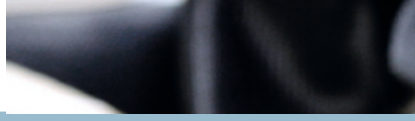
Bring Your Own Device

BITKOM



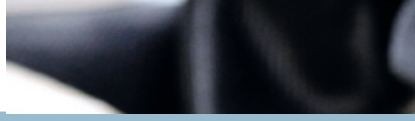
Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Susanne Dehmel (BITKOM) Tel.: 030.27576-223 s.dehmel@bitkom.org
Copyright:	BITKOM 2013
Redaktion::	Susanne Dehmel
Grafik/Layout:	Design Bureau kokliko / Astrid Scheibe, Eugen Regehr (BITKOM)
Titelbild:	Daniela Stanek (BITKOM)

Bring Your Own Device

BITKOM

Inhaltsverzeichnis



Vorwort

»Bring Your Own Device« (BYOD) war in der letzten Zeit eines der beliebtesten Themen in Sachen moderne Unternehmenskultur und wurde in unterschiedlichsten Artikeln und Studien beleuchtet. Doch was das Schlagwort eigentlich bedeutet und mit welchen Fragen sich Unternehmen auseinandersetzen sollten, wenn sie sich dem Thema nähern, ist im Einzelnen oft schwer zu überblicken. Im BITKOM entstand daher die Idee, in Zusammenarbeit mehrerer Fach-Arbeitskreise einen Leitfaden zu schaffen, der denjenigen den Einstieg ins Thema erleichtert, die im Unternehmen über die Einführung von BYOD entscheiden oder ein BYOD-Projekt umsetzen sollen. Der Leitfaden gibt einen ersten Überblick über bestehende rechtliche, technische und organisatorische Anforderungen, welche jedes Unternehmen mit Bezug auf seine individuellen Gegebenheiten prüfen sollte.

Mitgewirkt haben die Arbeitskreise Datenschutz, Intellectual Property, ITK-Vertrags- und Rechtsgestaltung, Personal und Arbeitsrecht, Sicherheitsmanagement und Steuern.

Besonderer Dank gilt den Autoren:

- Beate Beißwenger, Datev
- Sven Buschke, Deloitte
- Susanne Dehmel, BITKOM
- Stefan Dürnberger, Cisco
- Erika Friesen, Rohde und Schwarz
- Dr. Katharina Garbers-von Boehm, CMS Hasche Sigle
- Arne Gattermann, BITKOM
- Katja Gelhaar, Steria Mummert Consulting
- Torsten Gudjons, Deloitte
- Thomas Gronewald, admeritia GmbH
- Dr. Andreas Imping, DLA Piper
- Adina Kessler-Jensch, CMS Hasche Sigle
- Christian Kloeppel, CSC
- Jan Kochta, PwC Legal
- Lars Kroll, Symantec
- Thomas Kriesel, BITKOM
- Lars Kripko, Bitkom Servicegesellschaft
- Dr. Lutz Neugebauer, BITKOM
- Percy Ott, Cisco
- Tanja Pilachowski, Deutsche Post
- Dr. Mario Rehse, BITKOM
- Heiko Rudolph, admeritia
- Marcus Rumler, Steria Mummert Consulting
- Daniel Sattelhak, Deloitte
- Martin Schweinoch, SKW Schwarz
- Corinna Spohr, Symantec

Der Leitfaden erhebt keinen Anspruch auf Vollständigkeit. Die dargestellte Materie ist der fortlaufenden Entwicklung des Rechts und der Technik unterworfen. Der Leitfaden versteht sich daher als Einführung in die Problematik und Aufbereitung möglicher Handlungsmöglichkeiten, der jedoch die Einbindung professioneller unternehmensinterner oder externer Berater nicht überflüssig macht.

Berlin, im März 2013

1 Hintergrund und Einführung

Die Nutzung von privaten Geräten wie Smartphones und Tablet-Computern am Arbeitsplatz liegt im Trend. 43 Prozent der ITK-Unternehmen erlauben ihren Mitarbeitern, eigene Geräte mit dem Firmennetzwerk zu verbinden. Das Verfahren nennt man Neudeutsch »Bring Your Own Device«, kurz: BYOD. Fast zwei Drittel (60 Prozent) von ihnen haben dafür spezielle Regeln aufgestellt. Dies geht aus einer aktuellen Branchenbefragung des BITKOM hervor[1]. Von den Unternehmen, die BYOD zulassen, erhoffen sich 81 Prozent eine höhere Mitarbeiterzufriedenheit. Knapp drei Viertel (74 Prozent) erwarten Effizienzsteigerungen, weil die Mitarbeiter mit ihren Geräten vertraut sind. Rund 40 Prozent wollen so als moderner Arbeitgeber wahrgenommen zu werden. Vor allem jüngere Arbeitnehmer erwarten immer häufiger, ihre eigenen Smartphones und Tablet-Computer auch im Job einsetzen zu können. Jedes zweite befragte Unternehmen (53 Prozent) lehnt private Endgeräte am Arbeitsplatz jedoch ab. Zu den häufigsten Gründen gehört der erhöhte Wartungs- und Sicherheitsaufwand. Viele Unternehmen befürchten Sicherheitsprobleme, wenn eine Vielzahl verschiedener Geräte mit unterschiedlicher Software eingesetzt wird.

Dieser Leitfaden soll Unternehmen, die über die Einführung oder weitere Handhabung von BYOD in ihrem Unternehmen nachdenken, Orientierung bieten, welche Punkte zu berücksichtigen und zu regeln sind. Da der Begriff BYOD teilweise sehr unterschiedlich verwendet wird, wird im Folgenden zunächst ausgeführt, von welchen Definitionen dieser Leitfaden durchgehend ausgeht.

- **Bring Your Own Device (BYOD)**
  Unter dem Namen »Bring Your Own Device« versteht dieser Leitfaden ein Unternehmensprogramm zum Einsatz spezieller IT, wenn:
  - Das genutzte Gerät dem Mitarbeiter gehört (Eigentum des Mitarbeiters ist).
  - Das Gerät Zugriff auf IT-Ressourcen des Unternehmens erhält.

- **Gerät**
  Mit Gerät sind sowohl mobile als auch statisch genutzte Geräte gemeint.

- **IT**
  IT umfasst sowohl die genutzte Hardware im Sinne von eigenständigen Geräten, wie auch Software, die sich ohne Eigentum an Hardware nutzen lässt, insbesondere Web- und Clouddienste.

- **Mitarbeiter**
  Als Mitarbeiter werden zunächst nur die Arbeitnehmer und arbeitnehmerähnlichen Personen eines Unternehmens nach der Definition in § 5 des Arbeitsgerichtsgesetzes gezählt[2], also Arbeiter und Angestellte sowie Auszubildende. Inwieweit gleiches auch für Mitarbeiter von Dienstleistern o.ä. gelten kann, wäre in einem zweiten Schritt zu prüfen.

- **Chose Your Own Device**
  Von BYOD zu unterscheiden ist das Modell »Chose Your Own Device«, bei dem sich der Mitarbeiter ein Gerät aus einer deutlich erweiterten Produktpalette aussuchen kann, das Gerät also Eigentum des Arbeitgebers bleibt. In diesem Modell stellen sich die üblichen Fragen zur Erlaubnis der Privatnutzung.

- **Schatten IT**
  Von BYOD als bewusst eingeführtem Modell ist weiterhin der Zustand zu unterscheiden, in dem private Geräte von Mitarbeitern ohne Absprachen oder spezielle Vorkehrungen zu geschäftlichen Zwecken genutzt werden. Diesen Zustand gilt es zu vermeiden, weil er eine Reihe von Risiken birgt, die im Folgenden noch aufzuzeigen sind.

1 http://www.bitkom.org/73623_73615.aspx

2 http://dejure.org/gesetze/ArbGG/5.html

2 Rechtliche Anforderungen

2.1 Datenschutz-Anforderungen

Aus Datenschutz-Sicht ist grundsätzlich wohl nur eine freiwillige Nutzung von BYOD möglich, da das Unternehmen hinsichtlich der Einräumung von Kontrollrechten durch den Mitarbeiter auf die Kooperation des Mitarbeiters angewiesen ist.

2.1.1 Trennung von privaten und Unternehmensdaten

Bei der Nutzung privater Geräte im Unternehmensumfeld sollten private und geschäftliche Daten strikt getrennt werden. Das Unternehmen sollte jederzeit die Kontrolle über geschäftliche Daten wie E-Mails, Dokumente und Applikationen haben. Denn für dienstliche Daten, insbesondere personenbezogene Daten, trägt das Unternehmen die volle Verantwortung. Es muss die Erhebung, Verarbeitung und Nutzung vollständig kontrollieren können. Nach § 9 Bundesdatenschutzgesetz (BDSG) muss die verantwortliche Stelle, also das datenverarbeitende Unternehmen, die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die in der Anlage des BDSG genannten Anforderungen zu gewährleisten. Können für besonders sensible Daten diese Anforderungen auf den Privatgeräten der Mitarbeiter nicht gewährleistet werden, so sind sie von BYOD auszunehmen. Private Daten müssen davon allerdings unberührt bleiben. Eine solche Forderung kann sich u.a. schon aus §88 TKG ergeben, wonach der Arbeitgeber auf private Daten ohne entsprechende Einwilligung des Mitarbeiters nicht oder nur eingeschränkt zugreifen darf.

2.1.2 Umsetzung technischer und organisatorischer Anforderungen aus der Anlage zu § 9 Satz 1 BDSG:

In organisatorischer Hinsicht kann sich das Unternehmen an den Vorgaben aus der Anlage zum BDSG orientieren:

Anlage (zu § 9 Satz 1 BDSG):
»Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,...«

1. Zutrittskontrolle

...Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

Im Rahmen der Zutrittskontrolle entstehen prinzipiell keine zusätzlichen Risiken, soweit das Unternehmen bereits mit der Telearbeit und dem mobilen Einsatz von IT vertraut ist.

2. Zugangskontrolle

...zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

Unter Zugangskontrolle muss, wie bisher auch bei dienstlichen Geräten, die Nutzung durch Unbefugte, wie bspw. die eigenen Kinder, verhindert werden. In einem BYOD-Programm wäre zu regeln, dass auch die private IT Dritten nicht zugänglich gemacht werden darf. In diesem Sinne muss eine Regelung zur Wartung und Reparatur der privaten IT gefunden werden, da in diesem Falle tatsächlich ein Unbefugter Zugang zum IT-System bekommt. Ein solcher Zugang durch Dritte wäre nur unbedenklich, wenn sich zum Zugangszeitpunkt keine personenbezogenen Daten des Unternehmens auf dem jeweiligen Gerät befinden. Das BYOD-Programm sollte auf IT im Eigentum des Mitarbeiters beschränkt werden. Gehört die IT Dritten, bspw.

der Lebensgefährtin, einer Finanzierungs- oder Leasinggesellschaft, kann das Unternehmen den Zugang zur IT nicht wirksam vertraglich verhindern.

Durch Betriebssystem-Modifikation (z. B. Jailbreak oder Rooting) könnten die zu erwartenden Sicherheitsmaßnahmen des Gerätes gestört werden, insofern ist ein derartiges Kompromittieren des Systems durch die Vereinbarung auszuschließen und es sind nach Möglichkeit entsprechende technische Kontroll- und Sicherheitsmaßnahmen zu treffen.

3. Zugriffskontrolle

... zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

Die Zugriffskontrollmaßnahmen werden auf Unternehmens-IT üblicherweise vom Administratorenteam eingerichtet und überwacht. Auf ein adäquates Berechtigungssystem wird man auch bei privater IT nicht verzichten können. Hier wird demnach zu regeln sein, ob unterschiedliche Accounts auf dem privaten Gerät zu nutzen sind oder ob bestimmte Unternehmensdienste durch spezielle Authentifizierungsmaßnahmen zu schützen sind.

- Verpflichtende oder automatisierte Installation von Antiviren-Software auf betroffenen Plattformen (z. B. Android).
- Einschränkung des Zugriffes auf Daten & Applikationen, z. B. beim Öffnen von Unternehmensdaten in anderen, nicht-kontrollierten Applikationen («Öffnen mit...«).
- Unterbinden von Screenshot-Funktionen in Geschäftsanwendungen.
- Unterdrücken von Cloud-basierten Sprachassistenten (z. B. Siri) in Geschäftsanwendungen
- Sofern Zugriff auf unternehmensinterne Web-Portale (z. B. Intraweb etc.) erfolgen soll, empfiehlt sich der Zugang über einen eigenen, sicheren Browser, der die Kommunikation zwischen Portal und mobilem Endgerät zusätzlich verschlüsselt. So werden evtl. Sicherheitslücken in mobilen Browsern umgangen.

4. Weitergabekontrolle

...zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

In der Praxis stellen, auch außerhalb von BYOD, insbesondere mobile Datenträger ein Risiko dar. Auch dienstliche und private Mail-Accounts ermöglichen eine Datenweitergabe aus der Unternehmens-IT heraus. Je nach geplanter technischer Lösung (Webdienst, virtual Desktop, Container) können sich Risiken durch Kopiermöglichkeiten aus einer sicheren Unternehmenssoftware auf das private Gerät ergeben. Eine unautorisierte Datenweitergabe muss zumindest durch Sensibilisierung, Schulung und Kontrolle der Mitarbeiter verhindert werden. Dazu zählt u.a. das Verhindern der Nutzung nicht-vertrauenswürdiger Cloud-Dienste, die aus Geschäftsanwendungen heraus angesprochen werden könnten (z. B. Dokumentenaustausch, Location Based Services, etc.).

Unter der Weitergabekontrolle ist auch eine Regelung zur Fernlöschung und -sperrung zu treffen. Es sollte geregelt werden, dass und wann sich der Mitarbeiter zur Vornahme einer solchen Maßnahme verpflichtet bzw. wann das Unternehmen berechtigt ist, eine solche Maßnahme durchzuführen (z. B. bei Verlust oder Diebstahl).

5. Eingabekontrolle

...zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

Eine Protokollierung auf privater IT wird selten vereinbart werden können und ggf. nicht den Anforderungen an die Revisionsfähigkeit erfüllen. Eine unternehmensseitige Protokollierung der Datenverarbeitung sollte möglich und vereinbart sein.

6. Auftragskontrolle

...zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

Unternehmen müssen sich Kontrollmöglichkeiten auch auf privater IT schaffen, um die Umsetzung der getroffenen Regelungen und Anweisungen überprüfen zu können. Entsprechende Kontrollbefugnisse muss der Arbeitgeber in BYOD-Programmen ausdrücklich mit dem Mitarbeiter vereinbaren. Selbst wenn keine Kontrollen auf privaten Geräten geplant sind, müsste das Unternehmen Möglichkeiten zur Kontrolle durch Aufsichtsbehörden und Gerichte (e-Discovery) schaffen. Hierbei wäre auch der Einsatz von MDM-Lösungen (Mobile-Device-Management) mit Auswirkungen auf private Geräte zu regeln oder der Einsatz automatisierter Inventarisierungstools.

7. Verfügbarkeitskontrolle

...zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

Die Verfügbarkeit personenbezogener Daten wird vor allem durch Backups, Recovery- und Notfallpläne, durch Vorhalten von Ersatzteilen und Ersatzgeräten gesichert.

Geschäftliche Daten sollten stets auf Unternehmensservern vorgehalten werden. Bei der mobilen Verarbeitung von geschäftlichen Daten muss anhand der Sensibilität der Daten über die Frequenz der Synchronisierung mit den Unternehmensservern entschieden werden. Gegebenenfalls muss eine ergänzende Backup-Lösung für die mobilen bzw. privaten Geräte gefunden werden. Dabei sollten private Daten des Mitarbeiters nicht durch das Unternehmen gesichert werden. Sollte dies technisch nicht möglich sein, ist eine entsprechende organisatorische Regelung inklusive Löschverfahren für die privaten Daten zu vereinbaren.

Daneben ist eine Regelung zum persönlichen Backup des Mitarbeiters (auf eigene Backup-Ressourcen) zu treffen. Seine Möglichkeiten (z. B. über plattformeigene Mechanismen wie Apple's iCloud) müssen begrenzt werden, so dass geschäftliche Daten zumindest verschlüsselt werden, besser jedoch von solchen Backup-Funktionen komplett ausgeschlossen sind.

In welchem Umfang die Unternehmen Ersatzgeräte vorhalten müssen, ist im konkreten Einzelfall zu entscheiden. Die Ersatzgeräte müssen grundsätzlich die betrieblich notwendigen Funktionen erfüllen, nicht jedoch dem Leistungs- und Funktionsumfang des ursprünglichen Gerätes entsprechen.

8. Trennungsgebot

...zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der im vorigen Kapitel beschriebene Ansatz der Trennung von geschäftlichen und privaten Daten erlaubt dem Unternehmen die Kontrolle über geschäftliche Daten, wie es z. B. §7 BDSG fordert. Danach ist ein Unternehmen stets für die ordnungsgemäße Verarbeitung von personenbezogenen Daten haftungsrechtlich verantwortlich – auch wenn diese Verarbeitung auf privaten Geräten stattfindet.

9. Verschlüsselung

Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Hier ist zum einen an eine Verschlüsselung der Daten auf dem Transportweg zu denken, also über integrierte, individuelle Verschlüsselungsmechanismen oder über generische Methoden wie VPN.

Zum anderen denke man an die Verschlüsselung der Daten auf dem Gerät selbst über betriebssystemeigene Konzepte (Sandboxing) oder ergänzende Softwarelösungen, die geschäftliche Applikationen mit einem sicheren Container umschließen. Sofern das Gerät über austauschbare Datenträger verfügt (z. B. SD-Karten), sollte deren Nutzung durch geschäftliche Applikationen unterbunden werden.

Gibt das Unternehmen Daten zur Verarbeitung an ein anderes Unternehmen (Auftragsdatenverarbeiter), muss es die Einhaltung der in § 9 und Anlage festgelegten Anforderungen dadurch sicherstellen, dass es mit dem Auftragsdatenverarbeiter einen Vertrag mit den Punkten aus § 11 Abs. 2 BDSG abschließt. Diese Liste gibt auch Anhaltspunkte für die Regelungen, die mit dem jeweiligen Mitarbeiter getroffenen werden, der sein privates Gerät für die Verarbeitung von Unternehmensdaten nutzt.

2.1.3 Unternehmens-Richtlinien

Eine wichtige Voraussetzung für das Zulassen der Nutzung eigener Geräte der Mitarbeiter sind Unternehmens-Richtlinien. In der Richtlinie sollten – unter Beachtung der mitbestimmungsrechtlichen Vorgaben – klare Regeln und Vorgaben aufgestellt werden, damit die betroffenen Mitarbeiter und auch der Arbeitgeber eine eindeutige Orientierung haben, was erlaubt ist und was nicht. Zugleich wird hierdurch ggf. eine Rechtsgrundlage für erforderliche Zugriffe auf das Gerät durch den Arbeitgeber geschaffen.

- In der Richtlinie sollte einmal geregelt sein, ob es Einschränkungen bzgl. des Mitarbeiterkreises gibt (Voraussetzung ist, dass das Gerät dem Mitarbeiter gehört, evtl. ausgenommene Mitarbeitergruppen wie Personalabteilung o.ä.) und auch, ob alle möglichen mobilen Geräte zugelassen sind oder nur bestimmte. Weiterhin sollten die sicherheitstechnischen Vorgaben festgelegt sein, z. B. Einsatz von Verschlüsselungstechnologien, Verpflichtung zur Nutzung von Antivirensoftware, Vorgaben zur Trennung von privaten und Unternehmensdaten u.ä. (siehe hierzu auch unter Punkt 2.4.4 Betriebsvereinbarung)
- Sehr wichtig sind zudem Regelungen bezüglich Kontroll- und Zugriffrechten des Arbeitgebers auf das private Gerät (z. B. regelmäßig, nur im Verdachtsfall, in welcher Form usw.). Schließlich sollten Benachrichtigungs- und Verhaltensregeln für den betroffenen Mitarbeiter enthalten sein für den Fall des Verlusts/Diebstahls des Geräts.

Abschließend ist zu beachten, dass die Unternehmensrichtlinie auch aktiv kommuniziert wird, damit jeder Mitarbeiter Kenntnis des Inhalts hat.

2.1.4 Rechtliche Maßgaben zur Herausgabe der Unternehmensdaten und/oder der SIM-Karte bei Verlassen des Unternehmens

Auch zum Ende des Arbeitsverhältnisses wird der Arbeitgeber nur in den seltensten Fällen einen Anspruch auf Herausgabe privater IT oder privater SIM-Karten haben bzw. durchsetzen können. Die bereits beschriebene notwendige Trennung von dienstlichen und privaten Daten auf dem eingesetzten Gerät bekommt zum Ende des Arbeitsverhältnisses besondere Bedeutung. Der Arbeitgeber hat ein legitimes Interesse an der weiteren Nutzung der dienstlichen Daten. Er muss zudem sicherstellen, dass die dienstlichen personenbezogenen Daten nicht auf dem Gerät verbleiben und künftig von einem Unternehmensfremden genutzt werden können. Insofern sollte er sich einen Anspruch auf Herausgabe der dienstlichen Daten sichern, sofern diese nicht bereits durch die notwendigen Backups im Unternehmen selbst vorliegen.

Daneben muss der Arbeitgeber den Mitarbeiter frühzeitig verpflichten, die dienstlichen Daten spätestens zum Vertragsende vom privaten Gerät zu löschen und diese Löschung auch zu bestätigen.

Kernaussage:

Das Unternehmen muss die Verfügungsgewalt über dienstliche Daten behalten und ist für deren Sicherheit verantwortlich. Es darf, aber grundsätzlich nicht auf private Daten zugreifen und muss daher entsprechende organisatorische Maßnahmen und Regelungen mit dem Mitarbeiter treffen.

2.2 Lizenzrechtliche Fragestellungen

BYOD-Modelle bringen es mit sich, dass Software des Unternehmens für private Zwecke und Software, die der Mitarbeiter privat lizenziert hat, für betriebliche Zwecke eingesetzt werden kann.

Bei der Verwendung von Software für andere als die vertraglich vereinbarten Zwecke (zum Beispiel ausschließlich gewerbliche bzw. ausschließlich private Nutzung) kann es zu Nutzungshandlungen kommen, die urheberrechtliche Unterlassungsansprüche, sowie unter Umständen auch Schadensersatzansprüche auslösen. Diese werden in der Praxis vom Lizenzgeber als »Nachvergütungsansprüche« geltend gemacht.

Dies ist abhängig von der Ausgestaltung der betroffenen Softwarelizenzen und von der technischen Ausgestaltung des BYOD-Modells.

2.2.1 Nutzung von Unternehmenssoftware auf dem privaten Gerät

a) Ob der Einsatz von Unternehmenssoftware auf privaten Endgeräten von der bestehenden Lizenz umfasst ist oder eine Nachlizenzierung erfordert, die unter Umständen mit weiteren Kosten verbunden ist, hängt meist von dem innerhalb des konkreten Lizenzvertrages verwendeten Begriff des »Nutzers« ab, an den in aller Regel die Vergütung für die Software geknüpft ist. Ob das Privatgerät des Mitarbeiters als zusätzlicher Nutzer zu qualifizieren ist, hängt von der individuellen vertraglichen Ausgestaltung des Nutzerbegriffs in der jeweiligen Lizenz ab.

- In der Praxis sind verschiedene Nutzungsmodelle denkbar:
  So kann von dem Begriff des Nutzers beispielsweise innerhalb eines Unternehmens eine bestimmte Person oder aber ein konkreter Arbeitsplatz (vereinbart durch eine sog. »CPU-Klausel« im Lizenzvertrag) mit einem jeweiligen unbestimmten Personenkreis erfasst sein.
  In den Fällen sog. personal licenses ist dem Lizenznehmer in der Regel die Installation des Programms auf zwei Endgeräten (beispielsweise auf einem Desktop-PC und einem tragbaren Computer) gestattet, soweit sichergestellt ist, dass das Programm nicht auf beiden Geräten zeitgleich benutzt wird. Dies bedeutet allerdings nicht automatisch, dass eine private Nutzung von der Lizenz umfasst ist; dies hängt von der im Einzelfall vereinbarten Lizenz ab.

  Bei Software für Client-Server-Systeme wird häufig die Übertragung von Nutzungsrechten durch sog. Aufspaltungsverbote oder die Nutzung für Geräte, die nicht im Eigentum des Unternehmens als Lizenznehmer stehen, von vornherein vertraglich ausgeschlossen. Die meist für den betrieblichen Ablauf notwendige Vernetzung des Servers mit dem privaten Endgerät kann damit bereits die Lizenz überschreiten.

Im Rahmen von Volumen-und Paketlizenzen kann es darüber hinaus vorkommen, dass der Mitarbeiter die überlassene Software auf sein privates Gerät aufspielt und somit vervielfältigt. Dies bewirkt, dass das Unternehmen so behandelt wird, als würde es die Software öffentlich zugänglich machen oder anderweitig unberechtigt weitergeben.

Für Modelle der »Vermietung« der Software an den Mitarbeiter oder gar der Sublizenzierung ist gewöhnlich die Zustimmung des Rechteinhabers notwendig.

2.2.2 Betriebliche Nutzung von auf dem Privatgerät befindlicher Software

a) Privat durch den Mitarbeiter erworbene Software umfasst meist einfache, nicht übertragbare Nutzungsrechte, die vielfach auf eine private Nutzung beschränkt sind. Insoweit kann je nach Ausgestaltung schon die Vernetzung mit dem Netzwerk des Arbeitgebers und erst recht die betriebliche Nutzung unzulässig sein.

   Da eine Sublizenzierung an das Unternehmen in der Regel lizenzvertraglich ausgeschlossen ist, kann die Notwendigkeit bestehen, dass das Unternehmen zusätzliche Lizenzen der entsprechenden Software erwerben muss, wenn für private Zwecke erworbene Programme betrieblich eingesetzt oder innerhalb betrieblicher Client-Server-Systeme genutzt werden.

   Dies gilt ebenso für die Nutzung von Datenbanken durch einen Mitarbeiter, wenn diese ihm nur für private Zwecke zur Verfügung steht.

b) Schließlich stellt die etwaige Nutzung von »Raubkopien« durch den Arbeitnehmer im betrieblichen Kontext für das Unternehmen ein Risiko dar.

2.2.3 Haftung

a) Im Fall der Verwendung nicht korrekt lizenzierter Software in einem BYOD-Modell kommen zunächst Ansprüche des Rechteinhabers auf Unterlassung und bei Vorsatz auch auf Schadensersatz gegen die das Programm verwendende Person in Betracht.

b) Auch der Unternehmensinhaber kann für dieses Verhalten haftbar gemacht werden und in der Praxis Nachvergütungsansprüchen ausgesetzt werden. Dies gilt selbst dann, wenn er von dem Verstoß weder Kenntnis hatte, noch das Verhalten auf seinen Willen zurückzuführen war.

   - Diese verschuldensunabhängige, insbesondere auf Unterlassung gerichtete Haftung des Unternehmensinhabers setzt voraus, dass die Rechtsverletzung des Mitarbeiters oder Beauftragten in engem Zusammenhang mit dessen Tätigkeitsbereich steht.
     Soweit das Unternehmen von der rechtswidrigen Nutzung der Programme Kenntnis hatte oder aber hätte haben können, kommt darüber hinaus auch eine Haftung auf Schadensersatz in Betracht.
     Dabei ist zu beachten, dass jedes Endgerät, das erkennbar für eine betriebliche Aufgabe eingesetzt wird, unabhängig von der Eigentumsfrage dem Unternehmen zugerechnet werden kann.
     Soweit im Rahmen einer Lizenzkontrolle die Benutzung einer von einem Mitarbeiter im Interesse des Unternehmens verwendeten Raubkopie festgestellt wird, kann das Unternehmen auch dafür unter Umständen verantwortlich gemacht werden.

   - Des Weiteren können die für das Unternehmen handelnden Organe (insbes. die Geschäftsführung) selbst in Haftung genommen werden, soweit diese nicht nachweisbar dafür Sorge getragen haben, dass im Hinblick auf von den Mitarbeitern für Unternehmenszwecke genutzte Software entsprechende Nutzungsrechte bestehen.

2.2.4 Schlussfolgerungen/Empfehlungen

a) Zur Minimierung von Haftungsrisiken sind sämtliche Unternehmenslizenzen darauf zu überprüfen, ob von ihnen auch eine Nutzung auf privaten Geräten des Arbeitnehmers umfasst ist. Gegebenenfalls muss nachverhandelt werden, damit die wirtschaftlichen Konsequenzen der Einführung von BYOD richtig eingeschätzt werden können.

b) Mitarbeiter sind darauf hinzuweisen, dass eigene Software grundsätzlich nicht zu Betriebszwecken verwendet werden soll.

c) Um Nachverhandlungen und nachträglichen Vergütungsforderungen vorzubeugen, ist es für die Zukunft ratsam, sich bereits beim Abschluss von Lizenzverträgen die gewünschten Nutzungen auf privaten Geräten der Mitarbeiter gestatten zu lassen. Daneben sind auch im Verhältnis zu den Mitarbeitern klare vertragliche Regelungen und Guidelines hilfreich, die im Idealfall von regelmäßigen betriebsinternen Schulungen zum Thema Software und Urheberrecht flankiert werden.

Kernaussage:

- Software-Anbieter sehen für die private und die gewerbliche Nutzung von Programmen häufig unterschiedliche Lizenzbedingungen vor.
- Nutzt der Arbeitnehmer sein privates Gerät beruflich, so kann dies bewirken, dass privat lizenzierte Software gewerblich genutzt wird.
- Außerdem ist der Fall denkbar, dass vom Arbeitgeber lizenzierte Programme vom Arbeitnehmer privat genutzt werden, was das zulässige Maß – je nach Lizenz – sprengen kann.
- Daraus können sich Haftungsrisiken für Unternehmen und Geschäftsführung ergeben.

2.3 Steuerrechtliche Fragestellungen

2.3.1 Überblick

Aus steuerlicher Sicht sind bei der Zulassung von privaten Mitarbeitergeräten zum betrieblichen Gebrauch vor allem lohnsteuerliche und umsatzsteuerliche Aspekte abzuklären. Daneben kann auch die Absetzbarkeit der Gerätekosten als Betriebsausgabe bzw. als Werbungskosten eine Rolle spielen. Die Schwierigkeit in der Praxis wird darin bestehen, private Aufwendungen des Mitarbeiters und betriebliche Aufwendungen des Arbeitgebers nachkontrollierbar abzugrenzen und verursachungsgerecht zuzuordnen. Schließlich gibt es noch verfahrensrechtliche Aspekte der ordnungsgemäßen Bearbeitung und Aufbewahrung steuerrelevanter Daten und Unterlagen zu beachten. Fragen zur Entgegennahme, Bearbeitung und Archivierung steuerrelevanter Daten und Unterlagen sind jedoch immer zu beantworten, wenn ein Mitarbeiter im Geschäftsverkehr für ein Unternehmen tätig wird. Insoweit ergeben sich beim Einsatz privater Arbeitnehmergeräte keine Besonderheiten.

2.3.2 Rechtliche Grundlagen

Wesentliches Merkmal der verschiedenen Konstellationen von »Bring Your Own Device« ist die Nutzung eines im Eigentum des Arbeitnehmers stehenden Gerätes für betriebliche Zwecke des Arbeitgebers. Die Steuerrechtsordnung hat bisher aber nur den umgekehrten Fall explizit geregelt: der Arbeitnehmer nutzt im Eigentum des Arbeitgebers stehende und betrieblichen Zwecken dienende ITK-Geräte sowie betriebliche Software auch privat. Die Vorteile aus einer solchen Privatnutzung betrieblicher Geräte und betrieblicher Software sind nach § 3 Nr. 45 EStG von der Lohnsteuer befreit. Die Steuerbefreiung umfasst den Vorteil aus der Nutzung selbst sowie die bei der Nutzung anfallenden Kosten und Gebühren. Aus Sicht des Umsatzsteuerrechts ist die Verwendung eines betrieblichen Gegenstands für private Zwecke der Arbeitnehmer grundsätzlich einer sonstigen Leistung gleichgestellt und unterliegt damit der Umsatzsteuer (§ 3 Abs. 9a UStG). Soweit die Geräte jedoch aus überwiegend betrieblichem Interesse als Arbeitsmittel

unentgeltlich an den Arbeitnehmer überlassen werden, fällt für den Nutzungsvorteil aus einer untergeordneten privaten Gerätenutzung keine Umsatzsteuer an, da mit der Geräteüberlassung kein Leistungsaustausch bezweckt wird (vgl. Ziff. 1.8 Abs. 4 UStAE). Um einen umsatzsteuerrelevanten Leistungsaustausch sicher auszuschließen, kann der Arbeitgeber die Privatnutzung der betrieblichen Geräte untersagen. Für die steuerrechtliche Wirksamkeit eines solchen Verbots muss seine Einhaltung aber zumindest in Stichproben überwacht werden.

Da die Beurteilung von BYOD-Konstellationen im Steuerrecht bisher nicht ausdrücklich geregelt ist, muss insoweit auf die allgemeinen steuerrechtlichen Grundsätze zurückgegriffen werden. Diese stellen sich wie folgt dar:

- Gerätekosten des Arbeitnehmers (z. B. für die Anschaffung oder Reparatur des Gerätes sowie Verbindungsentgelte) können als Werbungskosten von den zu versteuernden Arbeitseinkünften abgezogen werden, soweit die Kosten durch die berufliche Tätigkeit veranlasst sind. Aufwendungen im Privatbereich des Arbeitnehmers dürfen steuerlich nicht berücksichtigt werden (§ 12 Nr. 1 EStG). Daher ist eine Aufteilung zwischen beruflich veranlassten und im Privatbereich des Arbeitnehmers entstehenden Kosten erforderlich.

- Kosten, die der Arbeitgeber im Zusammenhang mit Privatgeräten des Arbeitnehmers trägt, kann der Arbeitgeber als Betriebsausgaben steuermindernd berücksichtigen. Kommt die Kostenübernahme dem Arbeitnehmer auch privat zugute, liegt insoweit ein lohnsteuerpflichtiger Vorteil vor. Wiederum sind also die anfallenden Kosten in einen betrieblich veranlassten und einen dem Privatbereich zuzurechnenden Anteil aufzuteilen.

- Falls in BYOD-Konstellationen ein steuerpflichtiger Vorteil für den Arbeitnehmer entsteht, kann der Arbeitgeber in bestimmten Fällen die hierfür anfallende Lohnsteuer pauschal übernehmen.

- Soweit ein Vorteil des Arbeitnehmers lohnsteuerfrei ist oder vom Arbeitgeber pauschal versteuert wird, entfällt die Beitragspflicht zur gesetzlichen Sozialversicherung (§ 1 Abs. 1 Nr. 1 und Nr. 3 Sozialversicherungsentgeltverordnung).

- Das Umsatzsteuerrecht ist zu beachten, wenn von einem Unternehmer eine Leistung gegen Entgelt erbracht wird. Entgelt in diesem Sinn kann auch in der Arbeitsleistung eines Arbeitnehmers bestehen. Ein Arbeitnehmer kann im Rahmen eines bestehenden Arbeitsverhältnisses nicht als selbständiger Unternehmer tätig werden (§ 2 Abs. 1 S. 1, Abs. 2 Nr. 1 UStG).

- Unternehmen haben Buchungsbelege und geschäftliche Unterlagen, die für die Besteuerung relevant sind, über 10 Jahre aufzubewahren und für eine mögliche Nachprüfung der Finanzverwaltung verfügbar zu halten (§ 147 AO). Dies gilt unabhängig davon, ob die Daten und Unterlagen digital oder in Papierform erstellt wurden.

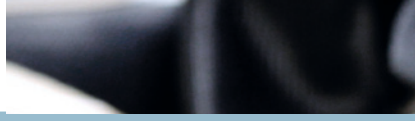
Für die Anwendung der steuerrechtlichen Grundsätze ist es ohne Bedeutung, ob ein mobiles Endgerät oder ein stationärer Arbeitsplatz zum Einsatz kommt. Es ist auch nicht relevant, ob der Arbeitsplatz vom Arbeitgeber gestellt wird oder ob es sich um ein Home-Office des Arbeitnehmers handelt. Steuerrechtlich bedeutsam ist nur die tatsächliche Nutzung eines Gerätes für betriebliche oder private Zwecke.

2.3.3 Einzelne Konstellationen

Die Anwendung der steuerrechtlichen Grundsätze soll in den folgenden Konstellationen beispielhaft verdeutlicht werden.

1. Fall

Das Gerät steht im Eigentum des Arbeitnehmers, der es für betriebliche und private Zwecke einsetzt. Die Kosten des Gerätes (z. B. Anschaffungskosten, Wartungskosten, Reparaturkosten, Kosten für Peripheriegeräte, Kosten für privat genutzte Software, Verbindungsentgelte) trägt der Arbeitnehmer. Software für betriebliche Belange



spielt der Arbeitgeber auf seine Kosten auf das Gerät auf und trägt auch die Lizenz- und Wartungskosten für diese Software.

Bewertung: Die Kosten des Arbeitgebers sind als Betriebsausgaben nach § 4 Abs. 4 EStG abziehbar. Der Arbeitnehmer kann den beruflich bedingten Kostenanteil als Werbungskosten nach § 9 Abs. 1 S. 1 und 2 EStG abziehen, wenn er seine Kosten in einen beruflich und einen privat veranlassten Nutzungsanteil aufteilt. Zum Nachweis des beruflichen Nutzungsanteils sollte er die zeitanteilige Nutzung über einen repräsentativen Zeitraum von drei Monaten aufzeichnen. Ohne einen solchen Nachweis erkennen Finanzgerichte und Finanzverwaltung beim Gerät selbst eine hälftige Aufteilung der Kosten und bei den Verbindungsentgelten einen beruflichen Anteil von 20%, höchstens 20 Euro pro Monat, an (R 9.1 Abs. 5 LStR). Ein umsatzsteuerrelevanter Leistungsaustausch liegt in diesem Fall nicht vor. Die Privatnutzung der betrieblichen Software ist nach § 3 Nr. 45 EStG von der Lohnsteuer befreit. Auch insoweit scheidet ein umsatzsteuerpflichtiger Vorgang aus.

2. Fall

Das Gerät steht im Eigentum des Arbeitnehmers, der es für betriebliche und private Zwecke einsetzt. Der Arbeitgeber sorgt für die Aktualisierung der betrieblich notwendigen Programme und zahlt dem Arbeitnehmer Zuschüsse zu den Internetkosten und zur Anschaffung des Gerätes sowie – falls erforderlich – für die Reparatur des Gerätes.

Bewertung: Im Privatbereich des Arbeitnehmers anfallende Gerätekosten sind steuerlich unbeachtlich. Wie in Fall 1 kann der Arbeitnehmer aber die beruflich veranlassten Gerätekosten als Werbungskosten in seiner privaten Einkommensteuererklärung geltend machen.

Die Zuschüsse des Arbeitgebers sind für diesen als Betriebsausgaben bei den Ertragsteuern abzugsfähig. Aus Sicht des Arbeitnehmers sind die Zuschüsse grundsätzlich als lohnsteuerpflichtiger Vorteil zu behandeln. Es kommt jedoch eine Steuerbefreiung nach § 3 Nr. 50 EStG in Betracht, soweit die Zuschüsse lediglich laufende Auslagen des Arbeitnehmers ersetzen sollen. Damit die Steuerbefreiung eingreift, muss der Arbeitnehmer im Einzelnen nachweisen, dass die ersetzten Kosten bei einer Tätigkeit im Interesse des Arbeitgebers angefallen sind. Zum Nachweis reicht eine Aufzeichnung der Kosten über einen Zeitraum von 3 Monaten aus. Ohne Nachweis sind höchstens 20% der Kosten und höchstens 20 Euro pro Monat steuerfrei erstattungsfähig (R 3.50 Abs. 2 LStR).

Darüber hinausgehende oder pauschale Erstattungen für laufende Kosten kann der Arbeitgeber nach § 40 Abs. 2 Nr. 5 EStG pauschal mit 25% zzgl. Solidaritätszuschlag und ggf. Kirchensteuer versteuern. Dadurch entfallen Steuerpflicht des Arbeitnehmers und Beitragspflicht zur Sozialversicherung für diese Kostenerstattungen. Die Pauschalierungsmöglichkeit besteht allerdings nur, wenn der Zuschuss zusätzlich zum vertraglich vereinbarten Arbeitslohn gezahlt wird. Es dürfen also keine Anteile des Arbeitsentgelts in solche steuervergünstigten Vorteile umgewandelt werden.

Zuschüsse zu einmaligen Anschaffungs- und Reparaturkosten eines privaten Gerätes des Arbeitnehmers sind weder steuerfrei noch kann der Arbeitgeber die Steuer für den Arbeitnehmer pauschal übernehmen. Solche Zuschüsse erhöhen also das Brutto-Entgelt des Arbeitnehmers, von dem Lohnsteuer und Sozialversicherungsbeiträge abzuführen sind.

Soweit Kostenzuschüsse steuerfrei sind oder vom Arbeitgeber pauschal versteuert werden, entfällt die Möglichkeit zum Ansatz als Werbungskosten in der privaten Einkommensteuererklärung des Arbeitnehmers.

Da die Zuschüsse im Rahmen eines bestehenden Arbeitsverhältnisses gezahlt werden und dazu dienen, die Arbeitsfähigkeit des Arbeitnehmers abzusichern, scheidet ein umsatzsteuerrelevanter Leistungsaustausch für den Kostenersatz aus. Allerdings kann der Arbeitgeber aus dem Kostenersatz auch keinen Vorsteuerabzug geltend machen.

3. Fall

Das Gerät steht im Eigentum eines freien Mitarbeiters (= Auftragnehmer), der für mehrere Auftraggeber tätig wird. Der Auftragnehmer setzt das Gerät für betriebliche und private Zwecke ein. Für den Einsatz zu betrieblichen Zwecken stellt der Auftragnehmer dem Auftraggeber einen Aufwendungsersatz in Rechnung, den der Auftraggeber auch entsprechend bezahlt.

Bewertung: Zwischen Auftraggeber und Auftragnehmer besteht kein Arbeitsverhältnis. Der Auftragnehmer hat seine Einnahmen als Einkünfte aus selbständiger Tätigkeit oder aus Gewerbebetrieb zu versteuern. Zu diesen Einkünften zählt auch der Aufwendungsersatz. Dabei kann er die Gerätekosten, einschließlich Abschreibungen, steuermindernd absetzen, soweit sie auf seine betriebliche Tätigkeit entfallen. Der betriebliche Nutzungsanteil ist durch geeignete Unterlagen nachzuweisen. Der Auftraggeber kann die Kosten des freien Mitarbeiters sowie den Aufwendungsersatz als Betriebsausgaben nach § 4 Abs. 4 EStG geltend machen.

Da der Auftragnehmer selbständig tätig wird und für eigene Rechnung handelt, ist er im umsatzsteuerlichen Sinn als Unternehmer anzusehen. Daher muss er die von ihm erbrachten Leistungen und den Aufwendungsersatz der Umsatzsteuer unterwerfen und hierüber eine Rechnung stellen. Der Auftraggeber kann die in der Rechnung ausgewiesene Umsatzsteuer als Vorsteuer abziehen.

4. Fall

Ein Arbeitnehmer schließt für seinen Arbeitgeber Umsatzgeschäfte oder ist an Geschäftsabschlüssen beteiligt. Zu diesem Zweck sammelt und speichert er Daten und Unterlagen für diese Geschäfte auf seinen Datenverarbeitungsgeräten.

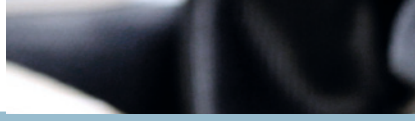
Bewertung: Damit der Arbeitgeber die Umsatzgeschäfte ordnungsgemäß der Besteuerung unterwerfen kann, muss gewährleistet sein, dass alle steuerrelevanten Daten und alle vorhandenen Unterlagen zu diesen Geschäften in der Buchhaltung des Arbeitgebers abgelegt und verbucht werden. Die Unterlagen müssen während der gesetzlich vorgeschriebenen Aufbewahrungsfristen (vgl. § 147 Abs. 3 AO) jederzeit verfügbar und für Außenprüfungen der Finanzverwaltung auch elektronisch zugänglich sein (§ 147 Abs. 6 AO). Dazu kann z. B. dem Mitarbeiter eine unterstützende Dokumentationssoftware zur Verfügung gestellt werden, die mit der Buchhaltung verbunden ist. Außerdem sollte der Mitarbeiter angewiesen werden, alle geschäftsrelevanten Aufzeichnungen und Unterlagen (z. B. E-Mail-Kommunikation mit dem Geschäftspartner, Bestellungen, Verträge) in einem Bereich abzulegen, der für die Buchhaltung ohne weiteres zugänglich ist und keine privaten Unterlagen des Mitarbeiters enthält.

5. Fall (Choose Your Own Device)

Der Arbeitgeber bietet seinen Arbeitnehmern innovative Geräte für die geschäftliche und die private Nutzung an. Der Arbeitnehmer kann sich sein bevorzugtes Gerät auswählen. Der Arbeitgeber schafft die Geräte an und übereignet sie unentgeltlich oder verbilligt dem Arbeitnehmer. Vor Übergabe an den Arbeitnehmer werden die betrieblich notwendigen Funktionen und Programme auf dem Gerät installiert.

Bewertung: Vorteile des Arbeitnehmers aus der vergünstigten oder unentgeltlichen Überlassung von Datenverarbeitungsgeräten unterliegen der Lohnsteuer. Der Arbeitgeber hat jedoch die Möglichkeit zur Lohnsteuerpauschalierung nach § 40 Abs. 2 Nr. 5 EStG. Die Pauschalierungsmöglichkeit erstreckt sich auf Zubehör, Software und die Internetanbindung des Arbeitnehmers. Sie besteht auch, wenn die Geräte zu rein privaten Zwecken an die Mitarbeiter ausgegeben werden.

Nach gegenwärtiger Rechtslage ist die Pauschalierungsmöglichkeit begrenzt auf Personalcomputer; Telekommunikationsgeräte sind also nicht erfasst (R 40.2 Abs. 5 LStR). Im Jahressteuergesetz 2013 ist jedoch eine Ausweitung der Pauschalierungsmöglichkeit auf »Datenverarbeitungsgeräte« vorgesehen. Dann wären auch Smartphones und Tablet-Computer erfasst. Das Jahressteuergesetz 2013 befindet sich gegenwärtig im Vermittlungsausschuss von Bundestag und Bundesrat.



Übernimmt der Arbeitgeber für den Arbeitnehmer zulässigerweise die pauschale Lohnsteuer von 25% zzgl. Solidaritätszuschlag und ggf. Kirchensteuer, entfällt die Steuerpflicht des Arbeitnehmers sowie die Beitragspflicht zur Sozialversicherung (§ 1 Nr. 3 Sozialversicherungsentgeltverordnung).

2.3.4 Empfehlungen

Obwohl die Möglichkeit zur Privatnutzung betrieblicher Geräte grundsätzlich der Lohnsteuerpflicht unterliegt, können hierbei Steuerbefreiungen und steuerliche Vergünstigungen genutzt werden. Voraussetzung dafür ist jedoch, dass der Arbeitgeber die Möglichkeit zur Privatnutzung zusätzlich zum vertraglich vereinbarten Arbeitsentgelt und nicht an dessen Stelle einräumt. Weitere Voraussetzung ist eine genaue Aufzeichnung der einzelnen Kosten und ein Nachweis für die Aufteilung privater und betrieblich veranlasster Kostenanteile zumindest während eines repräsentativen Zeitraums von 3 Monaten. Die Finanzverwaltung räumt aber hier Pauschalierungsmöglichkeiten ein. Die Voraussetzungen von Steuerbefreiungen und steuerlichen Vergünstigungen sollten genau eingehalten werden; denn in diesem Zusammenhang ist mit Nachfragen und Nachprüfungen der Finanzverwaltung zu rechnen.

Sollen Steuerbefreiungen oder steuerliche Vergünstigungen in Anspruch genommen werden, kann dies den Abwicklungsaufwand für die Lohnsteuerabrechnung erheblich erhöhen. Dieser höhere Aufwand sollte bei der Entscheidung über die Zulassung privater Mitarbeitergeräte zu betrieblichem Gebrauch berücksichtigt werden. Um den Aufwand beherrschbar zu halten, sollte die gewählte Konstellation flächendeckend für das gesamte Unternehmen eigeführt werden. Außerdem sollten die umgesetzten Konstellationen möglichst einfach und gut kontrollierbar gehalten werden. Der Einfachheit dienlich ist eine eindeutige Trennung von betrieblicher Sphäre des Arbeitgebers und privater Nutzung des Arbeitnehmers. Eine solche Trennung wäre z. B. möglich, indem der Arbeitgeber das Gerät mit den betriebsnotwendigen Funktionen und der erforderlichen Software ausstattet, ansonsten jedoch keine Kosten trägt.

Der Arbeitnehmer sollte sich bei der Nutzung privater Geräte bewusst sein, dass von ihm initiierte Geschäftsvorfälle in der Buchführung abgebildet werden müssen. Steuerlich relevante Daten und Unterlagen dürfen daher nicht im Privatbereich abgespeichert werden, der für den Arbeitgeber nicht zugänglich ist. Der Arbeitgeber sollte dies durch eine entsprechende Software und durch entsprechende Arbeitsanweisungen unterstützen.

Kernaussagen:

- Aufwendungen des Arbeitgebers für Geräte, die zu betrieblichen Zwecken eingesetzt werden, sind als Betriebsausgaben abzugsfähig.
- Umsatzsteuerpflichtige Leistungen an den Arbeitnehmer liegen nicht vor, soweit der Arbeitgeber Zahlungen und Leistungen erbringt, um betriebliche Prozesse zu unterstützen.
- Soweit der Arbeitnehmer betriebliche Geräte oder durch den Betrieb bereitgestellte Software privat nutzt, liegt darin ein lohnsteuerpflichtiger Vorteil. Dieser Vorteil ist teilweise durch Sondervorschriften von der Lohnsteuer befreit oder die Lohnsteuer kann pauschal vom Arbeitgeber übernommen werden.
- Der Arbeitnehmer kann Aufwendungen für seine beruflich genutzten Arbeitsmittel von seiner Einkommensteuer abziehen.
- Für steuerliche Zwecke ist der betriebliche und der private Nutzungsanteil gemischt genutzter Geräte zu ermitteln und nachzuweisen. Hierfür sieht das Steuerrecht Pauschalierungsmöglichkeiten vor.

2.4 Arbeitsrecht und Mitbestimmung

2.4.1 Arbeitsrechtliche Fragen

Da durch das BYOD-Konstrukt vom allgemeinen Grundsatz, dass der Arbeitgeber dem Arbeitnehmer die erforderlichen Arbeitsmittel zur Verfügung stellt, abgewichen wird, empfiehlt sich eine individualvertragliche Regelung oder eine entsprechende Richtlinie, die Bestandteil der Arbeitsverhältnisse werden sollte. Dies insbesondere vor dem Hintergrund, dass es zu diesem Themenbereich bisher kaum Rechtsprechung oder ausdrückliche Rechtsvorschriften gibt und somit keine klaren Regelungen, die der Rechtssicherheit der Parteien dienen.

Sofern die betriebliche Nutzung über Einzelfälle hinausgeht, ist eine vertragliche Absprache über ein vom Arbeitgeber an den Arbeitnehmer zahlbares Nutzungsentgelt sowie die Erstattung der vom Mitarbeiter verauslagten Kosten für Providergebühren, Reparatur- sowie Software- und Update-Kosten zwingend zu empfehlen, wobei der Arbeitgeber unbedingt Sorge dafür tragen sollte, dass ausreichende Lizenzen für die betriebliche Nutzung der auf dem privaten Endgerät gespeicherten Software vorhanden sind bzw. erworben werden, damit Urheberrechtsverletzungen vermieden werden (siehe dazu im Einzelnen Kapitel 2.2). Im Übrigen sollte zwischen den Parteien die Frage beantwortet sein, wer die rechtliche Verantwortung für das (auch) dienstlich genutzte Endgerät trägt, also wer für den Verlust des Gerätes, der Ersatzbeschaffung sowie die Konsequenzen des Nutzungsausfalls einzustehen hat.

Die Arbeitsvertragsparteien sollten ferner den gesetzlichen Vorgaben des Daten- und Geheimnisschutzes durch eine dem aktuellen Stand der Technik entsprechende technische Trennung von privaten und geschäftlichen Daten Sorge tragen, um den unberechtigten Zugriff Dritter zu unterbinden. Rechtlich sind diese technischen Maßnahmen durch entsprechende Vereinbarungen mit den Mitarbeitern einschließlich konkreter Handlungsanweisungen (z. B. Ausschalten der Roaming-Funktion bei Auslandsaufenthalten, Schutz vor Zugriff durch Familienangehörige o.ä.) zu flankieren. Weiterhin sollte geregelt werden, ob nur bestimmte Geräte zugelassen werden und ob BYOD für alle Mitarbeiter oder nur für bestimmte angeboten wird (kein Rechtsanspruch für Arbeitnehmer).

Schließlich sollten die Arbeitsvertragsparteien klare Absprachen für die Beendigung der Vertragsbeziehung treffen. Im Grundsatz ist der Arbeitnehmer ohne besondere Absprache verpflichtet, bei Beendigung des Arbeitsverhältnisses dem Arbeitgeber die in dessen Eigentum stehenden Gegenstände, zu denen auch Aufzeichnungen, Geschäftsunterlagen, Daten etc. zählen, herauszugeben. Dieses Grundprinzip greift bei BYOD nicht ohne weiteres. Das Endgerät steht im Eigentum des Arbeitnehmers, die darauf gespeicherten Daten sind häufig nur schwer eindeutig dem privaten und dem geschäftlichen Bereich zuzuordnen. Deshalb sollte abgestimmt werden, welche Daten vom Arbeitnehmer an den Arbeitgeber herauszugeben und von denen Kopien rückstandslos zu löschen sind. Erhebliche wirtschaftliche Bedeutung hat dieser Aspekt häufig in den Fällen ausgeschiedener Vertriebsmitarbeiter, bei denen der Arbeitgeber jedoch durchaus berechtigt die Herausgabe der beruflichen Kontakte begehrt.

2.4.2 Einbindung des Betriebsrats in das BYOD-Projekt

Die Einführung technischer Einrichtungen, die objektiv geeignet sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, löst ein Mitbestimmungsrecht der Belegschaftsvertretung aus (Leistungs- und Verhaltenskontrolle, § 87 Abs. 1 Nr. 6 BetrVG). Die Verknüpfung des privaten Endgeräts des Arbeitnehmers mit dem IT-System des Arbeitgebers eignet sich zur Überwachung und verpflichtet den Arbeitgeber, sich mit dem Betriebsrat über die Ausgestaltung der Überwachungsmaßnahmen im Rahmen einer Betriebsvereinbarung zu verständigen. Regelungsbedarf besteht insbesondere hinsichtlich der Frage, unter welchen Bedingungen der Arbeitgeber berechtigt ist, auf das private Gerät und die darauf gespeicherten Daten zuzugreifen.

Sind weitere Mitbestimmungsrechte zu beachten?

- Der Betriebsrat hat nach § 80 Abs. 1 BetrVG darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, also auch das BDSG, vom Arbeitgeber eingehalten werden. Der Belegschaftsvertretung ist in Bezug auf den Datenschutz jedoch lediglich eine Kontrollfunktion zugewiesen, die unabhängig und gleichberechtigt neben der als Selbstkontrolle des Unternehmens ausgestalteten Überwachung durch betriebliche Datenschutzbeauftragte und der behördlichen Überwachung besteht. Der Arbeitgeber ist dem Betriebsrat zur umfassenden Auskunft sowie zur Bereitstellung der notwendigen Informationen, ggf. durch Beistellung sachkundiger Arbeitnehmer verpflichtet, damit der Betriebsrat seine Kontrollfunktion auch wahrzunehmen in der Lage ist.

- Im Zeitalter der modernen Kommunikation ist eine zunehmende Vermengung von Frei- und Arbeitszeit zu beobachten. Die permanente Erreichbarkeit führt regelmäßig zu einem faktischen Zwang des Mitarbeiters, sich auch außerhalb der eigentlichen Arbeitszeit mit beruflichen Themen oder gar Anfragen des Vorgesetzten zu beschäftigen, zumal der Arbeitnehmer sich bei einem privat und beruflich genutzten Device dem Zugriff nur begrenzt durch schlichtes Abschalten entziehen kann. Der Betriebsrat sollte deshalb mit Blick auf sein Mitbestimmungsrecht hinsichtlich der Arbeitszeit (§ 87 Abs. 1 Nr. 2 BetrVG) auf klare und verlässliche Regeln zum arbeitszeitlichen Umgang mit dem Endgerät außerhalb der vereinbarten Arbeitszeiten drängen.

2.4.3 Welcher Betriebsrat ist zuständig?

Grundsätzlich ist der örtliche Betriebsrat für die Ausübung der Mitbestimmungsrechte zuständig. In Unternehmen mit mehreren Betrieben sowie in Konzernen mit mehreren Unternehmen liegt nicht zuletzt aus technischen Gründen eine unternehmens- bzw. konzerneinheitliche Betriebsvereinbarung zu BYOD nahe. Jedoch ist der Gesamtbetriebsrat nach dem BetrVG nur dann zuständig, wenn eine Angelegenheit das gesamte Unternehmen oder mehrere Betriebe betrifft und eine Regelung nicht durch die einzelnen Betriebsräte innerhalb der Betriebe erfolgen kann. Entsprechendes gilt für den Konzernbetriebsrat: Er ist zuständig für die Behandlung von Angelegenheiten, die den Konzern oder mehrere Konzernunternehmen betreffen und durch die einzelnen Gesamtbetriebsräte auf Unternehmensebene nicht geregelt werden können. Diese Voraussetzungen müssen zwingend vorliegen. Zur Vermeidung unnötiger Risiken ist deshalb zu erwägen, dass die örtlichen Betriebsräte oder die Gesamtbetriebsräte das übergeordnete Gremium mit dem Abschluss einer Gesamt- oder Konzernbetriebsvereinbarung beauftragen und hierdurch die Zuständigkeit kraft Auftrag begründen (§§ 50 Abs. 2, 58 Abs. 2 BetrVG).

2.4.4 Betriebsvereinbarung für Einsatz von privaten Geräten

Mögliche Inhalte einer Betriebsvereinbarung:

- Festlegung des Kreises berechtigter Mitarbeiter
- Festlegung des Charakters der Vertragsbeziehung zwischen Arbeitgeber und Arbeitnehmer
- Kostentragung
- Haftung für den Verlust des Gerätes
- Gewährleistung, Wartung des Gerätes
- Betriebsrisiko bei Ausfall des Gerätes
- Verhaltensmaßregeln zur Sicherstellung der datenschutzrechtlichen Anforderungen
- Kontroll- und Zugriffsrechte des Arbeitgebers unter Beachtung des Fernmeldegeheimnisses
- Nutzung der Kontrollergebnisse zu Leistungs- und Verhaltenskontrollen
- Zeitliche Regelungen zur dienstlichen Nutzung
- Löschung von Daten durch Arbeitgeber
- Beendigung des Arbeitsverhältnisses

2.4.5 Wer haftet in welchem Umfang bei Verlust des Device?

In einer solchen Vereinbarung sollte auch das Thema Haftung geregelt werden. Problematisch ist, wie im Falle des Verlustes oder der Beschädigung des vom Arbeitnehmer eingebrachten Gerätes vorzugehen ist.

Sofern die Beschädigung oder der Verlust des Gerätes durch den Arbeitgeber verschuldet wurde, ist er auch zum Ersatz des entstandenen Schadens verpflichtet.

Falls jedoch Verlust oder Beschädigung dem Bereich des Arbeitnehmers zuzuordnen sind, ist dies nicht mehr ganz so eindeutig. In diesen Fällen können je nach Ausgestaltung des Einzelfalles Arbeitnehmer oder Arbeitgeber zur Schadenstragung verpflichtet sein. Grundlegende Voraussetzung einer etwaigen Haftung des Arbeitgebers in einem solchen Fall ist, dass ein Zusammenhang mit der Arbeitsleistung gegeben ist – wobei die Grenzen gerade im Bereich von BYOD fließend sind. So haben sich viele Unternehmen – auch im Hinblick auf die Vorteile von BYOD – von vornherein dazu entschieden, die Haftung für die Geräte zu übernehmen oder zumindest Reparatur- und Wartungsleistungen anzubieten.

Für die Haftungsfrage kommt es neben arbeitsrechtlichen Fragestellungen besonders auf die von den Parteien für BYOD gewählte Vertragsart an. Die Haftungslage kann sich je nachdem, ob ein Leih-, Geschäftsbesorgungs- oder Mietvertrag vorliegt, gänzlich anders darstellen. Bei der Wahl des BYOD-Modells sollte daher speziell auch die Auswirkung auf die Haftungsfrage beleuchtet und diese dann je nach gewähltem Modell individuell mit dem Arbeitnehmer vereinbart werden. Zu beachten ist dabei, dass auch hier die allgemeinen Grundsätze der Überprüfung durch die §§ 305 ff BGB gelten und eine unangemessene Benachteiligung der Arbeitnehmer zwingend zu vermeiden ist.

Neben der Haftung für das Gerät,ist selbstverständlich auch die Haftung für die darauf befindlichen Daten, die Software u. ä. zu beachten. So kann bspw. auch eine Haftung des Mitarbeiters eintreten, wenn durch die Nutzung seines Gerätes Informationen und Daten unberechtigt veröffentlicht oder an Dritte weitergegeben werden oder gar Daten endgültig gelöscht und dem Zugriff des Unternehmens vollständig entzogen werden. Insoweit gelten die allgemeinen arbeitsrechtlichen Grundsätze, so dass eine diesbezügliche Haftungsregelung entbehrlich sein dürfte, nicht jedoch ein Hinweis auf den richtigen Umgang mit den Firmendaten.

Kernaussagen

Individualrechtliche Fragen

- Nutzungsverhältnis zwischen Unternehmen und Arbeitnehmer
- Haftung bei Verlust oder Beschädigung

Einbindung des Betriebsrats

- Einschlägige Mitbestimmungsrechte
- Checkliste für eine Betriebsvereinbarung

2.5 Vereinbarungen mit Mitarbeitern und Soft- und Hardwareanbietern

Der Einsatz mobiler Endgeräte im Rahmen einer Bring Your Own Device-Strategie benötigt ein abgestimmtes Konzept zur Lösung der rechtlichen Aspekte und eine dazu passende technische Umsetzung. Die rechtlichen Lösungen und die technische Umsetzung stehen in Wechselwirkung. Bei der Entwicklung der Bring Your Own Device-Strategie ist daher eine enge Verzahnung rechtlicher und technischer Aspekte notwendig.

Die Ausgangslage für eine Bring Your Own Device-Strategie ist im Unternehmen jeweils konkret zu ermitteln. Die spezifischen Ausgangssituationen mehrerer Unternehmen unterscheiden sich oft deutlich. Das betrifft nicht nur das technische Umfeld, sondern auch die rechtliche Ausgangssituation, etwa Existenz oder Inhalte von Betriebsvereinbarungen für die Nutzung von Informationstechnologie. Auch die technischen Lösungswege unterscheiden sich von Unternehmen zu Unternehmen. Ebenso unterscheiden sich die Zielsetzungen der Unternehmen. Das gilt schon für die Frage wirtschaftlicher Anreize für die Nutzung von Bring Your Own Device-Endgeräten. Auch für solche wirtschaftlichen Anreize sind entsprechende Vereinbarungen mit Mitarbeitern notwendig.

Diese unterschiedlichen und in ihren Inhalten variierenden Faktoren führen dazu, dass ein Unternehmen für die Einführung einer Bring Your Own Device-Strategie zunächst seine Ausgangssituationen in rechtlicher und technischer Hinsicht ermitteln sollte. Anhand der verfolgten Ziele ist dann eine unternehmensspezifische Umsetzung zu entwickeln und schließlich auch einzuführen. Deren Inhalte können sich ja nach Unternehmen deutlich unterscheiden.

Im Folgenden werden die oben näher dargestellten rechtlichen Aspekte kurz zusammengefasst und nur einige weitere rechtliche Themen kurz angesprochen:

2.5.1 Vereinbarungen mit Betriebsräten und Mitarbeitern

Wie unter Ziffer 2.4 dargelegt, empfiehlt sich dringend eine individualvertragliche Regelung mit den Mitarbeitern zur Nutzung von privaten Endgeräten, die beispielsweise ein zahlbares Nutzungsentgelt, die Erstattung der vom Mitarbeiter verauslagten Kosten für Providergebühren, Reparatur- sowie Software- und Update-Kosten regelt. Ferner sollte der Arbeitgeber dafür Sorge tragen, dass ausreichende Lizenzen für die betriebliche Nutzung der auf dem privaten Endgerät gespeicherten Software vorhanden sind bzw. erworben werden. Im Übrigen sollte zwischen den Parteien die Frage beantwortet sein, wer für den Verlust des Gerätes, eine Ersatzbeschaffung sowie die Konsequenzen des Nutzungsausfalls haftet. Die Arbeitsvertragsparteien sollten ferner den gesetzlichen Vorgaben des Daten- und Geheimnisschutzes Rechnung tragen und Maßnahmen gegen einen Datenabfluss vereinbaren. Rechtlich sind die diesbezüglichen technischen Maßnahmen durch entsprechende Vereinbarungen einschließlich konkreter Handlungsanweisungen zu flankieren. Schließlich sollten klare Absprachen für die Beendigung der Vertragsbeziehung getroffen werden.

Zusätzlich zu diesen individualvertraglichen Regelungen sind auch etwaige Mitbestimmungsrechte des Betriebsrates zu beachten, die sich bspw. aus den Bestimmungen zu Leistungs- und Verhaltenskontrolle, § 87 Abs. 1 Nr. 6 BetrVG, sowie zur Arbeitszeit, § 87 Abs. 1 Nr. 2, ergeben können. Insoweit sollte dringend ermittelt werden, mit welchem Gremium die Vereinbarung geschlossen werden muss, damit sie auch rechtswirksam ist (z. B. Konzernbetriebsrat, lokaler Betriebsrat, siehe dazu auch Kapitel 2.4.3 und 2.4.4). Regelungsbedarf besteht insbesondere hinsichtlich der Frage, unter welchen Bedingungen der Arbeitgeber berechtigt ist, auf das private Gerät und die darauf gespeicherten Daten zuzugreifen sowie wie sich der Umgang mit dem Endgerät außerhalb der vereinbarten Arbeitszeiten darstellt. Mögliche Inhalte einer entsprechenden Betriebsvereinbarung sind unter Ziffer 2.4 im Einzelnen dargestellt.

2.5.2 Vereinbarungen mit Softwareanbietern für Gerätesoftware und Apps

Für ein stimmiges BYOD-Konzept sind neben Arbeitsanweisungen bzw. Individual- und Betriebsvereinbarungen im Verhältnis zum Arbeitnehmer auch Vereinbarungen mit den Softwareanbietern selbst erforderlich.

Denn zumeist werden auf den privaten Endgeräten Gerätesoftware und Apps (»Software«) installiert sein, zu deren Nutzung der Arbeitnehmer im Zweifel ausschließlich für private Zwecke, nicht jedoch im geschäftlichen Verkehr, berechtigt sein wird. Sollte der Arbeitnehmer eine solche App dennoch für seine Arbeitstätigkeit nutzen, werden – meist unwissentlich – Urheberrechte des Softwareanbieters verletzt; im Falle einer Nutzungsbeschränkung der Gerätesoftware auf den privaten Bereich selbst dann, wenn die App (auch) für den beruflichen Bereich lizenziert sein sollte (siehe dazu Kapitel 2.2).

Der Haftung des Unternehmens für etwaige Urheberrechtsverletzungen wird idealerweise durch Vereinbarungen mit den Software-Anbietern im Vorfeld der Nutzung begegnet. Hierfür ist, soweit dienstliche Software auf private Endgeräte aufgespielt wird, möglicherweise eine Erweiterung der bestehenden Unternehmens-Lizenzverträge erforderlich. Sofern die dienstliche Nutzung privater Software nicht zulässig oder dies zumindest nicht gesichert ist, sind von den Softwareanbietern die noch fehlenden (betrieblichen) Nutzungsrechte zu erwerben. Aufgrund der erfahrungsgemäßen Vielzahl von Software auf privaten Endgeräten, sollte jedoch – allein schon aus praktikablen und kostenmäßigen Gründen – deren betriebliche Nutzung reglementiert werden.

Welche private Software schließlich auf den privaten Endgeräten für die dienstliche Nutzung zugelassen wird, die dann für die private und dienstliche Nutzung als Teil des BYOD Modells von den Vereinbarungen mit den Softwareanbietern umfasst wird und welche nicht und wie die Verwendbarkeit von nicht zugelassener privater Software für dienstliche Zwecke wirksam begrenzt werden kann, ist letztlich nur über ein aktives Lizenzmanagement im Unternehmen zu erzielen.

Zunächst sollte die auf den BYOD-Geräten installierte Software in einer Bestandsaufnahme erfasst, sowie die vorhandenen Lizenzen ermittelt und juristisch bewertet werden. Anschließend kann im Rahmen eines Compliance-Check ein Abgleich des Softwareinventars mit dem Lizenzinventar durchgeführt werden, also eine Prüfung, ob für die installierte Software auch Lizenzen vorhanden sind (Erstellung einer Lizenzbilanz).

Ohne aktives Mobile Device Management und eine valide Lizenzbilanz droht nicht nur Unterlizenzierung, es besteht auch die Gefahr, dass vorhandene Rechte ineffektiv genutzt werden und dadurch Einsparpotentiale verloren gehen.

Vorteile einer Lizenzverwaltung:

- Planbare und dem Geschäftszweck angemessen skalierbare Lizenzkosten und transparente Softwareauswahl,
- Vereinfachte Installation und Wartung von BYOD Software,
- Bilanzierung der Lizenz-«Reserven«, um Lizenzüberdeckung bzw. -unterdeckung zu reduzieren,
- Reduziertes Risiko für die Geschäftsführung durch nicht-lizenzkonforme Installationen.

Die Installation und das Lizenzmanagement von Unternehmenssoftware auf privaten Endgeräten kann beispielsweise durch sog. virtuelle Desktops erleichtert werden. Der Anwender des BYOD-Gerätes kann dort die Applikationen auswählen, die er benötigt. Die Software verbleibt im Unternehmen, da sie auf der virtuellen Infrastruktur installiert ist und nicht auf dem mobilen Endgerät. Diese Variante bietet zudem auch Vorteile im Hinblick auf die Themen Vertraulichkeit und Datenschutz. Darüber hinaus bieten sich ggf. pay per use Modelle an.

2.5.3 Weitere Aspekte

- Wartungs- und Supportverträge
  Bei der Gestaltung von Wartungs- und Supportverträgen für BYOD-Geräte ist zu differenzieren:

a) Der Arbeitnehmer ist frei in der Auswahl von Hardware und Software (Apps) seines BYOD-Geräts. Für den Arbeitnehmer ist das ideal, für den Arbeitgeber die deutlich schwierigere Konstellation.

b) Der Arbeitgeber akzeptiert nur bestimmte Hard- und Software für BYOD-Geräte. Dies ist der technisch und kommerziell bevorzugte Weg, der das Interesse der Arbeitnehmer an BYOD »light« reduzieren dürfte.

c) Der Arbeitnehmer hat einen Wartungs- und Supportvertrag, z. B. neues Gerät mit »2 Jahres Garantie«, oder der Arbeitnehmer hat eine zusätzliche Vereinbarung geschlossen. Umfang und Qualität dieser Leistungen müssten dem vom Arbeitnehmer vorgegebenen Leistungsumfang entsprechen und ihn auch als Leistungsempfangsberechtigten definieren. Der Schutz der Unternehmensdaten durch den Serviceprovider des Arbeitnehmers ist sicherzustellen. Derartige Leistungen sind im B2C Bereich regelmäßig stark standardisiert. Leistungsbeschreibungen und Vertragsklauseln innerhalb von AGBs erlauben kaum Änderungen.

d) Der Arbeitgeber stellt Wartungs- und Supportleistungen zur Verfügung. Der Leistungsumfang kann entsprechend den Bedürfnissen des Arbeitgebers gestaltet werden und der Arbeitnehmer als Leistungsempfangsberechtigter definiert werden. Zu prüfen ist, ob der Leistungsumfang jede vom Arbeitnehmer eingebrachte BYOD Hard- und Software abdeckt. Es muss sichergestellt werden, dass Erweiterungen des Umfangs weitgehend kostenneutral möglich sind und ausreichend Know-how verfügbar ist, um die Vielfalt von BYOD Hard- und Software professionell darzustellen.

Generelle Überlegungen zur Gestaltung von Vertragsregelungen:

a) Arbeitgeber und Arbeitnehmer müssen Empfangsberechtigte von BYOD Wartungs- und Supportleistungen sein. Eine Regelung, wer Weisung erteilen kann und welche vorgeht, erscheint sinnvoll.

b) Die Haftungsregelung muss auch Schäden Dritter (Geräte – bzw. Dateninhaber) abdecken und im Fall einer Haftungsbegrenzung eine für den Betrieb des Arbeitgeber ausreichende Höhe haben. Um der technischen Entwicklung zu folgen, ist ein Change Management Mechanismus vorzusehen, der nicht zu massiven Kostensteigerungen führt.

Soweit Wartungs- und Supportleistungsverträge inhaltlich nicht auf eine BYOD Situation, d.h. Nutzung für private und betriebliche Zwecke, unterschiedliche Datenbestände etc. angepasst werden können, kommt BYOD nicht in Betracht.

- Virenschutz und Sicherheitsmaßnahmen
  Statt der Verpflichtung des Arbeitnehmers, die IT-Nutzungs- u. Sicherheitsrichtlinien sowie Sicherheitsmaßnahmen des Unternehmens wie z. B. Nutzung des Geräts nur durch Arbeitnehmer persönlich, Virenscanner, PINs, etc. zu befolgen, nutzen und aktuell zu halten, ist zu überlegen, ob der Arbeitnehmer sich verpflichtet, das Sicherheitskonzept des Arbeitgebers zu akzeptieren und dieses so zu gestalten, dass es vom Nutzer nicht beeinflussbar völlig automatisch arbeitet.

- Absicherung gegen ungewollten Datenabfluss
  Zur Absicherung gegen ungewollten Datenabfluss haben Virtualisierungsanbieter oft Datenmanagementlösungen integriert. Soweit nicht mit solchen Komplettlösungen gearbeitet wird, sollten Datenmanagementlösungen wie z. B. von MobileIron oder Good Technology genutzt werden. So lässt sich Datenabfluss oder -missbrauch bei Geräteverlust oder anderen unberechtigten Eingriffen vermeiden.

Für die Bring Your Own Device-Strategie sind die oben angesprochenen Aspekte in einem einheitlichen Konzept zu lösen und mit der technischen Umsetzung eng abzustimmen. Dadurch lassen sich für viele Ziele, Bedürfnisse und Anwendungsszenarien rechtlich zulässige Lösungen schaffen und gestalten. Grenzenlos sind diese Möglichkeiten allerdings nicht. Für bestimmte Anwendungen und Daten kann die Nutzung privater Endgeräte rechtlich unzulässig sein.

Kernaussagen:

- Die Einführung von BYOD erfordert die enge Verzahnung rechtlicher und technischer Aspekte.
- Für die rechtlichen Aspekte sind zunächst die Vereinbarungen im Unternehmen für einzusetzende Software sowie mit Betriebsräten und Mitarbeitern für den Einsatz mobiler Endgeräte und die private Nutzung von IT-Ressourcen des Unternehmens zu analysieren.
- Zusätzlich erforderliche Nutzungsrechte für einzusetzende Software sind zu beschaffen und ergänzend notwendige Betriebsvereinbarungen abzuschließen.
- Das BYOD-Konzept ist in Vereinbarungen mit den Mitarbeitern abzubilden durch entsprechende Verhaltensregeln für die Mitarbeiter und definierte Zugriffsrechte des Unternehmens sowie Maßgaben für den Datenschutz.
- Auch Support und Wartung für Geräte und Software sowie Virenschutz und Sicherheitsmaßnahmen sind vertraglich zu regeln.
- Diese Vereinbarungen müssen das BYOD-Konzept eng abgestimmt nicht nur untereinander, sondern auch mit der technischen Lösung umsetzen.

3 BYOD in der Unternehmenspraxis

Unternehmen, die die Nutzung privater Geräte erlauben möchten, müssen verschiedene konkrete technische und organisatorische Herausforderungen meistern. Mit der raschen Verbreitung von neuen, mobilen Endgeräten wie Smartphones und Tabletcomputern sowie Web-Anwendungen definieren Mitarbeiter neu, was es bedeutet, »im Büro« zu sein. Zugleich verschwimmen die Grenzen traditioneller Unternehmensnetzwerke. Es stellt sich die Frage, wie zum Beispiel private und berufliche Daten getrennt, Datensicherheit, Datenintegrität und Datenschutz gewährleistet werden können. Unternehmen müssen daher Richtlinien für die Auswahl neuer Geräte, für die Echtzeit-Sicherheitskontrollen im Betrieb anhand der im Unternehmen geltenden Sicherheitsstandards, Vorkehrungen für den Verlust, für die Behandlung ausgemusterter Geräte sowie für das Ausscheiden von Mitarbeitern planen, verwalten und durchsetzen. An dieser Stelle sei darauf verwiesen, dass im weiteren Verlauf dieses Kapitels der Schwerpunkt der Betrachtung auf Smartphones und Tabletcomputern liegt, da hier derzeit im Hinblick auf BYOD der größte Handlungsdruck bei Unternehmen besteht. Im Vergleich zur Einbindung von Notebooks bestehen, insbesondere aus technischer Sicht, teilweise deutliche Unterschiede.

3.1 Voraussetzung für die sichere BYOD-Nutzung im Unternehmensnetzwerk

Im Mittelpunkt der Planung für eine BYOD-Lösung steht eine umfassende Analyse, ob und wenn ja, welcher Benutzer welches Gerät und von welchem Standort aus auf das Netzwerk, auf Daten und Services zugreifen darf. Unternehmen haben unterschiedliche Gründe für das Konzept einer freien Geräteauswahl. Die Analyse führt daher zu einer individuellen Sicherheitsstrategie, die folgende Punkte berücksichtigt:

1. **Infrastruktur:**
Integration aller eingesetzten mobilen Geräte und gegebenenfalls neuer Mitarbeiter in das vorhandene Sicherheitskonzept und die geltenden Sicherheitsstandards,

2. **Geräte:**
Geräte- und standortunabhängiger Zugriff, Datensicherheit, Datenintegrität und Datenschutz auf dem mobilen Endgerät hinsichtlich Malware-Schutz, Verschlüsselung, Austausch, Verlust und Diebstahl,

3. **Anwendungen und Services:**
Regelung der Nutzung von Anwendungen und Services auf den mobilen Endgeräten hinsichtlich Umfang, Anwendererlebnis und Sicherheit.

3.1.1 Geräteauswahl und Support

Für eine BYOD-Strategie gilt: Nicht jedes private Endgerät der Mitarbeiter kann ohne weiteres zugelassen werden. Unternehmen sollten sich vorab die folgenden Fragen stellen:

- Besteht die Möglichkeit zur Verschlüsselung des mobilen Endgerätes inklusive Wechselmedien?
- Lassen sich private Daten von Unternehmensdaten trennen?
- Bei Smartphones/Tablets: Befindet sich das Betriebssystem im Originalzustand – oder wurden vom Nutzer ein Rooting bzw. ein sogenannter Jailbreak, d.h. ein unautorisierter Eingriff (Entsperrung) in das Betriebssystem des Endgeräts, durchgeführt und damit Nutzungsbeschränkungen des Herstellers aufgehoben?
- Ist der Mitarbeiter bereit, sein privates Endgerät in das Mobile Device Management (MDM) der Firma integrieren zu lassen?

- Insbesondere bei Smartphones/Tablets: Stimmt der Mitarbeiter zu, dass die Daten aus dem Gerät im Falle eines Verlustes komplett gelöscht werden (bei Notebooks ist Festplattenverschlüsselung möglich)?

- Ist der Mitarbeiter damit einverstanden, dass die Handhabung des Gerätes ggf. durch die Sicherheitsrichtlinien des Unternehmens teilweise eingeschränkt werden kann?

- Stimmt der Mitarbeiter Kontrollen durch den Arbeitgeber und ggf. weiteren Stellen (Datenschutzaufsicht, Auftraggeber) zu?

Private Endgeräte, die dem individuellen Sicherheitsgrundkonzept des Unternehmens nicht entsprechen und etwa eine Verschlüsselung, weitere Sicherheitsmaßnahmen oder das Einbinden in ein MDM-System nicht unterstützen, dürfen bei einer BYOD-Lösung keinen vollständigen Remote-Zugriff erhalten bzw. nicht für den Zugriff auf Unternehmensdaten freigeschaltet werden.

- Empfehlung: Stimmen Sie mit Ihren Mitarbeitern entweder einen Katalog an Mindestanforderungen oder eine entsprechende Auswahl an Smartphones, Tablets und Laptops für die Nutzung im Rahmen Ihrer BYOD-Lösung ab. Bedenken Sie, die Nutzung der Endgeräte sollte Spaß machen und muss sicher sein.

3.1.2 Endgeräte klassifizieren (»Profiling«)

Die Möglichkeit zur freien Geräteauswahl durch die Mitarbeiter erfordert, dass die Endgeräte aufgrund von Sicherheitskriterien kategorisiert und verschiedenen Klassen zugeordnet werden, um daraufhin bei entsprechenden Zugriffen im Netzwerk entscheiden zu können, welche Ressourcen mit ihnen wann, wo und wie genutzt werden dürfen. Um das Endgerät eindeutig identifizieren zu können, sobald es mit dem Unternehmensnetzwerk verbunden ist, werden unter anderem RADIUS-, DHCP-, DNS- und HTTP-Informationen ausgewertet[3].

3.1.3 Sicherer Zugang zum Unternehmensnetzwerk

In einer Umgebung, in der Mitarbeiter lediglich von stationären Geräten, dem »klassischen« Desktop-Rechner, auf die Unternehmensdaten zugreifen konnten, genügten Benutzername und Kennwort für die Authentifizierung. Da die Mitarbeiter ihr Endgerät nun frei wählen und sich mobil mit einem Netzwerk verbinden, ist dies als Zugangskontrolle nicht mehr ausreichend. Hier garantieren dagegen digitale Zertifikate einen abgesicherten Netzwerkzugang. Voraussetzung dafür ist die Installation einer speziellen Software auf dem vom Mitarbeiter für seine Arbeit ausgewählten Endgerät, die Zertifikate zur automatischen Authentifizierung ausweisen kann. Weiterhin muss der Zugriff auf die ausstellende Zertifizierungsstelle gewährleistet sein, um das autorisierte Wurzelzertifikat auf die Endgeräte zu verteilen.

- Hierfür stehen technische Lösungen mittels Simple Certificate Enrollment Protocol (SCEP) zur Verfügung. Zusätzlich muss der Nutzer das Zertifikat bzw. das Schlüsselmaterial einmalig manuell in den entsprechenden Zertifikatsspeicher des Endgeräts einbinden. Bei der Verteilung von Schüsselmaterial ist generell zu beachten, dass nicht alle Betriebssysteme die gleichen Möglichkeiten bieten, um Zertifikate zu generieren, herunterzuladen und zu installieren. Dies gilt insbesondere bei Betriebssystemen für mobile Endgeräte, die eher auf den Konsumentenmarkt zielen.

  Für den sicheren Netzwerkzugang von Notebooks sind bereits seit Längerem auch sogenannte Token-basierte (z. B. separater USB-Stick) oder Smartcard-basierte Lösungen im Einsatz. Neben dem Wissen des Passworts ist auch der Besitz des Tokens oder der Smartcard Voraussetzung, um den Log-in ins Unternehmensnetzwerk vollziehen zu können.

3 RADIUS: Remote Authentication Dial-In User Service; DHCP: Dynamic Host Configuration Protocol; DNS: Domain Name System; HTTP: Hypertext Transfer Protocol

- MDM-Lösungen sind bei der Kontrolle der Endgeräte entscheidend. Zum einen bieten Sie den Komfort der zentralen Konfiguration der Endgeräte, zum anderen werden die Endgeräte zentral mit den Sicherheitsrichtlinien des Unternehmens konfiguriert – sowie vor allem auch kontrolliert. Die Kontrolle der Endgeräte ist notwendig, damit diese automatisch vom Zugriff auf Ressourcen des Unternehmens getrennt werden, sobald sie kompromittiert bzw. eine Infektion mit Schadsoftware oder ein sonstiger Sicherheitsverstoß auf ihnen erkannt wurde. Leistungsfähige MDM-Systeme unterscheiden dabei zwischen einem Unternehmens- und einem Privatgerät und können Maßnahmen auf Ereignisse in unterschiedlichen Härtegraden durchsetzen. Das entscheidende Ziel ist dabei stets, die Unternehmensdaten zu schützen.

  Wichtig bei einem MDM-System ist ebenfalls, dass neben Software auch die Zertifikate – entweder als Unternehmens- oder als Benutzerzertifikat – auf die Endgeräte verteilt werden können. Hinzu kommen Zertifikatstypen für VPN-Zugänge (Virtual Private Network) oder E-Mail-Verschlüsselung. Idealerweise werden diese Zertifikate automatisch vom MDM-System an der Zertifizierungsstelle des Unternehmens abgeholt, im Mitarbeiterdatensatz gespeichert und danach auf das mobile Endgerät verteilt. Dies wird ebenfalls automatisch dann durchgeführt, wenn das Zertifikat abgelaufen ist und erneuert wird.

3.1.4 Authentifizierung an kabelgebundenen und kabellosen Netzwerken

Die Authentifizierung basiert auf einem komplexen Regelwerk (Authentifizierung, Autorisierung und Berechtigungsprofil), das die jeweiligen Sicherheitsrichtlinien des Unternehmens mit den vorhandenen bzw. individuell genutzten Netzwerk- und Sicherheitskomponenten sowie Prozessen rund um den Nutzer verbindet.

Regeln für die Authentifizierung[4] setzen sich aus dem Authentifizierungsprotokoll und einer Identität zusammen, welche in unterschiedlichen Datenbanken wie z. B. Active Directory oder LDAP verwaltet werden können.

Autorisierungsrichtlinien bestimmen, welche Nutzer auf das Netzwerk bzw. auf dessen Ressourcen zugreifen dürfen. Sie bestehen aus einzelnen Regeln, die um konditionale Abhängigkeiten erweitert werden können.

Die jeweiligen Berechtigungen des Benutzers werden in Berechtigungsprofilen definiert. Zur Administrierung empfehlenswert sind Lösungen, mit denen sich komplexe Zusammenhänge in leicht verständliche Regeln umsetzen und steuern lassen.

3.1.5 Schützenswerte Daten und Datenverlust

Unternehmensdaten sind stets sensible Daten. Deshalb stellt sich die Frage, wie diese Daten am besten geschützt werden können? Werden sogenannte Enterprise Apps mit firmenspezifischen Anwendungen auf mobilen Endgeräten eingesetzt, gestattet dies möglicherweise den direkten Zugriff vom mobilen Endgerät aus in das Backend des Unternehmens. Dies ist dann problematisch, wenn ein Endgerät angegriffen wird, dessen Verbindung in das Unternehmensnetzwerk genutzt werden kann, um Daten zu entwenden. Hier können Middleware-Plattformen helfen, die als eigene »demilitarisierte Zone« (DMZ) bzw. Sicherheitszone zwischen dem Backend und den mobilen Endgeräten stehen. Diese Middleware-Plattformen lassen sich an jegliche Backends anschließen und das Unternehmen kann festlegen, welche Daten dem Benutzer angeboten werden. Handshake und Verschlüsselungsverfahren sowie ein MDM-System entscheiden dann, ob ein Endgerät Zugriff auf die Daten erhält oder nicht.

4 Hier kommen Protokolle wie z. B. EAP-TLS, PEAP, EAP-FAST zum Einsatz

Daneben sind die auf dem mobilen Endgerät gespeicherten Daten zu berücksichtigen. Hier empfehlen sich entweder verschlüsselte Datencontainer, die nur bestimmte Bereiche des Backend synchronisieren, oder die Daten werden durch ein Information Rights Management (IRM) geschützt. Letzteres legt Benutzerrechte jeweils für Dateien oder Ordner an. Nur ein Benutzer, der über eine Schreib- oder Leseberechtigung für die Datei oder den Ordner verfügt, kann mit diesen Dateien arbeiten. Die Rechte in einem IRM können sogar soweit eingeschränkt werden, dass selbst Screenshots unterbunden oder Dateien lediglich mit einer gewissen Offlinefunktion ausgestattet werden. Meldet sich der Client nicht innerhalb einer festgelegten Zeit, ist die Datei auf diesem Wege selbst für den Benutzer nicht mehr zu öffnen.

Empfehlung:
Die eingesetzte Lösung sollte auch einen Datenabfluss über diverse Schnittstellen verhindern können und sicherstellen, dass keine kritischen Daten lesbar in privat erstellten Backups auftreten.

3.2 Management von BYOD-Geräten

Allein schon aufgrund der großen Zahl an Geräten wird es für die IT-Abteilungen in Unternehmen zunehmend schwieriger, den Überblick zu behalten. Daher müssen die im Rahmen einer BYOD-Lösung zugelassenen Geräte einem Sicherheitsgrundkonzept entsprechen, um einen vollständigen Fernzugriff auf das Unternehmensnetzwerk zu erhalten.

3.2.1 Neue Endgeräte einbinden

BYOD-Lösungen müssen in der Lage sein, eine Vielzahl unterschiedlicher Endgeräte wie Desktop, Notebook, Netbook, Smartphone, Tablet und E-Reader zu unterstützen. Einige dieser Systeme werden durch das Unternehmen bereitgestellt und auch gewartet, andere vom Mitarbeiter erworben und vielleicht sogar im Rahmen eines firmeninternen Wiki-Projekts selbst technisch betreut.

Der Prozess für das erstmalige Einbinden eines neuen Endgeräts ins Unternehmensnetzwerk (Onboarding) muss leicht verständlich und praktikabel sein. Dies sollte mit geringem oder möglichst gar keinem Aufwand für die IT-Abteilung verbunden sein. Hier bieten sich Lösungen für ein eigenständiges Einbinden (»self-onboarding«) des privaten Endgeräts durch den Benutzer an. Im Anschluss wird ein vorkonfiguriertes Wirelss Lan Profil auf das Endgerät geladen, welches einen kontrollierten und sicheren Zugang zum kabellosen Unternehmensnetzwerk bietet.

MDM-Systeme bieten in der Regel für das Einbinden mobiler Endgeräte sogenannte User-Self-Service Portale an. Hier kann der Benutzer, aufgrund seiner Berechtigung, sein eigenes Gerät in das zentrale MDM-System des Unternehmens aufnehmen. Hat er dies getan, wird das Gerät automatisch konfiguriert. Weiterhin bietet ein User-Self-Service Portal die Möglichkeit das eigene Gerät zu sperren, zu entsperren oder zu löschen.

3.2.2 Anwendungen sicher verwalten

Der Vorgang der Bereitstellung einer Applikation durch das Unternehmen sollte sich daran orientieren, wie Mitarbeiter privat entsprechende Anwendungen kaufen bzw. laden. Eine Lösung hierfür könnte – je nach Betriebssystem – z. B. ein firmeneigener App-Store sein. Je einfacher die Lösung, desto weniger Aufwand kommt auf den IT-Support zu.

Um jedem Mitarbeiter die passenden Informationen bereitstellen zu können, ist die Umsetzung eines Berechtigungskonzeptes auch auf mobilen Geräten nötig. Das kann auch durch einen firmeneigenen App-Store oder ein MDM-System gelöst werden.

Insbesondere wenn sicherheitsrelevante Betriebssystemkomponenten gepatched werden müssen, kann sonst die Sicherheit des Gesamtsystems gefährdet werden. Das Vorgehen bei Security-Updates sollte daher analog des Patchmanagements im Unternehmen geregelt sein.

- Variante 1:
  Arbeitgeber übernimmt das Patchmanagement
- Variante 2:
  Arbeitnehmer übernimmt das Patchmanagement. Dann muss der Arbeitgeber die Möglichkeit haben, Geräte auszuschließen, die auf Grund fehlender Systempatches die Unternehmenssicherheit gefährden. Dieses sollte in den Nutzungsbedingungen verankert werden.

3.2.3 Verlust und Diebstahl von Endgeräten

Vorher bereits an nachher zu denken bedeutet bei einer BYOD-Lösung auch, einen Prozess für verloren gegangene oder entwendete private Endgeräte zu implementieren. Entscheidend ist, dass der Benutzer in diesen Prozess mit eingebunden wird, zumal er als Erster bemerkt, dass sein Gerät verloren gegangen ist oder gestohlen wurde. Die folgenden Schritte haben sich in diesem Zusammenhang bewährt.

- Benachrichtigung der IT-Abteilung durch den Nutzer und zeitgleich Sperrung des Zugriffs auf das Unternehmensnetzwerk für das betroffene Gerät
- Löschung der lokal auf dem Endgerät gespeicherten (Firmen-)Daten
- Ortung des Gerätes (bei Smartphones/Tablets)

Die nachstehend aufgeführten Maßnahmen zur Absicherung des mobilen Endgeräts sind Grundvoraussetzungen, um den mobilen Fernzugriff auf das Unternehmensnetzwerk zu gewähren. Eine erste Maßnahme ist die Zugriffssperre auf Smartphones und Tablets, die zumeist aus einer individuell konfigurierbaren, mehrstelligen Zahlenfolge besteht. Dies bietet nur ein relatives Sicherheitsniveau, da in der Vergangenheit mehrfach Fälle bekannt wurden, bei denen durch gezieltes Ausnutzen von Fehlern in der Endgeräte-Software diese Zugriffssperre umgangen werden konnte. Sie wegzulassen bedeutete jedoch ein höheres Risiko.

Empfehlenswert ist weiterhin, die lokal auf dem Endgerät abgelegten Daten nach einer mehrfachen Falscheingabe des Zugangscodes zu löschen bzw. eine ferngesteuerte Löschfunktion auszulösen. Das Sperren und das Zurücksetzen des Geräts bzw. das Löschen der Daten werden typischerweise über das MDM- System ausgeführt, welches von der IT-Abteilung gesteuert werden kann. Über ein entsprechendes Portal kann es auch vom Mitarbeiter selbst ausgelöst werden, wenn eine entsprechende Software auf dem mobilen Gerät installiert wurde. So können per Fernsteuerung Datendiebstahl und -missbrauch verhindert werden. Darüber hinaus ist es möglich, das Gerät auf einer Landkarte zu orten, die die jeweils letzten »Aufenthaltsorte« ermittelt und anzeigt.

Sobald der IT-Abteilung der Verlust eines Endgerätes angezeigt wurde, sollte das Nutzer- bzw. Endgeräte-Zertifikat zurückgezogen[5] werden. Mitentscheidend für die Leistungsfähigkeit der gesamten BYOD-Lösung sind die Flexibilität und die Integrationsfähigkeit des Authentifizierungssystems.

3.2.4 Behandlung von Daten auf ausgedienten Endgeräten

Bei der Ausarbeitung einer BYOD-Lösung sollte von Anfang an auch die Datensicherheit am Ende der geschäftlichen Nutzungsphase berücksichtigt werden – sowohl im Fall des regulär geplanten Austausches, als auch bei einem ungeplanten Ersatz eines Gerätes oder einer Speicherkomponente (z. B. bei Defekt oder Reparatur). Im Wesentlichen sind die entstehenden Aufwendungen, die entsprechende Integration in die

5 Die CA stellt periodisch Certificate Revokation Lists (CRL) aus, die von der Authentifizierungsinstanz, typischerweise ein RADIUS-System, angefordert wird. Somit ist das RADIUS-System in der Lage, das zur Authentifizierung vorgelegte Nutzer- bzw. Endgeräte-Zertifikat gegenüber der CRL zu überprüfen. Sollte eine Übereinstimmung vorliegen, wird der Zugang zum Unternehmensnetzwerk verwehrt. Darüber hinaus kann die IT-Abteilung z. B. Unique Device Identifier (UDID), Serien- oder International Mobile Equipment Identity (IMEI) Nummern für die Autorisierung des Endgerätes auf dem Authentifizierungsserver sperren. Dies ist notwendig, damit auch in der Zeitspanne vom Zurückziehen des Zertifikats bis zur Verarbeitung der CRL der Netzwerkzugang unterbunden bzw. eingeschränkt werden kann. Das Online Certificate Status Protocol bietet, anders als die Untersuchung nach CRL, eine Überprüfung in Echtzeit.

Nutzer-/Mitarbeitervereinbarung, als auch der Prozess zur Sicherstellung der Datensicherheit am Ende der Nutzung zu berücksichtigen.

Bei BYOD-Geräten ist – abhängig vom Datenkonzept – der Ort der Datenspeicherung sowie die Trennung zwischen geschäftlichen und privaten Daten gemäß Vereinbarung der Mitarbeiter mit dem Unternehmen zu beachten (s.o.). Es ist zwischen einer kompletten oder partiellen Datenlöschung (Löschung der Firmendaten unter Beibehaltung der persönlichen Daten des Mitarbeiters) zu unterscheiden. Ein einfaches Zurücksetzen auf den Auslieferungszustand eines Gerätes stellt in vielen Fällen keine ausreichende Löschung dar. Ein komplettes Datensicherheitskonzept beleuchtet zudem weitere wichtige Aspekte wie etwa die Auswahl geeigneter (Datenlösch-) Dienstleister, die Deinstallation von Firmensoftware zur Sicherstellung von Lizenzvereinbarungen oder die Gestaltung sicherer Logistikprozesse.

3.3 Sicherheit auf dem Endgerät

In den zurückliegenden Jahren hat sich die Art, wie Mitarbeiter auf das Unternehmensnetzwerk zugreifen, stark verändert. Sie reicht vom ehemals reinen internen Zugriff über eine zunehmende Unabhängigkeit vom Standort mittels von der IT-Abteilung verwalteter Geräte bis zum geräte-, service- und standortunabhängigen Fernzugriff in einer zunehmend virtualisierten Umgebung.

3.3.1 Spam-, Malware- und Virenschutz

Alle Geräte, die Zugriff auf Unternehmensdaten bieten, sollten mit einer Sicherheitssoftware versehen sein, wenn der Anbieter der jeweiligen Plattform dieses zulässt. Hier helfen reputationsbasierte Lösungen, die die Apps eines Benutzers auf Schadcode prüfen und nur die Apps zulassen, die als unbedenklich eingestuft werden. Da Schadsoftware auch über E-Mail-Anhänge verbreitet wird, ist eine Trennung von privaten und geschäftlichen E-Mail-Konten empfehlenswert. Mitarbeiter sollten grundsätzlich in Sicherheitsthemen geschult werden und beispielsweise wachsam sein, wenn es um E-Mail-Anhänge unbekannter Absender geht.

Ein Sicherheitsproxy bzw. ein E-Mail-Gateway kann die Bedrohung durch Schadsoftware drastisch reduzieren. Er sollte zusammen mit einem Schutz vor webbasierter Malware eingesetzt werden. Sinnvollerweise erfolgt der Schutz im Netzwerk, um Geräteschutz und Produktivität zu erhöhen.

3.3.2 Nativer Betrieb und virtualisierte Umgebung

Die Datensicherheit und der Schutz vor Datenverlust stehen bei einer BYOD-Lösung im Vordergrund. Zwei Ansätze lassen sich unterscheiden: Ein nativer, nicht-virtueller Modus und der virtuelle Betrieb.

Im nativen, nicht-virtuellen Modus kommunizieren Applikationen auf dem Endgerät direkt mit den Applikationsservern im Rechenzentrum oder in der Cloud. Das heißt, Daten werden lokal auf dem Endgerät verarbeitet und auch gespeichert. Der Vorteil dieser Betriebsart liegt in der Arbeitsgeschwindigkeit der einzelnen Anwendungen und gerade bei einem limitierten Zugang zu Ressourcen wie E-Mail, Kalender, Intranet oder SaaS-Anwendungen ist dies sinnvoll. Es gibt bereits erste Systeme, welche als demilitarisierte Zone und Sicherheitsinstanz zwischen den Backend Systemen und den Anwendungen auf den Geräten arbeiten. Diese Instanz kontrolliert den Datenfluss und lediglich authentifizierte und dem MDM-System bekannte Geräte können Daten austauschen, bearbeiten und abrufen.

Im Unterschied zum nativen, nicht-virtuellen Betrieb setzt eine Virtualisierung des mobilen Endgerätes eine aktive Netzwerkverbindung voraus. Bei diesem Modell werden Programme, Anwendungen, Daten und Services zentral verwaltet. Daher liegen im virtuellen Modus die Applikationsdaten im Rechenzentrum bzw. in einer Cloud und werden von einem Virtual Desktop Infrastructure-Client (VDI) verarbeitet. Lediglich der Bildschirminhalt wird ausgetauscht und auf dem mobilen Endgerät zwischengespeichert.

Angesichts dieser Unterschiede können im Rahmen einer BYOD-Lösung durchaus beide Betriebsarten eingesetzt werden, damit die Anwender einerseits nativ auf Standard-Applikationen und virtualisiert auf Applikationen und Inhalte mit höherem Schutzbedarf zugreifen können.

Eine weitere Möglichkeit ist das sogenannte »Application Wrapping«. Hierbei werden die Apps und Dokumente auch auf einem nicht verwalteten Gerät geschützt. Bei diesem Verfahren werden die Apps und Dokumente mit einer Sicherheitsrichtlinie kombiniert. Es wird also nicht mehr das ganze Gerät- sondern nur noch die relevanten Unternehmensdaten verwaltet. App-Wrapping bietet eine sichere Authentifizierung, Datenschutz und App-Management.

Hinzu kommt das so genannte »Sandboxing«. Dabei werden auf mobilen Endgeräten bestimmte Anwendungen oder Daten in einer speziellen Laufzeitumgebung, isoliert vom Rest des Systems, bereitgestellt und verarbeitet. Der Mitarbeiter besitzt weiter die Hoheit über das Gerät und seine eigenen Daten. Damit ist eine Trennung von privaten und geschäftlichen Daten auf einem privaten Gerät möglich.

3.3.3 Verschlüsselung von Gerät und Wechselmedien

Um eine ganzheitliche Sicherheit zu erreichen, sollten alle Daten, sowohl private, als auch geschäftliche, auf einem Endgeräte verschlüsselt werden. Die Daten auf Wechselmedien sind nicht nur mit dem Endgerät selbst lesbar, sondern auch durch externe Geräte. Dies stellt somit eine Gefahr für gespeicherte Unternehmensdaten dar, sollte das Gerät verloren gehen oder gestohlen werden.

Daher ist – entsprechend dem bestehenden Sicherheitskonzept des Unternehmens – eine Verschlüsselung der Daten sowohl auf dem internen, als auch auf eingesetzten Wechselmedien empfehlenswert. Hierfür können z. B. Verfahren wie ein symmetrisches Kryptosystem, AES (Advanced Encryption Standard) mit einer Schlüssellänge von 256 Bit eingesetzt werden. Ohne Mechanismen zur Datenverschlüsselung kann das Gerät nicht für den vollumfänglichen Fernzugriff auf das Unternehmensnetzwerk eingesetzt werden.

3.4 Sicherheitslösungen für besonders sensible Bereiche

Neben der gesicherten Verbindung zwischen den BYOD-Geräten und der Unternehmens-IT ist die Sicherheit vor dem Abhören von Gesprächen zu beachten. Hier kann beispielsweise eine Ende-zu-Ende-Verschlüsselung eingesetzt werden, die es ermöglicht, die verschlüsselte Sprache beispielsweise direkt zwischen zwei Smartphones zu übertragen. Umgesetzt werden kann diese zusätzliche Sicherheitsstufe zum Beispiel durch eine Softwarelösung oder auch die Verwendung eines zusätzlichen Sicherheitsmoduls im Smartphone, einem Wechselmedium. Darüber hinaus sind auch externe Sicherheitsgeräte erhältlich, die an das Mobilgerät angekoppelt werden und die Verschlüsselung während des Gespräches vornehmen.

Kernaussagen:

- BYOD muss im Rahmen des IT-Sicherheitskonzeptes des Unternehmens behandelt und entsprechende Regelungen getroffen werden.
- Neben der Sicherheit des Endgeräts und der sicheren Ablage von Daten sowie der Trennung von privaten und beruflichen Daten stellt die sichere Verbindung des mobilen Endgeräts mit dem Unternehmensnetzwerk eine besondere Herausforderung dar.
- Die wichtigsten Sicherheitsfunktionen lassen sich bereits heute in gängigen Verwaltungssystemen wie einem Mobile Device Management abbilden. Wesentlich ist hierbei allerdings eine saubere Konfiguration, die die Sicherheitsziele des Unternehmens stringent unterstützt.

4 Lösungsansätze anhand eines Beispiels

Nachdem bislang einzelne Aspekte betrachtet wurden, soll nachfolgend am Beispiel der Außendienstmitarbeiter einer Handelsmarke die Einführung einer BYOD-Lösung für den Vertrieb veranschaulicht werden. Angefangen vom Kontakt zum Einzelhändler bis hin zum Management der Warenbestände sind Außendienstmitarbeiter vor Ort bei ihren Kunden und nutzen daher ihre Endgeräte sowohl im Firmennetz, als auch extern.

Die Kategorien Chancen und Nutzen, Kosten und Risiken für die Einführung einer BYOD-Lösung werden anhand des Geschäftsprozesses untersucht. Hierbei zeigt sich, dass gegenläufige Effekte auftreten, so dass es kein eindeutiges Für und Wider bei der Einführung von BYOD gibt. Maßgebliches Kriterium ist die Bereitschaft des Mitarbeiters. Bei der Einführungsstrategie ist daher neben einer einheitlichen Einführung auch eine partielle Einführung von BYOD denkbar welche sich nur an die Mitarbeiter richtet, die tatsächlich mitmachen wollen.

4.1 Chancen und Nutzen

Nutzen für den Mitarbeiter

Maßgeblich für die erfolgreiche Einführung einer BYOD-Lösung ist der Nutzen, den die Mitarbeiter daraus ziehen. Je größer und offensichtlicher dieser Nutzen für sie ist, desto eher sind sie bereit, das Projekt zu unterstützen.

Ein Vorteil für Mitarbeiter liegt in der deutlich größeren Wahlfreiheit hinsichtlich der nutzbaren Endgeräte. Insbesondere beliebte und medial bekannte Marken und Betriebssysteme können jetzt auch am Arbeitsplatz und nicht mehr nur in der Freizeit eingesetzt werden. Dies steigert die Motivation und erhöht die Identifikation mit dem Unternehmen: Mitarbeiter stellen letztlich ihr Gerät in den Dienst der Firma.

Gleichzeitig übernehmen Mitarbeiter mehr Verantwortung für das von ihnen genutzte Endgerät, das sie im Unterschied zu einem Firmengerät auch behalten dürfen. Der so gewonnene Elan durch die höhere Identifikation von Mitarbeitern ist insbesondere im Handel, der durch Engagement getrieben wird, von Bedeutung.

Ein Nutzen entsteht für Mitarbeiter, falls die BYOD-Geräte vom Arbeitgeber finanziell bezuschusst werden. Schließlich verringert sich durch eine BYOD-Lösung für die Mitarbeiter auch die Anzahl der mitgeführten Geräte, da das Arbeits- und das Freizeit-Gerät identisch sind. Bei Firmengeräten (auch in Form von Choose Your Own Device, CYOD, bei der der Mitarbeiter zwar das Gerät auswählen darf, es aber im Eigentum des Unternehmens verbleibt) ist dies nicht immer der Fall.

Nutzen für das Unternehmen

Auch dem Unternehmen nutzt die Einführung von BYOD, denn motiviertere Mitarbeiter arbeiten in der Regel effizienter. Zudem kann davon ausgegangen werden, dass Mitarbeiter ihre eigenen Geräte besser behandeln als Firmengeräte, so dass die Reparaturbedürftigkeit der Geräte aufgrund von weniger unachtsamen Schäden zurückgehen dürfte.

Eine offizielle Zulassung von Eigengeräten im Rahmen einer BYOD-Lösung schafft Transparenz hinsichtlich der tatsächlich eingesetzten Endgeräte und vereinfacht die Kontrolle darüber, welche Geräte von welchem Außendienstmitarbeiter eingesetzt werden. Voraussetzung dafür ist natürlich, dass ein Prozess zur Einbindung bzw. Registrierung der Endgeräte etabliert ist.

Des Weiteren ist bei Mitarbeitern mit hoher Motivation für High-End- und markenstarke Geräte auch ein Imagenutzen vorhanden, da sie so ihr Unternehmen als modern und innovativ darstellen können. Dieses kann auch gerade im Vertrieb höherwertiger Marken zur Unterstützung des eigenen Images hilfreich sein.

Ein weiterer Nutzen für den Arbeitgeber bei BYOD ist die höhere Identifikation des Mitarbeiters mit seinem Gerät. Daraus ergeben sich in vielen Fällen höhere Fertigkeiten im Umgang mit dem Gerät, was sich effizienzsteigernd auswirken kann. Ein Außendienstmitarbeiter kann sich damit ganz auf sein Kerngeschäft, die Vermittlung, konzentrieren und muss sich nicht mit für ihn fremder Hardware abmühen.

Zusätzlich spart sich das Unternehmen einen Großteil des im Zusammenhang mit den Geräten entstehenden Aufwandes für die Evaluierung von Geräten, den Einkauf, die Geltendmachung von Gewährleistungsansprüchen bei Gerätefehlern und zumindest in Teilen der Finanzierung, da diese Aspekte auf den Mitarbeiter in seiner Freizeit abgewälzt werden.

Auch die Nutzung des Wissens der Mitarbeiter um Vorzüge der Geräte ist ein Vorteil für das Unternehmen. Es muss nicht allein auf die IT-Abteilung vertrauen, die oft nicht die Anforderungen der Mitarbeiter für ihr Tagesgeschäft kennen. So kann für einen Außendienstmitarbeiter ein schnelles Booten vor Ort eine wesentliche Anforderung sein, die der IT-Abteilung gar nicht so bekannt ist.

Zu den nicht auf den ersten Blick erkennbaren Vorteilen einer BYOD-Lösung zählt weiterhin, dass sie auch die WLAN-Infrastruktur in den Zweig- sowie vor allem in den Hauptniederlassungen von Unternehmen umfasst. Eine für BYOD angepasste WLAN-Infrastruktur bringt mehr Sicherheit, Geschwindigkeit und vor allem Flexibilität am Arbeitsplatz. Selbst wenn die mobilen Endgeräte der Außendienstmitarbeiter keinen Zugriff auf schnelle Mobilfunknetze bieten sollten, kann der Datenabgleich im Büro via WLAN bequem und schnell erledigt werden.

4.2 Kosten

Ob sich gerade auch im Handel die Kosten durch die Einführung von BYOD-Geräten senken lassen, liegt keineswegs klar auf der Hand. Dies hängt von der konkreten Ausgestaltung der Einführungsstrategie ab. So ließen sich zwar die Anschaffungskosten einsparen, falls die Mitarbeiter bereit sein sollten, für die Anschaffung komplett selbst aufzukommen. Hierdurch entfällt jedoch ein wesentlicher Nutzen für den Mitarbeiter und damit sinkt auch seine Bereitschaft zu diesem Schritt. Außerdem ist zu bedenken, dass die Anschaffungskosten nur ein kleiner Teil der Gesamtkosten sind, somit ist das Einsparpotenzial ohnehin nicht sehr groß.

Somit ist in aller Regel ein finanzieller Zuschuss durch das Unternehmen bei der Einführung von BYOD unumgänglich - wohl auch in gleicher Höhe wie für firmeneigene Geräte. Dafür gewinnt das Unternehmen aber ein höherwertiges Gerät für den Einsatz der Außendienstmitarbeiter vor Ort.

Gerade der Handel mit höherwertigen Marken ist permanentem Abwanderungsdruck der Kunden ausgesetzt, wobei das Image des Unternehmens für den Erfolg elementare Bedeutung hat. Ein höherwertiges Gerät mit modernen Apps ist dabei möglicherweise sehr hilfreich. Insofern kann die Außenwirkung des Unternehmens zur Abgrenzung gegenüber Mitbewerbern verbessert werden, wenn bei den Kunden auf hochwertigere, damit aber auch teurere Geräte gesetzt wird, was ohne BYOD aber einen großen Investitionsaufwand mit sich bringen würde. Mit BYOD und großer Bereitschaft der Belegschaft, das eigene Gerät in großen Teilen mitzufinanzieren, wird hier Abhilfe für das Unternehmen geschaffen.

Bei einer hohen Motivation der Mitarbeiter für neue Geräte und durch die Eigenbeteiligung des Mitarbeiters lassen sich auch höhere Austauschzyklen erreichen als bei Firmengeräten. Somit lässt sich das Bild einer modernen Handelsmarke nachhaltig aufrechterhalten.

Allerdings entfallen mögliche Mengenrabatte, was letztlich auch die Kosten wieder erhöht, zumindest in der Summe für Mitarbeiter und Unternehmen.

Neben den Anschaffungskosten sind auch die Softwarekosten und die Supportkosten zu beachten. Die weiteren Kostenfaktoren wie Lizenzen und der Betreuung- und Wartungsaufwand wurden bereits in früheren Kapiteln ausführlich erörtert. Gerade im Handel kann, anders als in IT-nahen Branchen, nicht davon ausgegangen werden, dass die Mitarbeiter die notwendigen Kenntnisse für eine selbst durchgeführte Wartung mitbringen, trotz der höheren Begeisterung für das eigene Gerät.

Sollten einige Teile der Mitarbeiter nicht bereit sein, sich an der Finanzierung der BYOD-Geräte zu beteiligen, ist bei einer gewollten reinen BYOD-Einführung möglicherweise eine höhere bis gänzliche Bezuschussung für diese Mitarbeiter notwendig, was letztlich zu Ungerechtigkeiten für die zahlbereiten Mitarbeiter führt.

4.3 Risiken

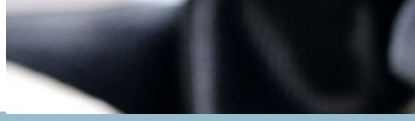
Risiko Datensicherheit

Gerade im Handel stellen sich Risiken im Hinblick auf Datensicherheit bei der Einführung von BYOD dar, da die verarbeiteten Daten für Mitbewerber einen besonderen wirtschaftlichen Nutzen darstellen würden. Insbesondere bei modernen Geräten mit intensiver Anbindung an Suchmaschinen und regem Datenaustausch sind die Geschäftsgeheimnisse wie auch personenbezogene Daten besonders zu schützen. Zur Trennung von Privat- und Geschäftsdaten gibt es bereits Standardlösungen, die schnell auch für eine BYOD-Einführungsstrategie nutzbar gemacht werden können.

Haftungsrisiko

Im obigen Kapitel zur Haftung wurde bereits dargestellt, dass der Nutzer viel leichter Schadsoftware installieren kann, auch ohne eine entsprechende Schädigungsabsicht und selbst unter Wahrung der erforderlichen Sorgfalt. Das Unternehmen kann weniger klar steuern, welche sonstigen Anwendungen der Mitarbeiter auf seinem Gerät installiert, die eventuelle Seiteneffekte auf die geschäftskritischen Anwendungen haben. Gerade bei wirtschaftlich entscheidenden Werten, wie Bestellmengen, Rabatten oder Einzelpreisen, darf sich kein Fehler einschleichen, z. B. wenn das gegenwärtige Datum durch andere Apps oder Programme abgeändert wird. Die Bedrohungslage hat sich somit geändert und entsprechende Schutzmaßnahmen sind notwendig. Ohne entsprechende Vorkehrungen durch beispielsweise eine virtualisierte Umgebung bei der Verarbeitung sensibler Daten ist somit die Wahrscheinlichkeit des Eintritts von Haftungsfällen bei BYOD-Geräten größer als bei firmeneigenen Geräten. Gerade im Falle einer Bestellung kann eine Fehlberechnung hohen wirtschaftlichen Schaden nach sich ziehen. Daneben ist auch der Imageschaden erheblich, wenn der Einzelhändler sich nicht auf die Zusammenarbeit mit dem Aussendienstmitarbeiter verlassen kann.

Zu prüfen ist, inwieweit der Mitarbeiter arbeitsvertraglich eingeschränkt werden kann. Bei einer zu großen Einschränkung ist allerdings auch der oben erwähnte Nutzen für den Arbeitnehmer fraglich, denn er hat dann nur noch formal Eigentum an seinem BYOD-Gerät, ohne eigenes Gestaltungsrecht. Die Bereitschaft des Arbeitnehmers dürfte dadurch stark sinken und die Einführung von BYOD hinfällig machen.



Risiko fehlender Bereitschaft der Mitarbeiter zu BYOD

Der erwähnte Imagevorteil und der geschilderte Nutzen kann sich bei mangelnder Bereitschaft der Mitarbeiter für High-End-Geräte ins Gegenteil verkehren und lässt das Markenunternehmen bei Verwendung von Low-End-Geräten eher als rückständig wirken als wenn es den Mitarbeitern selbst die Hardware gestellt hätte. Hier ist das Unternehmen gefordert, Wege hin zu einem Mindeststandard für BYOD-Geräte zu finden, ohne dass die Investitionsbereitschaft der Belegschaft hierfür sinkt. Außendienstmitarbeiter haben vor allem einen Vertriebsfokus. Offen ist, ob diese Mitarbeiter sich überhaupt für neueste technische Geräte interessieren wie etwa in IT-nahen Branchen und hohe Beträge investieren wollen und für die Erhaltung des erwähnten Images die Geräte auch oft durch die neuesten Geräte ersetzen möchten. Es ist durchaus denkbar, dass sie gar kein eigenes Gerät kaufen möchten. Einzukalkulieren ist, dass die Bereitschaft auch sinkt, wenn die Mitarbeiter arbeitsvertraglich zu Restriktionen verpflichtet werden wie die Installation von Apps. Wie oben erwähnt wird die Bereitschaft sinken, wenn der Mitarbeiter sich um defekte Geräte selber kümmern muss, während dieser Zeit der Vertrieb steht oder zumindest stark eingeschränkt ist.

Möglicherweise müsste in diesen Fällen das Unternehmen für diese Mitarbeiter weiterhin firmeneigene Geräte stellen, was die Einführung von BYOD dann in Frage stellt.

4.4 Einführungsstrategie, Fazit

Wie bereits erwähnt, gibt es keine eindeutigen Vor- und Nachteile, wie die Betrachtung der Bereiche Chancen, Nutzen, Kosten und Risiken gezeigt hat. Wie oben dargestellt, führt BYOD nur selten zu Kostensenkungen. Es bringt auch eine Reihe von zusätzlichen Risiken im Vergleich zu firmeneigenen Geräten mit, die zu adressieren sind. Auf der anderen Seite bringen gerade die Imagefaktoren neue Nutzen mit sich, die sich nicht ohne weiteres mit firmeneigenen Geräten erschließen lassen.

Die Bereitschaft der Mitarbeiter zu BYOD ist der entscheidende Erfolgsfaktor. Insofern ist das Unternehmen gut beraten, im Vorfeld von seinen Mitarbeitern zu erfahren, wie hoch ihre Investitionsbereitschaft für Geräte im oberen Preissegment ist. Dies hat Auswirkungen auf die Einführungsstrategie ob eine reine BYOD-IT-Landschaft eingeführt werden kann oder doch nur eine Mischform von BYOD- und für einen Teil der Belegschaft oder für besondere Geschäftsvorfälle firmeneigenen Geräten.

Kernaussagen:

- Eine Analyse zur Auswertung über die Bereitschaft der Mitarbeiter zu BYOD trägt maßgeblich zur Auswahl der richtigen Einführungsstrategie bei
- Die unternehmerische Bedrohungslage ist durch die Einführung einer BYOD Lösung neu zu bewerten, entsprechende Schutzmaßnahmen sind auch auf die Bedürfnisse der Mitarbeiter zuzuschneiden (insbesondere sollte sichergestellt werden das Mitarbeiter Ihre Arbeit effizient und »sicher« ausführen können).

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.200 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org