Kernkompetenzzentrum
Finanz- & Informationsmanagement

Fraunhofer FIT
Projektgruppe
Wirtschaftsinformatik

IT-Konsumerisierung: Strategien und Maßnahmen in mittelständischen Unternehmen

von

Matthias von Entreß-Fürsteneck, Nils Urbach, Christoph Buck[1], Torsten Eymann

in: HMD - Praxis der Wirtschaftsinformatik, 53, 2, 2016, S. 254-264

Die finale Publikation ist auch erhältlich unter
http://link.springer.com/article/10.1365/s40702-016-0211-3

[1] Universität Bayreuth

Universität Augsburg, D-86135 Augsburg
Besucher: Universitätsstr. 12, 86159 Augsburg
Telefon: +49 821 598-4801 (Fax: -4899)

Universität Bayreuth, D-95440 Bayreuth
Besucher: Wittelsbacherring 10, 95444 Bayreuth
Telefon: +49 921 55-4710 (Fax: -844710)

www.fim-rc.de

HMD (2016) 53:254–264
DOI 10.1365/s40702-016-0211-3

IT-Konsumerisierung: Strategien und Maßnahmen in mittelständischen Unternehmen

Matthias von Entreß-Fürsteneck · Nils Urbach · Christoph Buck · Torsten Eymann

Eingegangen: 9. Februar 2016 / Angenommen: 15. Februar 2016 / Online publiziert: 5. April 2016

Zusammenfassung Durch die zunehmende Konsumerisierung im Bereich der Informationstechnologie (IT) stehen IT-Abteilungen vor der Herausforderung, den Wunsch der Mitarbeiter, dieselben mobilen Endgeräte sowohl zu privaten als auch zu beruflichen Zwecken nutzen zu können, mit den Vorgaben und Möglichkeiten der Unternehmens-IT zu vereinbaren. Typischerweise wird zur Bewältigung dieser Anforderung das Konzept des „Bring Your Own Device" (BYOD) genannt, obwohl sich in den letzten Jahren auch alternative Ausgestaltungsformen herausgebildet haben. Unter der Annahme, dass mittelständische Unternehmen im Vergleich zu Großunternehmen signifikante Unterschiede in der Unternehmensorganisation im Allgemeinen als auch in der IT-Organisation im Speziellen aufweisen, sind bei der Strategiewahl die Anforderungen dieser Unternehmen berücksichtigen.

M. von Entreß-Fürsteneck (✉)
Professur für Wirtschaftsinformatik und Strategisches IT-Management, Universität Bayreuth
95440 Bayreuth, Deutschland
E-Mail: matthias.entress-fuersteneck@uni-bayreuth.de

N. Urbach (✉)
Lehrstuhl für Wirtschaftsinformatik, Universität Bayreuth
95440 Bayreuth, Deutschland
E-Mail: nils.urbach@uni-bayreuth.de

C. Buck (✉)
Kernkompetenzzentrum Finanz- & Informationsmanagement, Universität Bayreuth
95440 Bayreuth, Deutschland
E-Mail: christoph.buck@uni-bayreuth.de

T. Eymann (✉)
Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT, Universität Bayreuth
95440 Bayreuth, Deutschland
E-Mail: torsten.eymann@uni-bayreuth.de

Schlüsselwörter IT-Konsumerisierung · Bring Your Own Device · Company Owned Personal Enabled · Mittelstand

1 Das Phänomen der IT-Konsumerisierung in Unternehmen

IT-Konsumerisierung beschreibt den Trend, technologische Innovationen, die ursprünglich für den Konsumentenmarkt entwickelt wurden, auch im geschäftlichen Umfeld zu nutzen. Zentraler Treiber dieser Entwicklung ist, dass seit einiger Zeit Innovationen im Umfeld der Informations- und Telekommunikationstechnologie (IKT) oftmals zunächst in den Konsumentenmarkt eindringen, bevor sie Einzug in Unternehmen halten. Hierdurch entsteht eine veränderte Erwartungshaltung der Mitarbeiter an den Arbeitgeber, da diese nun im privaten Umfeld erfahrener im Umgang mit der Anwendung innovativer IKT sind und ihre Gewohnheiten auf die betriebliche Nutzung übertragen möchten. Da die aus dem privaten Kontext bekannten, technologischen Innovationen in der Regel durch hohe Bedienfreundlichkeit und neue Anwendungsmöglichkeiten hervorstechen, steigt gleichzeitig die Unzufriedenheit mit der im Unternehmen bereitgestellten Infrastruktur, da diese in der Wahrnehmung der Mitarbeiter nicht mehr den (gestiegenen) Anforderungen an eine moderne IT-Unterstützung entsprechen (Weiß und Leimeister 2012). Ein Resultat aus dieser Entwicklung ist, dass insbesondere sogenannte „Digital Natives“ (IT- und internetaffine Mitarbeiter, nach 1980 geboren), aber genauso auch Mitarbeiter aus dem Top-Management, vermehrt unkontrolliert private Endgeräte und Anwendungen im betrieblichen Umfeld nutzen. Vor allem aufgrund von Sicherheitsbedenken und Schwierigkeiten im Support wird der Einsatz privater IT-Lösungen in den meisten Unternehmen bislang nicht unterstützt. Das zunehmend größer werdende Interesse seitens der Belegschaften und der daraus resultierende Druck auf die IT-Abteilungen führen derzeit jedoch zu einem Umdenken (Weiß und Leimeister 2012).

Die aus dem Konsumentenmarkt übernommenen Innovationen sind typischerweise Web-2.0- Technologien sowie mobile Endgeräte und Anwendungen. Zu den Web-2.0-Technologien gehören unter anderem Social-Media-Anwendungen wie z. B. Facebook und Twitter oder Cloud-Computing-Dienste wie Dropbox. Sie dienen meist der Verbesserung der Kollaboration und des Informationsaustausches der Mitarbeiter. Unter mobilen Endgeräten und Anwendungen werden moderne Smartphones und Tablets wie z. B. das iPhone oder iPad von Apple verstanden, welche zunehmend klassische Unternehmensgeräte verdrängen (Weiß und Leimeister 2012, 2013).

Hinsichtlich der Nutzung von mobilen Endgeräten können drei wesentliche Vorteile für Unternehmen genannt werden, die mit der IT-Konsumerisierung einhergehen. So können monetäre Vorteile durch die Reduktion fixer und variabler Kosten erzielt werden. Diese Kostenreduktion kann beispielsweise durch den Wegfall von Beschaffungs- und Nutzungskosten erreicht werden. Durch die Nutzung mobiler Endgeräte sind die Mitarbeiter zudem in der Lage, zeit- und ortsunabhängig zu arbeiten und durch die Nutzung gewohnter Anwendungen ihre Arbeit effizienter zu gestalten. Hierdurch kann auf eine höhere Produktivität der Mitarbeiter geschlossen werden. Als weiterer Vorteil kann die Imageverbesserung für Unternehmen genannt werden. Unternehmen, welche den Einsatz von Konsumenten-IT zulassen,

werden von (potenziellen) Mitarbeitern meist als attraktiver angesehen und kommen daher eher als potenzielle Arbeitgeber infrage (Trend Micro 2011; Weiß und Leimeister 2012). Neben den genannten Vorteilen der IT-Konsumerisierung dürfen aus Unternehmenssicht die potenziellen Risiken im Bereich Datenschutz und Datensicherheit, die erforderlichen Maßnahmen zur Integration in die bestehende Unternehmens- und IT-Infrastruktur sowie die gesteigerten Aufwände für Wartung und Support nicht unterschätzt werden. Unternehmen, die mit der IT-Konsumerisierung häufig unvorbereitet konfrontiert werden, sind daher gefordert, sich dieser Themen anzunehmen, eine entsprechende Strategie zu definieren und diese schließlich auch umzusetzen (Aerospace Industries Association 2011; Weiß und Leimeister 2012; Boelmann 2013).

2 Strategien zum Umgang mit IT-Konsumerisierung

Als Strategien zum Umgang mit der IT-Konsumerisierung kommen unterschiedliche Lösungen in Betracht, die sich in einem Rahmen zwischen vollständiger Unternehmenskontrolle und völliger Freiheit des Nutzers bewegen. Faktoren wie Unternehmenskultur, Sicherheitsanforderungen und Kosten beeinflussen dabei die Strategiewahl. Entscheidet sich ein Unternehmen, die vollständige Kontrolle über seine IT-Infrastruktur behalten zu wollen, so stellt dies gewissermaßen eine Ablehnung der IT-Konsumerisierung dar. Das Unternehmen entscheidet über die Art und Anzahl von im Unternehmen verwendeten Geräten und Anwendungen, ohne die Mitarbeiter in den Auswahlprozess einzubinden. Dadurch sollen Kosten minimiert (Standardisierungsvorteil) sowie die Wartung und Sicherheitsmaßnahmen vereinfacht werden. Anwender dieser Strategie haben häufig einen exklusiven Vertrag mit einem einzigen Anbieter für IT-Infrastruktur, der im Extremfall in einem unternehmensweiten Standard für Technologie mündet (Harris et al. 2011; Harteveld 2012). Eine gegenteilige Strategie ist die Gewährung vollständiger Freiheit für den Nutzer hinsichtlich der Wahl seiner Endgeräte. Unternehmen, die diese Strategie verwenden, lassen Geräte und Anwendungen ohne Reglementierung im Unternehmen zu. Sie haben keinerlei Richtlinien, Vollmachten oder Anreize, oder setzen diese nicht durch. Vorteilhaft an dieser Strategie ist die Einsparung von IT-Kosten durch den Wegfall von Beschaffung und Support. Es entstehen jedoch auch Nachteile durch mögliche Produktivitätseinbußen, beispielsweise durch inkompatible Hard- und Software und den Selbstsupport durch den Mitarbeiter. Weiterhin entstehen Nachteile durch eine eingeschränkte Möglichkeit, für Datenschutz und -sicherheit zu sorgen. Diese Strategie ist häufig in kreativen oder innovativen Unternehmen sowie Universitäten vorzufinden (Harris et al. 2011; Harteveld 2012).

Zwischen diesen zwei Extremen sind weitere Strategien denkbar, die einen kontrollierten und reglementierten Umgang mit der IT-Konsumerisierung ermöglichen. Wir sprechen an dieser Stelle von sogenannten *proaktiven IT-Konsumerisierungsstrategien*. Ein Einstieg weg von standardisierter IT hin zu flexibleren Strukturen wird durch die Wahlmöglichkeit der Mitarbeiter aus ausgewählter Hard- und Software des Unternehmens erreicht. Bei dieser Strategie stellt das Unternehmen eine Auswahl aus unterschiedlichen Konsumentengeräten zur Verfügung und erweitert

die Palette von wählbaren Geräten sukzessive. Alternativ können auch alle Geräte zugelassen werden, die bestimmte technische Spezifikationen erfüllen, beispielsweise hinsichtlich Verschlüsselung, Passwortschutz, Remote-Zugriff oder Betriebssystemversion. Der Nutzer dieser Geräte muss einer Nutzungsrichtlinie zustimmen, die dem Unternehmen Rechte in Bezug auf den Zugriff auf das Endgerät einräumen. Darüber hinaus können Anwendungen zur Installation freigegeben werden, die der Nutzer für Unternehmenszwecke nutzen möchte, wenn diese nicht die bestehenden Unternehmensanwendungen behindern. Diese Strategie bietet einen sicheren Weg, sich der IT-Konsumerisierung zu öffnen. Sie hat jedoch zum Nachteil, dass die Auswahl der zugelassenen Geräte und Anwendungen ständig aktualisiert werden muss und der Nutzer durch die Vorauswahl in seiner Gestaltungsfreiheit dennoch eingeschränkt wird (Harris et al. 2011; Harteveld 2012). Erfolgt die Reglementierung in der eben beschriebenen Strategie über eine Beschränkung der Auswahl an Hard- und Software, so ist als weitere Strategie auch eine Beschränkung anhand bestimmter Mitarbeiterprofile denkbar. Diese Strategie basiert auf der Annahme, dass die Mitarbeiter eines Unternehmens unterschiedliche Ansprüche und Interessen hinsichtlich der Nutzung von Konsumententechnologie im Unternehmen haben. Für Unternehmen, die eine diversifizierte Mitarbeiterstruktur mit unterschiedlichen technologischen Anforderungen besitzen, erscheint es daher sinnvoll, die Mitarbeiter anhand ihrer Rollen und Aufgaben zu segmentieren und die IT-Richtlinien für jede Gruppe entsprechend anzupassen. Nachteilig bei dieser Strategie ist jedoch der umfangreiche Planungs- und Entwicklungsaufwand (Harris et al. 2011).

Die bislang vorgestellten Strategien sind in Ihrer Ausgestaltung tendenziell restriktiv und ermöglichen dem Unternehmen eine stärkere Kontrolle über die eingesetzten Konsumentengeräte. Die nachfolgend vorgestellte Strategie hingegen legt die Verantwortung stärker in die Hände des einzelnen Mitarbeiters und ist somit offener gestaltet. Kernelement dieser Strategie ist die Zurverfügungstellung eines Budgets durch das Unternehmen, mit dem sich der Mitarbeiter seine gewünschten und benötigten IT-Geräte und Anwendungen selbstständig zusammenstellen kann (z. B. Laptops, Smartphones, Tablets, Software und Zubehör). Die Mitarbeiter erhalten somit mehr Eigenständigkeit in der Wahl ihrer Ausstattung, sind jedoch zugleich aufgefordert von Supportanfragen an die IT abzusehen. Dadurch hat das Unternehmen den Vorteil, Supportkosten einzusparen und die IT-Abteilung stärker mit innovativen Aufgaben betrauen zu können. Jedoch ist es auch bei dieser Strategie notwendig, gewisse Rahmenbedingungen hinsichtlich der zugelassenen Technologien zu setzen und diese fortlaufend anzupassen (Harris et al. 2011; Harteveld 2012).

Neben den drei vorgestellten Hauptstrategien zum aktiven Umgang mit der IT-Konsumerisierung, sind durch Kombination dieser weitere Strategien denkbar. Die wenig restriktiv gestaltete Strategie der Gewährung eines Budgets kann beispielsweise dadurch eingeschränkt werden, dass bestimmte Gerätemarken und/oder -klassen ausgeschlossen werden oder nur bestimmte Mitarbeitergruppen einen Anspruch auf das Budget erhalten. Eine sehr restriktive Strategie lässt sich zudem gestalten, wenn nur bestimmte Mitarbeitergruppen aus einer eingeschränkten Auswahl von Konsumentengeräten, die durch das Unternehmen bereitgestellt werden, wählen dürfen. Eine weitere Differenzierung der Strategie der Rollensegmentierung und der Budgetstrategie kann zudem anhand des Merkmals des Eigentums an den eingesetzten

Konsumentengeräten erreicht werden. Ist der Mitarbeiter Käufer und Eigentümer der eingesetzten Konsumentengeräte (typischerweise als Bring Your Own Device bekannt), geht dies mit rechtlichen Schwierigkeiten und Kontrollverlust über Geräte und Daten für das Unternehmen einher. Bleibt das Unternehmen jedoch Eigentümer (ohne zwangsläufig auch Käufer zu sein) und gestattet seinem Mitarbeiter die private Nutzung, können diese Probleme eliminiert werden (sog. Choose Your Own Device; Computerwoche 2014).

3 Anforderungen einer proaktiven IT-Konsumerisierungsstrategie

Entscheidet sich ein Unternehmen dazu, der IT-Konsumerisierung durch eine proaktive Strategie zu begegnen, sind initiativ und fortlaufend Umsetzungsmaßnahmen in unterschiedlichen Unternehmensbereichen durchzuführen. Grundvoraussetzung dafür ist, dass das Management gewillt ist, sich von bestehenden Prozessen und Richtlinien in der (IT-)Organisation zu lösen (z. B. keine homogene IT-Infrastruktur, weniger Kontrolle über Geräte und Daten) und Veränderungen aktiv zu fördern. Erst durch die Auflösung starrer IT-Strukturen kann ein Unternehmen die mit der IT-Konsumerisierung einhergehenden Vorteilte realisieren. Die Anforderungen für die Einführung einer proaktiven Strategie lassen sich hinsichtlich der Anforderungen an das IT-Management und den regulatorische Anforderungen unterteilen.

3.1 Anforderungen an das IT-Management

Die IT-Konsumerisierung ist ein Trend, der viele Unternehmen relativ unvorbereitet trifft, so dass oftmals eher reagiert als agiert wird (Weiß und Leimeister 2012). Um einer unkontrollierten Nutzung von Kosumentengeräten durch die Mitarbeiter entgegen zu wirken, sollte die Unternehmensleitung eine Strategie zur IT-Konsumerisierung entwickeln, welche die Freiheitsgrade der Mitarbeiter mit den Anforderungen des Unternehmens nach Sicherheit und Kontrollierbarkeit unter Berücksichtigung personeller, technischer und finanzieller Möglichkeiten in Einklang bringt (Computerwoche 2014). Nach der Entscheidung für eine IT-Konsumerisierungsstrategie durch die Unternehmensleitung obliegt es dem IT-Management, diese operativ umzusetzen. Je nach gewählter Strategie ist zunächst festzulegen, welche Geräte und Software in die IT-Infrastruktur eingebunden und unterstützt werden können und welchen Mitarbeitergruppen die Nutzung von mobilen Endgeräten gestattet wird.

Weiterhin sind im IT-Management Prozesse für den Support der eingesetzten Geräte und Software zu schaffen. Dabei ist gegebenenfalls auch festzulegen, inwieweit Support auch für private mobile Endgeräte angeboten wird. Mobile Endgeräte aus dem Konsumentenbereich zeichnen sich unter anderem dadurch aus, dass ihr Produktlebenszyklus in der Regel relativ kurz ist und neuere Versionen oder Nachfolgeprodukte bereits nach wenigen Monaten erscheinen. Als Folge können sich auch die Einsatzzyklen im Unternehmen verkürzen. So ist es möglich, dass der Support von alten Geräten eingestellt wird und somit keine sicherheitsrelevanten Aktualisierungen mehr möglich sind oder das Gerät nicht mehr repariert werden kann. Auch bei der eingesetzten Software ist zu beachten, dass eine an die spe-

zifischen Bedürfnisse angepasste Unternehmenssoftware auf neueren Geräten oder Betriebssystemversionen eventuell nicht mehr genutzt werden kann oder dass der Support für Drittanwendungen nicht gewährleistet wird (Weiß und Leimeister 2012, 2013).

Hinsichtlich der technischen Anpassungen sind vom IT-Management je nach gewählter Strategie höhere Anforderungen an die IT-Infrastruktur zu berücksichtigen. So kann es notwendig sein, hardwareseitig beispielsweise WLAN-Kapazitäten oder Speicherkapazitäten anzupassen, wenn diese durch die gestiegene Anzahl an drahtlosen Geräten nicht mehr ausreichen sollten. Ebenso sollte eine Überprüfung der Kommunikationsverträge vorgenommen werden, um den gestiegenen Breitbandanforderungen von mobilen Endgeräten gerecht werden zu können (Aerospace Industries Association 2011; Weiß und Leimeister 2012).

Zudem sollten Konsumentengeräte auch technisch abgesichert und kontrolliert werden können. Je nach Größe der mobilen IT-Infrastruktur und der Art der genutzten Anwendungen und Daten sind hier unterschiedliche Konzepte denkbar. Werden unkritische geschäftliche Daten verarbeitet und ist lediglich eine geringe Anzahl an Geräten im Umlauf, ist die Absicherung gegebenenfalls noch über die im mobilen Endgerät enthaltenen Sicherheits- und Kontrollmechanismen möglich (z. B. Passwortschutz, Installationssperren, etc.). Mit steigender Anzahl an Geräten oder bei kritischen Unternehmensanwendungen und -daten sollte jedoch der Einsatz spezieller Software (zum Beispiel eine Sandbox-Lösung und/oder ein Mobile Device Management System) zur Wartung und Kontrolle von Geräten in Erwägung gezogen werden (Weiß und Leimeister 2012).

Sensible Unternehmensdaten sollten technisch so gespeichert werden, dass diese reglementiert für mobile Endgeräte freigegeben werden können. Dazu muss das Unternehmen initial festlegen, welche Arten von Daten auf mobilen Endgeräten gespeichert und verarbeitet werden dürfen. Als sicherheitstechnischer Standard sollten in Unternehmen mit IT-Einsatz heutzutage Anwendungen eingesetzt werden, die Daten und den Datenverkehr überwachen und kontrollieren (beispielsweise Firewall, Virenscanner, SPAM-Schutz), um sich vor Datenmissbrauch und Schadsoftware zu schützen. In dieses Gesamtkonzept sind mobile Endgeräte zu integrieren. Dazu gehört auch, das Risikomanagement für den Fall eines Sicherheitsvorfalles mit einem mobilen Endgerät zu überarbeiten (Aerospace Industries Association 2011; Boelmann 2013).

Eine umfassende technische Absicherung der eingesetzten mobilen Endgeräte umfasst neben der Nutzung von speziellen technischen Maßnahmen auch die Festlegung, welche (Sicherheits-) Standards ein mobiles Endgerät mindestens erfüllen muss bzw. welche Funktionen aktiviert werden müssen. Dies reicht von der Festlegung von Sicherheitseinstellungen (z. B. PIN-Schutz) bis hin zum Verbot von Geräten mit einem bestimmten Betriebssystem (Aerospace Industries Association 2011; Boelmann 2013).

3.2 Regulatorische Anforderungen

Unternehmen, die mit der IT-Konsumerisierung konfrontiert werden, haben verschiedenste regulatorische Anforderungen zu beachten. Es ist daher zunächst erfor-

derlich zu erfassen, welche regulatorische Anforderungen, in Abhängigkeit von der gewählten IT-Konsumerisierungsstrategie, beachtet werden müssen. Dazu gehören (Boelmann 2013):

- *Arbeitsrecht:* Regelungen für die Vergütung geleisteter Arbeitszeit mit einem mobilen Endgerät außerhalb der üblichen Arbeitszeit und -stätte.
- *Datenschutz:* Regelungen für die Verarbeitung von personenbezogenen Daten auf mobilen Endgeräten.
- *Datensicherheit:* Regelungen hinsichtlich der Sicherung von Daten auf mobilen Endgeräten.
- *Urheberrecht*: Regelungen, die die Speicherung und/oder Verarbeitung von urheberrechtlich geschütztem Material auf mobilen Endgeräten betreffen (z. B. Verantwortlichkeit bei Speicherung von illegal erworbener Musik).
- *Lizenzrecht*: Regelungen, die die Nutzungserlaubnis von Software auf mobilen Endgeräten betreffen (Einsatz von privater Software im kommerziellen Umfeld bzw. vom Unternehmen erworbener Software auf privaten Geräten).
- *Unternehmenssicherheit*: Regelungen, die den Zugriff auf Hard- und Software sowie die Speicherung von Daten festlegen (z. B. Zugriff durch das Unternehmen, Trennung von privaten und Unternehmensdaten, Anfertigung von Backups, Verlust von Geräten).

Wurden die betroffenen Rechtsgebiete im Unternehmen identifiziert, ist es anschließend notwendig, mit den Nutzern von privaten mobilen Endgeräten eine Nutzungsrichtlinie zu vereinbaren, welche entsprechende Regelungen zu den kritischen Rechtsgebieten festlegt sowie die Rechte und Pflichten des Unternehmens und des Nutzers absichert. Die Richtlinien für Nutzer sollten klar definieren, welche Anwendungen und Daten auf den eingesetzten Geräten installiert bzw. genutzt werden dürfen. Neben den Regelungen für den Nutzer, sollte sich das Unternehmen notwendige Rechte zur Wartung und Kontrolle der mobilen Endgeräte zusichern lassen. Dazu gehören beispielsweise das Recht, Anwendungen und Daten einzusehen und auf Schadsoftware zu überprüfen sowie im Zweifel das Gerät zu sperren und zu löschen (Aerospace Industries Association 2011; Weiß und Leimeister 2012; Boelmann 2013).

4 Interviewstudie: IT-Konsumerisierung in mittelständischen Unternehmen

Typischerweise wird von mittelständischen Unternehmen angenommen, dass diese im Vergleich zu Großunternehmen sowohl signifikante Unterschiede in der allgemeinen Unternehmensorganisation als auch im IT-Management aufweisen. So ist die Unternehmensorganisation oftmals durch eine geringere Formalisierung sowie Planungs- und Organisationsstruktur geprägt. Des Weiteren ist das IT-Management oft einem höheren Kostendruck ausgesetzt, da es ähnliche Anforderungen wie in Großunternehmen hat, aber keine entsprechenden Skaleneffekte realisieren kann. Dies geht einher mit einer begrenzten Anzahl an IT-Betreuungskräften. Zudem gibt es in mittelständischen Unternehmen häufig Nachholbedarf im Umgang mit Sicher-

heitsvorfällen, dem Notfallmanagement und in der Bewertung von Gefahrenbereichen (Payr 2003; Bundesamt für Sicherheit in der Informationstechnik 2011).

Unter Berücksichtigung dieser Annahmen stellt sich die Frage, welchen Stellenwert die IT-Konsumerisierung in mittelständischen Unternehmen hat und welche IT-Konsumerisierungsstrategien angewendet werden? Weiterhin ist zu ergründen, ob die Anforderungen an eine aktive IT-Konsumerisierungsstrategie umgesetzt werden? Zur Beantwortung dieser Fragen wurde eine qualitativ-empirische Interviewstudie in zwölf deutschen mittelständischen Unternehmen aus dem Industrie- und Dienstleistungssektor durchgeführt, in denen jeweils ein leitfadengestütztes Experteninterview geführt wurde. Als Experten wurden dabei ausschließlich IT-Verantwortliche des jeweiligen Unternehmens befragt, die entweder die Gesamtverantwortung für die Unternehmens-IT tragen oder speziell für die mobile IT-Infrastruktur zuständig sind. Durch die Befragung von IT-Verantwortlichen war es möglich, nicht nur die Gründe für die Strategieentscheidung durch die Unternehmensleitung zu erhalten, sondern auch ein umfassendes und detailliertes Bild über die konkrete Umsetzung durch die IT-Abteilung erhalten zu können.

4.1 Bedeutung und Umsetzungsstand

Im Rahmen der Interviewstudie konnte festgestellt werden, dass das Thema IT-Konsumerisierung bei allen befragten mittelständischen Unternehmen wahrgenommen, der Umgang mit der Thematik jedoch noch sehr unterschiedlich angegangen wird. Während die Hälfte der befragten IT-Verantwortlichen angab, dass sie bereits private mobile Endgeräte zu beruflichen Zwecken im Unternehmen zulassen, ist bei der anderen Hälfte die Ausgabe von ausgewählten Unternehmensgeräten die bevorzugte Strategie. Diese wird häufig kombiniert mit der Einschränkung auf bestimmte Mitarbeitergruppen mit einer speziellen Notwendigkeit an einem mobilen Endgerät (z. B. Außendienst, Bereitschaftsdienst und Führungskräfte). Der Hauptgrund zum Einsatz von Unternehmensgeräten ergibt sich zumeist aus der Notwendigkeit, bestimmte Mitarbeiter jederzeit erreichen zu können und eine gewisse Unabhängigkeit vom Arbeitsplatz zu ermöglichen. Die Zurückhaltung, auch private mobile Endgeräte zuzulassen begründet sich in diesen Fällen vor allem mit den fehlenden Zugriffsrechten auf das private mobile Endgerät sowie der fehlenden technischen Kontrolle.

4.2 Anforderungsumsetzung

Neben der Ermittlung der Bedeutung und des aktuellen Umsetzungsstand der IT-Konsumerisierung galt es im Wesentlichen zu klären, welche Anforderungen an eine proaktive Strategie in den befragten mittelständischen Unternehmen tatsächlich als relevant eingestuft und umgesetzt werden.

4.2.1 Umsetzungen des IT-Management

Wir haben im Rahmen der Interviews gefragt, ob die IT-Abteilungen mit Mitarbeiterschulungen, Mitarbeiterneueinstellungen oder zusätzlichem Budget gefördert

werden, um die Anforderungen der IT-Konsumerisierung bearbeiten zu können. Es zeigte sich jedoch, dass diese Maßnahmen in kaum einem Unternehmen umgesetzt werden. So wurden keine Neueinstellungen vorgenommen, und nur in einem Unternehmen wurde eine Schulung für IT-Mitarbeiter durchgeführt. Dies wird von den befragten IT-Verantwortlichen jedoch nicht als Nachteil empfunden, da sie nach eigener Aussage selbst in der Lage sind, sich das notwendige Wissen zum Umgang mit der IT-Konsumerisierung anzueignen.

Hinsichtlich der Anforderung, Produktlebenszyklen und Supportleistungen anzupassen, werden von den befragten IT-Verantwortlichen ebenfalls kaum Bedenken geäußert. In Unternehmen, die eigene mobile Endgeräte ausgeben, bestehen überwiegend Rahmenverträge mit den Serviceprovidern, sodass die Geräte regelmäßig erneuert werden. Support für mobile Endgeräte bereitzustellen ist zudem üblich. Sollten auf den mobilen Endgeräten jedoch auch private Anwendungen zugelassen werden, so ist der Support teilweise nur auf die vom Unternehmen bereitgestellten Anwendungen beschränkt.

Mehr als die Hälfte der befragten Unternehmen setzt bereits ein Mobile Device Management System (MDMS) ein oder plant zukünftig die Einführung eines solchen Systems. In einigen dieser Unternehmen wird zudem eine sogenannte Sandbox eingesetzt. Die Unternehmen haben dadurch die Möglichkeit, private und geschäftliche Daten voneinander zu trennen und auf die mobilen Geräte bzw. den darauf gespeicherten Daten zuzugreifen. Unternehmen, die noch kein MDMS einsetzen, haben angegeben, dass solch ein System für ihre Zwecke überdimensioniert wäre. Weitere Anpassungen an der IT-Infrastruktur werden von den meisten der befragten Unternehmen nicht oder nur im geringen Maße durchgeführt. In der Regel beschränken sich die Anpassungen auf den Ausbau der WLAN-Infrastruktur im Unternehmen.

Aufgrund von Sicherheitsbedenken ist die Bearbeitung und Speicherung von sensiblen Unternehmensdaten auf mobilen Endgeräten in den meisten Fällen nicht erlaubt. In Einzelfällen ist der Zugriff über Remote-Anwendungen möglich, so dass keine Daten auf den mobilen Endgeräten gespeichert werden. Typischerweise wird nur die Speicherung und Bearbeitung von vermeintlich unkritischen Daten wie E-Mail, Kalender und Kontakte gestattet. Eine kontinuierliche Überwachung und Kontrolle erfolgt üblicherweise durch die Überprüfung des Unternehmensnetzwerkes (Firewall, Virenscanner, etc.). Eine direkte Überwachung der mobilen Endgeräte ist hingegen eher unüblich. In Einzelfällen erfolgt eine Prüfung zu bestimmten Anlässen, beispielsweise bei der Einrichtung oder bei Aktualisierungen. Darüber hinaus hat die Mehrheit der befragten Unternehmen definierte Prozesse zum Umgang mit Sicherheitsvorfällen, insbesondere für den Fall eines Geräteverlustes, implementiert. In der Regel wird dann die SIM-Karte gesperrt und das Gerät aus der Ferne gelöscht. Hingegen ist eine Festlegung an (Sicherheits-)Standards, für die im Unternehmen eingesetzten mobilen Endgeräte noch nicht durchgehend vorhanden. Teileweise ist noch nicht einmal vorgeschrieben, dass das Gerät mit einem PIN-Code geschützt wird. Nur vereinzelt sind die Anforderungen weitreichender, indem beispielsweise bestimmte Betriebssystemversionen vorausgesetzt werden.

4.2.2 Umsetzung von regulatorischen Anforderungen

Alle befragten IT-Verantwortlichen haben angegeben, dass sie sich der Risiken, die mit der IT-Konsumerisierung einhergehen, bewusst seien. Jedoch werden diese Risiken nicht immer auf das eigene Unternehmen bezogen. So wurde vereinzelt argumentiert, dass aufgrund der Tatsache, dass keine sensiblen Daten auf den unternehmenseigenen oder privaten Konsumentengeräten gespeichert werden dürfen, der wirtschaftliche Schaden bei Verlust oder unberechtigtem Zugriff auf das Gerät gering sei. Es wurde zudem auch angegeben, dass die Gefahr, Ziel eines gezielten Datendiebstahls oder Spionageangriffs zu werden, als gering eingestuft wird, da das Unternehmen in einem Nischenmarkt agiere und somit uninteressant für potentielle Angreifer sei. Es kann angenommen werden, dass sich diese Risikoeinschätzung auch durch das Ausbleiben schwerwiegenden Sicherheitsvorfällen ausgebildet hat.

Auch wenn das Risiko in einigen wenigen Fällen als gering eingeschätzt wird, so haben doch fast alle befragten Unternehmen die Handlungsnotwendigkeit erkannt und eine Nutzungsrichtlinie verabschiedet oder sind dabei, eine solche einzuführen. Sehr restriktiv wird dabei die Möglichkeit der Installation von Drittanwendungen gehandhabt. In den meisten der beobachteten Fälle ist die Installation gänzlich untersagt oder unterliegt gewissen Einschränkungen, so dass nur nach Genehmigung, nur auf bestimmten Geräten oder nur für kostenfreie Anwendungen Installationen durchgeführt werden dürfen.

5 Gegenwärtiger Stand und Ausblick zur IT-Konsumerisierung im Mittelstand

Die Ergebnisse der Interviewstudie haben gezeigt, dass eine strikte Befolgung der vorgestellten Anforderungen zur Bewältigung der IT-Konsumerisierung in mittelständischen Unternehmen nicht zielführend sein muss. Vielmehr sind die individuellen internen und externen Gegebenheiten sowie die Ziele des Unternehmens zu berücksichtigen. Basis einer jeden Strategie ist eine solide regulatorische und technische Absicherung in Form von Nutzungsrichtlinien und IT-Systemen. Dieses Erfordernis wird von der überwiegenden Mehrheit der untersuchten mittelständischen Unternehmen bereits umgesetzt.

Weitere Maßnahmen hängen darüber hinaus von der gewählten IT-Konsumerisierungsstrategie ab. Da als Hauptziel der mittelständischen Unternehmen häufig lediglich die verbesserte Erreichbarkeit und Flexibilität bestimmter Mitarbeiter im Vordergrund steht, eignet sich eine restriktive IT-Konsumerisierungsstrategie, die die Ausgabe von vorausgewählten Geräten an bestimmte Mitarbeitergruppen vorsieht. Folglich können die Anpassungen des IT-Management (Schulungen und Neueinstellungen, Erhöhung des IT-Budgets, Anpassung der IT-Infrastruktur, Schaffung neuer Prozesse im Support) minimal gehalten werden oder sogar komplett entfallen, da nur eine geringe Anzahl an Konsumentengeräten mit einem stark reduzierten Anwendungsumfang verwaltet werden müssen. Andererseits birgt diese restriktive Strategie die Gefahr, dass Chancen nicht genutzt und die Attraktivität des Unternehmens bei (potenziellen) Mitarbeitern geschmälert wird.

Es ist daher zu empfehlen, dass durch das IT-Management auch nach der Implementierung eine regelmäßige Überprüfung der Eignung der Strategie erfolgt und die Entwicklung der IT-Konsumerisierung weiter verfolgt wird. Ändern sich die gegenwärtigen Rahmenbedingungen, beispielsweise durch die Einführung neuer Geräte und Anwendungen oder durch ein gestiegenes Bedürfnis der Mitarbeiter, sollte die gegenwärtig implementierte Strategie gegebenenfalls entsprechend angepasst werden. Dadurch kann zum einen sichergestellt werden, dass das Unternehmen weitere Vorteile realisiert (z. B. Kosteneinsparungen), und zum anderen die Schaffung einer Schatten-IT durch die Mitarbeiter, wenn diese ohne Kenntnis des Unternehmens eigenständig neue Geräte oder Anwendungen einsetzen, verhindert werden.

Literatur

Aerospace Industries Association (2011) Best Practices for Exploiting the Consumerization of Information Technologies – Leveraging the Benefits, Avoiding the Pitfalls. http://www.aia-aerospace.org/assets/report_consumerization.pdf, Zugegriffen: März 2016

Boelmann W (2013) Bring your own device? Disaster? Everything? Business Technology (1):10–16

Bundesamt für Sicherheit in der Informationstechnik (2011) Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen – Grad der Sensibilisierung des Mittelstandes in Deutschland. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile, Zugegriffen: März 2016

Computerwoche (2014) IDC-Studie: Choose your own Device hat Bring your own Device überholt (49):8–9

Harris J, Ives B, Junglas I (2011) The Genie is out of the Bottle: Managing the Infiltration of Consumer IT into the Workforce. Accenture Institute for High Performance. http://nstore.accenture.com/IM/FinancialServices/AccentureLibrary/data/pdf/genie-out-of-bottle-it-workforce.pdf, Zugegriffen: März 2016

Harteveld A (2012) How to build a consumerization of IT strategy. Microsoft recommendations for a consumerization of IT strategy. http://az370354.vo.msecnd.net/whitepapers/How-to-build-a-consumerization-of-IT-strategy.pdf, Zugegriffen: März 2016

Payr C (2003) IT-Organisation in KMU. Josef Eul, Lohmar, Köln

Trend Micro (2011) Consumerization of IT – managing and securing consumerized enterprise IT. http://www.trendmicro.co.uk/media/wp/consumerization-of-it-whitepaper-en.pdf, Zugegriffen: März 2016

Weiß F, Leimeister JM (2012) Consumerization. IT-Innovationen aus dem Konsumentenumfeld als Herausforderung für die Unternehmens-IT. Wirtschaftsinformatik 54(6):351–354

Weiß F, Leimeister JM (2013) Consumerization: Herausforderungen für das betriebliche Informationsmanagement durch iPhone und Co. 11th International Conference on Wirtschaftsinformatik, 27th February–01st March 2013, Leipzig, Germany