Bild: apinan / Fotolia.com

Private Phones – professionelle Probleme

Private Geräte im beruflichen Alltag zu nutzen, ist längst keine Seltenheit mehr. Arbeitgeber versprechen sich dadurch mobilere und effizientere Mitarbeiter. Für IT-Verantwortliche bedeutet dies jedoch in erster Linie mehr Aufwand und Fehlerquellen. Worauf zu achten ist, sagen Experten von Abraxas, Comsoft Direct, Nomasis, Novalink, Schaefer und Sophos. Interviews: Coen Kaat

Alen Sulejmanagic
Leiter Mobile & Workplace Transformation, Abraxas Informatik

Wie haben sich die Anforderungen an IT-Verantwortliche bezüglich mobiler Geräte in den vergangenen Jahren geändert?
Alen Sulejmanagic: Die Consumerization – sprich der Trend, dass private Geräte immer häufiger im Berufskontext verwendet werden – hat in den letzten Jahren stark zugenommen. Für IT-Verantwortliche ist dies immer eine Gratwanderung zwischen Sicherheit und Benutzerfreundlichkeit.

Worauf kommt es beim Enterprise Mobile Management besonders an?
Unsere Erfahrung bei verschiedenen Kundenprojekten zeigt, dass eine mobile Strategie zentral ist: Welche Use Cases müssen abgedeckt werden? Welche Geräte will man unterstützen? Welche Business-Apps sollen integriert werden? EMM ist hier das Tool, das diese Prozesse unterstützt.

Benutzerfreundlichkeit oder IT-Sicherheit – was wiegt bei Enterprise Mobile Management schwerer?
EMM kann beides abdecken. Je nach Businesskontext überwiegt das eine oder das andere. Wie es abgedeckt wird, ist eine reine Frage der Konfiguration. Wird der Sicherheitsaspekt höher gewichtet, können zum Beispiel mehrere PIN-Abfragen konfiguriert werden: Auf dem Gerät, beim Zugriff auf den Geschäftsteil und auf einzelnen Applikationen selbst.

Wo liegen die Chancen für IT-Dienstleister?
Spannend wird es dort, wo es um die Integration von Apps geht. Das ist der grosse Vorteil von Abraxas: Wir stellen nicht nur Infrastruktur und Betrieb von EMM sicher, sondern entwickeln für unsere Kunden auch eigene mobile Fachapplikationen entlang ihrer Businessprozesse. Wir bieten dieses verzahnte Know-how. Beispielsweise bei der Fahrzeuginspektion, wo Felddaten via Mobile erfasst und direkt mit der Fachlösung synchronisiert werden können.

Wie müssen IT-Dienstleister aufgestellt sein, um EMM optimal anbieten zu können?
Infrastrukur und Betrieb sind die Basis, die ein Dienstleister bieten muss. Den Mehrwert fürs Business erzielt man aber mit dem Applikationslayer. Dort – bei der Integration von Apps – sind die Fachkompetenzen und Skills rar. Und dort kann man als EMM-Anbieter aus dem Feld von Mitbewerbern herausstechen.

Stefan Walter
Key Account Manager, Schaefer

Wie haben sich die Anforderungen an IT-Verantwortliche bezüglich mobiler Geräte in den vergangenen Jahren verändert?
Stefan Walter: IT-Verantwortliche müssen sich aktiv mit Informationsschutz und Datensicherheit beschäftigen. Denn vor allem bei mobilen Geräten gibt es eine Vielzahl von Angriffspunkten. So sind heute bereits viele unternehmenskritische Daten auf mobilen Geräten gespeichert und können ohne entsprechende Schutzmassnahmen, relativ einfach abgegriffen werden. Dies kann zu groben Datenschutzrechtsverletzungen sowie zu Verlust von immateriellen Gütern führen.

Worauf kommt es beim Enterprise Mobile Management besonders an?
Die Anschaffung und Integration einer EMM-Lösung ist schnell erfolgt. Eine ganzheitliche Integration mobiler Endgeräte verlangt aber unweigerlich ein mobiles Arbeitsmodell mit entsprechenden Verhaltensempfehlungen als auch den Einsatz von Sicherheitstechnologien. Ohne diese Grundlagen sind Gefahren jeder Art Tür und Tor geöffnet.

Benutzerfreundlichkeit oder IT-Sicherheit – was wiegt bei Enterprise Mobile Management schwerer?

Beides muss in einem hohen Grad gewährleistet sein. Mit der richtigen EMM-Lösung stellt sich die Frage «Benutzerfreundlichkeit oder IT-Sicherheit» nicht. Die Schwierigkeit liegt eher bei der Balance zwischen User Privacy und IT-Sicherheit.

Wo liegen die Chancen für IT-Dienstleister?
Viele KMUs müssen zum Beispiel aus Gründen verschärfter Datenschutzbestimmungen oder Gefahren vor Datenklau ein EMM einführen. Wer sich mit EMM auskennt oder einen geeigneten Partner hat, kann diese Kundenbedürfnisse befriedigen und so in ein neues Geschäftsfeld expandieren.

Wie müssen IT-Dienstleister aufgestellt sein, um EMM optimal anbieten zu können?
EMM anzubieten bedeutet, wie bei allen Geschäftsbereichen auch, die richtigen Leute oder Partner an Bord zu haben. Ein EMM-Projekt umzusetzen, braucht entsprechend Ressourcen und sehr gute Planungsfähigkeiten. Eine ganzheitliche und langfristige Integration eines EMM-Systems braucht eine ganzheitliche Herangehensweise auf organisatorischer und technischer Ebene. Da muss ein breites Know-how vorhanden sein.

Beat Brunschwiler
Head of Services, Comsoft Direct

Wie haben sich die Anforderungen an IT-Verantwortliche bezüglich mobiler Geräte in den vergangenen Jahren verändert?
Beat Brunschwiler: Die Vielzahl der Endgeräte hat sich drastisch verändert. Tablets und Smartphones sind geschäftlich sowie privat im Einsatz. Die Mobilität ist ein stetig wachsender Arbeitsansatz in allen Unternehmen und fordert die Unternehmens-IT ständig. Vom Einsatz der Mittel, sprich von der Unternehmensstrategie bis hin zum Rollout von Lösungen und Geräten – das Thema Security wird uns in den nächsten Jahren enorm beschäftigen. Die Kontrolle und Steuerung der Geräte für geschäftliche Unternehmensdaten oder auch privat genutzte Geräte mit solchen Zugriffen müssen zwingend geschützt sein.

Worauf kommt es beim Enterprise Mobile Management besonders an?
Eine Mobile-Device-Management-Strategie im Unternehmen zu haben, ist eine Grundvoraussetzung. Diese beinhaltet auch Mobile-, Content-, Identity- und Access-Management. Damit wird sichergestellt, dass Mitarbeiter von überall Aufgaben angehen und Anwendungen nutzen können.

Benutzerfreundlichkeit oder IT-Sicherheit – was wiegt bei Enterprise Mobile Management schwerer?
Keine einfache Frage, wenn ich unkritische Daten verwenden will, gilt sicher der Anspruch der Benutzerfreundlichkeit. Bei sensitiven Daten gilt es, diese bestmöglich zu schützen. Zusätzlich möchten wir mit EMM den Workload des Mitarbeitenden reduzieren und verbessern. Daher gilt die Regel, erstens die Daten zu klassifizieren und zu priorisieren. Dann sind Sie in der Lage die Daten nach Benutzerfreundlichkeit für Anwender und IT-Sicherheit für das Unternehmen ausgewogen bereitzustellen.

Wo liegen die Chancen für IT-Dienstleister?
In der Ausbildung der Mitarbeiter sich den verschiedenen oben erwähnten Themen in der Tiefe zu widmen. Zusätzlich ist es wichtig, einen gutes Know-how in den unterschiedlichen Industriesegmenten zu haben, da die Ansprüche der Segmente sehr verschieden sind. Denken Sie an ein führendes Hochtechnologieunternehmen, das selbst entwickelt, versus eine Marketingfirma als Zielsegment. Der Umgang mit Daten und der Einsatz der Technologien sind sehr unterschiedlich. Zusammenfassend kann gesagt werden, dass die Mitarbeiter mit fachspezifischer Ausbildung und Know-how das Kapital der Zukunft sind.

Wie müssen IT-Dienstleister aufgestellt sein, um EMM optimal anbieten zu können?
Mit einer nahen Präsenz zum Kunden und mit Fachspezialisten für die oben genannten Bereiche. Diese haben sich nicht sonderlich verändert, aber der Umstand der technologischen Mittel und die wachsende Kriminalität im Umgang mit Daten. Dem Rechnung tragen zu dürfen, ist die Veränderung für die kommenden Jahre.

Martin Blattmann
Leiter Engineering und Support, Nomasis

Wie haben sich die Anforderungen an IT-Verantwortliche bezüglich mobiler Geräte in den vergangenen Jahren verändert?
Martin Blattmann: Vor einigen Jahren lag der Fokus vor allem auf der Synchronisation der PIM-Daten – etwa Mail, Kontakte und Kalender. Heute werden viel mehr «Line of Business»-Apps verteilt. Damit kommen auch immer mehr geschäftsrelevante Daten auf mobile Geräte, die nicht nur administriert, sondern auch gesichert werden müssen. Auch die neue Datenschutz-Grundverordnung der EU birgt neue Herausforderungen. Zudem muss durch den häufigeren Zugang zu Cloud-Services gewährleistet sein, dass nur freigegebene Apps von administrierten und authorisierten Geräten genutzt werden können.

Worauf kommt es beim Enterprise Mobile Management besonders an?
Damit Smartphones und Tablets erfolgreich im Unternehmen etabliert werden können, müssen die Businessprozesse und Apps unter Einhaltung der Sicherheit benutzerfreundlich sein.

Benutzerfreundlichkeit oder IT-Sicherheit – was wiegt bei Enterprise Mobile Management schwerer?
In erster Linie ist das Kundenbedürfnis abzuwägen. Grundsätzlich gilt, dass die Sicherheit nicht auf Kosten der Benutzerfreundlichkeit erfolgen soll. So ist beispielsweise mit der Nutzung von Zertifikaten die Authentifizierung an einen Dienst gewährleistet, ohne dass der Benutzer ein Passwort eingeben muss.

Wo liegen die Chancen für IT-Dienstleister?
Die Chancen liegen im spezifischen Wissen, das es für das EMM braucht. Ob die Lösung direkt beim Kunden oder in der Cloud betrieben wird, hängt von den Bedürfnissen an Verfügbarkeit, Sicherheit und Funktionalität ab. Eine EMM-Lösung muss so integriert sein, dass Prozesse möglichst einfach und automatisiert abgebildet werden können. Letztlich soll die mobile IT-Umgebung während der ganzen Betriebszeit optimal unterhalten werden. Entsprechend bieten sich mit Managed-Service-Angeboten weitere Geschäftsfelder.

Wie müssen IT-Dienstleister aufgestellt sein, um EMM optimal anbieten zu können?
Es braucht breites Systemwissen in den Bereichen Exchange, Active Directory, Zertifikate, Microsoft und Google Cloud Service, Informationssicherheit, Android und iOS. Der Markt ist sehr dynamisch und tiefes IT-Wissen auf der IT-Infrastrukturseite, Cloud-Services wie Google Cloud, Microsoft Azure sowie im Bereich Smartphones und deren Schnittstellen und Sicherheitsmechanismen sind unumgänglich. Das Angebot sollte Dienstleistungen von der Beratung über die Konzeption und Integration bis hin zu fundierten Managed Services umfassen. Ohne grosse IT-Erfahrung und entsprechenden Services ist es eine Herausforderung, die Komplexität von EMM richtig anzubieten und die Erwartungen von Unternehmen zu erfüllen.

Zekeria Oezdemir
CTO, Novalink

Wie haben sich die Anforderungen an IT-Verantwortliche bezüglich mobiler Geräte in den vergangenen Jahren verändert?
Zekeria Oezdemir: Mitarbeiter haben das Bedürfnis, von unterwegs zu arbeiten, und das auf mobilen Geräten wie Tablets, Smartphones oder eigenen, nicht von den Unternehmen verwalteten Geräten. Die grosse Herausforderung ist deshalb, dies auf eine sichere Art und in Einklang mit den Sicherheitsanforderungen des Unternehmens zu erledigen. Der Schutz mobiler Geräte wird seit 20 Jahren gewährleistet und ist sozusagen Alltag. Der Fokus liegt heute auf dem garantierten Schutz von Firmendaten und der komfortablen Anwendung für den Mitarbeiter.

Worauf kommt es beim Enterprise Mobile Management besonders an?
Für EMM-Hersteller sind Innovationen im Bereich der Integration von Back-end-Systemen sowie die Bereitschaft, neue Technologien von Google, Microsoft, Samsung und Apple möglichst schnell zu adaptieren und zu integrieren, zukunftsentscheidend. Die Welt dreht sich im Bereich Mobility sehr schnell, und die Entwicklungszyklen werden immer kürzer. Als EMM-Partner ist es wichtig, sein Handwerk zu verstehen und als Visionär den Kunden auf die Zukunft vorzubereiten und die mögliche Richtung vorzugeben. Dies gelingt nur mit Know-how-Transfer und Beratung beim Kunden direkt vor Ort.

Benutzerfreundlichkeit oder IT-Sicherheit – was wiegt bei Enterprise Mobile Management schwerer?
Mit der richtigen Lösung ist beides machbar. Der Kunde wählt die Lösung, die für ihn am besten passt. Die Entscheidung ist sehr davon abhängig, wie eine Firma aufgestellt ist und wo die speziellen Anforderungen liegen. Jede moderne EMM-Lösung kann sowohl Komfort und als auch Sicherheit bieten.

Wo liegen die Chancen für IT-Dienstleister?
Mit EMM-Systemen werden heutzutage hauptsächlich Android- und iOS-Geräte verwaltet. Diese Betriebssysteme haben sich in den letzten Jahren zu den Marktführern bei mobilen Geräten entwickelt. Der Trend zu leistungsfähigeren mobilen Geräten steigt immer weiter und dank «Modern Management» im Bereich Windows 10 übernehmen EMM-Systeme zukünftig die Verwaltung aller mobilen Geräte. Gartner geht davon aus, dass im Jahre 2022 etwa 30 Prozent der firmeneigenen Windows-10-PCs mit EMM-Lösungen verwaltet werden. Deshalb ist es wichtig, dass IT-Fachhändler den Anschluss nicht verpassen.

Wie müssen IT-Dienstleister aufgestellt sein, um EMM optimal anbieten zu können?
Es ist essenziell, sich als traditioneller IT-Fachhändler weiterzuentwickeln. Wer nur reagiert, verpasst den Anschluss. IT-Dienstleister, die EMM-Systeme anbieten, benötigen nicht nur Profiwissen in der EMM-Software, sondern auch Wissen im ganzen Umfeld: Android Enterprise, Modern Management, Apple DEP, Samsung Knox, Microsoft-Technologien wie Azure, Intune App Protection Policies, Identifity-Themen und allgemeine Security-Themen, um hier nur einige zu nennen. Es reicht heutzutage nicht aus, sich nur mit der EMM-Software auszukennen, sondern es ist notwendig, auch den persönlichen Service beim Kunden anzubieten. Ein weiterer wichtiger Punkt ist zusätzlich die Projektbegleitung, der Betrieb und die professionelle Unterstützung im Supportfall sowie die Weiterentwicklung der Mobility-Strategie des Kunden.

Michael Veit
Technology Evangelist, Sophos

Wie haben sich die Anforderungen an IT-Verantwortliche bezüglich mobiler Geräte in den vergangenen Jahren verändert?
Michael Veit: Anfangs ging es Unternehmen bei Mobilgeräten um die klassischen Mobile-Device-Management-Funktionen wie die Verwaltung von Apps und Geräteeinstellungen sowie das Löschen der Gerätedaten bei Verlust oder Diebstahl. Im Zuge von Bring your own Device und Compliance-Anforderungen zum Datenschutz wurde MDM zu Enterprise Mobility Management mit dem Fokus auf der Trennung privater und geschäftlicher Daten. Ausserdem sollte die Compliance des Geräts beim Zugriff auf Unternehmensdaten sichergestellt werden. Die Zielplattformen bei MDM und EMM waren die klassischen Mobilplattformen wie iOS, Android und Windows Mobile. Da BYOD und mobiles Arbeiten in immer mehr Unternehmen auch Desktop-Plattformen wie MacOS und Windows 10 einbezieht, verschieben sich aktuell die Anforderungen von EMM hin zu Unified Endpoint Management, das zusätzlich die Verwaltung von Desktop-Betriebssystemen ermöglicht.

Worauf kommt es beim Enterprise Mobile Management besonders an?
Heute sind Unternehmen vor allem daran interessiert, den Verwaltungsaufwand für IT-Sicherheitslösungen so gering wie möglich zu halten und zudem IT-Prozesse zu automatisieren. Der traditionelle Best-of-Breed-Ansatz, bei der unterschiedliche Konsolen für die Verwaltung von Endpoints, Servern, Mobilgeräten, Firewalls, E-Mail oder WLAN zum Einsatz kamen, ist heute nicht mehr zeitgemäss. Unternehmen wollen eine einzige Verwaltungsplattform, in der zentral Richtlinien für die Benutzer definiert und auf allen Geräten und Plattformen nahtlos umgesetzt werden. Für die Automation von IT-Sicherheit müssen alle Geräte eines Unternehmens heute zudem als System agieren und miteinander kommunizieren, damit beispielsweise ein Smartphone, das sich einen Virus eingefangen hat, automatisch aus dem Unternehmens-WLAN und -VPN ausgesperrt wird.

Benutzerfreundlichkeit oder IT-Sicherheit – was wiegt bei Enterprise Mobile Management schwerer?
In der Vergangenheit wurde die Trennung geschäftlicher und privater Daten oft über Container oder separate Apps realisiert, wodurch etwa bei eingehenden Anrufen nicht der Name des Kontakts sichtbar war. Heute bieten aktuelle iOS- und Android-Versionen die Trennung geschäftlicher und privater Daten mittlerweile ab Werk ohne solche Komforteinbussen. Insofern stellt sich die Frage nach der Benutzerfreundlichkeit oder IT-Sicherheit nicht mehr – im Gegenteil: Aktuelle UEM-Lösungen in Kombination mit aktuellen Mobilbetriebssystemen bieten beides.

Wo liegen die Chancen für IT-Dienstleister?
Unternehmen sind zunehmend daran interessiert, IT-Services auszulagern, und die IT-Sicherheit im Allgemeinen und UEM im Speziellen eignen sich hervorragend dafür. Gerade für kleine Unternehmen, die sich kein eigenes EMM/UEM plus Softwareverteilung leisten wollen, können Systemhäuser diese Dienstleistung als Managed Service Provider bereitstellen. Das Thema UEM eignet sich sehr gut für Systemhäuser als ersten Schritt vom Verkauf von Produkten zum Bereitstellen von Dienstleistungen als MSP. Es schafft ausserdem die Basis für den MSP, mit geringem Aufwand weitere Services zu verkaufen, da der bereits per UEM verwaltete Agent auf den Kundengeräten direkt zum Ausrollen weiterer Dienste wie Endpoint-Schutz, Verschlüsselung etc. genutzt werden kann.

Wie müssen IT-Dienstleister aufgestellt sein, um EMM optimal anbieten zu können?
Für den klassischen Verkauf von EMM/UEM als Produkt wird – wie bei allen IT-Sicherheitslösungen – die technische Expertise bei der Beratung und Implementierung benötigt. Wenn jetzt auch MSP-Dienstleistungen angeboten werden sollen, dann müssen Systemhäuser hierzu oft komplett neue Strukturen in organisatorischer und personeller Hinsicht aufbauen. Der Vertrieb von MSP-Dienstleistungen unterscheidet sich deutlich vom Verkauf von Hard- und Software, ebenso muss für den technischen Betrieb ein 24/7 erreichbares SOC aufgebaut werden. Der Schritt zum MSP erfordert für Systemhäuser meist hohe Investitionen, bietet aber die Chance auf langfristige Kundenbindung und sehr gute Cross-Selling-Potenziale.