BYOD (Bring Your Own Device): Chancen und Risiken

Oliver Speck

Hochschule der Medien - Nobelstraße 10, 70569 Stuttgart - os035@hdm-stuttgart.de

Kurzfassung: Der Trend „Bring Your Own Device“ (BYOD) ist beginnend ab den 2010er Jahren zu einem sehr großen Thema innerhalb der modernen IT-Abteilungen geworden. Die Entwicklung führt zu einem Umdenken in vielen Bereichen der IT und greift tief in etablierte (Sicherheits-) Konzepte ein. Dieses Paper zeigt neben naheliegenden Vorteilen wie Kosteneinsparungen durch Senkung der Anschaffungskosten für Endgeräte und einer erhofften Effizienzsteigerung der Mitarbeiter auch Nachteile auf und wägt diese gegeneinander ab. Große Risiken bestehen vor allem in den Bereichen Datensicherheit und Rufnummernmitnahmen entstehend durch die Parallelität von privaten und geschäftlichen Daten auf den jeweiligen Endgeräten. Weitere Probleme zeigen sich im Anwendersupport und der Belastung für die Netzwerk-Infrastruktur. Je nach Anwendungsfall, der Unternehmensstruktur und der Sensibilität der verarbeiteten Daten können die Risiken von BYOD somit dessen Chancen untergraben.

1 Einleitung

Mittlerweile werden Smartphones in fast allen Lebensbereichen und –Situationen mitgeführt und das in der Gesellschaft etablierte Selbstverständnis mit den Geräten jegliche Informationen zu jeder Zeit an jedem Ort abrufen zu können macht auch vor den Geschäftsdaten und Ressourcen des eigenen Arbeitsgebers nicht mehr Halt. Daraus hat sich Anfang der 2010er Jahre, kurz nach der Markteinführung der ersten Smartphones, der Trend BYOD entwickelt. Beschrieben wird dadurch genauer das Verwenden von privaten Mobilgeräten als Arbeitsmittel durch Mitarbeiter und die Einbindung der Geräte in das Firmennetzwerk. Der Begriff ist eng verwandt mit dem Prozess „Consumerization“ [1]. Dieser bezieht sich auf die Verschmelzung von beruflich und privat genutzter Systeme, Programme und Dienste in der Informationstechnik. Hierbei möchten Mitarbeiter diese Systeme, die sie aus dem privaten Umfeld kennen, auch auf den Endgeräten ihres Arbeitsgebers nutzen. Darüber hinaus existiert mit „Choose Your Own Device“ ein Konzept, bei dem Mitarbeiter ihr Gerät aus einem breiteren Portfolio des Firmenbestandes auswählen können [2]. Dieses Paper konzentriert sich jedoch ausschließlich auf das Thema BYOD, welches hingegen Geräte behandelt, die nicht Eigentum der Institution sind. Es soll einen möglichen Mehrwert für Unternehmen und Mitarbeiter dokumentieren und auf potenzielle Gefahren und Schwachstellen aufmerksam machen.

2 Chancen und Risiken von BYOD

Immer mehr Mitglieder der Generation “Digital Natives” betreten den Arbeitsmarkt und sind in Unternehmen sehr gefragt. Sie bringen neue Ansprüche in die Unternehmen, mit denen sich die IT-Abteilungen zunehmend konfrontiert sehen. Die Aussicht, mit dem eigenen Smartphone arbeitsrelevante Daten zu bearbeiten und geschäftlichen E-Mail-Verkehr orts- und zeitunabhängig abzuwickeln, sehen viele Mitarbeiter als sehr verheißungsvoll an, was sich sogar als Kriterium in ihrer Wahl des Arbeitsgebers niederschlägt [4]. Den resultierenden Umschwung innerhalb der Firmen zeigt eine Studie von Gartner Inc. laut welcher 38 Prozent der Unternehmen planmäßig bis 2016 die Ausstattung der eigenen Mitarbeiter mit Mobilgeräten der Firma einstellen wollen. Bis zum Jahr 2017 werden laut Studie sogar die Hälfte aller Unternehmen keine entsprechenden Geräte mehr an Mitarbeiter ausgeben.

2.1 Chancen für Unternehmen

2.1.1 Produktivitätssteigerung der Mitarbeiter

Ein Hauptgrund für die grundlegende Umstellung der unternehmensweiten IT und die Konzeptionierung für eine BYOD-Landschaft innerhalb eines Konzerns ist für viele Entscheidungsträger in der IT die aussichtsreiche Steigerung der Produktivität der Mitarbeiter [5]. Deren Motivation ein Gerät öfter und vor allem auch außerhalb der regulären Arbeitszeiten in die Hand zu nehmen steigt, wenn es sich dabei um ihr persönliches Smartphone handelt. Der regelmäßige Kontroll-Blick in private Messenger- und Social-Media-Apps geht zukünftig einher mit einer kurzen Kontrolle nach neu-erhaltenen, geschäftlichen E-Mails. Auch die telefonische Erreichbarkeit steigt. Mitarbeiter kennen ihr eigenes Smartphone besser und kommen damit oft geschickter zurecht als mit den durch Arbeitgeber zugewiesenen, auf andere Faktoren ausgelegten Devices. Auch etwaige Schulungen der Angestellten zur Bedienung ihres Gerätes entfallen, da die Mitarbeiter den Umgang mit ihrem Privat-Gerät meist schon autodidaktisch erlernt haben. Daher versprechen sich 64 Prozent der IT-Entscheidungsträger eine Steigerung der Mitarbeiter-Produktivität, wobei ganze 84 Prozent ein funktionierendes BYOD-Konzept als regelrechten Wettbewerbsvorteil sehen [5].

2.1.2 Imagegewinn und Zufriedenheitssteigerung

Gleichzeitig nimmt die Zufriedenheit der Mitarbeiter zu mit der Freiheit, ihre eigenen Mobilgeräte benutzen zu dürfen und zu können [1]. Sie fühlen sich in ihren Bedürfnissen besser wahrgenommen und ihre Identifikation mit dem Unternehmen steigt. Damit einher geht ein allgemeiner Image-Gewinn, der den entscheidenden Vorteil bringen kann, wenn stark gefragte Hochschulabsolventen gewonnen werden sollen. Ergänzend empfinden die Mitarbeiter es als praktisch, anstatt einem privaten und einem geschäftlichen Endgerät nun nur noch ein einziges Gerät mit sich führen zu müssen.

2.1.3 Kosteneinsparungen

Ein weiterer Vorteil von BYOD sind mögliche Kosteneinsparungen durch den Wegfall von Beschaffung, Wartung und Austausch von Mobilgeräten seitens der IT-Abteilung. Insbesondere bei kurzzeitig beschäftigten Mitarbeitern wie zum Beispiel externen Freiberufler wären keine teuren, standardisierten Geräte mit allen dazugehörigen Lizenzen anzuschaffen. Die in den vergangenen Jahren stark gewachsene Kapazität einer Unternehmens-IT ist verbunden mit einer regelrechten Kostenexplosion in den technischen Ausgaben einer Firma. Somit wird die IT oftmals ohnehin nur als reiner Kostenfaktor eines Konzerns gesehen, was eine immer weitere Budgeterhöhung schwierig werden lässt. Die zusammengesetzten Kosten zur Bereitstellung von Mobilgeräten auf die eigenen Mitarbeiter zu verlagern ist daher eine willkommene finanzielle Erleichterung.

2.1.4 Moderne Hardware in den Händen der Mitarbeiter

BYOD kann zusätzlich dafür sorgen, dass die Arbeitnehmer mit neuerer Hardware ausgestattet sind als zuvor, da der Upgrade-Zyklus persönlicher Elektronikgeräte um einiges kürzer ist als der von geschäftlichen Geräten. Die angesprochenen finanziellen Einschränkungen machen IT-Bereiche träge, während neue Entwicklungen immer schneller und schnelllebiger werden. Unternehmen können auf Dauer nicht mit der Technologie Schritt halten. Außerdem ist dieser Punkt nicht zu vernachlässigen bei den Angestellten in einem Unternehmens-Bereich für die Mobilgeräte unerlässlich sind: bei den Angestellten im Außendienst. Sie repräsentieren (auch durch ihre Hardware-Ausstattung) den Konzern beim Kunden und ihre technologische Aktualität trägt das Firmenimage direkt nach außen und entscheidet mit über Umsatz und Auftragslage.

2.2 Allgemeine Risiken

Die Einführung von BYOD in einem Unternehmen bringt nicht nur Vorteile mit sich. Tatsächlich sind es zum Teil bedrohliche Risiken, Eingriffe in hochsensible Sicherheitsstrukturen und ein Umdenken in etablierten Prozessen, die der Trend mit sich bringt. Wägt man die Vorteile gegen die möglichen Risiken ab, zeigt sich, dass je nach Unternehmensbereich und letztendlich eingeführtem Konzept von BYOD die Chancen durchaus von den dazugehörigen Nachteilen untergraben werden können.

2.2.1 Parallelität von privaten und geschäftlichen Daten

Mit der Einführung von BYOD in eine Unternehmensstruktur wird durch die Durchlöcherung der Firmenabgrenzung nach außen ein großer Risikofaktor geschaffen. Die auf den Endgeräten der Mitarbeiter vorhandenen Firmendaten sind physikalisch nicht mehr abgetrennt von privaten Daten und privaten Kommunikationskanälen [1]. Neben dem Schutz der Firmendaten wird es außerdem Aufgabe des Arbeitgebers, mit den Privatdaten eines Mitarbeiters verantwortungsvoll und rechtskonform umzugehen [6].

2.2.2. Eignung von Consumer-Geräten für geschäftliches Umfeld

Die Parallelität von privaten und geschäftlichen Daten erfordert somit klare und einheitliche Sicherheitskonzepte. Bei Mobilgeräten aus dem Consumer-Bereich, die durch BYOD haufenweise von Mitarbeitern als Arbeitsmittel genutzt werden würden,

stehen häufig jedoch Aspekte wie ästhetisches Design, intuitive Bedienbarkeit und Schlichtheit im Vordergrund. Die vorhandenen Konfigurationsmöglichkeiten im Hinblick auf Sicherheit entsprechen oftmals nicht dem Stand der Technik, wie er bei Endgeräten aus dem professionellen Bereich umgesetzt ist. Diese Schwachstelle wird auch von vielen Entscheidungsträgern innerhalb der IT gesehen, von welchen 49 Prozent einer Studie in Zusammenarbeit von BT und Cisco zufolge angaben, aufgrund potentieller Risiken wie Malware oder Viren bisher noch kein BYOD eingeführt und es in Zukunft auch nicht geplant zu haben [5]. Hinzu kommt, dass viele Benutzer erwartungsgemäß nicht dazu bereit sein werden, für ihre eigenen Geräte Einschränkungen hinzunehmen.

2.2.3 Soft- und Hardware-Vielfalt

Hinzu kommt, dass selbst wenn ein Unternehmen klare Sicherheitskonzepte für die Geräte formuliert hat, es diese auf der entstehenden, breiten Produktpalette an Mobilgeräten nicht für alle Gerätemodelle in gleichem Maße umsetzen kann. Am Beispiel des Betriebssystems Android existieren sogar von jedem Gerätehersteller eigens angepasste Varianten des Haupt-Betriebssystems mit unterschiendlichen Funktionsumfängen [1].

Dieser Beispielpunkt führt außerdem zu einem weiteren Risiko. Die Betriebssystem-Unterarten unterscheiden sich zusätzlich in ihrem Look-and-Feel und falls ein IT-Support für die besagten Geräte angeboten wird, stößt man hier aufgrund der vorhandenen Vielfalt schnell auf Probleme hinsichtlich der gezielten Mitarbeiter-Unterstützung. Auch dadurch entstehen innerhalb der IT höhere Kosten für die zusätzlichen Administrations- und Sicherheitsmaßnahmen [2].

2.2.4 Datensicherheit

In fast jedem Konzern gibt es einen mehr oder minder großen Kern an sensiblen Unternehmensdaten. Mehr als die Hälfte aller Organisationen schätzte ihre Daten im Rahmen einer Umfrage von Gartner Inc. in Punkto Datensicherheit als hochsensibel ein [3]. Die IT-Sicherheitsarchitektur wächst beständig und die Ausgaben für den Schutz der besagten Daten belaufen sich auf hohe Summen. Den Zugang zu diesen Daten und die zugehörigen Sicherheitsmechanismen zu vereinfachen stellt ein weiteres, großes Risiko dar.

2.2.5 WLAN-Infrastruktur

Wenn Mitarbeiter anfangen, ihre privaten Mobilgeräte in die Firma mitzubringen kann dieser Vorgang eine ernstzunehmende Belastung der vorhandenen WLAN-Infrastruktur mit sich bringen. Der rasante Anstieg der verbundenen Geräte führt zu einer höheren Auslastung der Bandbreite, wie sie bei 84 Prozent aller Umfragen-Teilnehmer der BT und Cisco Studie festgestellt werden konnte [2]. Zusätzlich sehen 56 Prozent der IT-Manager eine Abnahme der Performance einiger Applikationen, die dadurch entsteht, dass die Mitarbeiter nun mit mehreren Geräten gleichzeitig auf System und Dienste zugreifen.

2.2.6 Rufnummernmitnahme

Ein weiteres Problem entsteht, sobald ein Mitarbeiter aus dem Unternehmen austritt. Da er kein geschäftliches Mobilgerät als Arbeitsmittel erhält, war er zu seiner

Beschäftigungszeit, auch für Kunden und andere externe Kontakte der Firma unter seiner Privatnummer erreichbar, falls ihm von Seiten seines Arbeitgebers auch keine entsprechende SIM-Karte zur Verfügung gestellt wird. Verlässt er nun die Organisation, nimmt er seine Telefonnummer entsprechend mit und künftige, telefonische Kontaktaufnahmen durch Firmenkunden könnten ab sofort bei Konkurrenzunternehmen eingehen, bei denen der ehemalige Mitarbeiter mittlerweile angestellt ist.

2.4 Relativierung der Chancen durch potentielle Risiken

Dieses Kapitel soll dazu dienen, die anfänglich aufgeführten Chancen für Unternehmen zu relativieren und darauf hinzuweisen, dass die zugrunde liegenden Punkte nicht nur zu Verbesserungen führen können beziehungsweise durch eine differenziertere Argumentation durch entstehende Nachteile geschwächt werden können. Die Reihenfolge der Punkte orientiert sich dabei an der Gliederung aus dem Kapitel „Chancen für Unternehmen“.

2.4.1 Produktivitäts-Minderung

Anstatt die Produktivität eines Mitarbeiters aufgrund der aufgeführten Argumente zu steigern, könnte die Benutzung des privaten Gerätes stattdessen dazu verführen, das Gerät am Arbeitsplatz für Spiele oder Social Media zu nutzen. Nicht nur sind die dafür benötigten Apps oftmals ohnehin schon auf dem privaten Gerät (vor-)installiert, sondern die psychologische Hemmschwelle ist im Vergleich zu einem Gerät aus dem Firmeneigentum geringer.

2.4.2 Frust über fehlenden Support

Eine anfängliche Zufriedenheit seitens der Mitarbeiter eigene Geräte benutzen zu dürfen kann schnell umschwenken, wenn es zu Problemen und Fragestellungen mit ihrem Gerät kommt. Da ein Gerätesupport durch die IT-Abteilung aufgrund des breiten Portfolios der eingesetzten Geräte nicht mehr so einheitlich und detailreich ausfallen kann, könnte es schnell zu Frustrierung auf Seiten der Mitarbeiter kommen, wenn ihnen bei ihren alltäglichen, technischen Problemen nicht mehr in der gewohnten Qualität geholfen werden kann.

2.4.3 Kosteneinsparungen gegen Sicherheit

Hier ist die Überlegung wichtig, ob Kosteneinsparungen wirklich als Chance gesehen werden, wenn die Sicherheit dafür in weiten Teilen aufgegeben wird. Einhergehend ist die Frage wie stark die eingesparten Kosten durch BYOD argumentativ gewichtet werden können, wenn ein Datendiebstahl verheerende Folgen und weitaus höhere Kosten verursachen würde.

2.4.4 Veraltete Geräte aus Privatbestand

Um bei dem Beispiel des Außendienstmitarbeiters aus Punkt 2.1.4 zu bleiben: Anstatt der erhofften Selbst-Ausstattung der Mitarbeiter mit Mobilgeräten der neuesten Generation besteht ein mögliches Risiko, dass viele nicht bereit sind eigenes Kapital in die Anschaffung technischer Geräte zu investieren, welche auch als Arbeitsgerät

benutzt werden sollen. Diese Einstellung führt zu einem exakt gegenläufigen Effekt. Nämlich dazu, dass die eigenen Mitarbeiter nun mit veralteten Gerätschaften als Arbeitsmittel ausgestattet sein könnten.

3 Fazit

Die Schwachstellen und Risiken von BYOD überwiegen in starkem Maß. Die Vorteile des Trends können kaum alleinstehend betrachtet werden, ohne dabei die einhergehenden Nachteile zu beachten. Eine letztendliche Entscheidung für oder gegen BYOD sollte individuell unter Betrachtung des jeweiligen Unternehmenstyps, der Sensibilität der verarbeiteten Daten und der Wahrnehmung möglicher Worst-Case-Szenarien getroffen werden. Zu vielen kritischen Punkten in direktem Zusammenhang mit den eigenen Mitarbeitern sollte durch vorangehende Umfragen ein klares Meinungsbild erstellt werden, welches die Motivationen und Einschätzungen der Arbeitsnehmer darstellt. Eine Auseinandersetzung mit dem Thema BYOD ist in jedem Fall unerlässlich, da BYOD zu ignorieren die unkontrollierte Consumerisation umso mehr fördern würde in Form von Workarounds wie Mitarbeiter-eigenen Cloud-Lösungen, um trotzdem auf geschäftliche Dateien von privaten Mobilgeräten aus zugreifen zu können.

4 Literaturverzeichnis

[1] Überblickspapier des Bundesamtes für Sicherheit in Informationstechnik zu Consumerisation und BYOD (Version 1.2, Juli 2013) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile, aufgerufen am 03.06.2015

[2] Leitfaden BYOD, BITKOM Bundesverband Informationswirtschaft - Telekommunikation und neue Medien e.V. (April 2013) http://www.bitkom.org/files/documents/20130404_LF_BYOD_2013_v2.pdf, aufgerufen am 06.06.2015

[3] Studie: Bring Your Own Device: The Facts and the Future (englisch) - Gartner Inc. (Mai 2013) http://www.gartner.com/newsroom/id/2466615, aufgerufen am 14.06.2015

[4] Bring your own device: the mobile computing challenge (englisch) - BCS, the Chartered Institute for IT. ISBN: 978-1-78017-189-0

[5] Beyond Your Device Research (englisch), BT und Cisco (Juni 2013) http://www.globalservices.bt.com/static/assets/pdf/campaign/beyondyourdevice/BT_Cisco_Beyond_Your_Device_research.pdf, aufgerufen am 08.06.2013

[6] Bring Your Own Device (BYOD): Security Risks and Mitigating Strategies Volume 4 (englisch), Journal of Global Research in Computer Science. (April 2013) http://jgrcs.info/index.php/jgrcs/article/download/654/477, aufgerufen am 17.06.2013