren, wird es remote in den Auslieferungszustand versetzt. „So können die Daten nicht in fremde Hände geraten“, sagt Rackow.

„Im laufenden Betrieb konnten wir den Zeitaufwand für das Einrichten eines Geräts halbieren. Noch wichtiger sind die gesunkenen Supportzeiten: Die Betreuung erfordert rund fünf Stunden im Monat; vorher war es ein Mann-Tag. Durch die strikte Umsetzung unserer Sicherheitsrichtlinien sind Geräteausfälle aufgrund von Benutzereingriffen selten geworden“, sagt der Projektleiter. Die Mobile Device Management-Lösung habe sich deswegen, so Rackow, für die Stadt Hannover innerhalb von vier bis fünf Monaten bezahlt gemacht.

Korrektur: In der ursprünglichen Überschrift war von Android als Handy-Betriebssystem die Rede. Es handelt sich aber um Windows Mobile. "Mit Android lassen sich nach meiner Einschätzung derzeit unsere Anforderungen an Sicherheit und Gerätemanagement nicht erfüllen", so der Projektverantwortliche Rackow.

Quelle: **CIO**⁵

Links im Artikel:

¹ <http://www.hannover.de/>

² <http://www.htc.com/de/>

³ <http://www.ubitexx.de/>

⁴ https://www.bsi.bund.de/cIn_183/DE/Home/home_node.html

⁵ <https://www.cio.de/public-ict/communication/2233918/index.html>
