Kommunikationstechnik für Profis

funkschau

Ausgabe 17/2012 14. September 2012 € 4,90 sfr 8,90

funkschau.de

IfKom Ingenieure für Kommunikation

Mobile-Office

- Mobile-Device-Management
- BYOD: Bring-Your-Own-Disaster
- UC wird mobil
- Neue Euro-Tarife

ab Seite 14

NGN

Schlüsseltechnologien für zukunftssichere Netzwerke

Seite 32

Profifunk

Migration auf DMR

Seite 40

Bestimmen Sie mit!

Die funkschau Leserbefragung

Seite 44

Mobile-Device-Management

IT-Abteilungen befinden sich im Wandel, denn die Anforderungen an die Infrastruktur haben sich in den letzten Jahren verändert. Unternehmen setzen neben Desktop-Systemen zunehmend mobile Endgeräte ein. Fünf MDM-Anbieter über ihre Lösungen und die Herausforderungen, die die Integration mobiler Endgeräte mit sich bringt.

Von Diana Künstler

Frage 1:

Wie realisieren Sie Mobile-Device-Management bei Ihren Kunden?

Frage 2:

Mit welchen Kosten pro User müssen Unternehmen bei Ihrer MDM-Lösung rechnen?

Frage 3:

Das Thema Sicherheit ist bei neuen IT-Mechanismen allgegenwärtig. Wo liegen die größten Sicherheitslücken beim Einsatz mobiler Endgeräte im Unternehmensumfeld?

Frage 4:

Was sollte ein Entscheider im Unternehmen bei der Umsetzung einer Mobile-Device-Management-Lösung generell beachten?

Frage 5:

Der Trend geht in vielen Firmen zu "Bring your own device" (BYOD), also dass Mitarbeiter ihre eigenen Geräte verwenden wollen. Welche Auswirkungen hat das auf das Mobile-Device-Management?

Andreas Stein,
Managing-Director, Dell Services Deutschland

Dell

Dell setzt auf integrierte Mobile-Device-Managementlösungen wie beispielsweise „KACE" und die von unserem Zukauf Wyse angebotenen Produkte. Bei einzelnen Outsourcing-Kunden haben wir auf deren Wunsch seit längerem spezifische MDM-Lösungen der bekannten Anbieter im Einsatz.

Die Kosten sind nicht nur von der eingesetzten Lösung, dem angestrebten Sicherheitslevel und dem in Anspruch genommenen Service, sondern auch von dem zu betreuenden Gerätevolumen und der Heterogenität der Betriebssysteme abhängig. In der Regel sprechen wir bei einer Total-Cost-of-Ownership-Betrachtung von wenigen Euro pro Gerät und Monat.

Das Device selbst kann je nach eingesetztem Betriebssystem die größte Sicherheitslücke darstellen. Hinzu kommt die Gefahr des Geräteverlusts. Die Datenverschlüsselung ist deshalb genauso notwendig wie die Möglichkeit, die gespeicherten Daten aus der Ferne löschen zu können. Device-Managementlösungen stellen das in der Regel sicher und zwingen die Benutzer in die sinnvollen, aber nicht immer beachteten Sicherheitsmechanismen.

Die Mobile-Strategie bestimmt die Anforderungen an die Device-Managementlösung und die möglicherweise einzukaufenden Dienstleistungen. Eine reine Windows-7-/Windows-8-Umgebung erfordert andere Lösungen als eine BYOD-Umgebung. Im Rahmen von Manged-Services unterstützt Dell alle diese Anforderungen.

Die Anzahl der zu unterstützenden Plattformen treibt den Aufwand im Device-Management – auch wenn die meisten Betriebssysteme zwischenzeitlich von den Lösungen unterstützt werden. Die Frage der Datenhoheit und rechtliche Aspekte beim Fernlöschen eines Mitarbeitergeräts durch Unternehmen werden zur Zeit intensiv diskutiert und erfordern unter Umständen Sonderlösungen.

Michael Melzig,
Senior-Product-Marketing-Manager Business-Clients bei Fujitsu Technology Solutions

Fujitsu

Mit unserem Managed-Service verwalten wir für unsere Kunden ihre Smartphones und decken mit unseren Services den gesamten Lebenszyklus ab. Das gilt unabhängig von Modelltyp und Hersteller, Betriebssystem und Telefonprovider. Fujitsu ermöglicht eine effiziente, sichere Unterstützung und Kontrolle mobiler Geräte bei gleichzeitiger Verbesserung der Transparenz zu optimalen Kosten.

Der Kunde ist gut beraten, ab einer Größenordnung von 5 Euro (zuzüglich Mehrwertsteuer, per Device, per Monat) und den einmaligen Transitionkosten, die von der Mitarbeiterzahl und dem gewünschten Lösungsansatz abhängig sind, zu planen. Über das Self-Service-Portal können Endanwender selbst tätig werden und beispielsweise ihre eigenen Geräte zurücksetzen – sie tragen so selbst zu Kostensenkung bei.

Bedenken bestehen zum ausreichenden Schutz der Unternehmensdaten vor Manipulation, Missbrauch oder Diebstahl. Bei Verlust, Diebstahl oder anderer unbefugter Nutzung eines Geräts kann dieses mit nur wenigen Klicks in Echtzeit außer Betrieb gesetzt werden. Der „Jailbreak" wird erkannt und das betroffene Smartphone solange ausgesperrt aus der Unternehmensinfrastruktur, bis der Auslieferzustand wieder hergestellt ist.

Nur mit einer realistischen Einschätzung kann er aus unternehmerischer Sicht entscheiden: Kann und will er das Verwalten der mobilen Endgeräte noch selber leisten, bei deutlich kürzeren Lebenszyklen der Betriebssysteme und Hardware. Es gilt, „vorher" aus dem ganzheitlichen Ansatz heraus die Fragen zu klären mit der IT-Organisation, Legal, Personalwesen und Betriebsrat: Welche Strategie ist für unser Unternehmen die passende?

Für Kunden und Mitarbeiter ergibt sich ein Portfolio an unterstützen Endgeräten, das keine Wünsche offen lässt. In der Praxis bedeutet das für Freelancer, dass nur die Corporate-Daten des Auftraggebers gelöscht werden und die privat gekaufte Musik auf dem Smartphone erhalten bleibt. Gerade bei BYOD sind die rechtlichen Aspekte im Vorfeld zu klären, dass auch der Zugriff auf das Smartphone für das gerade beschriebene selektive Wipe garantiert ist.

Robert Himmelsbach,
Leitung Geschäftsentwicklung, MPC Mobilservice

MPC Mobilservice

Bei „mobile.dm“ handelt es sich um eine skalierbare Platform-as-a-Service-Lösung aus der Cloud. Damit lassen sich über ein zentrales Webportal Einstellungen, Sicherheits-Policies und Applikationen einer Geräteflotte aus der Ferne ausrollen und steuern – unabhängig von Endgerätetyp oder Betriebssystem. Der Kunde kann das Management seiner Mobilgeräte dabei selbst übernehmen oder an MPC abgeben.

Das Preismodell ist sehr einfach und richtet sich nach einer Preisstaffel je nach Anzahl der Lizenzen. Unser Abrechnungsmodell ist dabei sehr flexibel: Vom Volumen-Modell bis hin zum Prepaid-Paket können wir jeden Kundenwunsch bedienen. Im Lizenzpreis sind sämtliche Kosten enthalten – sogar künftige Updates und Migrationen. Damit gibt es bei uns eine klare Preiszusage, ohne versteckte Kosten.

Neben Apps und deren Management ist vor allem die gemischt privat-geschäftliche Nutzung von Geräten kritisch – hier mangelt es oft sowohl an der Definition und konsequenten Durchsetzung von Sicherheitsrichtlinien als auch an einem ausreichenden Risikobewusstsein der Nutzer. Auch eine fehlende Übersicht zum Compliance-Status der Geräte und deren Softwarestand durch die IT sind bedenklich.

Die Lösung sollte flexibel skalierbar sein und die Integration diverser Gerätetypen und Betriebssysteme ermöglichen. Von Insellösungen ist aufgrund hoher Lizenzkosten und Schnittstellenproblemen abzuraten. Ein Anbieter muss Sicherheit nach europäischem Datenschutzrecht gewährleisten, Folgekosten transparent machen und zudem eine nachhaltige Geschäftsstrategie mit kurzen Entwicklungszyklen bieten.

Das Thema wirft umfassende sicherheitstechnische und juristische Fragestellungen auf – Stichwort Haftung oder Supportzuständigkeiten – und kann den Management-Aufwand der Geräteflotte signifikant erhöhen. Unternehmen sollten das Thema proaktiv angehen, eine Strategie mit klaren Compliance-Prozessen entwickeln und dabei auf eine vertragliche Vereinbarung mit den betroffenen Mitarbeitern setzen.

Marcus Hock,
Consultant für Sicherheitslösungen bei Profi Engineering Systems

Profi Engineering Systems

Die Verwaltung mobiler Endgeräte realisieren wir üblicherweise mit „Sophos Mobile Control“ oder „IBM Tivoli Endpoint Management“. Das hängt vor allem von der Größe und Komplexität der Umgebung sowie den geforderten Management-Funktionen ab.

Die Kosten für „Sophos SMC“ liegen grob zwischen 30 und 50 Euro pro Jahr und Benutzer, je nach Lizenzmodell und Laufzeit. Durch das vergleichsweise einfache Management und das Self-Service-Portal können die laufenden Kosten für den administrativen Aufwand gering gehalten werden.

Die größten Risiken sehe ich im Bereich Malware auf den Endgeräten und Datenverlust durch Verlieren beziehungsweise Diebstahl der Endgeräte. Beide Bedrohungen bergen ein hohes Risiko, bezogen auf Eintrittswahrscheinlichkeit und Schadenshöhe, daher sind die Maßnahmen zur Verringerung dieser Risiken essenzieller Bestandteil einer Mobile-Device-Policy.

Wichtig: Es müssen eine Reihe von Entscheidungen noch vor der Wahl einer MDM-Lösung getroffen werden. Welche Geräte werden eingesetzt, welche Daten transportiert, wie werden Rollout und Management stattfinden. Kurz: Es muss zentral eine Policy definiert werden. Diese wird mit der endgültigen Implementierung eventuell noch angepasst, aber ein MDM-System bleibt immer nur ein Werkzeug zur Durchsetzung einer Policy.

Zunächst einmal wird die Endgeräte-Landschaft zwangsläufig sehr heterogen, mit allen direkten Folgen für Sicherheit und Administration. Hinzu kommen insbesondere Fragen bezüglich der Administrationshoheit, da es natürlich schwierig ist, dem Benutzer Vorschriften bezüglich der Verwendung seines Privateigentums zu machen. So müssen diese organisatorischen Aspekte zunächst vollständig geklärt werden, bevor Firmendaten auf privaten Endgeräten gespeichert werden.

Ferri Abolhassan,
in der Geschäftsführung von T-Systems zuständig für den Bereich Production

T-Systems

So flexibel wie möglich. Wir bieten Kunden zwei Optionen: Erstens ein sofort verfügbares Portal aus der Cloud, mit dem der Kunde seine Endgeräte selbst administrieren kann. Die zweite Option umfasst den Betrieb der Endgeräte über eine dedizierte Infrastruktur von T-Systems. Damit die Infrastruktur die Geschäftsziele perfekt unterstützt, bieten wir professionelle Beratungsleistungen als Basis an.

Das hängt von der Komplexität der Lösung ab und insbesondere vom Umfang der Integration in die Unternehmensprozesse. Die Kosten für die Portal-Lösung für Unternehmen, die ihre Endgeräte selbst verwalten wollen, sind sehr transparent. Jedes Endgerät kostet 6,95 Euro monatlich ab dem ersten Monat, ohne Zusatzkosten für das erste oder nachfolgende Endgeräte.

Ein großes Risiko stellen der Diebstahl von Endgeräten oder Fremdzugriffe dar. Unabdingbar sind daher Compliance- und Datenschutzrichtlinien. Je sensibler die Information, umso ausgefeilter muss das Security-Konzept sein. Unsere Kunden können ihre Unternehmensdaten über unsere zentrale Cloud datenschutzkonform absichern. Ohne Authentifizierung von Nutzer und Endgerät wird der Zugriff verweigert.

Fachbereiche müssen von Anfang an mit genau definierten Nutzungsszenarien eingebunden sein, und ein klares Security-Konzept ist Voraussetzung. Es gilt, frühzeitig zu konkretisieren, wie die ICT-Infrastruktur aussehen soll und in welchem Umfang das Unternehmen diese sowie Endgeräte und Anwendungen selbst betreiben will. Fehlentscheidungen führen schnell zu hoher Komplexität und Sicherheitslücken.

Bei BYOD kommt es auf eine gut balancierte Lösung von Sicherheit und Benutzerkomfort an. Beides als alleiniges Ziel zu „übertreiben“, verfehlt das Thema. Eine solche Plattform erfordert eine gute Produktkonzeption und -architektur. Sie erlaubt es, dem Nutzer seine „gewohnte“ Umgebung bei größter Sicherheit zur Verfügung zu stellen. Das können wir unseren Kunden schon heute anbieten.