PRIVACY TOPICS

Dr. Sebastian Brüggemann, M.A., Rechtsanwalt, SGT Rechtsanwälte, Stuttgart

Bring Your Own Device – Einsparungspotenzial mit Sicherheitsrisiko?

Daten-/IT-Sicherheit, Haftung und Risikomanagement beim Einsatz privater IT-Systeme im Unternehmen

Dr. Sebastian Brüggemann, M.A.

Der Einsatz privater Endgeräte erfreut sich bei einer wachsenden Zahl von Mitarbeitern wie Unternehmen zunehmender Beliebtheit. Während erstere anstatt mehrerer Geräte nunmehr dasjenige ihrer Wahl auch im Büro nutzen können, ohne die Belange ihrer Privatnutzung aus dem Auge zu verlieren oder ständig Daten synchronisieren zu müssen, sparen sich Unternehmen die Anschaffungskosten und stellen gleichzeitig die dauerhafte Erreichbarkeit ihrer Mitarbeiter sicher. Was auf den ersten Blick wie eine Win-Win-Situation erscheint, stellt IT-Verantwortliche und Rechtsabteilungen von Unternehmen vor erhebliche Herausforderungen.

I. BYOD – Eine Einführung

Die fortschreitende Technisierung unseres Alltags hat schon vor Jahren die Grenze zwischen der Arbeitswelt und dem Privatleben der Nutzer überwunden. Dies zeigt am deutlichsten die Entwicklung der vergangenen Jahre. Die privaten Nutzungsgewohnheiten avancieren immer mehr zur Triebfeder des technischen Fortschritts, während in vielen Unternehmen oftmals überholte, wenngleich zuverlässige, Technologien zum Einsatz kommen.[1] Technik als Lifestyle ist nicht neu. Firmenhandy, Notebook und andere Endgeräte sind auch nach wie vor ein Statussymbol, mit dem Unternehmen Mitarbeiter an- und umwerben, ebenso wie mit dem Einsatz bestimmter Geräte das Image des Unternehmens nach außen hin transportiert wird. Dies wird aufgrund des veränderten Nutzungsverhaltens jedoch zusehends schwieriger, denn wenn ich privat ohnehin ständig ein Mobiltelefon, ein Tablet und vielleicht sogar ein Notebook mit mir herumtrage, wieso dann auch noch ein weiteres für den Beruf? Erst recht, wenn es sich dabei um ein „Downgrade" handelt.

Auch die veränderte Arbeitsmentalität zu einem Zustand dauerhafter Erreichbarkeit hat dazu beigetragen, dass aus Sicht des Nutzers ein (berufliches) Zweitgerät eher als Bürde, denn als Statussymbol empfunden wird. Die zunehmende Verschmelzung von Beruflichem und Privatem schlägt sich auch in unserem Kommunikationsverhalten nieder, was Unternehmen zunehmend vor technische und datenschutzrechtliche Herausforderungen stellt.

Einer Umfrage des Branchenverbandes BITKOM zufolge nutzen 71 % der deutschen Beschäftigten ihre eigenen Geräte auch für berufliche Zwecke, während immerhin 21 % der Unternehmen diese in ihre IT-Infrastruktur implementiert haben oder ihnen zumindest Zugriff gewähren[2] – Tendenz steigend.[3] In der Gründer- und Start-Up-Szene dürfte dieser Anteil deutlich höher liegen. Insbesondere für junge und kleinere Unternehmen spielen die finan-

1 Dieser Trend wird mitunter auch als „Consumerization" bezeichnet, vgl. *Heinzelmann*, DSB 2012, 11; *Hemker*, DuD 2012, 165; *Franck*, RDV 2013, 185.

2 Presseinformation des Branchenverbandes BITKOM v. 11.04.2013, BYOD – Mitarbeiter verwenden ihre privaten Geräte für den Job, http://www.bitkom.org/files/documents/BITKOM_Presseinfo_BYOD-Umfrage_und_Leitfaden_11_04_2013.pdf [Stand: 09.11.2013].

3 Pressemitteilung der Unternehmensberatung Gartner v. 01.05.2013, Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes, http://www.gartner.com/newsroom/id/2466615 [Stand: 09.11.2013].

ziellen Einsparungen bei der Anschaffung eine bedeutende Rolle. Die wenigsten verfolgen dabei allerdings eine Strategie, von einer fundierten Risikoanalyse beim Einsatz von BYOD ganz zu schweigen.[4] Der folgende Beitrag beleuchtet daher die Chancen und Risiken beim Einsatz von BYOD im Unternehmen, wobei arbeits-, lizenz- und steuerrechtliche Fragestellungen weitestgehend außen vor bleiben. Im Fokus steht das Datenschutzrecht unter Berücksichtigung der Belange von IT-Organisation und -Sicherheit. Er kann und soll eine einzelfallbezogene Risikoanalyse des Einsatzes von BYOD im Unternehmen nicht ersetzen, sondern bietet Leitlinien zur Orientierung.

II. Chancen und Risiken beim Einsatz von BYOD

Die zu erwartenden Einsparungen bei den Anschaffungskosten stehen vor allem bei kleineren und jungen Unternehmen im Vordergrund der Überlegungen zur Einführung von BYOD. Diese werden ganz oder zumindest anteilig vom jeweiligen Mitarbeiter getragen. Weitere Kostenersparnisse sowie Effizienzgewinne erhoffen sich die Unternehmen durch das Wegfallen von Einarbeitungs- und Gewöhnungszeiten, ist der Mitarbeiter mit seinem eigenen Gerät doch bereits bestens vertraut. Gleichzeitig steigt die Zufriedenheit des Mitarbeiters,[5] der nicht nur mit dem Gerät der Marke seiner Wahl arbeiten, sondern auch komfortabel ohne ständigen Gerätewechsel seine beruflichen wie privaten Kontakte pflegen kann. Bei immer kürzeren Produktzyklen spart das Unternehmen zudem die Kosten für Wartung und Neuanschaffungen.[6] Individuelle Anschaffungen benötigen weniger Zeit und Aufwand als die unternehmensweite Einführung neuer Geräte und erfolgen ebenfalls in der Freizeit. Daneben kommuniziert eine individuelle und (stets) dem neusten Stand der Technik entsprechende Ausstattung der Mitarbeiter gegenüber Außenstehenden, seien es (potenzielle) Kunden oder Bewerber, bestimmte Botschaften, etwa in Bezug auf die Technikaffinität, die finanzielle Ausstattung, aber auch die Wertschätzung eines Unternehmens gegenüber seinen Mitarbeitern und ist somit aus Marketinggesichtspunkten nicht zu vernachlässigen.[7]

Derlei Einsparungen könnten sich angesichts des erhöhten Integrationsaufwands in die bestehende IT-Infrastruktur des Unternehmens schnell relativieren. Hinzu kommt, dass bei einer Vielzahl unterschiedlicher Geräte, Betriebssysteme und zusätzlich, zum Privatgebrauch, installierter Software, ein Überblick über die unterschiedlichen Schwachstellen und Sicherheitslücken kaum möglich sein dürfte. Das gilt ebenso für entsprechende Vorkehrungen (bspw. Updates, vorübergehende Deaktivierung) und Reaktionen im Ernstfall. Hier gilt: Eine Kette ist immer nur so stark wie ihr schwächstes Glied. Die Inhomogenität der IT kann sich allerdings dann als vorteilhaft erweisen, wenn der Angriff flächendeckend erfolgt und nicht auf die Erlangung von Daten, sondern auf das Lahmlegen der Infrastruktur an sich gerichtet ist. Auch die private Nutzung eröffnet zusätzliche Sicherheitsrisiken. Dies beginnt mit dem Verbringen des Geräts in das private Umfeld außerhalb des Unternehmens (heimische/öffentliche Funknetze), über den weiteren Anwendungs-/Nutzungsbereich (Installation ungeprüfter Software) bis hin zu einem möglicherweise erweiterten Kreis der Personen, die Zugriff auf das Gerät und die darauf enthaltenen Daten haben. Zwar lassen sich diesbezüglich vor allem im Wege des Arbeitsrechts vertragliche Vorkehrungen treffen, letztendlich sind dem Eingriff in die Privatsphäre des Nutzers i. d. R. enge Grenzen gesetzt. Hier treffen erweiterte Nutzungsräume und Anwendungsszenarien auf eingeschränkte Zugriffs- und Kontrollmöglichkeiten. Dies bedeutet einen deutlich erhöhten Sicherungsaufwand und vor allem neue, detaillierte Sicherheitskonzepte, die unterschiedliche Update- und Verifikationsprozesse berücksichtigen sowie Inkompatibilitäten einzelner Komponenten Rechnung tragen.

Die Inhomogenität der unterschiedlichen Gerätetypen stellt die IT-Verantwortlichen eines Unternehmens auch im Hinblick auf die Gewährleistung der Interoperabilität vor zusätzliche Herausforderungen. Hier bietet sich der Einsatz einer zentralen, virtuellen Arbeitsumgebung an. Letztendlich ist aber auch dies keine Garantie für eine reibungslose Integration.

Von den Einsparungen der Anschaffungs-, Reparatur- und Wartungskosten dürfte angesichts der zu erwartenden Mehrausgaben in die eigene IT-Infrastruktur am Ende wenig übrig bleiben, wenn überhaupt.[8]

III. Rechtliche Anforderungen

Abseits der in der Literatur bereits hinlänglich diskutierten arbeits-, steuer- und lizenzrechtlichen Fragestellungen[9] stellt der Einsatz von BYOD Unternehmen insbesondere im Hinblick auf das Recht der Datenverarbeitung vor ungeahnte, aber sicherlich nicht unüberwindbare Herausforderungen.[10] Zu diesen zählen neben einer datenschutzrechtskonformen Ausgestaltung auch die Berücksichtigung haftungs- wie auch strafrechtlicher Fragestellungen im Zusammenhang mit Datenverarbeitungsvorgängen.

1. BYOD und Datenschutz

Unabhängig davon, wie das BYOD-Konzept im Einzelfall vertraglich gestaltet und organisatorisch umgesetzt wird, muss den Unternehmen bewusst sein, dass sie durch die Vermischung von privater und beruflicher Sphäre ihrer Mitarbeiter sich ein Stück weit in deren Abhängigkeit begeben und zugleich eine erhebliche Einschränkung ihrer Zugriffs- und Kontrollrechte hinnehmen müssen. Mit der Möglichkeit zur Privatnutzung sind die Anwendungsbereiche des Fernmeldegeheimnisses (Art. 10 GG, § 88 TKG)[11] sowie des Allgemeinen Persönlichkeitsrechts mit seinen Ausprägungen des Rechts auf informationelle Selbstbestimmung ebenso wie des vom BVerfG entwickelten Computergrundrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) eröffnet. Die Einführung von BYOD

4 *Imping/Pohle*, K&R 2012, 470, 471.

5 *Göpfert/Wilke*, NZA 2012, 765; *Herrenleben*, MMR 2012, 205; *Imping/Pohle*, K&R 2012, 470; *Franck*, RDV 2013, 185.

6 Vgl. *Göpfert/Wilke*, NZA 2012, 765; *Heinzelmann*, DSB 2012, 11; *Imping/Pohle*, K&R 2012, 470; *Franck*, RDV 2013, 185.

7 Ähnlich wohl *Hemker*, DuD 2012, 165; *Franck*, RDV 2013, 185.

8 Vgl. *Bergstein*, IBM Faces the Perils of "Bring Your Own Device", MIT Technology Review v. 21. 05. 2012, http://www.technologyreview.com/news/427790/ibm-faces-the-perils-of-bring-your-own-device/ [Stand: 09. 11. 2013].

9 Ausführlich hierzu *Franck*, RDV 2013, 185 ff.

10 BSI, Überblickspapier Comsumerization und BYOD, 2013, S. 7 f., https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf?__blob=publicationFile [Stand: 09. 11. 2013]; a. A. Tätigkeitsbericht des ULD Schleswig Holstein, 2009, LT-Drs. 16/2439, S. 115; *Ronellenfitsch*, Handreichung zur Nutzung von Smartphones und Tablet-Computern in Behörden und Unternehmen, 2013, S. 16, http://www.datenschutz.hessen.de/download.php?download_ID=271&download_now=1 [Stand: 09. 11. 2013].

11 Insoweit wird das Unternehmen regelmäßig zum Provider, vgl. BT-Drs. 13/3609, S. 53; *Braun/Hoppe*, MMR 2010, 80, 81; *Minnerup*, ITRB 2012, 47; *Imping/Pohle*, K&R 2012, 470, 472.