Mittelstand 4.0
Agentur Prozesse

LEITFADEN

Abb. © kristina rütten - Fotolia.com

Private Endgeräte geschäftlich nutzen

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Inhalt

0 Editorial....3

1 Bring Your Own Device....4

2 Wer erhofft sich was?....6

3 Anwendungsszenarien in Unternehmen....7

Smartphones....7

Tablets/Notebooks....8

Desktop-PCs....9

4 Voraussetzung für eine erfolgreiche Umsetzung....10

5 BYOD in der Praxis....11

6 Vor- und Nachteile....12

7 Zu beachtende Regeln....13

Regeln für Arbeitgeber....13

Regeln für Arbeitnehmer....14

8 Zusammenfassung und Fazit....15

9 Weiterführende Informationen & Quellen....16

10 Projektpartner und Kontaktdaten....17

Editorial

Liebe Leserinnen und Leser,

dank moderner IT-Anwendungen sind Menschen heute jederzeit und allerorts online: Ob vom Desktop zuhause, ob mit mobilen Endgeräten wie Smartphone, Tablet oder Laptop - grundsätzlich ist es möglich, bei entsprechender Bandbreite in Echtzeit elektronische Daten auch in großem Umfang abzurufen und zu bearbeiten. Ein Verzicht auf diese Anwendungen ist für Unternehmen inzwischen undenkbar, stellen sie für die Optimierung von Prozessabläufen und dien Erleichterung von Arbeitsschritten eine große Hilfestellung dar, sparen Zeit und Kosten.

Was aber ist, wenn die Geräte nicht aus Ihrem Hause sind, sondern die Mitarbeitenden ihre eigenen Geräte in den betrieblichen Alltag mit einbringen? „Bring Your Own Device“ (BYOD) lautet die Devise, nach der sich dies prinzipiell realisieren lässt. Für Sie als Unternehmer bedeutet dies aber auch, eine nicht ganz leichte Entscheidung zu fällen, ob sie dies zulassen. Wo einerseits große Chancen in der Prozessoptimierung liegen, sind anererseits (Sicherheits-)Risiken zu bedenken. Welches sind die Voraussetzungen, Anforderungen und regulatorischen Maßnahmen, unter denen Sie BYOD umsetzen können?

Wir möchten Ihnen mit dieser Broschüre konkrete Hinweise an die Hand geben, die Sie bei Ihrem Entscheidungsprozess unterstützen. Wie auch immer Ihre Entscheidung ausfallen mag - ich hoffe, die Broschüre liefert Ihnen geeignete Hilfestellungen und Anregungen. Ich wünsche Ihnen viel Freude beim Lesen!

Mit den besten Grüßen

Holger Schneider
Konsortialleiter Mittelstand 4.0-Agentur Prozesse

FTK - Forschungsinstitut für Telekommunikation und Kooperation e.V.

Bring Your Own Device

Abb. © Andy Smith – Fotolia.com

Bring Your Own Device (BYOD) kann man sinngemäß so übersetzen: „Nutze dein eigenes Gerät“. Gemeint ist damit, dass private elektronische Endgeräte für die berufliche Arbeit eingesetzt werden. Dabei geht es meist um ein Smartphone, Tablet oder auch einen Laptop. BYOD ist ein (IT-)Konzept und gibt vor, wie die Nutzung solcher Geräte im geschäftlichen Bereich zu handhaben ist. Dies betrifft beispielsweise den Umgang mit unternehmensinternen Daten. Darunter fallen E-Mails und kundenspezifische Informationen, aber auch der Zugriff privater Endgeräte auf das Firmennetzwerk.

Die Arbeitswelt lässt sich schon lange nicht mehr in ein privates und berufliches Umfeld einteilen. Arbeitnehmer erledigen Geschäftliches zu Hause und persönliche Angelegenheiten am Firmenrechner. Der BYOD-Trend weicht diese Grenzen weiter auf. Mitarbeiter wollen zusätzlich private elektronische Endgeräte im geschäftlichen Umfeld nutzen. VMware und das Marktforschungsinstitut Vanson Bourne fanden heraus, dass 80% der IT-Verantwortlichen BYOD unterstützen oder in nächster Zeit unterstützen wollen.

Dieser Leitfaden zeigt auf,

- was sich Arbeitgeber und Arbeitnehmer von BYOD versprechen,
- welche unterschiedlichen Anwendungsszenarien vorstellbar sind,
- welche rechtlichen und technischen Herausforderungen zu bedenken sind,
- welche Vorteile und Nachteile mit BYOD einhergehen,
- welche Regeln Arbeitgeber und Arbeitnehmer beachten müssen.

Viele deutsche Unternehmen greifen Mitarbeitern bereits dabei unter die Arme, private Endgeräte im geschäftlichen Rahmen zu nutzen. Dies geschieht teilweise durch klare Vorgaben, aber auch durch finanzielle Anreize. Sie erhoffen sich dadurch unter anderem eine höhere Mitarbeiterzufriedenheit und Effizienzsteigerungen ihrer Arbeitnehmer. Andere wollen als moderner Arbeitgeber auftreten und somit attraktiver für Nachwuchskräfte werden.

Gegner von BYOD führen jedoch häufig erhöhte Anforderungen an Wartung, Sicherheit und Datenschutz sowie eine komplexere Administration als Gründe an, diesen Trend nicht zu unterstützen. In der Tat dürfen diese Aspekte von den Verantwortlichen nicht unterschätzt werden.

Auch unter Mitarbeitern gibt es Bedenken. Jeder Vierte ist laut einer Studie des IT-Dienstleisters CSC aktuell mit dem Einsatz standardisierter Firmenendgeräte nicht zufrieden, knapp 40 Prozent beklagen Mängel bei der Nutzung von privaten Endgeräten.

Jedoch geben 61 % der befragten Arbeitnehmer in einer Studie von MobileIron 2015 an, dass das Vertrauen durch Maßnahmen des Arbeitgebers gestärkt werden kann.

Eine wichtige Voraussetzung für die sinnvolle gemeinsame Nutzung privater Endgeräte im geschäftlichen Bereich ist deshalb die Einführung einer BYOD-Organisationsrichtlinie, um Vertrauen zwischen Arbeitgeber und Arbeitnehmer aufzubauen. Gängige Vorurteile und Ängste werden so aus dem Weg geräumt und eine sachliche Diskussion mit den Arbeitnehmern kann angestoßen werden. Auch für die Unternehmen sind solche Vorgaben eine wesentliche Hilfe, damit keine parallele Schatten-IT entsteht.

INFOBOX

Endgeräte in Firmenbesitz sind immer noch weit verbreitet

Noch entscheiden sich Arbeitgeber oft für das vorherrschende Modell: Das Unternehmen kauft die Endgeräte und stellt sie dem Arbeitnehmer zur Verfügung, sie bleiben jedoch Firmeneigentum. Der Arbeitgeber erlaubt dem Arbeitnehmer bei diesem Konzept die private Nutzung des Endgeräts unter seinen Bedingungen. Somit ist eine umfassende Kontrolle über das Endgerät und die darauf befindlichen Daten gewährleistet.

Im Zusammenhang mit dem Begriff BYOD wird dies auch unter folgenden Bezeichnungen diskutiert: CYOD („Choose Your Own Device“) bzw. COPE („Corporate Owned Personally Enabled“). Danach werden Geräte für die Angestellten angeschafft, die Angestellten können aber selbst wählen, mit welchem Modell sie arbeiten möchten.

PUOCE („Private Use Of Company Equipment“). Hier stellt nicht der Mitarbeiter, sondern das Unternehmen die Geräte, der Mitarbeiter darf dieses Gerät auch privat nutzen – allerdings unter von der Firma definierten Rahmenbedingungen.

Schatten-IT bezeichnet IT-Systeme und IT-Prozesse, die neben der offiziellen IT-Infrastruktur betrieben werden. Sie werden nicht von IT-Verantwortlichen verwaltet, sondern in der Regel inoffiziell von den Mitarbeitern eines Unternehmens. Dies kann zu sicherheitstechnischen und rechtlichen Problemen führen.

Wer erhofft sich was?

Mehr Komfort für die Mitarbeiter

Mitarbeiter erhoffen sich durch BYOD mehr Freiheit in ihrer Arbeitsorganisation. Sie können eigene elektronische Endgeräte und Programme nutzen und werden teilweise durch den Arbeitgeber finanziell beim Kauf eines Endgerätes unterstützt. Gerade in Verbindung mit dem großen Thema Home-Office, das Arbeiten von zu Hause aus, kann das Nutzen von privaten Endgeräten eine erhebliche Erleichterung versprechen. Auch entfällt gerade bei Außendienstmitarbeitern das Mitführen von mehreren Geräten, weil Handy, Laptop oder andere elektronische Endgeräte sowohl dienstlich als auch privat genutzt werden können. Des Weiteren wollen Mitarbeiter ihre privaten Anwendungen (Apps) auch im geschäftlichen Kontext anwenden und natürlich gewohnte Endgeräte verwenden, da sie mit deren Handhabung vertraut sind.

Mehr Effizienz für den Arbeitgeber

Der Arbeitgeber erhofft sich eine höhere Mitarbeiterzufriedenheit, Effizienzsteigerung und das Image eines modernen Arbeitgebers. Des Weiteren geht er davon aus, dass die Anschaffung von IT-Infrastruktur wie Smartphones oder Laptops teilweise oder ganz auf den Mitarbeiter verlagert werden kann. Dadurch spart das Unternehmen Kosten und Zeit. Aber auch andere Kostenaufteilungen sind möglich. Arbeitnehmer sind somit selbst für ihre Arbeitsendgeräte zuständig und treiben die Modernisierung des Unternehmens voran. Weiterhin gehen Mitarbeiter mit eigenen Endgeräten potenziell sorgsamer um, so die Einschätzung der Arbeitgeber. Auch erwarten Arbeitgeber von der Einführung von BYOD eine effizientere Bedürfnisbefriedigung der Kunden und somit auf lange Sicht zufriedenere Kunden.

Anwendungsszenarien in Unternehmen

BYOD umfasst alle elektronischen Endgeräte, die eine direkte Interaktion mit dem Nutzer ermöglichen. Dies kann ein Smartphone, Tablet, Laptop oder der Desktop-PC sein. In der unternehmerischen Praxis ist es nicht ratsam, alle diese Geräte durch Arbeitnehmer auswählen und „mitbringen“ zu lassen. Vielmehr ist es für ein Unternehmen sinnvoll, zusammen mit den Mitarbeitern die primären Anwendungsszenarien für BYOD zu definieren. Dann entscheiden beide Parteien, welche Endgeräte in einer BYOD-Richtlinie berücksichtigt werden und welche nicht. Das Ausschließen bestimmter Endgeräte aus der BYOD-Richtlinie reduziert die Komplexität. Zudem erhöht es die Kontrolle über die eingesetzten IT-Geräte.

Das Smartphone reicht völlig aus, wenn Mitarbeiter Nachrichten, z.B. E-Mails, checken oder Kalendereinträge einsehen sollen. Auch oberflächliche Recherchen, das Verwenden von kleinen Anwendungen (Apps) und der Zugriff auf Firmenkontaktdaten sind damit unkompliziert möglich.

Das Unternehmen muss dafür sorgen, dass ein sicherer Zugang und eine verschlüsselte Datenübertragung in das Firmennetzwerk zur Verfügung stehen. Wenn Daten nur konsumiert und nicht auf dem Endgerät gespeichert werden, ist das Sicherheitsrisiko begrenzt.

Als Unternehmen stellen Sie sich folgenden Fragen:

- Welche Anwendungsszenarien gibt es?
- Sollen sensible Daten zum Zugriff freigegeben werden und wenn ja, welche?
- Kann das Endgerät selbst abgesichert werden?
- Lässt sich das Gerät in eine vorhandene IT-Infrastruktur und ein bestehendes Sicherheitskonzept einbinden?
- Was wollen die Arbeitnehmer und was erhoffen sie sich von BYOD?

Wann macht es Sinn, Smartphones in eine BYOD-Richtlinie aufzunehmen?

Beim Zugriff auf Nachrichten aus dem Firmennetzwerk, E-Mails, Kalender und Kontakte, die Verwendung kleinerer Tools und für oberflächliche, schnelle Recherchen.

© Antonioguillem – Fotolia.com

Wann macht es Sinn, zusätzlich zu Smartphones auch Tablets / Notebooks in einer BYOD-Richtlinie zu berücksichtigen?

Wenn neben den oben genannten Gründen ein erweiterter Zugriff auf Firmendaten inkl. Bearbeitung stattfinden soll.

Ihre Mitarbeiter wollen zum Beispiel nicht nur von unterwegs E-Mails, Nachrichten oder Kalendereinträge einsehen, sondern darüber hinaus auf umfangreichere Daten aus dem Unternehmensnetzwerk zugreifen. Hier empfiehlt sich die Nutzung eines Tablets oder Notebooks.

Auf Geräten mit größerem Bildschirm und höherer Auflösung lässt es sich außerdem besser arbeiten, Tastatur und ggf. eine Maus sind bei einer umfangreichen Bearbeitung von Dateien komfortabler. Es sollte definiert werden, was genau mit dem Endgerät getan werden soll. Tablets haben gegenüber dem Notebook den Vorteil, dass der Akku mehrere Tage hält und auch bei Dauernutzung einen vollen Arbeitstag zur Verfügung steht. Sie eignen sich vor allem dann, wenn man hauptsächlich Daten anzeigen und schnell einen Bearbeitungsstatus einsehen will. Benutzerfreundlichkeit, geringes Gewicht und wenig Platzbedarf sind hier weitere Vorteile.

Soll der Zugriff und die Bearbeitung umfangreicher Daten ermöglicht werden, empfiehlt sich die Nutzung eines Notebooks. Der größere Bildschirm, die vollwertige Tastatur und eine externe Maus ermöglichen professionelles und rasches Arbeiten. Sogenannte Ultrabooks sind leistungsfähige Laptops, die kaum mehr als 1000 Gramm wiegen.

In diesem Szenario ist ein sicherer Zugang zum Unternehmensnetzwerk und die Verschlüsselung der zu übertragenden Daten erforderlich. Zusätzlich sollte ein Sicherheitskonzept regeln, wie gespeicherte Unternehmensdaten auf den Endgeräten vor unbefugtem Zugriff geschützt werden. Des Weiteren ist die mögliche Vermischung privater und geschäftlicher Daten ein wichtiges Thema. Durch konsequent getrennte Speicherplätze für private und geschäftliche Daten können Arbeitgeber und Arbeitnehmer eine Vermischung der Daten vermeiden. Dadurch wird die Privatsphäre des Mitarbeiters respektiert und der Arbeitgeber hat maximale Kontrolle über geschäftliche Daten. Ein möglicher Weg, diese Datentrennung zu erreichen, ist die Containerization.

INFOBOX

Schützen Sie Ihre Daten auf mobilen Endgeräten und bei der Übertragung

Mobile Betriebssysteme bringen bereits Verschlüsselungsfunktionen mit. Für einen umfassenden Schutz reichen sie jedoch nicht aus, denn oft werden externe Speicher wie die SD-Karte nicht berücksichtigt. Hier helfen Verschlüsselungs-Apps weiter, die Dateien, Verzeichnisse und Apps auf allen Speichermedien des Smartphones verschlüsseln.

Des Weiteren benötigen Sie bei der Übertragung von sensiblen Daten weitere Schutzmaßnahmen wie eine Virtual Private Network (VPN)-Verbindung in das eigene Netzwerk. Auch das lässt sich durch zusätzliche Apps und Programme realisieren.

Weitere Informationen dazu finden Sie im Leitfaden:

- Smartphones absichern - Informationen über die Sicherheit von Smartphones und anderen mobilen Endgeräten (siehe Downloadlink im Literaturverzeichnis)

Abb. © everythingpossible – Fotolia.com

Wann macht es Sinn, zusätzlich zu Smartphones, Tablets und Notebooks auch Desktop-PCs in einer BYOD-Richtlinie zu berücksichtigen?

Dieses Szenario macht Sinn, wenn der Zugriff auf das Unternehmensnetzwerk und auf Daten über das Home-Office stattfindet.

Arbeitet ein Mitarbeiter zum großen Teil von zu Hause aus, macht es Sinn, den privaten Desktop-PC zu nutzen. Dadurch steigt die Benutzerfreundlichkeit stark an. Mittlerweile sind die Bildschirme im Privathaushalt vernünftig groß und meist sind auch eine gute komfortable Maus und Tastatur vorhanden. Des Weiteren kann jeder Arbeitnehmer am Desktop-PC seiner Wahl arbeiten: ob Windows-, MAC- oder Linux-Rechner spielt in der Regel keine Rolle mehr.

Auch hier müssen Zugang und Datenübertragung gesichert und verschlüsselt werden. Ebenso muss der Zugriff auf das Unternehmensnetzwerk geregelt werden und gespeicherte Daten sind ausreichend zu schützen. Unterschiedliche Benutzerkonten auf dem Desktop-PC ermöglichen die Trennung der Daten und der privaten bzw. betrieblichen Software. Somit können viele Probleme umgangen bzw. minimiert werden.

Abb. © photon_photo – Fotolia.com

Voraussetzungen für eine erfolgreiche Umsetzung

Den schon genannten Vorteilen und Chancen für Unternehmen und Mitarbeiter stehen auch Risiken und Nachteile gegenüber. Diese können durch das konsequente Anwenden einer gut ausgearbeiteten BYOD-Richtlinie vermieden oder zumindest abgeschwächt werden. Des Weiteren hilft es kleinen Unternehmen, den Umfang von BYOD auf bestimmte Mitarbeiter, bestimmte Gerätetypen und/oder bestimmte Anwendungsszenarien einzuschränken.

Im Einzelnen lassen sich folgende Anforderungen für eine sichere und erfolgreiche Umsetzung von BYOD für Unternehmen und für Mitarbeiter identifizieren.

Der Arbeitgeber muss besonders Rücksicht auf den Datenschutz und die Datensicherheit nehmen und konkrete Vorgaben machen, um gesetzliche Anforderungen einhalten zu können. Des Weiteren müssen personal- und arbeitsrechtliche sowie lizenz- und steuerrechtliche Anforderungen bzw. Risiken beachtet werden.

Wie stark diese Risiken ausgeprägt sind, hängt vom Umfang bzw. dem Anwendungsszenario von BYOD im Unternehmen ab.

Der Arbeitnehmer muss geschult werden und lernen, Verantwortung zu übernehmen. Dies umfasst die Einhaltung datenschutzrechtlicher Bestimmungen, sicherheitstechnischer Aspekte und generelle Sorgfalt im Umgang mit den mobilen Endgeräten und den darauf gespeicherten geschäftlichen Daten.

Durch das Ermitteln klar umrissener Anwendungsfelder für das Konzept BYOD können Risiken effektiv umgangen werden.

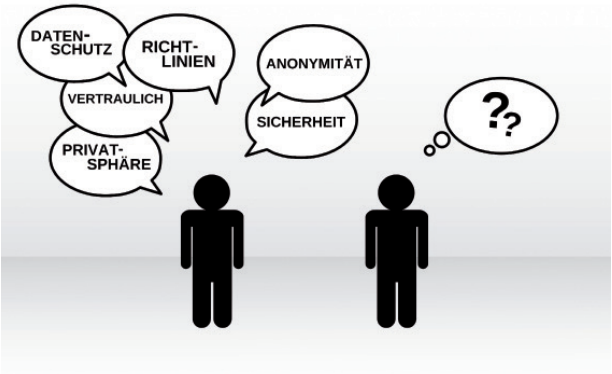


Abb. © buyman - Fotolia.com

Worauf speziell KMU bei BYOD achten sollten:

1. Datenschutz
   Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten kommt das Bundesdatenschutzgesetz (BDSG) zur Anwendung. Darüber hinaus müssen weitere Vorgaben wie das Telekommunikationsgesetz (TKG) beachtet werden.

2. Datensicherheit
   Das Aufweichen der Grenze zwischen privater und dienstlicher Nutzung eines Endgeräts erhöht die Anforderungen an die Datensicherheit, auch im privaten Umfeld.

3. Softwarelizenzen
   Die private und betriebliche Nutzung von Software muss klar geregelt sein und durch entsprechende Softwarelizenzen abgedeckt werden.

4. Steuerrechtliche Aspekte
   Steuerrechtliche Aspekte beim BYOD-Konzept sollten mit einem Steuerberater erörtert werden.

5. Arbeitsrechtliche Aspekte
   Es müssen klare Regelungen bzw. Richtlinien erarbeitet werden, die arbeitsrechtliche Fragen klären und z.B. Kostentransparenz schaffen.

BYOD-Anforderungen in der Praxis

Anforderungen an einem Beispiel

Ein Unternehmen mit zehn Mitarbeitern möchte dienstliche Mobiltelefone durch das BYOD-Konzept ersetzen. Der Firmeninhaber hat folgendes Anwendungsszenario ermittelt:

- Die Mitarbeiter sollen auf ihren privaten mobilen Endgeräten dienstliche E-Mails abrufen und dienstlich telefonieren können.
- Es sollen keine betrieblichen Daten (außer Telefon- und E-Mail-Kontakte) auf dem mobilen Endgerät gespeichert oder weiterverarbeitet werden.
- Auch soll kein Zugriff auf das Firmennetzwerk stattfinden.
- Die private Nutzung des Endgeräts ist ganz normal möglich.
- Die Kosten des Mobilfunkvertrages werden von dem Unternehmen übernommen.

Datenschutz und Datensicherheit

Das Datenschutzrisiko wird minimiert durch Beschränkung auf E-Mails und Telefonkontakte. Diese beiden Funktionen bzw. die zugehörigen Apps werden jeweils vor fremdem Zugriff mit einem Passwort geschützt. So kann sichergestellt werden, dass keine unbefugte Person (un-)bewusst auf diese beiden sensiblen Anwendungen Zugriff erlangen kann. Des Weiteren besteht kein Risiko des Datenverlustes, da keine Daten auf dem Telefon selbst gespeichert werden. Die Mitarbeiter des Unternehmens haben sich per Unterschrift verpflichtet, mit dem mobilen Endgerät sorgfältig umzugehen und Sicherheitseinstellungen wie die Pin-Eingabe zur Entsperrung zu aktivieren.

Softwarelizenzen

Da nicht aktiv auf dem Endgerät gearbeitet wird, sondern nur E-Mails abgerufen und Telefonate geführt werden, beschränkt sich die Software auf eine Sicherheitslösung in Form einer Anti-Virus-Software und gegebenenfalls auf eine professionelle E-Mail-App. Durch diesen simplen Ansatz ist sichergestellt, dass das Unternehmen keine Unterlizenzierung aufweist.

Arbeitsrechtliche Aspekte

Der Firmeninhaber hat eine klare BYOD-Organisationsrichtlinie ausgearbeitet, in der alle Aspekte berücksichtigt werden. Hierzu gehören zum Beispiel Sicherheitsrichtlinien und eine klare Kostenverteilung. Es muss auch geregelt werden, wer bei Verlust des Gerätes haftet und wer welche Reparaturen bezahlen muss. Die Mitarbeiter müssen diese detaillierte Richtlinie akzeptieren und unterschreiben, um BYOD anwenden zu können. Eine BYOD-Richtlinie schafft Klarheit, wer wann was wie verantwortet. Sie dient als Wegweiser für Firmeninhaber und Mitarbeiter.

Steuerrechtliche Aspekte

In Zusammenarbeit mit dem Steuerberater wird eine Lösung erarbeitet und auf alle Mitarbeiter angewendet. Es werden keine so genannten Insellösungen bzw. Einzelfälle akzeptiert, damit der Einsatz von BYOD nicht zu komplex wird. Steuerrechtliche Aspekte sind z.B. die korrekte Erfassung anfallender Kosten als Betriebsausgaben des Unternehmens sowie die Abzugsfähigkeit anfallender Kosten für den Mitarbeiter im Rahmen der Einkommensteuer bzw. die Berücksichtigung geldwerter Vorteile bei der Kostenübernahme durch das Unternehmen.

Abb. © pico - Fotolia.com

Vor- und Nachteile

Die Fakten von BYOD sind in den vorherigen Kapiteln erklärt worden. Die Vor- und Nachteile aus Arbeitgebersicht kann man folgendermaßen zusammenfassen:

Arbeitgeber	Arbeitnehmer
Vorteile ► Anschaffungskosten für Endgeräte sinken ► Mitarbeiterzufriedenheit erhöht sich ► Mitarbeiterproduktivität steigt ► Arbeitgeberattraktivität steigt ► Effiziente Befriedigung der Kundenbedürfnisse ► Mitarbeiter gehen sorgsamer mit den Endgeräten um	**Vorteile** ► Flexibleres Arbeiten möglich ► Höhere Motivation ► Mehr Spaß am Job ► Innovationsfähigkeit steigt durch Nutzung bevorzugter Technik und Technologie ► Moderne Endgeräte fördern die Kommunikation
Nachteile ► Erstellen umfangreicher Regelwerke erforderlich ► Evtl. unzureichende Kontrolle über Endgeräte und geschäftliche Daten ► Evtl. mehr technische Probleme ► Rechtliche Risiken aufgrund teils unsicherer Rechtslage ► Tatsächliche Auswirkungen auf das Unternehmen und den Arbeitnehmer lassen sich vorher nur schlecht abschätzen ► Evtl. zeit- und kostenintensivere Verwaltung mobiler Endgeräte	**Nachteile** ► Endgerät gehört dem Arbeitnehmer, steht aber nicht völlig unter seiner Kontrolle ► Kosten für Anschaffung und Wartung des Endgeräts ► Umfangreiche Regularien und Richtlinien müssen beachtet werden ► Evtl. Installation zusätzlicher Software erforderlich, um den Richtlinien zu entsprechen ► Möglicher Zugriff auf private Daten durch das Unternehmen

Wichtige Regeln

Eine Schritt-für-Schritt-Anleitung für „Das richtige BYOD“ wird man nicht finden, da es immer auf den Einzelfall ankommt. „Deutschland sicher im Netz e.V.“ hat aber 8 allgemeingültige Regeln für Arbeitgeber und Arbeitnehmer identifiziert, die als Fundament dienen können. Darauf kann das Unternehmen aufbauen und spezifische Regeln und Richtlinien ableiten. Der Aufwand hängt maßgeblich vom Umfang des BYOD-Konzepts ab und kann bei kleinen und mittleren Unternehmen durchaus geringer sein.

Regeln für Arbeitgeber

1. Ziele definieren, die mit BYOD erreicht werden sollen

Ausarbeitung einer klaren Strategie, was mit BYOD erreicht werden soll. Ziele können sein:

- Mitarbeiterzufriedenheit erhöhen
- Effizienz steigern
- Arbeitgeberattraktivität steigern
- Unternehmensnetzwerk für orts- und zeitunabhängige Zugriffe öffnen
- Sicherheit durch einheitliche Regelungen erhöhen

2. Risiken bewerten, die für das Unternehmen entstehen können

Analyse aller potenziellen Risiken und Herausforderungen. Der Fokus liegt dabei auf rechtlichen und technischen Anforderungen in Bezug auf:

- Komplexität
- Datenschutz
- Datensicherheit
- Arbeitsrecht
- Lizenzrecht
- Steuerrecht

3. Transparenz durch klare Richtlinien schaffen

Mitarbeiter müssen die Einhaltung und Umsetzung der erforderlichen Maßnahmen schriftlich bestätigen. Darunter fallen auch haftungsrelevante Regelungen sowie die Festlegung der Kostenübernahme für die Anschaffung und Wartung von privaten Endgeräten.

4. Technische Voraussetzungen schaffen

Zur Nutzung von BYOD muss ein Betriebskonzept ausgearbeitet werden. Dieses Konzept klärt technische Sicherheitsmaßnahmen, den Umfang der Nutzung privater Endgeräte und Voraussetzungen für Mitarbeiter, um sich an BYOD zu beteiligen. Des Weiteren soll dieses Konzept sicherstellen, dass Unternehmensanforderungen bezüglich Sicherheit und Verwaltbarkeit eingehalten werden.

5. Organisatorische Voraussetzungen schaffen

Organisatorisch müssen von der Zulassung einzelner Endgeräte bis zum Ausscheiden eines Mitarbeiters alle relevanten Prozesse definiert werden.

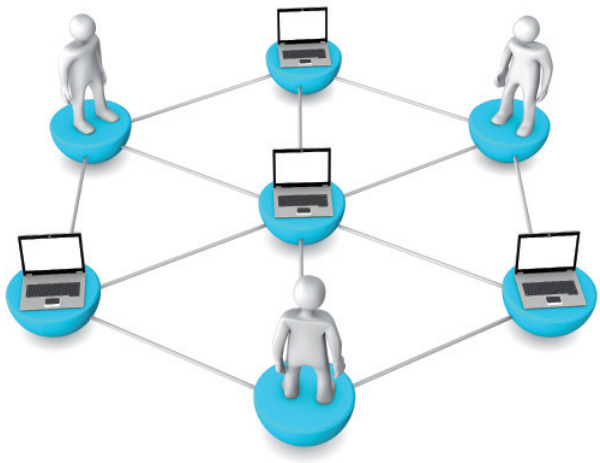


Abb. © style-photography.de - Fotolia.com

Regeln für den Arbeitnehmer

1. Verantwortung übernehmen

Der Arbeitnehmer muss im Umgang mit Unternehmensdaten auf privaten Endgeräten geschult werden. Er muss für die Verantwortung sensibilisiert werden, die unterschriebenen Richtlinien und Vereinbarungen einzuhalten. Einzelne Aspekte dieser Verantwortung sind:

- Der Zugriff auf Unternehmensdaten muss entsprechend der Unternehmensregeln geschützt werden.
- Software muss aktuell gehalten werden.
- Endgeräte dürfen nicht an Dritte weitergegeben werden.
- Vorgaben des Geräteherstellers müssen eingehalten werden (keine Jailbreaks …).
- Private Daten müssen von den geschäftlichen Daten getrennt werden.
- Lizenzvereinbarungen für verwendete Software müssen eingehalten werden.

2. Für Sicherheit sorgen

Es muss ein aktuelles Virenschutzprogramm installiert sein. Des Weiteren sind Schutzmechanismen wie das Verschlüsseln und das Löschen von Daten nach mehrmaligem misslungenem Anmelden zu aktivieren. Auch sollte im Fall von Verlust oder Diebstahl des Endgerätes die Löschung der Daten über das Internet möglich sein.

3. Vereinbarungen akzeptieren

Die berufliche Nutzung von privaten Endgeräten muss mit dem Vorgesetzten abgesprochen werden. Dies erlaubt die richtige Integration des Endgerätes in das BYOD-Betriebskonzept und somit eine erhöhte Sicherheit für Arbeitnehmer und Arbeitgeber. Arbeitnehmer müssen sich bei unklaren Verhältnissen, die nicht durch Vereinbarungen geregelt sind, an den Vorgesetzten wenden.

Jailbreak kommt aus dem Englischen und bedeutet wörtlich „Gefängnisausbruch“. Hier bedeutet es die Umgehung von Nutzungsbeschränkungen auf elektronischen Endgeräten, um Funktionen freizuschalten, die vom Hersteller gesperrt sind. Der Begriff stammt aus der Apple-Welt und ist auf deren strikte Beschränkung ihrer Geräte auf eigene Software aus dem Apple-Store zurückzuführen. Dieser Begriff wird nur für manipulierte Endgeräte mit dem Betriebssystem iOS verwendet.

Rooten (Root-Rechte erlangen) ist dasselbe wie Jailbreak, bezieht sich aber auf Nicht-Apple-Geräte wie Smartphones mit dem mobilen Betriebssystem Android.

Abb. © deagreez – Fotolia.com

Abb. © iceteastock – Fotolia.com

Zusammenfassung und Fazit

BYOD ist speziell in Deutschland mit vielen rechtlichen und technischen Herausforderungen verbunden. Die Rechtslage ist in einigen Bereichen noch unklar. Inwieweit sich BYOD nachteilig für den Arbeitgeber auswirken könnte, hängt maßgeblich vom Umfang der praktizierbaren Kontrolle über das Endgerät und von der Art des privaten Endgeräts ab (Smartphone, Tablet, Notebook oder Desktop-PC).

BYOD bietet Vorteile für Arbeitgeber wie höhere Mitarbeiterzufriedenheit und Mitarbeiterproduktivität, aber auch Herausforderungen wie Datenschutz, Datensicherheit, Lizenz-, arbeitsundsteuerrechtliche Anforderungen. Der Arbeitnehmer wiederum profitiert von mehr Flexibilität und Freiheiten, muss sich aber an den Kosten beteiligen und zum Teil umfangreiche Regeln einhalten.

Wenn sich ein Arbeitgeber gegen BYOD entscheidet, kann er sich dem Druck zur Integration von mobilen Endgeräten mitunter trotzdem nicht entziehen. Ein Kompromiss ist jedoch möglich, denn BYOD muss nicht immer alle Möglichkeiten ausschöpfen, sondern kann sich auf wenige Funktionen und Endgeräte-Typen beschränken wie zum Beispiel E-Mail-Abruf, Kalenderfunktionen oder Abruf von Informationen zu einem bestimmten Auftrag via Smartphone und Tablet. Dies vermindert die Komplexität erheblich und organisatorische Probleme entstehen unter Umständen erst gar nicht.

Ein überschaubares Anwendungsspektrum macht auf jeden Fall den Einstieg leichter.

Für kleine Unternehmen macht es durchaus Sinn, den Arbeitnehmern private Endgeräte am Arbeitsplatz zu erlauben, denn Funktionen wie E-Mail-Abruf oder Kalendersynchronisation sind einfach umzusetzen. Rechtliche und technische Herausforderungen bleiben auf einem beherrschbaren Niveau. Des Weiteren verursacht die Verwaltung der privaten Endgeräte hier weniger Aufwand durch die geringere Vielfalt im Vergleich zu großen Unternehmen. Unterstützt durch grundlegende Vorgaben bzw. Richtlinien ist BYOD ein erfolgsversprechendes Konzept.

INFOBOX

Im Zuge von BYOD werden Konzepte zur Verwaltung mobiler Endgeräte immer wichtiger

Eine Lösung für die auftretende Komplexität ist eine Mobile Device Management Software (MDM). Die MDM Software unterstützt Sie als Verantwortlichen, die aufkommende Vielfalt an mobilen Endgeräten (sowohl private als auch firmeneigene) zu managen und optimal zu nutzen.

Ein zweiter Ansatz zur Gewährleistung der Sicherheit ist das Konzept Containerization.

Weiterführende Informationen

Mobile Endgeräte absichern

Leitfaden
Smartphones absichern - Informationen über die Sicherheit von Smartphones
https://www.mittelstand-digital.de/ im Wissenspool unter dem Schlagwort IT-Sicherheit für KMU

Sicher im Internet unterwegs

Deutschland sicher im Netz e.V.
https://www.sicher-im-netz.de/

Mobile Device Management

http://www.computerwoche.de/schwerpunkt/Mobile%20Device%20Management

Quellen

VMware & Vanson Bourne

http://www.vmware.com/de/company/news/releases/vmw-mobile-rebellen-20130529.html

Aruba Networks

http://www.arubanetworks.com/pdf/solutions/EB_mdmreport.pdf

MobileIron

http://www.mobileiron.com/de/whitepaper/mobiles-arbeiten-ist-vertrauenssache

Projektpartner und Kontaktdaten

Über die Mittelstand 4.0-Agentur Prozesse

Im Rahmen der Förderinitiative „Mittelstand 4.0-Digitale Produktions- und Arbeitsprozesse“ des Bundesministeriums für Wirtschaft und Energie wird die Mittelstand 4.0-Agentur Prozesse unterstützt. Ziel dieser Agentur ist es, die Wettbewerbsfähigkeit der Unternehmen zu stärken und neue Geschäftsfelder im Kontext einer zunehmenden Digitalisierung im Themenspektrum Prozesse, Prozessmanagement und Ressourcen zu erschließen.

Der Auftrag an die Agentur besteht in der Schulung bzw. Qualifizierung von Multiplikatoren zu Fragen des Einsatzes von digitalem Prozessund Ressourcenmanagement und damit eng verbunden in der fachgerechten Information für Mittelstands- und Handwerksunternehmen.

Fachliches Know-how wird dazu unternehmensorientiert anhand von Beispielprozessen aufbereitet, weiterentwickelt und mittelstandgerecht vermittelt. Fragestellungen in Unternehmen von der Geschäftsführungsebene bis zum Hallenboden werden fachkundig und allgemeinverständlich beantwortet.

Weitere Informationen finden Sie unter
www.prozesse-mittelstand.digital

Ansprechpartner für das Projekt:

Holger Schneider
FTK – Forschungsinstitut für Telekommunikation und Kooperation e.V.
Martin-Schmeißer-Weg 4
44227 Dortmund
Fon: +49 (0)231. 97 50 56 21
E-Mail: hschneider@ftk.de

Ansprechpartner Öffentlichkeitsarbeit:

Roland Hallau
tti Technologietransfer und Innovationsförderung Magdeburg GmbH
Bruno-Wille-Straße 9
39108 Magdeburg
Fon: +49 (0)391. 74 43 52 4
E-Mail: rhallau@tti-md.de

Partner der Mittelstand 4.0- Agentur Prozesse

FTK – Forschungsinstitut für Telekommunikation und Kooperation e.V.
www.ftk.de

FTK Forschungsinstitut für Telekommunikation und Kooperation

tti Technologie und Innovationsförderung Magdeburg GmbH
www.tti-magdeburg.de

tti TECHNOLOGIETRANSFER UND INNOVATIONSFÖRDERUNG MAGDEBURG GmbH

Industrie und Handelskammer Chemnitz
www.chemnitz.ihk24.de

IHK Industrie- und Handelskammer Chemnitz

Technische Universität Chemnitz
Professur Fabrikplanung und Fabrikbetrieb
www.tu-chemnitz.de/mb/FabrPlan

TECHNISCHE UNIVERSITÄT CHEMNITZ

Impressum

Verleger:

FTK Forschungsinstitut für Telekommunikation und Kooperation e.V.
Martin-Schmeißer-Weg 4
44227 Dortmund
Telefon: 0231 975056-0
Telefax: 0231 975056-10
E-Mail: info@ftk.de
Web: www.ftk.de

Vertretungsberechtigter Vorstand:
Prof. Dr. Dominic Heutelbeck

Umsatzsteuer-Identifikationsnummer gem. §27a USTG: DE153303875

Vereinsregister: Amtsgericht Dortmund
Registernummer: VR 4128

Soweit keine redaktionelle Kennzeichnung für den Inhalt Verantwortlicher gem. §§ 5 TMG, 55 Abs. 2 RStV:
Holger Schneider
Martin-Schmeißer-Weg 4
44227 Dortmund

Text und Redaktion:

Holger Schneider, FTK e.V.

auf der Basis einer Broschüre des
eBusiness-Lotsen Oberschwaben-Ulm
c/o Hochschule Ravensburg-Weingarten
Lazarettstraße 1, 88250 Weingarten
Redaktion: Prof. Dr. Werner Höpken,
Autor: Arne Winterfeldt

Gestaltung und Produktion:

LP Concept UG (haftungsbeschränkt)
Brunnenstraße 11
45128 Essen

Vertreten durch:
Marius Gasse,
Michael Dabrowski

Bildquellen:

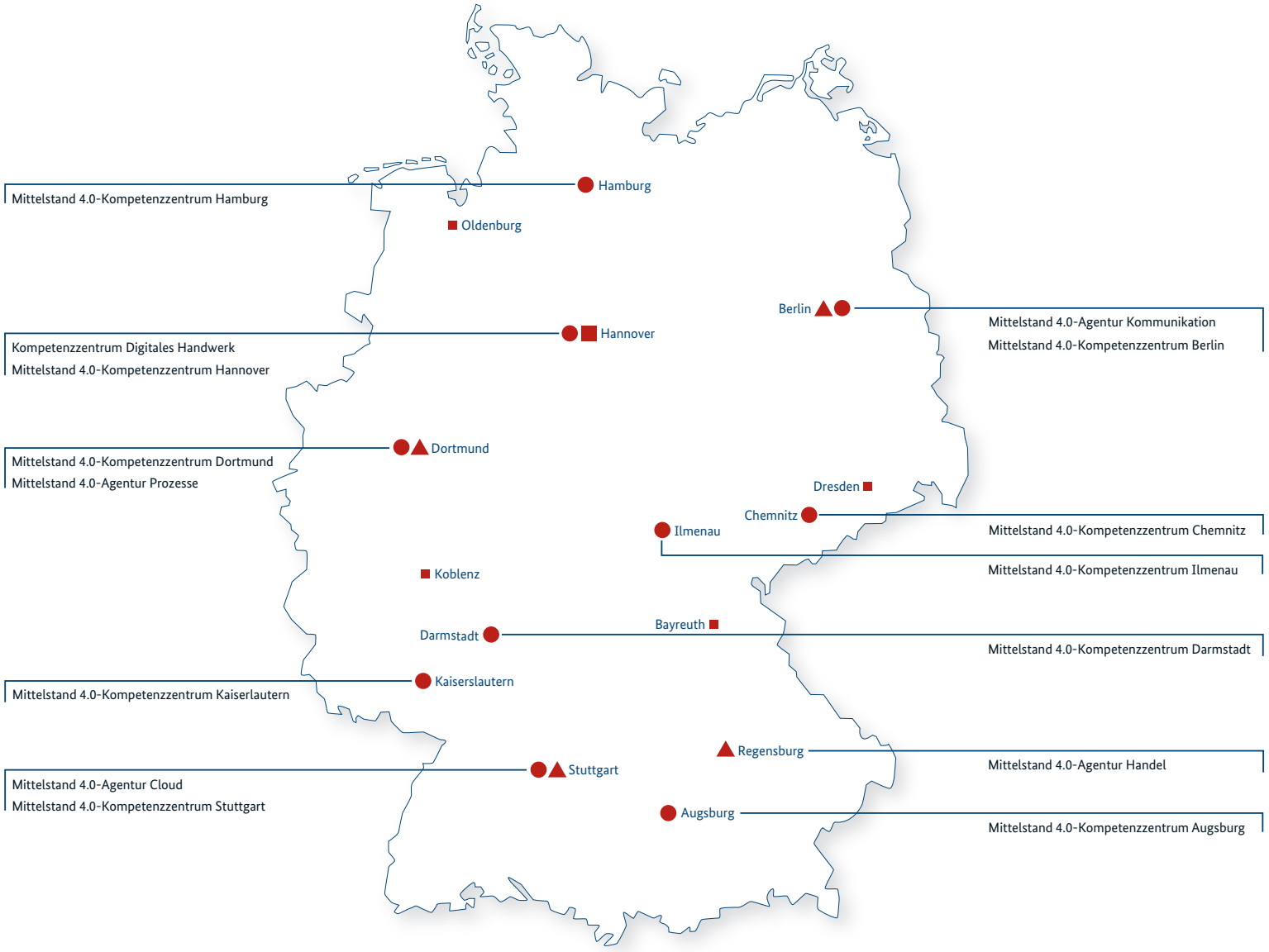
Titel: Abb.: © kristina rütten – Fotolia.com
Seite 4: © Andy Smith – Fotolia.com
Seite 7: © Antonioguillem – Fotolia.com
Seite 9: © everythingpossible – Fotolia.com
Seite 9: © photon_photo – Fotolia.com
Seite 10: © buyman – Fotolia.com
Seite 11: © pico – Fotolia.com
Seite 13: © style-photography.de – Fotolia.com
Seite 14: © iceteaimages – Fotolia.com
Seite 15: © iceteastock – Fotolia.com

Druckerei:

FLYERALARM GmbH
Alfred-Nobel-Str. 18
97080 Würzburg

Stand:

Juni 2017



Kompetenzzentren der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“

Agenturen der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“

Kompetenzzentrum Digitales Handwerk

Regionale Schaufenster

Mittelstand-Digital - Strategien zur digitalen Transformation der Unternehmensprozesse

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Regionale Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenlose Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen zu Mittelstand-Digital finden Sie unter www.mittelstand-digital.de