Mobile Device Strategy

Wie Sie die richtige Strategie für mobile Endgeräte in ihrem Unternehmen finden

Inhalt

Executive Summary

Warum sich Enterprise Mobility lohnt

Mobiles Arbeiten wird zum zentralen Thema für deutsche Unternehmen. Die „mobile Workforce“ wächst nach Prognosen von IDC jährlich um fünf Prozent[1]. Mitarbeiter mit zeitgemäßen mobilen Endgeräten und Applikationen auszustatten kommt deshalb eine immer wichtigere Bedeutung zu. Für Unternehmen steigt die Notwendigkeit, ein ganzheitliches Mobility-Konzept aufzustellen, das verschiedene Facetten abdeckt. Denn „Enterprise Mobility“ ist weit mehr als der Zugriff auf Firmen-E-Mails vom Smartphone oder Tablet aus. Hinter dem Begriff verbirgt sich vielmehr eine Strategie, Arbeitsabläufe und Anwendungen so zu gestalten, dass sie jederzeit unabhängig vom Zugriffsort oder Endgerät genutzt werden können. Durch diese Flexibilisierung können Unternehmen schneller auf die Anforderungen des Marktes reagieren, Prozesse optimieren und die Arbeitszeit ihrer Mitarbeiter effizient ausnutzen.

Auswahl, Verwaltung sowie Festlegung der Eigentumsrechte von mobilen Endgeräten sind ein wichtiger Bestandteil jeder Enterprise-Mobility-Strategie. Es gilt, den Anforderungen einer veränderten, mittlerweile mobilen Arbeitswelt gerecht zuwerden. Dazu gehört zum einen der Einsatz leistungsfähiger, multifunktionaler Endgeräte, die Dank großen Displays, starker Rechenleistung und langer Akkulaufzeiten mobile Geschäftsanwendungen begünstigen. Zum anderen besteht das Bedürfnis, mobile Endgeräte gleichzeitig privat und geschäftlich zu verwenden, was den Angestellten Flexibilität und Produktivität ermöglicht. Sie müssen nur ein Gerät mit sich führen, sind unter einer Nummer erreichbar und haben sowohl private als auch geschäftliche Daten immer bei sich.

Traditionelle Endgerätestrategien wie COBO (Corporate Owned, Business Only) werden den derzeitigen Anforderungen nicht immer gerecht. Um Anwendern entgegenzukommen und diese bestmöglich im Tagesgeschäft zu unterstützen, sind moderne Lösungsansätze gefragt: Werden Mitarbeiter befähigt, ihre eigenen, privaten Smartphones und Tablets auch beruflich zu nutzen, spricht man vom sogenannten BYOD-Ansatz (Bring Your Own Device). Dem gegenüber steht das COPE-Modell (Corporate Owned, Personally Enabled), bei dem der Arbeitgeber seinen Mitarbeitern Endgeräte zur Verfügung stellt und ihnen auch eine private Nutzung erlaubt. Eine Mischform ist Choose Your Own Device (CYOD). Dabei wählt der Nutzer aus einem Warenkorb das Gerät aus, das am besten zu seinen individuellen Anforderungen passt. Der Arbeitgeber behält sich jedoch Eigentum und Verwaltung vor.

Jeder der drei Ansätze birgt Chancen und Risiken, die sich auf die Enterprise-Mobility-Strategie auswirken. Dabei gibt es keine Musterlösung, die sich über Branchen und Geschäftsmodelle hinweg anwenden lässt. Stattdessen bedarf es einer individuellen, auf die Anforderungen des einzelnen Unternehmens abgestimmten Lösung. Wie sich diese entwickeln lässt, erläutert das vorliegende Whitepaper und liefert damit eine Entscheidungsstütze im Umgang mit mobilen Endgeräten in Unternehmen. Außerdem geht es auf die Möglichkeiten ein, unabhängig vom gewählten Ansatz mit Hilfe der Lösung Samsung KNOX verschiedene Risikofaktoren zu minimieren.

1 „Enterprise Mobility in Deutschland 2013: Strategien und Perspektiven“, IDC, 2013 (bit.ly/1r2PYPh)

Enterprise Mobility – Status Quo

Im Jahr 2015 werden laut IDC über 1,3 Milliarden Beschäftigte – 37,2 Prozent der weltweiten Erwerbsbevölkerung – mobile Computer oder Smartphones nutzen.[2]

Mobilgeräte sind dabei jedoch nicht einfach nur Geräte mit kleinerem Bildschirm, auf denen dieselben Websites oder Anwendungen laufen, wie auf Desktops oder Notebooks. Der Wandel geht wesentlich tiefer: Mit Smartphones und Tablets kommunizieren Menschen immer und überall, nutzen Apps unabhängig von Standort und Uhrzeit und verbinden auch immer öfter berufliches und privates auf demselben Gerät. Fast drei Viertel (71 Prozent) aller Berufstätigen in Deutschland nutzen einer Umfrage des Branchenverbandes BITKOM zufolge privat angeschaffte Geräte für ihre tägliche Arbeit.[3]

Für die Mitarbeiter bedeutet das einerseits zusätzlichen Komfort: Sie können viele Aufgaben bereits auf dem Weg zur Arbeit, im Home Office oder direkt beim Kunden erledigen. Unternehmensanwendungen, die früher nur vom Arbeitsplatz aus zugänglich waren, laufen womöglich auf beliebigen Endgeräten. Arbeitszeit lässt sich so effektiv nutzen.

Auf der anderen Seite stehen große Anforderungen an die Hardware: Jeder Nutzer hat andere Vorlieben, was das Endgerät betrifft. Die Erwartungshaltung gegenüber Unternehmen hinsichtlich neuester Technologie ist mittlerweile so hoch wie nie. Während im privaten Umfeld kurze Produktzyklen und leistungsfähige Geräte praktisch Standard sind, bestimmt im beruflichen Umfeld oft noch ältere Hardware das Bild. Eine Folge dessen ist die sogenannte Consumerization der IT, also ein Vordringen leistungsstarker privater Geräte ins berufliche Umfeld, oftmals begründet durch die eingeschränkten Möglichkeiten durch unternehmenseigene Geräte.

67 Prozent der deutschen Büroangestellten glauben beispielsweise nicht, dass ihr Unternehmen ihnen die nötigen mobilen Geräte für produktives und flexibles Arbeiten von unterwegs bereitstellt. Fast die Hälfte der IT-Entscheider in Deutschland (45 Prozent) räumt ein, dass ihre Abteilung den Bedarf an mobilen Geräten nicht decken kann.[4] Es ist also kaum verwunderlich, dass immer mehr Unternehmen es zulassen oder gar fördern, dass Mitarbeiter ihre eigenen mobilen Geräte an den Arbeitsplatz mitbringen und für berufliche Aufgaben einsetzen. Aus dieser Not wurde eine Tugend, „Bring Your Own Device“ wurde zum Trend der vergangenen Jahre.[5]

Aber auch die Arbeitswelt an sich hat sich verändert. Während früher noch von einer Work-Life-Balance die Rede war, muss man heute von einer Work-Life-Mischung reden. Denn: eine klare Trennung zwischen Arbeitsplatz und privatem Umfeld gibt es mit mobilen Geräten kaum noch. Fast 70 Prozent der Arbeitnehmer in Deutschland erledigen laut des „People Inspired Security Report“ private Aufgaben während der Arbeitszeit, umgekehrt arbeiten aber 77 Prozent in ihrer Freizeit.[6] Gleichzeitig gaben mehr als 40 Prozent der Befragten an, dass sie die Verwendung eines einzigen mobilen Geräts für privates und berufliches produktiver mache.[7]

Dabei spielt es für viele Mitarbeiter keine Rolle, ob der Einsatz privater Geräte von der IT-Abteilung erlaubt ist. 29 Prozent der Angestellten in Europa nutzen ihre privaten Endgeräte für die Arbeit, ohne zu wissen oder darüber nachzudenken, ob sie dies überhaupt dürfen. Vor allem die Generation Y, für die der Umgang mit mobilen Geräten selbstverständlich ist, sieht die Nutzung privater Geräte im Unternehmen nicht nur als Privileg sondern als ihr gutes Recht.[8]

Das bedeutet: Selbst wenn Unternehmen BYOD nicht explizit unterstützen oder den Einsatz privater Geräte sogar verbieten, findet BYOD dennoch statt. Der „People Inspired Security Report“ spricht gar von „Hired Hackers“. Demnach hat mehr als ein Viertel der Befragten schon eigene Hard- oder Software dazu benutzt, um interne Sicherheitsmaßnahmen zu umgehen – beispielsweise um Daten beim Cloud-Storage-Anbieter Dropbox hochzuladen.

Zitiert nach: CIO Playbook: „Wie mobile IT Ihr Unternehmen transformieren kann“, Seite 3 (bit.ly/1Fwg6Gp) | 3 „Mitarbeiter verwenden ihre privaten Geräte für den Job“, Pressinformation des BITKOM, April 2013 (bit.ly/1tI4WuZ) | 4 Laut einer Umfrage von Vanson Bourne im Auftrag von vmware. Befragt wurden 1.500 IT-Entscheider und 3.000 Büroangestellte in Europa in Unternehmen mit 100 – 5.000 Angestellten. (vmw.re/1tI5KjH) | 5 In der Studie „Mobility Management: Does Outsourcing Make Sense?“ vom Dezember 2008 berichtete beispielsweise die Aberdeen Group, dass der Prozentsatz der Unternehmen, die ihren Mitarbeitern gestatten, eigene Mobilgeräte für Arbeitszwecke einzusetzen, im Jahresvergleich um das Vierfache gestiegen sei. (bit.ly/1Dwa8Dp) | 6 Siehe „People Inspired Security Report“, Samsung, Juni 2014. (bit.ly/1vH7HM5, Anmeldung erforderlich). | 7 Siehe „People Inspired Security Report“, Samsung, Juni 2014 (bit.ly/1vH7HM5, Anmeldung erforderlich) | 8 Christiane Pütter: „Deutsche Generation Y besonders BYOD-affin“, in: CIO online (bit.ly/ZEtoPX)

Enterprise Mobility – Status Quo

Für IT-Abteilungen stellt sich die Frage, wie die Anforderungen des Anwenders bestmöglich erfüllt werden können, um den Aufbau einer sogenannten Schatten-IT einzuschränken. Das Projektziel bei der Einführung mobiler Lösungen ist immer, die Mitarbeiter im Tagesgeschäft bestmöglich zu unterstützen und gleichzeitig die IT-Sicherheit sicherzustellen. Denn nur wenn sowohl die Datensicherheit, als auch der reibungslose Zugriff vom jeweils berechtigten Mitarbeiter auf Unternehmensdaten und -applikationen sichergestellt ist, können Unternehmen davon profitieren. Für IT-Abteilungen bedeutet das: Sie benötigen eine durchdachte Strategie, um den Herausforderungen des mobilen Arbeitens zu begegnen und dieses bestmöglich zu unterstützen. Abbildung 1 zeigt Einflüsse und Herausforderungen auf die Mobile Device Strategy von Unternehmen.

So ist eine zentrale Aufgabe einer Mobility-Strategie, geschäftliche Informationen bzw. den Zugriff auf Business-Applikationen auch mobil zur Verfügung zu stellen. Je mobiler Daten jedoch werden, desto konsequenter müssen sie gesichert werden. Dabei muss das Sicherheitskonzept mindestens zwei Bereiche abdecken:

1. Gespeicherte Daten auf mobilen Geräten (Data at Rest)

Verliert ein Mitarbeiter sein Smartphone oder wird es gestohlen, dürfen Unberechtigte dennoch keinen Zugriff erlangen. Dasselbe gilt für gezielte Angriffe von außen durch Hacker oder Malware.

2. Datenübertragung von und zu mobilen Geräten (Data in Transit)

Drahtlose Verbindungen bergen grundsätzlich das Risiko unberechtigten Zugriffs, etwa über öffentliche WLAN-Verbindungen (Hotspots) oder durch ungesicherte Verbindungen auf das Unternehmensnetzwerk.

Herausforderungen für IT-Abteilungen

Verwaltung

- Verwaltung von Endgeräten und Applikationen
- Integration in die bestehende IT-Infrastruktur
- Koordination verschiedener Geräteklassen und Plattformen
- Implementierung adäquater mobiler
- Applikationen
- Auswahl Serviceanbieter und einer globalen Lösung
- Ausfallsicherheit der Geräte und Gewährleistung des Supports

IT-Sicherheit

- Einhaltung nationaler/internationaler Datenschutzrichtlinien
- Einhaltung der Compliance
- Trennung von privaten und geschäftlichen Daten
- Sicherung von Unternehmensdaten auf Geräten und Netzwerken
- Geeignete Maßnahmen bei Geräteverlust/Missbrauch
- Durchsetzung von IT-Richtlinien zur Vermeidung von Fehlverhalten der Anwender
- Sicherer mobiler Zugriff auf Unternehmensdaten und -applikationen

Kosten

- Begrenzte IT-Ressourcen
- Schwierig zu messender Return-on-Investment (RoI)
- Kurze Lebenszyklen mobiler Endgeräte
- Risiko erhöhter Supportkosten durch Heterogenität der Geräte und Plattformen

Mobile Enterprise

Abbildung 1: Einflüsse und Herausforderungen auf die Mobile Device Strategy von Unternehmen

Herausforderungen bei der Wahl der richtigen Mobile Device Strategy

Betriebssystemsicherheit:

Android für den Geschäftseinsatz gewappnet Mit einer passenden Mobility-Strategie können Unternehmen den oben genannten Herausforderungen begegnen. Die Aufgabe der IT ist es dabei, den Anforderungen beider Seiten – also der Anwender und des Unternehmens – gerecht zu werden.

Mehr als jeder zweite Angestellte (57 Prozent) verbringt einer IDC-Umfrage zufolge zumindest einen Teil seiner Arbeitszeit auf Messen, Kundenterminen oder Geschäftsreisen – sprich fernab seines Arbeitsplatzes.[9] Flexible Arbeitsplatzkonzepte wie die Möglichkeit, vom Home-Office aus zu arbeiten, tragen zu dieser Entwicklung bei. Der Ausstattung dieser Mitarbeiter mit mobilen Endgeräten und Applikationen kommt somit eine immer wichtigere Bedeutung zu. Vor dem Hintergrund dieser Entwicklung steigt die Notwendigkeit für Unternehmen, ein Mobility-Konzept aufzustellen, das verschiedene Facetten umfassend abdeckt. Dazu gehört vor allem das Thema Gerätemanagement (Mobile Device Management). In diesem Hinblick ergeben sich für Unternehmen Wahlmöglichkeiten, die mit Vor- und Nachteilen bzw. Zielkonflikten einhergehen und deshalb sorgfältig geprüft werden sollten.

Privateigentum vs. Firmeneigentum

Die grundsätzliche Frage lautet: Wem gehört das Gerät? Oder besser: Wer ist dafür verantwortlich? Können Mitarbeiter ihre privaten Geräte auch für das Unternehmen einsetzen, erwarten sie Unterstützung bei Schwierigkeiten in der Anwendung. Für IT-Abteilungen bedeutet das unter Umständen einen hohen Support-Aufwand, etwa durch unterschiedliche Betriebssysteme, Release-Stände oder Hardware-Restriktionen.
Dem gegenüber stehen geringere Kosten für die Anschaffung von Hardware. Gleichzeitig ergibt sich oft ein geringerer Aufwand für Schulungen oder technische Einweisungen, da die Nutzer in der Regel mit ihren eigenen Geräten bereits vertraut sind. Die Risiken, die beispielsweise mit einer Speicherung von Unternehmensinformationen auf persönlichen Mitarbeitergeräten einhergehen, sind für Firmen allerdings beachtlich.

Flexibilität vs. Sicherheit

Der größte Widerstand gegen mobile Endgeräte – vor allem wenn es sich um private Hardware der Mitarbeiter handelt – rührt von Sicherheitsbedenken her. Unternehmen fürchten Sicherheitslücken, Datenverlust und unautorisierten Zugang zu Unternehmensressourcen. Hinzu kommt Malware, die das Firmennetzwerk über mobile Endgeräte infizieren kann.[10] Grundsätzlich ist die Integration privater Geräte, die nicht unter einem zentralen Management stehen und somit einheitliche Sicherheitsstandards erfüllen, mit Risiken behaftet. Dieses Risiko lässt sich durch den Einsatz von Mobile Device Management (MDM), also einem Programm zur Verwaltung von mobilen Geräten hinsichtlich Sicherheit und Datenverteilung, minimieren. Dadurch wird aber womöglich die Flexibilität der Mitarbeiter bei der Wahl des Endgeräts eingeschränkt.

Konsolidierung vs. Individualität

Nach der bislang meist vorherrschenden – von IT-Abteilungen durchgesetzten – Maßgabe der Geräte-Standardisierung, zeichnet sich nun der Trend zu einer Individualisierung der Geräte ab, vor allem aufgrund höherer Anforderungen der Anwender. Statt einer einheitlichen Hardwarelandschaft sind dabei Plattform-übergreifende, geräteunabhängige Prozesse und Lösungen gefordert. Davon können Unternehmen wiederum profitieren: Über Plattformen, die von verschiedenen Endgeräten und Nutzern gleichermaßen genutzt werden können, können Unternehmen die Möglichkeit schaffen, für Kunden, Mitarbeiter und Lieferanten eng zusammenzuarbeiten oder eine bessere Servicequalität anzubieten.

Rechte vs. Pflichten

Eine Mobility-Strategie bedeutet für Unternehmen auch rechtlich eine Herausforderung auf vielen Ebenen: Angefangen bei den Eigentumsrechten (Wer ist haftbar bei Verlust?), über Datenschutz (etwa nachlässiger Umgang mit sensiblen Daten), Arbeitsrecht (z. B. bestehende Arbeitszeitregelungen) und Persönlichkeitsrechte (Zugriff auf private Informationen wie Fotos), bis hin zu Fernmeldegeheimnis, Lizenz-Management und steuerrechtlich relevanten Fragen (Stichwort „geldwerter Vorteil“).[11] Gleichzeitig verfügen Mitarbeiter über Unternehmens- oder Kundendaten, für die sie beim Einsatz mobiler Geräte die Verantwortung tragen.

2 Enterprise Mobility in Deutschland 2013. Mobile Enterprise Management und Applications im Fokus“, IDC, 2013, Seite 2. (bit.ly/1pwU8ZK) 10 Symantec: „State of Mobility“, Studie zur Datensicherheit, 2012 (bit.ly/1r81uTO). 11 Vgl. Leitfaden „Bring Your Own Device“, BITKOM, April 2013 (bit.ly/1t8XYNu)

Die richtige Strategie entwickeln – Lösungsansätze

„If you don't have a mobile strategy, you don't have a future strategy!"[12]
Eric Schmidt, CEO von Google

Zur Festlegung der Mobility-Strategie müssen die im vorangegangenen Kapitel erörterten Zielkonflikte in Einklang mit der Unternehmensstrategie gebracht werden. Dies hängt von zahlreichen Faktoren ab, etwa Unternehmenszielen, der bestehenden Infrastruktur, den finanziellen und technischen Möglichkeiten oder der Zahl der Mitarbeiter. Als Ausgangspunkt sollte zunächst folgende Frage geklärt werden: „Wem gehört das mobile Endgerät?"

Dabei gibt es drei grundsätzliche Herangehensweisen: Auf den ersten Blick erscheint „Bring Your Own Device" als einfachste Möglichkeit: Jeder Mitarbeiter kann sein eigenes, bevorzugtes Gerät nutzen, das seinen persönlichen Präferenzen entspricht.

Eine weitere Option für Unternehmen ist der sogenannte COPE-Ansatz. Beim Modell „Corporate Owned, Personally Enabled" gehört das Endgerät dem Arbeitgeber, der Mitarbeiter kann es aber auch privat nutzen.

Eine dritte Variante, die Teile aus beiden Ansätzen enthält, ist „Choose Your Own Device" (CYOD). Dabei wählt der Mitarbeiter sein Lieblingsgerät aus einer Produktpalette, die vom Unternehmen vorgegeben ist. Anschaffung und Verwaltung liegen dann im Verantwortungsbereich des Arbeitgebers, die private Nutzung ist – mit Einschränkungen – möglich. Im folgenden werden die drei Ansätze erläutert und die jeweiligen Vor- und Nachteile diskutiert.

Bring Your Own Device (BYOD)

Die Vorteile von BYOD liegen vor allem auf Seiten der Nutzer, aber auch die IT-Abteilungen profitieren davon. So bietet der Ansatz maximale Freiheit bei der Wahl des Endgeräts und der Verwendung im Unternehmen: Die Geräte sind nach den Bedürfnissen der Endanwender eingerichtet, Funktionen und Steuerung bekannt und persönliche Apps installiert. Gleichzeitig bedarf es in der Regel keinerlei Schulungen, da der Anwender mit seinem Gerät ohnehin vertraut ist. Das reduziert meist den Aufwand für die IT. Auf der anderen Seite muss der Mitarbeiter selbst für den Kaufpreis aufkommen und im Verlustfall für Ersatz sorgen.

Gleichzeitig bedeutet BYOD für Unternehmen finanziell eine Erleichterung in Form der Anschaffungskosten. Dem gegenüber stehen zahlreiche Herausforderungen. Die schiere Vielfalt an Geräten macht ein durchgängiges Sicherheitskonzept sehr aufwändig. Zudem ist eine Beschränkung von Applikationen – etwa zur Absicherung gegen Schadsoftware – oft kaum gegeben. Zugriff durch die IT-Abteilung, um beispielsweise verlorene Geräte aus der Ferne zu löschen, sind nur im Einzelfall und mit Zustimmung des Mitarbeiters möglich. Für Unternehmen stellt sich hier zudem das Problem, dass die Bereitstellung von Schnittstellen zu internen Informationssystemen sowie kompatiblen Geschäftsapplikationen mit hohem Aufwand verbunden sind: Sie müssen für verschiedene Betriebssysteme und Versionsstände programmiert werden.

Selbst wenn die Mitarbeiter dem Zugriff des Arbeitgebers durch ein MDM zustimmen und damit eingeschränkte Administrationsrechte auf ihrem Gerät einräumen, sind nicht alle Probleme behoben. So stehen Firmen in diesem Fall vor der Frage der Persönlichkeitsrechte und des Datenschutzes, da die IT-Abteilung möglicherweise Zugriff auf persönliche Informationen des Nutzers erlangt, die nicht durch den Arbeitsvertrag gedeckt sind – etwa private Fotos oder Adressdaten.

Corporate Owned Personally Enabled (COPE)

Anders als bei BYOD verbleiben beim COPE-Ansatz mobile Geräte vollständig im Besitz des Unternehmens – mit allen Rechten und Pflichten. So muss der Arbeitgeber hier die Kosten für die Anschaffung tragen, unabhängig von der Plattform für ausreichend Support sorgen, die Sicherheit der Daten auf dem Gerät garantieren und gleichzeitig die Privatsphäre des Mitarbeiters bei der Verwendung sicherstellen.

12 Olivia Solon: „2013 is the last year you can wait to develop a mobile strategy", in: Wired.co.uk, 3. Oktober 2013 (bit.ly/1yUOYio)

Die richtige Strategie entwickeln – Lösungsansätze

Das Interessante an diesem Ansatz ist: Bevor das Gerät an die Mitarbeiter übergeben wird, hat das Unternehmen das Gerät in seiner Verantwortung und kann so z. B. aktuelle Sicherheitssoftware aufspielen. Das ermöglicht Kontrolle in vielen Bereichen und gleichzeitig eine grobe Steuerung der eingesetzten Endgerätetypen, etwa durch die Vorgabe von Release-Ständen von Betriebssystemen.

Davon abgesehen erlaubt COPE meist weitaus tiefere Eingriffe in die Verwaltung der mobilen Endgeräte und erleichtert damit beispielsweise die Absicherung der Daten. In Kombination mit einem MDM ist hier etwa die Fernlöschung meist einfacher möglich, Richtlinien wie die Vergabe von Passwörtern lassen sich leichter kontrollieren und die Installation bestimmter Apps ausschließen.

Choose Your Own Device (CYOD)

Eine Mischform aus beiden Lösungsansätzen verspricht „Choose Your Own Device". Dieses Modell, bei dem Mitarbeiter aus einer vom Unternehmen festgelegten Palette an Endgeräten ihr Lieblingsmodell aussuchen können, ist in vielerlei Hinsicht gut für den Business-Einsatz geeignet. So haben Arbeitgeber hier etwa die Möglichkeit, sich auf bestimmte Merkmale für die Endgeräte zu fokussieren und damit zum einen die Verwaltung deutlich zu vereinfachen, zum anderen die Risiken innerhalb der Mobility-Strategie zu minimieren.

Mit dem CYOD-Ansatz fallen also viele Herausforderungen automatisch weg, die bei den anderen Ansätzen gegeben sind. Wird als Auswahlkriterium für Hardware beispielsweise die Android-Plattform gewählt, entfällt bereits ein erheblicher Verwaltungsaufwand für andere Betriebssysteme in der IT-Abteilung.

Eine Sicherheitslösung wie Samsung KNOX ermöglicht es zudem, ein durchgängiges Konzept über alle kompatiblen Endgeräte hinweg zu realisieren. Gleichzeitig bietet CYOD noch genügend Spielraum, um Nutzern eine Auswahlmöglichkeit anzubieten.

Übersicht der Lösungsansätze

	BYOD	COPE	CYOD
Wem gehört das Gerät?	Arbeitnehmer	Arbeitgeber	Arbeitgeber
Wer leistet Support?	Arbeitnehmer/-geber	Arbeitgeber	Arbeitgeber
Vorteile	• Volle Flexibilität des Nutzers • bei der Wahl des mobilen Endgeräts • Anschaffungskosten • Mobilitätsgewinn	• Effizientes Gerätemanagement durch standardisierte Geräte • reduzierter Supportaufwand • klare Zuständigkeiten	• Erhöhte Flexibilität bei der Wahl an mobilen Endgeräten • relativ guter Support/Kontrolle • klare Zuständigkeiten
Nachteile	• Potenzielle Sicherheitsrisiken, z. B. durch Schadsoftware • Höherer administrativer Aufwand durch vielfältige Endgeräte und Betriebssystemen	• Vorgegebenes Endgerät erfüllt evtl. nicht alle Anforderungen des Mitarbeiters im geschäftlichen und privaten Kontext	• kostenintensiv • Supportaufwand höher • als bei homogener Flotte • „Neidfaktor" unter Mitarbeitern
Fazit: Praxistauglich?	●●○○○	●●●○○	●●●●○

Abbildung 2: Übersicht der Lösungsansätze für eine Mobility-Strategie im Unternehmen.

Enterprise Mobility Management mit Samsung KNOX

Bestimmte Sicherheitsrisiken beim Einsatz mobiler Endgeräte lassen sich nicht wegdiskutieren: Etwa der unbefugte Zugriff auf lokal gespeicherte Daten bei Verlust oder Diebstahl, das Risiko der Datenübermittlung in ungesicherten Netzen oder die Installation von Apps, über die Schadcode eingeschleust wird. Allerdings geht die Sicherheit im Bereich Mobility weit über die Verwaltung von Endgeräten hinaus: Die Möglichkeit mobiler Geschäftsprozesse muss ebenso berücksichtigt werden wie die Verwaltung von mobilen Inhalten. Application Management ist ein weiterer wichtiger Aspekt. Ein reines MDM hingegen greift meist zu kurz: Lokale Verschlüsselungen auf den Endgeräten wird in der Regel nicht berücksichtigt, die private Nutzung der Geräte lässt sich damit nicht regeln und bleibt daher außen vor.

Statt dessen bedarf es einer ganzheitlichen Lösung, einem Enterprise Mobility Management (EMM), das alle Aspekte hinsichtlich Verwaltung und Sicherheit abdeckt, gleichzeitig für eine Entlastung der IT sorgt und den Anwendern Raum für Produktivität lässt.

Auf diese Aspekte fokussiert sich die EMM-Lösung Samsung KNOX. Sie bietet beispielsweise für kompatible Android-Devices geräteübergreifend die Grundlage für Datensicherheit auf mobilen Geräten und gleichzeitig eine Möglichkeit, private von beruflichen Daten zu trennen. Innerhalb des privaten „Containers“ können Nutzer beispielsweise ungehindert Anwendungen installieren und nutzen.

Samsung KNOX erweitert dabei die Basisfunktionen des Android-Betriebssystems um wichtige Merkmale – beispielsweise eine Datenverschlüsselung auf dem Gerät oder „Secure Boot“, eine Zugriffskontrolle, die beim Boot-Vorgang nicht autorisierte Soft- oder Firmware entdeckt und ausschaltet.

Darüber hinaus dient die Lösung auch der Kontrolle von Applikationen und der sicheren Verbindung zu Unternehmensnetzwerken, etwa via Virtual Private Network (VPN). Die MDM-Funktionalität von KNOX schließlich vereint die Merkmale Sicherheit und Kontrolle zu einer umfassenden Anwendung, mit der Administratoren die Einstellungen und Maßnahmen festlegen können, die zu den Sicherheitsrichtlinien des jeweiligen Unternehmens passen. Dadurch schafft Samsung KNOX die Möglichkeit, den Verwaltungsaufwand für den effektiven Einsatz mobiler Endgeräte im Unternehmen deutlich zu reduzieren und gleichzeitig die notwendigen Sicherheitsanforderungen an Daten und Anwendungen zu erfüllen.

Mehr Informationen zum Thema finden Sie in den Whitepapers „An Overview of Samsung KNOX“[13] und „Meeting Evolving Mobility Challenges with Samsung KNOX“[14] oder unter **www.samsungknox.com**

13 „An Overview of Samsung KNOX“, Samsung, 2013, (bit.ly/ZMsnFL)
14 „Meeting Evolving Mobility Challenges with Samsung KNOX“, Samsung, 2013 (bit.ly/1vH2MKX)

Fazit

Mobiles Arbeiten ist bereits heute ein zentrales Thema für Unternehmen.
Immer mehr Mitarbeiter gehen ihrer Tätigkeit unabhängig von festen Arbeitsplätzen nach, der Bedarf an mobilen Lösungen zur Verbesserung von Geschäftsprozessen wächst. Mobile Lösungen sind dadurch eine zentrale Aufgabe geworden, um ein produktives und effizientes Arbeiten von überall zu ermöglichen.

Gleichermaßen stehen auch Sicherheitsaspekte im Zusammenhang mit dem mobilen Arbeiten im Fokus. Beispielsweise beim Verlust von Endgeräten, dem Zugriff auf Unternehmensinformationen über unsichere Netze oder der Durchsetzung von Richtlinien. Die Vielfalt an mobilen Geräten und Betriebssystemen ist für die IT nach wie vor eine große Herausforderung. Zum einen hinsichtlich deren Verwaltung, aber auch im Hinblick auf die Entwicklung und Bereitstellung von Applikationen.

Die drei Ansätze Bring Your Own Device (BYOD), Company Owned Personally Enabled (COPE) und Choose Your Own Device (CYOD) ermöglichen eine grundlegende strategische Abgrenzung hinsichtlich des Eigentums und der Verwaltung mobiler Geräte, die jeweils unterschiedliche Vor- und Nachteile mit sich bringen. Grundsätzlich lässt sich sagen, dass die Risiken und Herausforderungen mit zunehmender Hersteller und Betriebssystem-Diversifizierung ansteigen. Für Unternehmen sollte deshalb eine einheitliche Plattform für alle Geräte im Fokus stehen. Eine zusätzliche Sicherheitslösung, wie etwa Samsung KNOX, bietet dann genügend Möglichkeiten, mobile Geräte, zu verwalten, abzusichern, und den Mitarbeitern gleichzeitig ausreichend Freiheit bei der Wahl des passenden Endgeräts zu lassen. Gleichzeitig kann sich die IT-Abteilung durch die gewonnene Entlastung stärker auf ihre neue Kernaufgabe fokussieren: der Mobilisierung von Geschäftsprozessen.

Haben Sie Fragen zu Ihrer Mobile Device Strategy oder möchten Sie Näheres zum Produktangebot von Samsung erfahren? Dann wenden Sie sich gerne per E-Mail an das Team von Samsung Enterprise Solutions: enterprisesolutions@samsung.de

Mehr Informationen unter www.samsungknox.com/de

Rechtliche und weiterführende Informationen

Über Samsung Electronics

Samsung Electronics Co. Ltd. inspiriert Menschen und gestaltet die Zukunft mit Ideen und Technologien, die unser Leben verbessern. Das Unternehmen verändert die Welt von Fernsehern, Smartphones, Wearable Devices, Tablets, Displays, Haushaltsgeräten, Druckern, medizintechnischen Geräten, Netzwerksystemen, Halbleitern und LED-Lösungen. Entdecken Sie die neuesten Nachrichten, Hintergrundinformationen und Pressematerialien auf **samsung.de** und im Samsung Newsroom unter **news.samsung.com**

Samsung Electronics GmbH
Am Kronberger Hang 6
65824 Schwalbach/Taunus
Info: 0180 6 726 78 64* oder 0180 6 SAMSUNG*
Fax: 06196 934 02 88

* 0,20 €/Anruf aus dem dt. Festnetz,
aus dem Mobilfunknetz max. 0,60 €/Anruf
(aus dem Ausland abweichend)

SAMSUNG