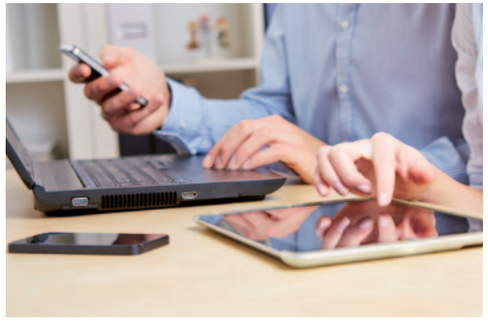
Warum Bring Your Own Device?



Viele Mitarbeiter möchten inzwischen eigene Geräte im Unternehmen nutzen. Unternehmen sehen sich zunehmend mit der Forderung konfrontiert, dass private Smartphones und Tablets auch beruflich eingesetzt werden. Dadurch können persönliche Angelegenheiten während der Geschäftszeit und geschäftliche Aufgaben während der Freizeit schneller und effizienter erledigt werden. 81 Prozent der Unternehmen, die BYOD zulassen, erwarten eine höhere Mitarbeiterzufriedenheit. 74 Prozent erwarten Effizienzsteigerungen.[1]

Auch einzelne Unternehmensbereiche sehen die Notwendigkeit zu handeln: Unternehmensinvestitionen im Bereich der mobilen Hardware sollen reduziert werden. Bereits mit dem Unternehmensnetzwerk verbundene private Geräte sollen ermittelt und technisch wie auch rechtlich abgesichert werden. Das Unternehmen soll attraktiver werden für versierte Mitarbeiter. Der Zugang zu Internet und Netzwerken soll für Mitarbeiter jederzeit gewährleistet werden.

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

Weiterführende Informationen unserer Mitglieder und Kooperationspartner

Informieren Sie sich als mittelständisches oder kleines Unternehmen bzw. als deren Mitarbeiter, wie private Smartphones und Tablets im Unternehmen genutzt werden können.
www.sicher-im-netz.de/BYOD

Ausführliche Hinweise zum Thema „Bring Your Own Device" finden Sie dort in dem **BYOD-Leitfaden für Unternehmer** des BITKOM.

Weitere Informationen zum Download:

Sicheres Arbeiten von unterwegs
Broschüre von DsiN und der DATEV

Beispielrichtlinie zur Absicherung von Mobilgeräten
Broschüre von Sophos

Mobile Device Management Buyers Guide
Broschüre von Sophos

IT-Consumerisation und BYOD
Überblickspapier des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Strategieempfehlungen zum Thema Consumerization of IT
Überblickspapier von Microsoft

Über Deutschland sicher im Netz e.V.

Produktneutral und herstellerübergreifend ist Deutschland sicher im Netz e.V. (DsiN) zentraler Ansprechpartner für Verbraucher und mittelständische Unternehmen zu Fragen der IT-Sicherheit.

DsiN unterstützt Unternehmen bei der Umsetzung eines bedarfsgerechten Sicherheitsmanagements, zum Beispiel mit leicht verständlichen Informationen zum Thema IT-Sicherheit, praxisrelevanten Checklisten, Leitfäden und konkreten Handlungsempfehlungen. Denn IT-Sicherheit ist eine wesentliche Grundlage für reibungslose Geschäftsabläufe. NEU: Ihre Handlungsempfehlung für die Cloud – der Cloud Scout unter www.dsin-cloud-scout.de.

Kontakt:

Deutschland sicher im Netz e.V.
Albrechtstraße 10 a
10117 Berlin
Tel. +49 (0) 30 27576-310
Fax +49 (0) 30 27576-51310
info@sicher-im-netz.de

www.sicher-im-netz.de
www.dsin-blog.de

Projektpartner: SAP

Mit Unterstützung von: BITKOM, Bundesdruckerei, eco, Telekom, Google, Microsoft, Open Limit, SOPHOS

Bring Your Own Device

Regeln für KMU und Nutzer

DEUTSCHLAND DsiN.de SICHER IM NETZ

Bring Your Own Device für wen?

Diese Informationsbroschüre richtet sich an mittelständische und kleine Unternehmen sowie deren Mitarbeiter, die Interesse haben, private Smartphones oder Tablets im Unternehmen für betriebliche Zwecke zu nutzen bzw. auf IT-Ressourcen des Unternehmens zuzugreifen.

Sie soll die Breite der Anforderungen aufzeigen, die bei einer solchen Entscheidung vom Unternehmen, aber auch vom Mitarbeiter berücksichtigt werden muss.

BYOD für das Unternehmen

Regeln für eine erfolgreiche Nutzung

1. **Ziele definieren, die mit BYOD erreicht werden möchten**
   Für Ihr Unternehmen muss eine klare Strategie ausgearbeitet werden. Maßgeblich für die Umsetzungsschritte und die Unterstützung durch die verschiedenen Abteilungen im Unternehmen ist das Ziel, das mit BYOD erreicht werden soll. Ziele können sein:
   - eine höhere Mitarbeiterzufriedenheit
   - Effizienzsteigerungen
   - Bereits verwendete private Geräte sollen ermittelt und abgesichert werden
   - Steigerung der Unternehmensattraktivität
   - Zugang zu Internet und Netzwerken soll für Mitarbeiter jederzeit gewährleistet sein
   - Sicherheit der Unternehmensinformationen muss gleichzeitig gewährleistet werden

2. **Risiken bewerten die für das Unternehmen entstehen**
   Folgende Aspekte/Risiken für Ihr Unternehmen müssen analysiert werden:

   - Datenschutzrechtliche Anforderungen (z. B. Datenschutzgesetze):
     - klare Trennung von Geschäfts- und Privatdaten
     - Unversehrtheit der Privatdaten
     - Wiederherstellbarkeit von Daten

     → Vereinbarungen mit Ihren Mitarbeitern müssen getroffen werden.

   - Personal- und arbeitsrechtliche Anforderungen
     - Die Haftungsregelung bei Verlust oder Beschädigung
     - Einhaltung länderspezifischer Bestimmungen

     → Vereinbarungen mit Ihren Mitarbeitern müssen getroffen werden.

   - Lizenz- und steuerrechtliche Anforderungen
     - Lizenzbedingungen von Softwareanbietern enthalten unterschiedliche Regeln für privaten und gewerblichen Gebrauch. Diese sind zu prüfen, ob eine Nutzung auf Privatgeräte abgedeckt ist, um Haftungsrisiken für das Unternehmen zu vermeiden.
     - Steuerliche Auswirkungen für Ihre Mitarbeiter wie geldwerter Vorteil bzw. für Ihr Unternehmen wie eine Ertragssteuer, sind zu prüfen.

     → Vereinbarungen mit Ihren Mitarbeitern müssen getroffen werden.

3. **Transparenz durch klare Richtlinien schaffen**
   Eine schriftliche Zustimmung der Mitarbeiter zur Einhaltung der Regeln und Umsetzung der erforderlichen Maßnahmen sind erforderlich. Klare Regeln bezüglich der Erstattung von Kosten sind festzulegen und sollten kommuniziert werden.

4. **Technische Voraussetzungen schaffen**
   Ein Betriebskonzept für die BYOD-Geräte ist zu erstellen. Schaffen Sie Klarheit, welche technischen Sicherheitsmaßnahmen (z.B. Zugangsschutz, Verschlüsselung, Virenschutz, Möglichkeit des Löschens bei Verlust) genutzt bzw. geschaffen werden müssen. Nur vom Unternehmen freigegebene Geräte von Mitarbeitern, die die Verpflichtungserklärung unterzeichnet haben, dürfen für BYOD verwendet werden. Es ist sicherzustellen, dass die Unternehmensanforderungen bezüglich Sicherheit und Verwaltbarkeit der BYOD Geräte gewährleistet werden kann.

5. **Organisatorische Voraussetzungen schaffen**
   Klar zu regeln sind Prozesse für die Zulassung privater Geräte sowie auch das Entfernen der Unternehmensdaten von privaten Geräten, z.B. im Falle der Beendigung des Arbeitsverhältnisses.

BYOD für den Mitarbeiter

Regeln für den BYOD Nutzer

1. **Verantwortung übernehmen**
   Die Sicherheit der Unternehmensinformationen liegt in den Händen des Mitarbeiters. Beeinträchtigungen durch erhöhte Sicherheitsmaßnahmen bei der Nutzung von privaten Geräten für Geschäftszwecke sind zu akzeptieren.
   - Der Zugriff auf das Gerät ist entsprechend der Unternehmensregeln zu schützen.
   - Die Verschlüsselung des Geräts ist zu aktivieren.
   - Updates sind zeitnah einzuspielen.
   - Das Gerät sollte nicht unbeaufsichtigt an Dritte weitergegeben werden.
   - Vorgaben des Geräteherstellers sind einzuhalten, z.B. darf das Betriebssystem nicht modifiziert werden.
   - Geschäfts- und Privatdaten sind strikt zu trennen.
   - Verträge mit Netz- und Softwareanbietern sind zu prüfen, ob eine berufliche Nutzung möglich ist.

2. **Für Sicherheit sorgen**
   Aktuelle Virenschutz-Programme sollten eingesetzt werden. Schutzmechanismen sind zu aktivieren wie z.B. das automatische Löschen der persönlichen Daten auf dem Gerät im Falle von zu vielen misslungenen Anmeldeversuchen. Im Fall von Diebstahl oder Verlust des Geräts sollten die Daten auf dem BYOD-Gerät über das Internet gelöscht werden können.

3. **Vereinbarungen akzeptieren**
   Falls Interesse an der beruflichen Nutzung des Privatgeräts besteht, sollte dies mit dem Vorgesetzten besprochen werden und nicht einfach das private Gerät mit dem Unternehmensnetzwerk verbunden werden oder Firmendaten auf das private Gerät übertragen werden. Mitarbeiter müssen sich an die Unternehmensvorgaben halten und sich im Zweifel rückversichern, welche Möglichkeiten bestehen.