

Link: <https://www.computerwoche.de/a/byod-prozessqualitaet-rauf-security-risiken-auch,2532386>

Studie zu Bring your own Device

ByoD - Prozessqualität rauf, Security-Risiken auch

Datum: 07.03.2013
Autor(en): Andreas Schaffry

Flexible Arbeitszeiten, mehr Kreativität, kürzere Innovationszyklen und verbesserte Zusammenarbeit im Team sind die Hauptvorteile von ByoD. Massive Probleme gibt es mit der Sicherheit.

Potential corporate gains from BYOD



CIOs erwarten von ByoD, dass Beschäftigte produktiver arbeiten, schneller auf Kundenanfragen reagiert wird und Arbeitsprozesse verbessert werden.

Foto: Dell / Quest

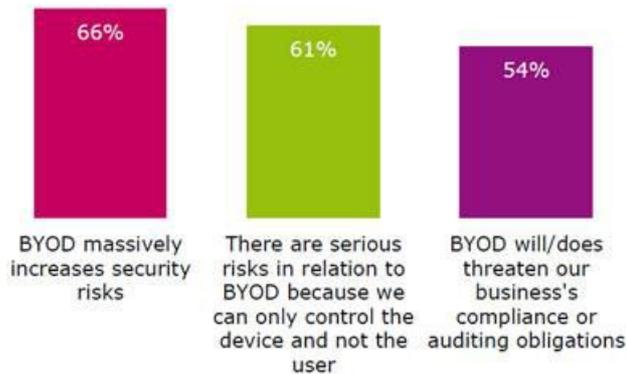
Nutzen Mitarbeiter private Smartphones und Tablet-PCs nach der Devise "Bring your own Device (**ByoD**¹)" für geschäftliche Zwecke sehen CIOs darin vor allem Vorteile. Rund 70 Prozent der IT-Verantwortlichen gehen davon aus, dass sie mit **ByoD**² die Arbeitsprozesse in ihrem Unternehmen verbessern können. Mitarbeiter würden von flexiblen Arbeitszeiten, mehr Raum für Kreativität und einer verbesserten Zusammenarbeit profitieren sowie schneller auf Kundenanfragen reagieren. Zudem trage ByoD dazu bei, Innovationszyklen zu verkürzen.

ByoD: Bei Verbot Wettbewerbsnachteil

Das geht aus einer aktuellen Studie hervor, die der britische Marktforscher Vanson Bourne im Auftrag des Dell-Unternehmens **Quest Software**³, einem Anbieter von Lösungen für das IT-Management, durchführte. Allerdings liefere ByoD nur dann einen nachhaltigen Erfolg, wenn die Anforderungen und Rechte jedes einzelnen Nutzers berücksichtigt werden. Das teilten rund Dreiviertel der Umfrageteilnehmer mit.

Immerhin 59 Prozent der IT-Leiter sind der Ansicht, dass ein Verbot der Nutzung privater Mobilgeräte am Arbeitsplatz Wettbewerbsnachteile gegenüber der Konkurrenz zur Folge hätte. Jeweils 64 Prozent der Befragten sind der Meinung, mit ByoD ließen sich Geschäftsziele besser erreichen und IT-Kosten senken. Laut Studie wirke sich zudem eine anwenderbezogene **ByoD-Strategie**⁴ mit klaren Richtlinien positiv auf die Datenverwaltung und Datensicherheit aus.

BYOD increases risk



Als Hauptnachteil von ByoD sehen IT-Verantwortliche die unkalkulierbaren Sicherheitsrisiken.

Foto: Dell / Quest

Unternehmen, die sich nach diesen Vorgaben richten, seien weniger mit Problemen konfrontiert. Laut Studie haben mehr als ein Viertel der IT-Entscheider keine Schwierigkeiten mit ByoD.

Sicherheitsrisiken durch unkontrollierte User

Allerdings ist das nur ein Teil der ByoD-Realität, denn die Nutzung privater Mobilgeräte am Arbeitsplatz erhöht die **Sicherheitsrisiken**⁵ für die Business-IT drastisch. Davon sind zwei Drittel der befragten IT-Verantwortlichen überzeugt. Für 61 Prozent resultieren die ernsthaften Risiken daraus, dass nur die Mobilgeräte kontrolliert werden können, nicht aber das Verhalten der User.

54 Prozent befürchten, dass ByoD die internen **Compliance-Richtlinien**⁶ sowie die Anforderungen an die Auditierung verletze. Ein Grund liege darin, dass durch die Einführung von ByoD die IT-Landschaft komplexer wird. Das mache es schwierig, private Mobilgeräte und die darauf installierten Business-Apps abzusichern, die Endpoint-Security und **Data-Governance**⁷ zu gewährleisten oder mobile Recovery-Szenarien umzusetzen.

Für die Studie wurden knapp 1.500 leitende IT-Verantwortliche in den USA, Großbritannien, Frankreich, Deutschland, Indien, Spanien, Italien, Australien, Singapur und China (Peking) befragt. Sie kommen aus Unternehmen verschiedener Branchen und dem öffentlichen Sektor. Vorreiter bei ByoD sind Firmen in den USA, China und Australien. Hier werden alle Geräte, die Mitarbeiter mitbringen, aktiv unterstützt. Europäische Länder wie Frankreich, Deutschland und Großbritannien hinken dagegen hinterher.

Links im Artikel:

¹ <https://www.computerwoche.de/schwerpunkt/BYOD>

² <https://www.computerwoche.de/a/der-byod-hype-ebbt-ab%2C2522856>

³ <http://www.quest.com/documents/byod-putting-users-first-produces-biggest-gains-fewest-setbacks-datasheet-19142.pdf>

⁴ <https://www.computerwoche.de/a/wie-sich-eine-sichere-byod-strategie-durchsetzen-laesst%2C2521618>

⁵ <https://www.computerwoche.de/a/was-bei-bring-your-own-device-wichtig-ist%2C2369063%2C4>

⁶ <https://www.computerwoche.de/a/wie-sie-richtlinien-effizient-einhalten%2C1898018>

⁷ <https://www.computerwoche.de/a/tipps-fuer-das-richtige-stammdaten-management%2C2489894>