

Fallstudie

Zu Kapitel 13: Die Vor- und Nachteile von „Bring-Your-Own-Device“

Fast jeder, der ein Smartphone besitzt, möchte es gern mit zur Arbeit bringen und dort auch nutzen. Und was spricht dagegen? Mitarbeiter, die ihr eigenes Smartphone verwenden, bieten dem Unternehmen alle Vorteile einer mobilen Belegschaft, ohne dass die Kosten der Anschaffung und Unterhaltung der Geräte zu Lasten des Unternehmens gehen. Kleinere Unternehmen können so im Netz aktiv sein, ohne selbst große Investitionen in Geräte und mobile Dienste tätigen zu müssen. Eine von IBM finanzierte Studie von Forrester Consulting stellte fest, dass ein BYOD-Programm (Bring Your Own Device), das die mobilen Unternehmensdiensten von IBM nutzt, eine Rendite von 108 Prozent erzielt und sich innerhalb eines Monats amortisiert. Der jederzeit und überall mögliche Zugriff auf mobile Geräte steigerte die Produktivität am Arbeitsplatz und erhöhte die effektive Arbeitszeit des Mitarbeiters um 45–60 Minuten pro Woche. Laut Gartner Inc. werden 2017 über 50 Prozent der Arbeitgeber von ihren Mitarbeitern erwarten, dass sie ihre eigenen mobilen Geräte mit zur Arbeit bringen. BYOD wird die „neue Normalität“.

Doch ... warten Sie einen Augenblick. Gemäß einer Umfrage unter 162 Unternehmen, die Osterman im Auftrag von Dell Inc. durchführte, meinen beinahe drei Fünftel aller Unternehmen, dass BYOD ein wachsendes Problem für ihre Organisation darstellt. Obwohl BYOD die Arbeitsplatzzufriedenheit und Produktivität erhöht, kann es auch eine Reihe von Problemen aufwerfen, wenn es nicht ordnungsgemäß kontrolliert wird: Die Unterstützung für private mobile Geräte ist schwieriger als für unternehmenseigene Geräte, die Kosten für die Kontrolle der mobilen Geräte können steigen und der Schutz der Unternehmensdaten und Netzwerke wird immer komplizierter. Untersuchungen der Aberdeen Group ergaben, dass ein Unternehmen mit 1.000 mobilen Geräten im Schnitt 170.000 US-Dollar jährlich zusätzlich ausgibt, wenn BYOD erlaubt ist. Es ist also nicht so einfach.

BYOD bindet einen großen Teil der IT-Ressourcen eines Unternehmens, um die vielen verschiedenen privaten Geräte zu kontrollieren und zu warten. In der Vergangenheit versuchten die Unternehmen, die Smartphone-Nutzung auf eine Plattform zu beschränken. Dadurch wurde es

einfacher, die einzelnen mobilen Geräte zu verfolgen und Software-Upgrades und -Bugfixes zur Verfügung zu stellen, da alle Mitarbeiter die gleichen Geräte oder zumindest das gleiche Betriebssystem verwendeten. Am populärsten war das BlackBerry von Research in Motion, da es die sicherste mobile Plattform bot. (Mobile BlackBerry-Geräte greifen über eine proprietäre Software- und Netzwerkplattform auf die Firmendaten und E-Mails zu, die vom Unternehmen kontrolliert und gegen Angriffe von außen geschützt ist.)

Heutzutage ist die digitale Landschaft viel komplizierter, denn es gibt eine Vielzahl von Geräten und Betriebssystemen auf dem Markt, deren Verwaltungs- und Sicherheitstools nicht ausgereift sind. Android hat einen Anteil von über 79 Prozent am weltweiten Smartphone-Markt, ist aber aus Unternehmenssicht am Arbeitsplatz problematischer als die mobilen Geräte von Apple mit ihrem sogenannten geschlossenen iOS-Betriebssystem, das nur auf einer begrenzten Anzahl von verschiedenen Apple-Geräten läuft. Die Vielfalt von Android macht die Kontrolle hingegen sehr schwierig und kostspielig für die IT-Abteilungen der Unternehmen. Juli 2013 gab es über 11.868 verschiedene Android-basierte Geräte von 1.700 verschiedenen Herstellern gemäß einem Bericht von OpenSignal, der drahtlose Netzwerke und Geräte untersucht. Außerdem lockt Android mit seinem großen Marktanteil viele Hacker an und ist aufgrund seiner Open-Source-Architektur und seiner vielen Versionen leicht verwundbar.

Wenn Mitarbeiter die Erlaubnis haben, mehrere mobile Geräte und Betriebssysteme auf der Arbeit zu verwenden, benötigen Unternehmen einen effektiven Weg, alle diese Geräte zu verfolgen und zu verwalten. Damit die Geräte eine Verbindung zu den Netzwerken des Unternehmens herstellen und auf die Unternehmensdaten zugreifen können, müssen die Netzwerke des Unternehmens entsprechend konfiguriert sein. Wenn Mitarbeiter Änderungen an ihrem Handy vornehmen (z.B. ihren Provider wechseln oder ihre Telefonnummer ändern, oder ein ganz neues Handy kaufen, müssen Unternehmen schnell und flexibel sicherstellen, dass ihre Mitarbeiter auch weiterhin produktiv sind. Unternehmen benötigen ein effizientes Bestandsführungssystem, das festhält, welcher Mitarbeiter welches Gerät nutzt,

► Forts.

den Standort der einzelnen Geräte, ob es gerade verwendet wird und mit welcher Software es ausgestattet ist. Für nicht vorbereitete Unternehmen könnte sich die Bemühungen im Überblick zu behalten, wer Zugriff auf welche Daten erhält, als Alptraum erweisen.

Angesichts der großen Vielfalt an Handys und Betriebssystemen auf dem Markt ist die Bereitstellung technischer Unterstützung für jeden Mitarbeiter problematisch. Wenn Mitarbeiter auf wichtige Daten nicht zugreifen können oder andere Probleme mit ihren Mobilgeräten haben, benötigen sie Hilfe von der IT-Abteilung. Unternehmen, die vornehmlich Desktop-PCs einsetzen, haben in der Regel viele identische Computer, mit den gleichen technischen Daten und dem gleichen Betriebssystem, was den technischen Support um Vieles einfacher macht. Mobilität bedeutet eine neue Ebene der Vielfalt und Komplexität für die technische Unterstützung, worauf die Unternehmen vorbereitet sein müssen.

Unternehmensdaten zu sichern, auf die über mobile Geräte zugegriffen wird, bereitet erhebliche Probleme. Wenn ein Gerät gestohlen oder manipuliert wurde, benötigen Unternehmen Wege, um sicherzustellen, dass keine sensiblen oder vertraulichen Daten nach Draußen gelangen. Mobilität stellt für Geräte und Daten ein größeres Risiko dar, als wenn diese sich innerhalb der Unternehmenswände bzw. auf Unternehmensrechnern befinden. Unternehmen verwenden oft Technologien, mit denen sich Daten aus der Ferne verschlüsseln oder sogar ganz von den Geräten entfernen lassen, sodass sie bei Diebstahl nicht in fremde Hände geraten. Eine ausführliche Diskussion des Themas mobile Sicherheit finden Sie in *Kapitel 8*.

Jeanette Horan, CIO von IBM, ist der Meinung, dass BYOD genauso viele Probleme aufwirft, wie es löst. IBM sparte damit kein Geld; vielmehr stellte BYOD die IT-Abteilung vor neuen Problemen, da die Geräte der Mitarbeiter voll mit Software waren, die IBM nicht kontrollierte. IBM statete deshalb 40.000 seiner 400.000 Mitarbeiter mit sicheren BlackBerrys aus, während es 80.000 weiteren Mitarbeitern erlaubte, mit eigenen Smartphones oder Tablets auf die IBM-Netzwerke zuzugreifen.

Die IT-Abteilung von IBM erkannte, dass sie keine Ahnung hatte, welche Apps und Dienste ihre Mitarbeiter auf ihren Geräten verwendeten

und die Mitarbeiter selbst waren „in seliger Unwissenheit“, welche Sicherheitsrisiken ihre Lieblings-Apps darstellten. IBM entschied, die Nutzung solch populärer Dienste wie den cloudbasierten Cyberlocker von Dropbox zu verbieten, in der Furcht, dass Mitarbeiter unabsichtlich sensible IBM-Daten in ihre persönlichen Dropbox-Konten stellten, interne E-Mails an öffentliche Webmail-Dienste weiterleiteten oder ihre Smartphones als mobile Hotspots nutzten. Wie Untersuchungen der International Data Company (IDC) zeigen, räumten 20 Prozent der Unternehmensmitarbeiter ein, die Cloud-Speicherdienste in Anspruch nahmen, dass sie Unternehmensdaten in der Cloud speicherten, was ein ernst zu nehmendes Problem darstellt.

Bei IBM dürfen die Mitarbeiter erst dann mit ihren eigenen Geräten auf die Unternehmensnetze zugreifen, wenn die Geräte den Sicherheitscheck bestanden haben. Die IT-Abteilung konfiguriert die Geräte, sodass der Speicher aus der Ferne gelöscht werden kann, wenn das Gerät gestohlen wird oder verloren geht. Die IT-Gruppe deaktiviert außerdem öffentliche File-Transfer-Programme wie iCloud von Apple. Die Mitarbeiter verwenden stattdessen eine von IBM gehostete Version namens MyMobileHub. IBM schaltet sogar Siri aus, den sprachaktivierten persönlichen Assistenten auf den iPhones, da gesprochene Anfragen auf die Apple-Server hochgeladen werden.

Jedes Mitarbeitergerät wird individuell in Abhängigkeit von dem Modell und den beruflichen Verantwortlichkeiten konfiguriert. Einige Mitarbeiter dürfen nur IBM-interne E-Mails, Kalender und Kontakte auf ihren Geräten empfangen, während andere auf interne IBM-Anwendungen und -Dateien zugreifen können (siehe *Kapitel 8*). Letztere Geräte stattet IBM mit zusätzlicher Software aus, um zum Beispiel die Daten auf ihrem Weg von und zu den Unternehmensnetzen verschlüsseln.

Ein Unternehmen, das BYOD erfolgreich implementiert hat, ist der Halbleitergigant Intel Corporation. Fast 70 Prozent der im Unternehmensnetzwerk registrierten 39.000 Geräte sind private Geräte. Intel ging positiv an BYOD heran und suchte nach Wegen zu einer erfolgreichen Umsetzung, anstatt es vollständig abzulehnen.

Der damalige CIO bei Intel, Diane Bryant, wollte nicht von einem einzigen Anbieter von mobilen Geräten oder Betriebssystemen abhängig sein.

► Forts.

Intel arbeitete eine BYOD-Strategie aus und entwickelte eine Dienstgütevereinbarung für Endnutzer, die klarstellte, dass die Endnutzer sich freiwillig auf BYOD einließen und nicht von Intel dazu gezwungen wurden. Das Unternehmen legte verschiedene Richtlinien, Regeln und Zugangsberechtigungen für die einzelnen Arten von Geräten fest – Smartphone, Tablet oder Laptop – mit jeweils unterschiedlichen Kontrollstufen. Intel führt eine Liste der zugelassenen Geräte. Wenn ein Gerät die für ihn spezifizierten Anforderungen nicht erfüllt, wird sein Zugriff auf das Netzwerk gesperrt. Intels BYOD-Programm bietet zurzeit 40 proprietäre Anwendungen, einschließlich Reise-Tools, mit denen sich Flüge und Konferenzräume suchen und buchen lassen. Das Unternehmen bietet einen internen „App-Store“ und setzt eine Reihe von verschiedenen Software- und Sicherheitstools ein (u.a. für mobiles Gerätemanagement und mobiles App-Management).

Intels Ziel beim Einsatz von BYOD ist nicht, Geld zu sparen, sondern seine Mitarbeiter zufriedener und produktiver zu machen. Mitarbeiter lieben es, ihre eigenen Geräte und neben den Intel-Apps auch ihre eigenen Apps verwenden zu können. Intel-Mitarbeiter berichten, dass die Nutzung ihrer eigenen Geräte ihnen pro Tag ungefähr 57 Minuten spart, was sich unternehmensweit auf 5 Millionen Stunden jährlich beläuft.

Canadian Tire ging den anderen Weg und stattdessen seine 3.000 Mitarbeiter mit den neuen BlackBerry-Smartphones Q10 und Z10 aus. (Canadian Tire ist eines der größten kanadischen Einzelhandelsunternehmen, verfügt über einen Online-Store und 1.200 Ladengeschäfte in den Sparten Autozubehör, Sport-, Freizeit- und Arbeitskleidung, betreibt Tankstellen und Waschstraßen und bietet Finanzdienstleistung.) Das Unternehmen war der Meinung, dass für seine Zwecke das BYOD-Modell nicht sicher genug war. Eugene Roman, der CTO bei Canadian Tire, befürchtete, dass E-Mails einen Virus in die Kerninfrastruktur des Unternehmens einschleusen könnten. Zurzeit hält das Canadian Tire Management BYOD zwar für interessant, aber noch nicht

für ausgereift genug für die wichtigsten Geschäftsanwendungen des Unternehmens.

Um erfolgreich mobile Geräte einsetzen zu können, müssen Unternehmen ihre Geschäftsprozesse sorgfältig analysieren und entscheiden, ob Mobilität für sie wichtig ist oder nicht. Nicht jedes Unternehmen profitiert von Mobilität im gleichen Maße. Ohne eine klare Vorstellung, wie sich mobile Geräte mit den langfristigen Plänen des Unternehmens genau vereinbaren lassen, verschwenden Unternehmen nur unnötig ihr Geld für überflüssige Geräte und Programme.

Quellen: Dennis McCafferty, „Surprising Facts About Mobility and BYOD“, Baseline, 29. Januar 2014; Beatrice Piquer-Durand, „BYOD and BYOA: Dangers and Complications“, Techradar Pro, 24. März 2014; Tam Harbert, „Android Invades the Enterprise“, Computerworld BYOD Consumerization of IT, November 2013; Forrester Consulting, „The Total Economic Impact of IBM Managed Mobility for BYOD“, Mai 2013; Fred Donovan, „The Growing BYOD Problem“, FierceMobileIT, 13. Februar 2013; Brian Bergstein, „IBM Faces the Perils of ‘Bringing Your Own Device’“, MIT Technology Review, 21. Mai 2013; Matt Hamblen, „Canadian Tire forgoes BYOD, Issues BlackBerry to Workers“, Computerworld, 20. Mai 2013.

FRAGEN ZUR FALLSTUDIE

1. Welches sind die Vor- und Nachteile, wenn Mitarbeiter ihre privaten Smartphones am Arbeitsplatz nutzen?
2. Welche Faktoren in Management, Organisation und Technik sollten bei der Entscheidung berücksichtigt werden, ob Mitarbeiter ihre privaten Smartphones am Arbeitsplatz nutzen dürfen?
3. Vergleichen Sie die BYOD-Erfahrungen von IBM mit denen von Intel. Warum funktionierte BYOD bei Intel so gut?
4. Ein Unternehmen, das seinen Mitarbeitern erlaubt, eigene Smartphones auf der Arbeit zu nutzen, kann damit Geld sparen. Sind Sie der gleichen Meinung? Warum beziehungsweise warum nicht?

Blickpunkt Management

Zu Kapitel 13: Das Abrechnungssystem von Austin Energy zündet nicht

Austin Energy ist ein kommunaler Betrieb der Stadt Austin, Texas, und für die Strom- und Wasserversorgung sowie die Abwasser- und Abfallentsorgung von mehr als 1 Million Einwohnern der Stadt und den umliegenden Gemeinden zuständig. Das Unternehmen erwirtschaftet jedes Jahr Profite für die Kommune und hat von 1976 bis heute das Unternehmen Dividenden in Höhe von 1,5 Milliarden US-Dollar an die Stadt Austin ausgeschüttet, mit denen unter anderem öffentliche Ausgaben für Feuerwehr, Polizei, medizinischen Notdienst, Parks und Bibliotheken bestritten wurden.

Austin Energy hat eines der größten Erneuerbare-Energien-Programme des Landes, aber die dafür erforderlichen intelligenten Messgeräte und neueren Technologien ließen sich nicht in die veralteten Abrechnungssysteme integrieren. Außerdem gab es keine kundenfreundlichen Angebote, wie die Möglichkeit, den monatlichen Zeitpunkt der Rechnungsbegleichung zu wählen. Um sein Abrechnungssystem zu modernisieren und seine Informationssysteme auf den gleichen aktuellen Stand wie seine neuen Methoden zur Energieeinsparung zu bringen, beauftragte Austin Energy 2009 IBM mit der Erstellung eines zentralen Abrechnungssystems einschließlich Betrieb für die folgenden fünf Jahre. Austin einigte sich mit IBM auf eine Gesamtsumme von 55 Millionen US-Dollar, von denen 38 Millionen auf die Erstellung und Installation des neuen Abrechnungssystems entfielen und 17 Millionen auf den Betrieb des Systems für fünf Jahre nach Fertigstellung. Das neue System war für die Abrechnung von Wasser, Abfall und Recycling ausgelegt. Austin war optimistisch, dass eine erfolgreiche Installation sich am Ende durch die Ersparnisse rechnen würde.

Bisher war das Projekt eine einzige Enttäuschung. Das System sollte 2011 in Betrieb genommen werden, aber es ist immer noch nicht voll funktionstüchtig. Softwarefehler haben zu Abrechnungsfehlern in Tausenden von Rechnungen geführt. Über 65.000 Kunden haben nie eine Rechnung erhalten und 35.000 weitere Kunden erhielten fehlerhafte Rechnungen. Ein Unternehmen, das Austin Energy 3.000 US-Dollar schuldet, erhielt beispielsweise eine Rechnung über 300.000 US-Dollar. Obwohl Austin Energy die

betroffenen Konten ermitteln konnte und mit den einzelnen Kunden jeweils eine Lösung erarbeitete, war das Unternehmen nicht auf die große Unzufriedenheit seiner Kunden mit dem neuen System vorbereitet. Die Kundendienstabteilung wurde mit Beschwerden entrüsteter Kunden förmlich bombardiert.

Laut Larry Weiss, einem Manager bei Austin Energy, hat Instabilität auf Dauer ernste und kostspielige Auswirkungen auf das Geschäft und schreckt die Kunden ab. Aufgrund hartnäckiger Systemfehler konnte das Unternehmen den Wasserverbrauch der Bewohner von Mietwohnungen nicht berechnen, die Bücher nicht abschließen und die Auditberichte nicht abgeben. Ohne die Möglichkeit, die Versorgungsleistungen in Rechnung zu stellen, gingen der Stadt Austin Einnahmen verloren.

Vertreter von Austin Energy sehen die Schuld für die Probleme mit dem Projekt bei IBM. Der CIO von Austin Energy, Alan Claypool, behauptete in einem Interview „wir haben immer noch kein stabiles System (und) wir sind zutiefst von der Qualität des Services, den wir bisher von IBM erhalten haben, enttäuscht“. In einer Nachricht von September 2011 stellte er fest, dass IBM bei der Implementierung des Systems wiederholt ein und derselbe Fehler unterlaufen war. Zwei getrennte Fehler von IBM verzögerten das Projekt um 37 Stunden, und einen dieser Fehler hatte dasselbe Team bereits im Dezember 2010 gemacht. „Wir sind schwer enttäuscht über die Verzögerungen und der offensichtlichen stümperhaften Vorgehensweise bei der Betreuung dieses Projekts“, so Claypool.

Das Unternehmen plant jetzt, in zukünftigen Verträgen mit IBM Bestimmungen vorzusehen, die das Unternehmen gegen ähnliche Pannen schützen und vor allem die Verfügbarkeit des Systems sicherstellen sollen. Zurzeit hält Austin Energy einen Betrag in Höhe von 3,8 Millionen US-Dollar zurück, den IBM erst erhält, wenn das System die grundlegenden Leistungsbenchmarks erfüllt.

Claypool und andere hochrangige Manager bei Austin Energy haben sich mehrmals direkt an die IBM-Führungsriege gewandt, von den Betreuern des Abrechnungssystem-Projekts bis hin zum damaligen IBM CEO Sam Palmisano. Zuerst

schrieb Claypool direkt an Marc Lautenbach, den Leiter der IBM-Abteilung Global Business Service in Nordamerika, der für das Abrechnungssystem-Projekt verantwortlich war. Er erläuterte, dass sie bei Tausenden von Kunden individuelle Hilfe benötigten, um auf deren Konten zuzugreifen und Abrechnungsfehler zu korrigieren. Daraufhin wurde Lautenbach als Leiter für Global Business durch Frank Kern ersetzt, der an Austin zurückschrieb und einen Fünf-Stufen-Plan vorstellte, mit dem IBM die Probleme mit dem Abrechnungssystem beheben wollte.

Kerns Plan war es, die Kommunikation zu verbessern, um sicherzustellen, dass die Probleme mit dem System und deren betriebliche Auswirkungen an die richtigen Personen weitergeleitet werden. Außerdem wollte er Best-Practices-Prozesse implementieren, um den Erfolg auf Dauer zu sichern, stärker mit Drittanbietern wie Oracle zusammenarbeiten und Lücken außerhalb des Projektrahmens und der empfohlenen Lösungen identifizieren. Doch kurz darauf trat Kern in den Ruhestand und Claypool schrieb erneut an IBM, um mitzuteilen, dass das Abrechnungssystem von Austin Energy seit der Aufstellung des Fünf-Stufen-Plans keine Fortschritte mehr gemacht hatte. Der Vorstand von Austin Energy lehnte außerdem den Vorschlag von IBM ab, als Lösung leistungsstärkere Server zu erwerben, da dies die Kommunalwerke zwingen würde, mehr als ursprünglich geplant für das Projekt auszugeben.

Trotz aller Patzer hofft Austin Energy immer noch auf eine erfolgreiche und einvernehmliche Lösung des Problems. Die Beziehung zwischen Austin Energy und IBM besteht bereits seit etlichen Jahren, seit die beiden Unternehmen einen Vertrag schlossen, zusammen ein Lagerverwaltungssystem für die Stadt zu entwickeln. Obwohl es auch bei diesem System Probleme gab, sind diese nichts im Vergleich zu dem Abrechnungssystem-Fiasco. Austin Energy behauptet außerdem, dass die Fehler von IBM dem Unternehmen seit Projektbeginn bereits 8 Millionen US-Dollar gekostet hätten, sodass ein Wechsel zu einem anderen Anbieter die Sache nur verschlimmern würde – vor allem in Anbetracht der Tatsache, wie viel Geld Austin Energy bereits in die

Produktentwicklung bei IBM investiert hat. Als IBM um eine Stellungnahme gebeten wurde, hieß es nur, dass das Unternehmen zusammen mit Austin Energy daran arbeitet, eine Lösung für das Abrechnungssystem zu finden.

IBM hat in der Vergangenheit bereits andere Projekte wie dieses erfolgreich betreut. Das IBM-Abrechnungssystem besteht aus Oracle-Datenbanken, die auf einer IBM-WebSphere-Middleware und Tivoli-Management-Tools aufsetzen. Die Probleme mit dem System waren nicht nur auf eine, sondern auf mehrere Ursachen zurückzuführen. Das neue Abrechnungssystem mit seinen 73 verschiedenen Schnittstellen ist sehr komplex und es war unbestritten sehr schwierig sicherzustellen, dass alle Schnittstellen nahtlos ineinandergriffen. Kunden konnten nicht auf das Onlineportal des Systems zugreifen und die Mitarbeiter von Austin Energy machten durchweg negative Erfahrungen mit dem System, denn angesichts der vielen Fehler und Probleme, die es in einer Live-Version eigentlich nicht geben sollte, fühlten sie sich als „Alpha-Tester“.

Ungefähr einer von vier Austin-Kunden hatte Probleme mit dem IBM-System. Einigen Kunden wurde ihr Konto gekündigt, was nur mittels diverser Telefonanrufe geklärt werden konnte. Der Kummer mit dem Abrechnungssystem kam für Austin Energy zu einem äußerst ungünstigen Zeitpunkt, da sie planten, die erste Gebührenerhebung seit 17 Jahren vorzunehmen. Doch das PR-Desaster aufgrund des fehlerbehafteten Abrechnungssystems, zwang das Unternehmen, diese Pläne vorerst auf Eis zu legen.

Seit Februar 2012 sind die meisten – wenn auch nicht alle – Fehler des Abrechnungssystems behoben. Claypool war zuversichtlich, dass Austin Energy auch weiterhin eine einvernehmliche Geschäftsbeziehung zu IBM unterhalten und die Arbeit erfolgreich beenden könnte. IBM habe auf die Beanstandungen zwar reagiert, so Claypool, aber leider nur schrittweise. „Wir erwarten eigentlich eine schnellere Reaktion.“ In Zukunft werden die Outsourcing-Verträge von Austin Energy höhere Strafen vorsehen bei Nichterfüllung seitens des Anbieters, einschließlich der Frage der Systemverfügbarkeit.

► Forts.

Quellen: Paul McDougall, „Chronology of an Outsourcing Disaster“, Information Week, 23. Februar 2012; „Austin Energy Fixes Billing System Bug“, MyFoxAustin.com, 22. Februar 2012; www.austinenergy.com vom 22. März 2012.

FRAGEN ZUR FALLSTUDIE

- 1.** Ist das Austin-Energy-Projekt fehlgeschlagen? Erläutern Sie Ihre Antwort.
- 2.** Beschreiben Sie die betrieblichen Auswirkungen des ins Stocken geratenen Projekts von Austin Energy.
- 3.** Inwiefern war IBM verantwortlich für die Probleme beim Abrechnungsprojekt von Austin Energy? Oder war Austin Energy schuld an den Problemen? Erläutern Sie Ihre Antwort.
- 4.** Welche Organisations-, Technik- und Managementfaktoren waren am Misserfolg des Projekts beteiligt?
- 5.** Beschreiben Sie die Schritte, die Austin Energy und IBM hätten ergreifen sollen, um dieses Projekt besser zu stemmen.