



Das neue BYOD

Die besten
Methoden für
produktive BYOD
Initiativen


airwatch
by **vmware**

Das neue BYOD

Die besten Methoden für produktive BYOD Initiativen

Eine [Google Trendsuche für "BYOD"](#) ergibt, dass es sich dabei um einen relativ neuen Begriff handelt, der in Nachrichtenveröffentlichungen zum ersten Mal im Spätjahr 2011 auftritt. BYOD ist lediglich ein Teil eines viel größeren, tiefer verwurzelten Trends: dem der IT-Konsumerisierung, die bis zum Beginn des 21. Jahrhunderts zurückverfolgt werden kann. Um diesen Zeitpunkt herum besaß fast jede Person einen Privatrechner, der es dem Benutzer ermöglichte nach der Arbeit von zu Hause aus zu arbeiten – sowie die Vorteile und den Komfort der Benutzung eines sorgfältig selbst ausgewählten Gerätes im Vergleich zu den von der IT-Abteilung zur Verfügung gestellten Firmengeräten zu erkennen.

BYOD, sowie die IT-Konsumerisierung, wuchsen weiterhin während Geräte preiswerter und besser vernetzt wurden. Waren die IT-Administratoren einst lediglich darauf bedacht all die unangemeldeten Geräte, die nun Zugriff auf das Firmennetzwerk hatten im Zaum zu halten, [berichten Intel und Readwrite](#), dass 49 Prozent der U.S. IT-Manager „sich nachhaltig einig sind, dass BYOD die Angestelltenproduktivität verbessert.“ Die nächste Epoche des BYOD-Zeitalters ist bereits angebrochen und IT-Abteilungen betrachten es mehr als eine strategische Aufwertung, als eine Bedrohung, die kontrolliert werden muss.

„Unternehmen werden in Ihrer Handhabung von BYOD gewandter“, sagt Nick McQuire, CEO von Global Enterprise Mobility Alliance (GEMA). „Die ursprüngliche Attraktion lag darin die Kosten auf den Arbeitnehmer übertragen zu können. Das ist wohl immer noch ab und zu der Fall, aber viele Firmen fanden, dass es dabei eine Menge Nuancen gibt,“ erklärt McQuire. Da ist zum Beispiel die schiere Anzahl an Geräten, die in die Betriebe einfließt. Laut einer Studie des Pew Research Centers ist in den letzten paar Jahren [der Besitz an Mobilgeräten sprunghaft angestiegen](#). Der Durchschnittsbenutzer [besitzt bereits mehrfache Mobilgeräte](#).

Unabhängig davon, ob eine Firma Geräte zur Verfügung stellt, haben Angestellte ihre eigenen, persönlichen Geräte, die sie an das Firmennetzwerk anschließen wollen. Da heutzutage die meisten Benutzer mehrere Geräte besitzen, müssen Geschäftsführer und IT-Abteilungen Strategien entwerfen, um die BYOD-Geräte, die unumgänglich ein Teil des Arbeitsplatzes werden, zu verwalten und abzusichern. BYOD-Programme gewähren Benutzern eine sichere, IT-genehmigte Methode des Zugriffs auf Firmenressourcen mit ihren persönlichen Geräten.

Über das Angebot von notwendiger Sicherheit hinaus, haben Geschäfts- und IT-Leiter, die das BYOD-Konzept bereitwillig aufgenommen haben, das Potential des Programms erkannt etliche Geschäftsbereiche aufzuwerten. „Diese Firmen“, sagt McQuire, „verstehen die Vorteile besser, so wie aus welchem Grund BYOD implementiert wird. Sie können BYOD gut mit übergreifenden Geschäftsinitiativen verbinden. Sie erkennen, dass das Programm sich lohnt, da sie sehen wie es Kunden-Engagement, IT-Zufriedenheit, Mitarbeiterbindung oder Rekrutierung sichtlich antreibt.“

Während es schwierig sein mag, genaue Werte in der Steigerungen der Produktivität als Resultat des BYOB-Programms zu bestimmen, sind einige Vorteile jedoch sofort ersichtlich. Die Einführung von BYOD-Programmen für Angestellte, denen keine firmeneigenen Geräte zur Verfügung gestellt werden, führt in den meisten Fällen zu einem erheblichen Anstieg der mobilerreichbaren Belegschaft eines Unternehmens. [Laut Gartner](#) könnte BYOD die Gesamtanzahl der Mobilbenutzer eines Betriebs um 50 Prozent oder mehr erhöhen. Sollten sämtliche Geräte eines Benutzers firmenverbunden sein, erhöht sich der Zugriff sogar noch mehr.

Die cleversten Unternehmen von heute nutzen BYOD-Programme als Hilfsmittel zur Steigerung von mobiler Verfügbarkeit, um IT-Aufsicht zu erhöhen, sowie es Angestellten auf kürzester Frist zu ermöglichen eine Geschäftsaufgabe auf jeglichem verfügbaren Gerät zu absolvieren. Dieses Whitepaper zeichnet die Grundmaßnahmen auf, die von Geschäftsführern und IT-Fachkräften getroffen werden, um ihre BYOD-Programme in bedeutende Produktionsgewinne ummünzen.

Betrachten Sie BYOD als einen Befähiger

Für IT-Abteilungen ist es wichtig, dass BYOD-Benutzer sich im Enterprise Mobility Management registrieren, um unbefugten Zugriff auf das Unternehmensnetzwerk zu minimieren und den Betrieb somit vor Sicherheitsverletzungen zu schützen. Um Angestellte zum Registrieren zu bewegen, müssen Geschäftsführer und IT-Personal diese darüber aufklären, wie ihnen die Registrierung in das Programm von Vorteil wird.

Als Erstes stellen Sie BYOD als eine Sonderzulage dar. BYOD bietet Angestellten die Wahl nach ihrem eigenen Zeitplan auf Geräten ihrer Wahl (oder die sich bereits in ihrem Besitz befinden) zu arbeiten. Es ist sowohl zum Vorteil der Angestellten, als auch der Arbeitgeber, dass die Geräte der Angestellten zum Großteil bereits mit Benutzer-Apps und Produktionshilfen individualisiert wurden, die von den Benutzern als hilfreich befunden wurden. Indem man die Auswahlmöglichkeiten und Flexibilität des BYOD-Programms hochspielt, hilft man das Programm in einer Weise darzustellen, die es den Angestellten erlaubt ihre Aufgaben produktiver und effizienter zu erledigen.

Außer den Angestellten eine Wahl anzubieten, können BYOD-Programme Angestellten und Unternehmen im Ganzen dabei helfen übergreifende Geschäftsziele zu erreichen. Denken Sie darüber nach, wie BYOD Ihre bestehenden Unternehmensziele fördern. Könnte Ihre Vertriebsangestellte ihre Mobilgeräte im Außendienst zum Engagement von Geschäftsaussichten und Kunden benutzen? Ist es durch den globalen Umfang Ihres Unternehmens nötig, dass Ihre Angestellten rund um die Uhr E-Mails empfangen können? Sind Ihre Angestellten an Telearbeit oder alternativen Arbeitsschichten interessiert? Ein BYOD-Programm kann dabei helfen Geschäftsprozesse zu optimieren, Verkaufszahlen voranzutreiben und Kundenengagement zu verbessern.

Die GA Communications Group, eine Firma aus Chicago, hat mit Erfolg ein BYOD-Programm implementiert, das den Benutzern deutliche Vorteile bietet. Laut Jason Dittmer, Technology Director, liegt hierbei die Hauptattraktion in der Möglichkeit des Zugriffs auf die täglichen Arbeitszeitznachweisberichte, um abrechnungsfähige Dienststunden eintragen zu können – eine Tätigkeit, die täglich durch eine Verbindung mit einem virtuellen privaten Netzwerk (VPN) durchgeführt werden muss. Das VPN-Profil wird über eine Web-App auf Benutzergeräte geschoben. In der App können Angestellte ihre Arbeitszeitznachweise ausfüllen und abgeben. „In der Agenturwelt regieren Arbeitszeitznachweise“, betont Dittmer. „Sie sind ein großer Teil des Arbeitsalltags. Wenn Sie also in der Eile vergessen haben Ihren Bericht auszufüllen, können Sie jetzt im Zug schnell Ihr Handy herausziehen, eine Verbindung zum VPN herstellen und Ihren Bericht immer noch rechtzeitig abgeben.“

In der Zukunft plant Dittmer iBeacons und eine Zeitplanungs-App zu benutzen, um die Buchung von Konferenzräumen zu vereinfachen. Sollte ein Angestellter einen Konferenzraum benötigen, kann er/sie eine Verbindung zu iBeacons im Büro herstellen und die Buchungsliste wird auf sein Handy geladen.

Herauszufinden, wie das BYOD-Programm den Angestellten behilflich sein wird, kann die Aufnahme des Programms beschleunigen und das Programm in einem positiven Licht darstellen. Bevor Geschäftsführer und IT-Fachkräfte jedoch diese

Haltung einnehmen können, müssen sie sichergehen, dass ihre Prioritäten – IT-Aufsicht und strengste Sicherheit – gewährleistet sind.

Die richtigen Mittel ins Spiel bringen

Die Einführung des iPhones unterbrach den Enterprise Mobility Markt und verursachte einen Welleneffekt, der heute immer noch deutlich erkennbar ist. Angestellte brachten ihre persönlichen iPhones zur Arbeit und bevorzugten diese gegenüber ihren alten Dienstgeräten. Einige fanden Wege des Zugriffs auf ihre E-Mail und andere Ressourcen und das IT-Personal musste unautorisierten Zugriff im Zaum zu halten und den drohenden Verlust von Daten zu verhindern. Da es dem IT-Personal nicht möglich war den Zustrom von iPhones und anderen Smart-Geräten einzudämmen, mussten sie stattdessen Wege finden einem sich ständig wachsenden Feld von Gerätearten sicheren Zugriff auf Firmenressourcen anzubieten.

Bevor eine BYOD-Initiative eingeführt wird, sollte das IT-Personal sich auf den Zufluss, sowohl auf dem Gebiet der Netzwerkarchitektur, als auch in Management, vorbereiten. Die IT-Abteilung muss sicherstellen, dass ihre Netzwerkarchitektur den erhöhten WLAN Verkehr verkraften kann. Sie muss weiterhin gewährleisten, dass die bereits existierende Geräteverwaltungsplattform in der Lage ist zu skalieren, um sich der Verwaltung von mitarbeitereigenen Geräten anpassen zu können. Sollte IT bereits in ein Enterprise-Mobility-Management-System investiert haben, müsste dieses idealerweise in der Lage sein bereits bestehende Richtlinien für firmeneigene Geräte auf die nötigen Richtlinien, Apps und Inhalte von derselben Konsole aus zu erweitern.

In einem BYOD-Szenarium sind die Geräte, die in das Firmenmilieu einfließen äußerst unterschiedlich. Eine Enterprise-Mobility-Management -Lösung, die nur eine limitierte Anzahl von Gerätetypen und Betriebssystemen unterstützt, verbessert im Bestfall die Produktivität eines Bruchteils der Angestellten. Im schlimmsten Fall führt es zu Angestellten mit nicht unterstützten Geräten, die Zugriff auf Umwegen finden und somit die Firma Sicherheitsverletzungen aussetzen. Eine Mobile-Device-Management-Lösung, wie AirWatch sie bietet, die alle gängigen Gerätearten und Plattformen unterstützt, regt zur universellen Registrierung an und ist somit das beste Mittel zum Schutz vor Datenverlust.

Es ist außerdem wichtig eine Lösung zu finden, die mit dem Tempo des Fortschritts auf dem Markt mithalten kann. Mobile Betriebssystem-Updates werden fast alle zwei Wochen veröffentlicht und neue Geräte werden ununterbrochen eingeführt. Jeder neue Gerätetyp oder Betriebssystem-Update stellt eine Möglichkeit für potentielle Sicherheitsschwachstelle dar. AirWatch ist OEM-agnostisch und kann dadurch Support am selben Tag für alle gängigen Gerätearten und Betriebssysteme bieten. AirWatch stellt IT-Administratoren auch eine einzige Konsole zur Verfügung, die Übersicht über sämtliche Geräte, seien sie nun firmeneigene, BYOD oder Gemeinschaftsgeräte. AirWatchs mandantenfähige Architektur ermöglicht es Administratoren die Verwaltung von mitarbeitereigenen Geräten einzugrenzen, während firmeneigene Geräte hingegen vollständig verwaltet werden.

Einige Betriebe werden jedoch keinen Zugriff für alle Gerätetypen und Betriebssysteme anbieten wollen, und Angestellte erhalten stattdessen eine Liste von zugelassenen Geräten, die von der Firma als sicher erachtet werden. AirWatch bietet die Möglichkeit den Zugriff auf Inhalte, basierend auf Gerätetyp, Betriebssystem oder Betriebssystems-Version einzuschränken. Außerdem kann AirWatch die Anzahl der Geräte, die ein einzelner Benutzer registrieren kann, einschränken. Dadurch können Unternehmen Grenzen setzen und ihr Netzwerk vor einem Überschuss an Geräten schützen, bis die Architektur eingerichtet ist diesen Verkehr zu unterstützen.

Die Planung eines BYOD-Programms ist nur ein Teil eines viel größeren Enterprise-Mobilitäts-Puzzles und sollte im Kontext gesehen werden. Technologie ist von Natur aus zyklisch und wenn Marktbedürfnisse umgehend angesprochen werden müssen, ist oft schnell eine Heftpflasterlösung oder ein Verkäufer zur Hand, um die Lücke abzudecken. Bevor eine Übergangslösung verwendet wird, um ein Datenleck zu stopfen und unbewachte Geräte vor dem Zugriff in das Firmennetzwerk abzuhalten, haben die meisten modernen mobilen Unternehmen von heute umfassende Lösungen entwickelt, die in der Lage sind zu skalieren wenn ihre Mobilitätsinitiativen expandieren.

Ihre höchste Priorität mag zum Beispiel darin liegen Ihren Angestellten E-Mail Zugang auf ihren persönlichen Geräten zu bieten. Es ist jedoch unvermeidbar, dass Angestellte sich mehr und mehr auf ihre Mobilgeräte verlassen und IT-Abteilungen müssen bedenken, wie sie ihr BYOD-Angebot über E-Mail Zugriff hinaus erweitern werden. Denken Sie voraus und eignen Sie sich eine Lösung an, die Apps, Inhaltszugriff, sichere Verbindungen zu Betriebsrepositorien sowie nahtloses Intranet-Browsen auf mitarbeitereigenen Geräten unterstützen kann.

Der schwere Teil kommt nachdem die Technologie eingesetzt worden ist. Nachdem das IT-Personal seine nötigen Instrumente ausgesucht hat, muss es sich nun mit den Geschäftsleitern und weiteren relevanten Abteilungen absprechen, um Richtlinien zu entwickeln, die die rechtlichen und privaten Auswirkungen des BYOD-Programms ansprechen.

Kommunikation ist der Schlüssel: Schaffen Sie klare BYOD Richtlinien und Nutzungsbedingungen

Eine Studie vom April 2014 ergab, dass viele Angestellte [BYOD immer noch nicht ernstnehmen](#). BYOD-Richtlinien können dabei helfen Angestellte zum Registrieren zu bewegen, indem sie sowohl die Risiken unautorisierten Zugriffs, als auch die Vorteile des BYOD-Programms zusammenfassen. Die BYOD-Richtlinien sollten die Regeln des Programms, nach gesetzlichen Regulierungen und firmeneigenen Sicherheitsrichtlinien, im Klartext beschreiben. Sie sollten weiterhin sehr klar darstellen, welche Daten für IT-Personal auf mitarbeitereigenen Geräten sichtbar sind und verwaltet werden können, um der Furcht vorzubeugen, dass persönliche Daten kompromittiert oder bloßgelegt werden können. Bevor das Programm unternehmensweit eingesetzt wird, sollten die IT-Abteilungen die Akzeptanz der Führungsebene, sowie Stellungnahmen verschiedener Abteilungen einholen, um sicherzustellen, dass alle Anliegen berücksichtigt und alle Bedürfnisse erfüllt wurden.

Datenschutz ist von bedeutender Wichtigkeit für viele Angestellte und kann ein Hindernis bei der Registrierung in BYOD-Programme darstellen. AirWatch ermöglicht es Betrieben je nach der Art des Gerätebesitzes Firmen- und persönliche Daten auf Geräten durch maßgeschneiderte Datenschutzrichtlinien zu trennen. Administratoren können Richtlinien konfigurieren, die die Datensammlung von persönlicher E-Mail, Inhalten oder Apps auf einem mitarbeitereigenen Gerät nicht zulassen. GPS-Standorte, persönliche Nutzerinformationen und Telekomdaten verbleiben ebenfalls privat und persönliche Geräte können außerdem vor einer kompletten Löschung der Firmendaten oder Remotesteuerung geschützt werden. AirWatch erlaubt es Unternehmen auch Risiken zu mindern, die durch den Zugriff mitarbeitereigener Geräte auf Geschäftsressourcen auftreten können. Durch maßgeschneiderte Nutzungsbedingungen, die auf Benutzerrolle, Organisationsgruppe und Geräteplattform basiert sind, können Angestellte über die Daten, auf die das Unternehmen Zugriff hat, sowie die Benutzungsregeln für ihre Geräte, aufgeklärt werden.

Mohegan Sun, ein Kasino und Feriencenter in Connecticut (USA), führte vor kurzem mit Erfolg ein BYOD-Programm ein. Danny Lynn, der Director of Information Technology, erklärt, dass das diesjährige Budget es leider nicht erlaubte die firmeneigenen iPhones 4 und 4s aufzurüsten. Er hat deshalb ein BYOD-Programm entwickelt, das es den Angestellten ermöglicht den Vertrag zu übernehmen, ihre Geräte zu aktualisieren und sich in das BYOD-Programm zu registrieren.

Beim Entwurf der Details des Programms wurde ihm bewusst, dass er BYOD-Richtlinien benötigen würde, die die Regeln und Upgrade-Möglichkeiten klar definieren würden, und gleichzeitig die Registrierung weiterer Privatgeräte ermöglichten. Laut Lynn, hatten mehrere Angestellte mit firmeneigenen Smartphones Zugriff auf ihre E-Mail auf ihren privaten iPads beantragt. Angestellte ohne firmeneigene Geräte hatten ebenfalls darum gebeten ihre Privatgeräte zu registrieren.

Lynn und Mohegan Suns Vice President of IT, entwickelten die Richtlinien und Nutzungsbedingungen für das BYOD-Programm von Grund auf und basierten sie vollkommen auf die Bedürfnisse der Angestellten, sowie individuelle Nutzerfälle. Das Team stimmte sich mit der Rechtsabteilung ab und nachdem es dort abgesegnet worden war, starteten sie das Programm. Der Vertrag ist kurz und klar, erklärt Lynn: Er macht absolut deutlich, welche Daten für Administratoren auf angestellteneigenen Geräten eingesehen werden können und gibt Mohegan Sun die Erlaubnis kompromittierte Geräte zu löschen.“ Obwohl Lynn keinen Druck von Angestellten erhielt, die um Datenschutz besorgt waren, „sind einige Angestellte doch besorgt alle Daten zu verlieren. Aus diesem Grund schlagen wir immer vor regelmäßige Datensicherungen durchzuführen.“

Um BYOD-Geräte an das Netzwerk anzuschließen, können Angestellte nun zuerst den Vertrag einsehen, den AirWatch Agent installieren und die Nutzungsbedingungen akzeptieren, die Lynn durch die AirWatch Konsole individualisiert hat.

GEMA CEO Nick McQuire empfiehlt mit einem BYOD-Grundprogramm zu beginnen und es dann auf den Industriezweig oder die Firmenbedürfnisse maßzuschneidern. „Organisationen, wie Gartner und Vox bieten eine breite Auswahl an Instrumenten an“, erläutert McQuire, der Gartner als eine gute Quelle für Orientierungshilfe empfiehlt. „Firmen können mit einem Basisplan beginnen und auf diesen mit ihren eigenen Nachträgen und Eingaben aufbauen.“

Jason Dittmer, Director of Technology für die GA Communications Group, führte Online-Recherchen durch und fand passende BYOD-Richtlinien, die er an seine Rechtsabteilung zur Durchsicht weiterleitete. Daraufhin entwickelte er mit seinen IT-Kollegen ein individualisiertes Verfahren, um Angestellte zur Akzeptanz des Programms zu bewegen.

Die Kleinfirma mit Sitz in Chicago macht BYOD von Anfang an zu einem Teil der Betriebskultur, indem sie das BYOD-Programm und die Richtlinien sofort während des Einführungstrainings vorstellt. „Jeder, der Teil des Netzwerks werden will, bekommt Anweisungen zur Registrierung in das Mobile-Device-Management-Programm, oder wird zur Einrichtung des Geräts an die IT-Abteilung verwiesen“, sagt Dittmer. Momentan bietet die GA Communications Group Zugriff auf abgesichertes WLAN, E-Mail, VPN, sowie einen Firmen-App-Katalog.

Teil der Einrichtung besteht darin den Angestellten den Zugriff zum Self-Service-Portal zu erklären, wo sie alle verwalteten Aspekte ihres Geräts einsehen können. Für Angestellte, die um Datenschutz besorgt sind, war das Self-Service-Portal oft der entscheidende Faktor sie zur Registrierung zu überzeugen, erklärt Dittmer. Durch das Self-Service-Portal können Angestellte genau einsehen, welche Daten von der IT-Abteilung auf ihren Geräten verwaltet werden.

Hier sind einige Links zu Online-Ressourcen für BYOD-Richtlinienmuster, die als gute Basis für benutzerdefinierte Richtlinien zur Abdeckung der Bedürfnisse Ihrer Firma dienen können:

- [TechRepublic BYOD Policy](#)
- [White House Bring Your Own Device Toolkit](#)
- [IT Manager Daily BYOD Policy Template](#)
- [Gartner BYOD Mobile Device Policy Template](#)
- [Vox BYOD Ressourcen Seite](#)

Der Übergang von Firmeneigentum auf BYOD: Den Angestellten Auswahl anbieten

Sollten Sie sich langsam von firmeneigenen Geräten entfernen und zum Großteil ein BYOD-Modell einführen wollen, kann es den Angestellten bei der Umstellung behilflich sein, wenn ihnen mehrere Angebote zur Auswahl gestellt werden. Das Mohegan Sun Kasino und Ferienzentrum hat einen Plan eingeführt ihre Benutzer schrittweise auf ein BYOD-Modell umzustellen.

„Als die iPhones 5 raus kamen, wollten die Angestellten auf das neueste Gerät aufrüsten“, erzählt IT Director Danny Lynn. Lynn machte Angestellten das Angebot ihre Mobilverträge von Mohegan Sun auszukaufen, ihre Geräte zu aktualisieren und sich in das BYOD-Programm der Firma zu registrieren. Obwohl die aufgerüstete Hardware nun Eigentum und somit die Verantwortung des Angestellten ist, werden die monatlich Kosten dennoch von Mohegan Sun gedeckt. „Angestellte wollen Auswahl und dieser Punkt hat unsere BYOD-Richtlinien bestimmt.“

„Von diesem Punkt an werden alle Hardwareaktualisierungen, -reparaturen, -probleme oder was auch immer mit dem Handy selbst zu tun hat, zur Verantwortung des Angestellten“, erklärt Lynn. „Das kommt den Unternehmen zugute, da zukünftige Kapitalauslagen für Handy-Upgrades reduziert werden.“ Angestellte, die die Kosten für einen Upgrade nicht tragen wollen behalten einfach ihre bereits vorhandenen Geräte.

Während teilweise oder volle Rechnungserstattungen den Übergang von firmeneigenen Geräten auf BYOD erleichtern mögen, kann die Erstattung von Handyrechnungen das Potential haben den Reingewinn einer Firma negativ zu beeinflussen. Ein Telekom-Kostenmanagementprogramm kann Datenpläne in Grenzen halten. AirWatch hat integrierte Kostenmanagement-Funktionen, wie zum Beispiel die Möglichkeit Dokumente nur über WLAN herunterladen zu können oder den Zugriff auf systemeigene Funktionen, wie Videoanrufe, die große Datenmengen verschlingen können, ganz zu unterbinden. AirWatch schließt sich außerdem mit Telekom-Kostenmanagementanbietern, wie [Wandera](#) zusammen, die Datenkomprimierung und -verwaltung anbieten.

Bevor das BYOD-Programm zur Einführung bereit ist, sollte das IT-Personal sich überlegen, ob und wie es angestellteneigene Geräte unterstützen wird.

Hilfestellung anbieten: ITs neue Rolle als Berater in einem BYOD-Umfeld

Der Anstieg an Mobilgeräten in Firmennetzwerken – sowie die Cloud-verwalteten Daten, auf die sie zugreifen – hat die Arbeitsweise der Angestellten, und konsequenterweise die der IT-Abteilungen, grundlegend geändert. Mobilität bietet die Möglichkeit effizienter zu arbeiten. Leistungsfähigkeit wächst, wenn Zugriff auf E-Mail oder arbeitsverbundene Tätigkeiten

auf allen Privatgeräten besteht. Es mag einfach klingen, aber Zugang für verschiedene Gerätetypen – und oft für mehrere Geräte pro Benutzer – herzustellen, stellt eine Unzahl neuer Herausforderungen für IT-Abteilungen dar, berichtet VDC-Researcher Eric Klein.

„Wenn Unternehmen diese Geräte so verwalten soll, dass es nicht nur kosteneffizient ist, sondern die Firma auch vor den Risiken, die mit dem Öffnen der Unternehmensdaten auf diesen Plattformen in Verbindung stehen, dann ergibt sich da eine ganze Reihe von Problemen, die gelöst werden sollen“, sagt Klein. MDM-Kontrollen können Grundprobleme, wie das Löschen von Firmendaten oder die Sperrung eines im Taxi oder Flugzeug vergessenen Geräts, beseitigen. „Es gibt aber noch so viele andere Dinge, die ein Unternehmen zu bedenken hat.“

GA Communications Technology Director Jason Dittmer erklärt, dass der Übergang auf die Cloud ein großer Entscheidungsfaktor in der Einführung des BYOD-Programms seiner Firma war. „Wir haben großen Druck gemacht den Großteil unserer internen Systeme in die Cloud zu schieben. In den traditionellen Einstellungen schützte jeder seinen eigenen Verwaltungsbereich im Serverraum.“ IT-Abteilungen von heute sind jedoch mehr darauf bedacht ein ganzes Spektrum an Leistungen zu verwalten, wie Cloud-Speicheranbieter und MDM, meint Dittmer.

IT-Abteilungen, die BYOD-Programme verwalten, werden auch regelmäßig zur Fehlerdiagnose und-behebung an einem breiten Angebot von Gerätetypen herangezogen. Laut Dittmer hat sich dadurch die Art der Zusammenarbeit zwischen IT und Angestellten verändert. „BYOD bewirkte eine enorme Verlagerung in der gewohnten Arbeitsweise und Interaktion von Mitarbeitern. Da in einer BYOD-Sphäre so viel mehr Variablen ins Spiel kommen, nimmt die IT-Abteilung eher eine Beraterfunktion an.

Einige Firmen haben eine IT-Genius Bar eingerichtet, wo Angestellte sich während bestimmter Zeiten Hilfe holen können, wenn sie Verbindungsprobleme mit ihren Geräten haben oder auch zur Fehlerdiagnose. Obwohl Dittmers Firma klein genug ist, dass Angestellte bei Fragen jederzeit unproblematisch die IT-Abteilung besuchen können, erklärt er, dass die Einführung einer vereinfachten Verwaltungsplattform für BYOD und firmeneigene Geräte, seiner Abteilung die zusätzliche Zeit gegeben hat die Beraterrolle anzunehmen, wann immer sie benötigt wird. Dieses Konzept hat außerdem sowohl sein eigenes, als auch das IT-Wissen seiner Kollegen erweitert.

„Ich glaube, dass das Personal in einer IT-Abteilung ein breiteres und tiefgründliches Wissen braucht, da es auf einmal so viele verschiedene Systeme verwalten muss“, meint Dittmer. „Jetzt macht niemand hier [in unserer IT-Abteilung], der nur noch eine bestimmte Aufgabe. Alle vier Angestellten, mich selbst eingeschlossen, müssen sich mit all diesen Systemen auskennen.“ Für Unternehmen, die die Ressourcen nicht besitzen ihren Angestellten IT-Unterstützung für Privatgeräte bieten zu können, ist das AirWatch Self-Service-Portal ein sehr nützliches Instrument, das Angestellten bei der Konformitätsbestätigung, sowie bei Fehlerdiagnosen und -behebungen behilflich sein kann.

Was kann nun, da Sie Ihre Angestellten befähigt haben ihre eigenen Geräte zu verwalten und technisch instand zu halten –als Nächstes erwartet werden?

Bereiten Sie sich auf die Zukunft von BYOD vor: BYO-Alles

„Unsere Arbeitsweise befindet sich im Wandel“, stellt VDC Researcher Eric Klein fest. „Nicht nur die nächste Generation von Arbeitern – wir alle sind betroffen.“

Die mobile Revolution hat das Geschäftsleben neu definiert. Es ist schwer sich heute vorzustellen nicht mit mindestens ein oder zwei Mobilgeräten als unerlässlichen Arbeitsmitteln ausgerüstet zu sein. Es liegt jedoch noch mehr Änderung in der Luft. Tagtäglich scheint ein neues, IP-vernetztes Gerät auf den Markt zu dringen. Es wird nicht lange dauern bis diese Geräte alle als unentbehrlich betrachtet werden und schnell eingepackt - oder aufgesetzt – werden, bevor wir das Haus auf dem Weg ins Büro verlassen.

Und während das „Internet of Things“ uns enorme Möglichkeiten bietet unsere Geschäftspraktiken zu revolutionieren, bringt es auch neue Herausforderungen und Sicherheitsbedrohungen mit sich. IT-Abteilungen müssen diese Herausforderungen und Bedrohungen bereits jetzt ansprechen. Die Einführung eines soliden BYOD-Programms, Richtlinien und Verwaltungsmittel mag wohl der beste Weg sein, wie sich Unternehmen auf eine hypervernetzte Zukunft vorbereiten können.

Des Weiteren liegt hierin auch eine außerordentliche Gelegenheit für IT-Führungskräfte ihren Wert zu demonstrieren. IT steht an einem Scheideweg. Da mehr Technologie täglich in die Arbeitsplätze eindringt als je zuvor, haben IT-Führungskräfte die beispiellose Chance die Initiative zu ergreifen und zum Mittelpunkt der Geschäftsstrategie zu werden. „Lange Zeit wurde IT dazu relegiert hinter den Kulissen zu arbeiten“, sagt Klein. „Mobile Technologie ändert diese Gleichung auf einmal komplett; hier bietet sich jetzt eine großartige Gelegenheit für IT sich in der Geschäftswelt wieder zu behaupten. Da es nun offensichtlich möglich ist Mobilgeräte in Firmen zu integrieren, hat sich eine vollkommen neue Welt an Möglichkeiten aufgetan.“