SOPHOS
Security made simple.

Die ersten Schritte mit Enterprise Mobility Management

Übersicht

Mobile Geräte haben sich längst zum unverzichtbaren Business Tool entwickelt und ermöglichen, dass Mitarbeiter von überall aus flexibel und produktiv arbeiten können. Da jedoch immer mehr E-Mails und Unternehmensdaten auf mobilen Geräten abgerufen und verarbeitet werden, steigt auch die Gefahr von Datenverlusten. Deshalb suchen viele Unternehmen nach Enterprise Mobility Management (EMM) Lösungen, mit denen sie Unternehmensdaten auf mobilen Geräten schützen können, ohne die Produktivität der Mitarbeiter zu beeinträchtigen. In diesem Whitepaper beschäftigen wir uns mit mobilen Arbeitstrends und den Herausforderungen, die diese für heutige Unternehmen mit sich bringen. Außerdem erklären wir die Vorteile von EMM-Lösungen und geben praktische Tipps zum Schutz von Daten auf mobilen Geräten.

Sophos Whitepaper März 2016

Mobile Geräte überall

Mobile Geräte sind die Endpoints, die uns im Bereich IT-Sicherheit vor die größten Herausforderungen stellen. Immer mehr E-Mails werden auf mobilen Geräten abgerufen und verarbeitet.[1]

Der Forrsights Workforce Employee Survey[2] zufolge nutzen 74 % der datenverarbeitenden Angestellten zur Erledigung ihrer Arbeit mindestens zwei Geräte, u. a. Desktops, Laptops, Smartphones und Tablets. Ein anderer Bericht von Strategy Analytics[3] geht davon aus, dass die Anzahl der pro Person verbundenen Geräte bis 2020 auf 4,3 ansteigen wird. Multipliziert man dann noch die Anzahl der Geräte mit der durchschnittlichen Anzahl der von einem typischen Benutzer genutzten Apps, fällt es schwer, den Überblick zu behalten. Es ist daher höchste Zeit, den Umgang mit mobilen Technologien in Ihrem Unternehmen zu überdenken.

Die Anzahl der pro Person verbundenen Geräte soll bis 2020 auf 4,3 ansteigen.

Unternehmen dürfen die Gefahren, die mit der mobilen Produktivität einhergehen, nicht ignorieren.

Die Umfrage „2015 Mobile Trends in the Workplace“ von theEMPLOYEEapp offenbart:

- 55 % aller Angestellten unternehmen Geschäftsreisen und 40 % arbeiten nicht in einer traditionellen Büroumgebung.

Welche Konsequenzen ergeben sich hieraus? Wie bleiben diese Angestellten mit ihrer Arbeitsumgebung verbunden?

- Der Umfrage zufolge nutzen 49 % Mobiltelefone und 28 % Tablets, um mit ihrer Arbeitsumgebung verbunden zu bleiben.

„NEIN“ ist keine Antwort – Mobilität und Mitarbeiterzufriedenheit sind untrennbar miteinander verbunden

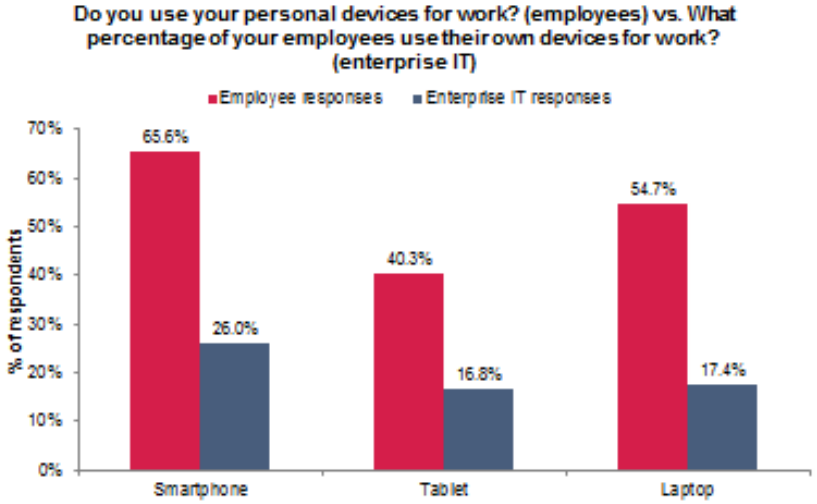
Tools wie Cloud-Speicher können Risiken bergen.

Ihre Mitarbeiter sind längst integraler Bestandteil der stetig wachsenden Community versierter App-Konsumenten, die ihre ganz individuelle Zusammenstellung mobiler Apps nutzen, um ihr Privatleben besser zu organisieren. Eine einzige Unachtsamkeit kann jedoch die vielen positiven Aspekte der Mobilität mit einem Schlag zunichte machen und Unternehmen ernsthaft gefährden. Tools wie Cloud-Speicher bergen zum Teil erhebliche Risiken. Zwar sind Speicherdienste, Apps und Tools hilfreich, da Mitarbeiter über sie schneller auf Unternehmensinformationen zugreifen und so mehr Aufgaben erledigen können. Gleichzeitig erhöhen sie jedoch das Risiko, Opfer eines Angriffs zu werden. Unternehmen müssen sich der neuen Realität stellen: Auch wenn damit Risiken verbunden sind – ein einfacher und komfortabler Zugriff auf Unternehmensdaten fördert die Motivation und die Produktivität der Mitarbeiter[4]:

- 62 % der Angestellten geben an, dass ein einfacher Zugriff auf Unternehmensdaten sich direkt auf ihre Arbeitszufriedenheit auswirkt.
- 51 % sind produktiver, wenn sie arbeitsrelevante Materialien über ein mobiles Gerät abrufen können.

Was die IT nicht weiß, kann nicht gefährlich sein für uns

Umfragen von Ovum aus dem Jahr 2014, bei denen über 5.000 Angestellte und mehr als 2.700 IT-Manager befragt wurden, zeigen ein klares Ungleichgewicht zwischen Informationsstand des Arbeitsgebers und realem Arbeitnehmerverhalten im Bereich Mobilität. Während tatsächlich 65,6 % der Angestellten ihr Smartphone beruflich nutzten, gingen die jeweiligen IT-Abteilungen nur von einem Anteil in Höhe von 26 % aus. Dies deutet auf eine hohe Diskrepanz zwischen Realität und subjektiver Warnehmung hin.



Source: Ovum Employee Mobility Survey 2014 (N=5,187), Ovum ICT Enterprise Insights Survey 2014 (N=2,708)

In einer weiteren Studie mit dem Titel „The Security Impact of Mobile Device Use by Employees“, die im Januar 2015 vom Ponemon Institute (gesponsert von Accellion) durchgeführt wurde, räumten alarmierende 66 % der Befragten ein, schon einmal mobile Apps ohne die Zustimmung ihres Arbeitgebers heruntergeladen zu haben. Zudem vergewisserten sich nur 19 % dieser Mitarbeiter, dass die Apps keine Viren oder Malware enthielten, und nur 22 % waren der Meinung, dass ein solches Verhalten eine Gefährdung für ihr Unternehmen darstellen könnte.

Viele Mitarbeiter setzen die Sicherheit ihrer Unternehmen aufs Spiel und IT-Abteilungen bekommen das Ausmaß der Gefährdung zunehmend zu spüren. Eine weltweite Befragung von InsightExpress deckt auf, dass 70 % aller IT-Experten nicht autorisierte Programme in ihren Unternehmen für die Hälfte der dort vorgefallenen Datenverluste verantwortlich machen. Und Datenverluste sind nur eine von vielen Sicherheitsgefahren, die mit fahrlässigem Mitarbeiterverhalten einhergehen.

DEINS und MEINS war einmal

Während Arbeitgeber von ihren Angestellten immer mehr Produktivität fordern, verschmelzen die privaten und beruflichen Mobilitätstools der Mitarbeiter zunehmend. Einer Umfrage von theEMPLOYEEapp zufolge nutzen 70 % der Angestellten ihre Privatgeräte für berufliche Zwecke. Und diejenigen, die ihre privaten Geräte zur Arbeit mitbringen, erwarten nur geringe oder gar keine Einschränkungen auf ihren Geräten; insbesondere dann, wenn sie selbst für die Geräte zahlen.

Mobilität vs. Sicherheit vs. Produktivität

„Für eine effektive Mobility-Management-Strategie müssen alle Grundpfeiler erhalten bleiben – Mobilität, Produktivität und Sicherheit“

Sicherheit ist in Unternehmen sowohl Mobilitätshürde Nr.1 als auch verbesserungswürdiger Bereich Nr.1.[5]

Im Zeitalter des mobilen Arbeitens benötigen Unternehmen Transparenz und Kontrolle darüber, wer ihre Unternehmensdaten wo, wann und mit welchen Apps und Geräten bewegt. Sie benötigen eine innovative Lösung, die ihren Mitarbeitern ermöglicht, Berufs- und Privatleben über ein und dasselbe Gerät zu managen, und die gleichzeitig berufliche und private Daten sauber trennt. Benutzer sind sich in der Regel nur unzureichend darüber bewusst, welche Daten und Apps sie auf mobile Geräte herunterladen und wie ihr Verhalten die Sicherheit ihres Unternehmens gefährden kann. Deshalb benötigen Unternehmen eine Lösung, die mobile Geräte in ihrem Netzwerk vor Malware und anderen Infektionen schützt und dafür sorgt, dass die Apps und Inhalte auf diesen mobilen Geräten sicher bleiben.

Eine effektive Strategie bedeutet nicht, sich zwischen Mobilität, Sicherheit oder Produktivität zu entscheiden, sondern die Mobilität so zu steuern, dass sowohl das Unternehmen insgesamt als auch die einzelnen Mitarbeiter von ihr profitieren. Eine EMM-Lösung kann Unternehmen helfen, sich von strengen Geräte- und Inhaltsrichtlinien zu verabschieden und sichere Umgebungen zu implementieren, in denen geschützte Daten problemlos von überall für mobile Mitarbeiter zugänglich sind.

Enterprise Mobility Management

Enterprise Mobility Management ermöglicht Unternehmen, alle Aspekte des mobilen Arbeitens zu verwalten und sicher zu gestalten: Benutzer, Daten, Anwendungen und Geräte. EMM-Lösungen sind auf Smartphones und Tablets zugeschnitten und sollten mehrere Betriebssysteme unterstützen. Zu den Hauptkomponenten von EMM zählen Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Security und Mobile Content Management (MCM).

In Anbetracht der weit verbreiteten beruflichen Nutzung mobiler Geräte entwickelt sich EMM zunehmend zur unverzichtbaren Technologie für Unternehmen jeder Größe. Diese These wird von einer aktuellen Studie des Marktforschungsinstituts 451 Research untermauert, die zum Schluss kommt, dass der Markt für Enterprise Mobility Management (EMM) von einem Umsatz in Höhe von 3,8 Mrd. $ im Jahr 2014 auf 9,6 Mrd. $ im Jahr 2018 wachsen wird. Dies deutet auf eine immense und wachsende Nachfrage von Unternehmen nach EMM-Lösungen hin.

Dieser Trend ist für Unternehmen aller Größen zu beobachten – für Großunternehmen gleichermaßen wie für KMUs. Laut einer Umfrage der SMB Group vom November 2014, in der mehr als 700 KMUs zu Wort kamen, stuft eine wachsende Mehrheit mobile Lösungen als „wesentlichen Business Enabler" ein und 60 % geben an, dass mobile Lösungen ein ausschlaggebender Faktor für ihren Geschäftserfolg sind.

In 3 Schritten zur richtigen EMM-Strategie

Sie arbeiten für ein Unternehmen, in dem Unsicherheit darüber herrscht, wie ein EMM-Programm am besten angegangen werden sollte? Im Folgenden finden Sie eine 3-Schritte-EMM-Strategie, mit der Sie für sichere Mobilität in Ihrem Unternehmen sorgen:

Schritt 1 – Schützen Sie Benutzer und Geräte
Immer mehr Mitarbeiter verlassen sich heutzutage auf ihre mobilen Geräte, um ihr berufliches und ihr Privatleben zu organisieren. Hier erfahren Sie, wie eine EMM-Lösung Ihnen dabei helfen kann, Ihre Benutzer und deren mobile Geräte zu schützen:

1) ***Implementieren Sie eine Passwortrichtlinie*** – Mit den mobilen Geräten Ihrer Mitarbeiter bleiben auch Ihre Unternehmensdaten ständig in Bewegung. Ein ungeschütztes oder ungesperrtes mobiles Gerät gleicht einer offenen Tür – alle auf ihm gespeicherten sensiblen Daten sind für jedermann zugänglich.

2) ***Helfen Sie Benutzern, verloren gegangene Geräte zu finden oder Daten auf verloren gegangenen/gestohlenen Geräten selektiv/vollständig zu löschen*** – Wenn Mitarbeiter das Unternehmen verlassen oder Geräte verlieren (bzw. diese gestohlen werden), müssen die fehlenden mobilen Geräte von zentraler Stelle gesperrt oder die Unternehmensdaten entfernt werden, damit Ihre Unternehmensinformationen vor potenziellen Veruntreuungen und Compliance-Risiken geschützt sind.

3) ***Stellen Sie Benutzern Tools zur Selbshilfe zur Verfügung, mit denen sie ihre Passwörter selbst zurücksetzen und so die IT entlasten können***

4) ***Stellen Sie sicher, dass Ihr Virenschutz/Ihre Mobile Security auf dem neuesten Stand ist –*** Schützen Sie Ihre mobilen Benutzer mit aktuellem und wirksamem Viren- und Webschutz (gilt insbesondere für Android-Geräte) vor schädlichen Apps, Websites und sonstigen Bedrohungen.

Schritt 2 – Schützen Sie Ihr Netzwerk

Stellen Sie die Sicherheit in Ihrem Unternehmensnetzwerk sicher. Sorgen Sie außerdem dafür, dass die mobilen Geräte, die auf Ihre Netzwerkressourcen zugreifen, ein sicheres WLAN nutzen.

1) ***Führen Sie Richtlinien für den WLAN- und Netzwerkzugriff sowie Compliance-Maßnahmen ein*** – Blockieren Sie den WLAN-Zugriff nicht richtlinienkonformer mobiler Geräte auf Ihr Unternehmensnetzwerk, um Datenpannen und Richtlinienverstößen vorzubeugen.

2) ***Definieren Sie Sicherheitsgrundeinstellungen, indem Sie unerwünschte Funktionen beschränken*** – Gewähren Sie Ihren mobilen Benutzern Zugriff auf Apps und Funktionen, die sie für die Erledigung ihrer Aufgaben wirklich benötigen, und sperren Sie gleichzeitig den Zugriff auf Apps und Funktionen, die riskant oder unerwünscht sind. Blockieren Sie beispielsweise den Zugriff auf Facebook.

3) ***Erleichtern Sie sicheres Browsen für häufig aufgerufene mobile Apps*** – Erstellen Sie einen sicheren Browser für Ihre Arbeitsumgebung, indem Sie eine Auswahl von Websites, die Ihre Benutzer am häufigsten nutzen, mit einer zusätzlichen Schutzschicht umgeben.

Schritt 3 – Schützen Sie Unternehmensdaten

Wichtige Informationen müssen mobilen Mitarbeitern zugänglich gemacht werden. Diese Dateien, z. B. die aktuelle Preisliste, werden auf den mobilen Geräten der Benutzer gespeichert. Mitarbeiter benötigen uneingeschränkten Zugriff auf Informationen. Mitarbeiter müssen in der Lage sein, über File-Sharing-Systeme und Diskussionen (z. B. IM) zusammenzuarbeiten. Für Ihre Unternehmensdaten bedeutet all dies eine Gefährdung.

1) ***Schützen Sie E-Mails, Dateien usw. mit Containern –*** Schützen Sie Unternehmens-E-Mails mit einem E-Mail-Container, der Ihre Unternehmens-E-Mails auf dem mobilen Gerät eines Benutzers isoliert. So müssen Sie sich keine Sorgen machen, dass die Sicherheit Ihrer E-Mails gefährdet sein könnte. E-Mails sind verschlüsselt, damit unbefugte Dritte nicht auf sie zugreifen können, und E-Mail-Anhänge werden in einem sicheren Inhaltscontainer geöffnet, damit keine Daten an Drittanbieter-Apps verlorengehen können. Genauso können Sie sicherstellen, dass File Sharing und andere Formen der Zusammenarbeit und des Informationsaustausches in sicheren Containern und Arbeitsbereichen erfolgen, oder Richtlinien zur Rechteverwaltung erstellen, um wichtige Dateien zu schützen.

2) ***Standardisieren Sie den Cloud-Zugriff und etablieren Sie sichere Formen der Zusammenarbeit –*** Fördern Sie eine sichere Zusammenarbeit Ihrer Benutzer, indem Sie einen sicheren Austausch von Dokumenten über Cloudspeicher-Dienste wie Dropbox, Google Drive usw. erlauben. Sie können auch Verschlüsselungsrichtlinien für solche Cloud-Speicherorte verwalten, indem Sie einen sicheren Inhaltscontainer zur Verfügung stellen.

3) ***Schützen Sie wichtige unternehmensspezifische Geschäftsanwendungen –*** Ergänzen Sie Ihre wichtigen unternehmensspezifischen Geschäftsanwendungen (z. B. Bestellverwaltung oder Kunden-Support) mit App-SDKs oder App Wrapping um eine zusätzliche Schutzschicht und Verwaltungsfunktionen.

Zusammenfassung

Da immer mehr Unternehmen sich mit dem Gedanken anfreunden müssen, dass ihre Mitarbeiter mehrere mobile Geräte beruflich nutzen, wächst auch die Herausforderung, die richtige Balance zwischen Mobilität, Sicherheit und Mitarbeiterproduktivität zu finden. Tatsächlich ist bei vielen Enterprise Mobility Management Suites der neuesten Generation kein Kompromiss zwischen Mobilität, Sicherheit und Produktivität mehr notwendig. EMM-Lösungen ermöglichen Unternehmen, die privaten und beruflichen Identitäten ihrer Mitarbeiter klar zu trennen. Mit einem strategischen, schrittweisen EMM-Ansatz können Unternehmen die Produktivitätsvorteile des mobilen Arbeitens uneingeschränkt nutzen, ohne Kompromisse bei der Sicherheit eingehen zu müssen.

Quellen

1. 2015 Q2 Email Benchmark Report

2. Forrsights Workforce Employee Survey, Q4 2011

3. Connected World The Internet of Things and Connected Devices in 2020

4. 2015 Mobile Trends in the Workplace survey by theEMPLOYEEapp

5. TechInsights Report: Enterprise Mobility–It's All About the Apps

Sophos Mobile Control

Mit Sophos Mobile Control können Ihre Mitarbeiter einfach, sicher und produktiv zusammenarbeiten, im gesamten Unternehmen. Mit Sophos Mobile Control können Sie mobile Geräte und die auf ihnen gespeicherten Daten schützen. Sophos Mobile Control lässt sich einfach testen, kaufen, bereitstellen und verwalten. Sophos Mobile Control ist eine komplette Standalone Enterprise Mobility Management Lösung und kann für umfassende Mobile Security und Security Compliance gemeinsam mit Sophos UTM und Sophos SafeGuard Encryption genutzt werden.

Sie möchten Sophos Mobile Control testen?

Kostenlose Testversion unter
www.sophos.de/mobile

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

Oxford, GB | Boston, USA

2016-11-03 WP-DE (MP)

SOPHOS