



HOCHSCHULE LANDSHUT
HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN

Heft 1



Zur Organisationsrichtlinie „Bring your own Device“ – eine empirische Untersuchung

GORDON MÜLLER
CHRISTIAN SEEL

Erschienen am: 5.8.2013

Landshuter Arbeitsberichte zur Wirtschaftsinformatik

Herausgeber: Prof. Dr. Christian Seel, Prof. Dr. Dieter Greipl,
Prof. Dr. Peter Scholz, Prof. Dr. Jürgen Wunderlich

Landshuter Arbeitsberichte zur Wirtschaftsinformatik

ISSN: 2197-4497

Herausgeber: Prof. Dr. Christian Seel, Prof. Dr. Dieter Greipl,
Prof. Dr. Peter Scholz, Prof. Dr. Jürgen Wunderlich

Kontakt: Hochschule Landshut, Am Lurzenhof 1, 84036 Landshut

Zitation:

Gordon Müller; Christian Seel: Zur Organisationsrichtlinie „Bring your own Device“ – eine empirische Untersuchung. In: C. Seel;D. Greipl;P. Scholz;J. Wunderlich (Hrsg.):
Landshuter Arbeitsberichte zur Wirtschaftsinformatik. Heft 1, 2013.

GORDON MÜLLER
CHRISTIAN SEEL

Zur Organisationsrichtlinie „Bring your own Device“ – eine empirische Untersuchung

Heft Nr. 1

Inhaltsverzeichnis

Inhaltsverzeichnis	2
1. Einleitung und Terminologie	3
2. Wissenschaftliche Methodik	4
3. Empirische Untersuchung der Organisationsrichtlinie Bring your own Device	5
3.1 Konzeption der Untersuchung	5
3.2 Thesen der empirischen Untersuchung	6
4. Bewertung der Thesen	9
4.1 Bewertung der ersten These	9
4.2 Bewertung der zweiten These	13
4.3 Bewertung der dritten These	17
4.4 Bewertung der vierten These	19
4.5 Bewertung der fünften These	23
5. Zusammenfassung und Ausblick	27
Abbildungsverzeichnis	29
Literaturverzeichnis	30
Anhang: Rohdaten der Umfrage (bereinigt von Leereinträgen)	32

1. Einleitung und Terminologie¹

In jüngerer Zeit ist eine zunehmende Verbreitung der Organisationsrichtlinie „Bring your own Device“ (ByoD) zu beobachten. Unter dem Terminus „Bring your own Device“, soll im Folgenden eine Organisationsrichtlinie in Unternehmen verstanden werden, welche es Mitarbeitern erlaubt, private Geräte auch beruflich zu nutzen. Zwar ist ByoD ein Sammelbegriff, demnach weniger auf einen konkreten Gerätetyp, wie Smartphones oder Notebook festgelegt, jedoch wird in erster Linie das Nutzen des privaten Smartphones darunter verstanden. In allen Fällen von ByoD wird zusätzlich zu der Nutzung des Geräts auch der Zugriff auf das Unternehmensnetzwerk sowie Unternehmensdaten verstanden.²

Für das Unternehmen und den Mitarbeiter ergeben sich hieraus zahlreiche Chancen, wie z. B. gesteigerte Produktivität der Mitarbeiter durch den Einsatz von Smartphones, erhöhte Erreichbarkeit des Mitarbeiters außerhalb der üblichen Bürozeiten und Kosteneinsparungen bei der Anschaffung. Außerdem wird von einigen Quellen ein Imagevorteil im Recruiting neuer Mitarbeiter aus der Altersgruppe der sog. Millennials³ durch ByoD postuliert. Abgesehen von diesen Vorteilen wirft ByoD aber auch Probleme im IT-Management der Geräte auf. Neben Sicherheitsrisiken ist hier vor allem auch der erschwerte Support zu nennen.

Ziel dieses Beitrags ist es eine empirische Untersuchung durchzuführen, welche die in der Literatur genannten Chancen und Risiken verschiedener Aspekte von ByoD (Sicherheit, Arbeitsaufwand, Fortschritt, Recht und Recruiting) beleuchtet. Die durchgeführte Untersuchung erlaubt eine Einschätzung des Status-Quo der Organisationsrichtlinie ByoD in Deutschland in Bezug auf die Haltung der Unternehmen zum generellen Einsatz von ByoD, sowie der Chancen und Risiken, die dabei jeweils gesehen werden.

Dazu wird zunächst im zweiten Abschnitt die Forschungsmethodik, die diesem Beitrag zugrunde liegt, vorgestellt. Daran schließt sich im dritten Abschnitt die Konzeption der Untersuchung sowie die Vorstellung der untersuchten Thesen an, welche im vierten Abschnitt einer Bewertung, anhand der Studienergebnisse, unterzogen wird. Der Beitrag schließt im

¹ Bei dem Beitrag handelt es sich um eine erweiterte Version von: Müller, Seel: Zur Organisationsrichtlinie „Bring your own Device“ – eine empirische Untersuchung. In: Proceedings zur AKWI-Tagung 2013, September 2013.

² Vgl. Gartner(2013).

³ Vgl. Gertz (2007).

fünften Kapitel mit einer Zusammenfassung und einem Ausblick auf weitere Forschungsfragen.

2. Wissenschaftliche Methodik

Aufgrund der Fragestellung nach Chancen und Risiken von ByoD in der Praxis, ist die Anwendung des Instrumentariums der empirischen Sozialforschung angeraten. Dabei gilt der Grundsatz, dass die gewählte empirische Untersuchungsmethode jeweils dem individuellen Untersuchungsgegenstand angemessen zu wählen und an ihm zu entwickeln ist⁴. Grundsätzlich erfolgt eine Differenzierung in qualitative und quantitative Verfahren der empirischen Sozialforschung⁵. Welche Verfahrensgruppe vorzuziehen ist, hängt im Wesentlichen davon ab, ob der Untersuchungsgegenstand die Verwendung hypothesenprüfender Verfahren zulässt oder es zunächst des Einsatzes hypothesenentwickelnder, explorativer Verfahren bedarf⁶. Da bereits aus der Literatur Hypothesen extrahiert werden können, wird ein hypothesenprüfendes Verfahren in Form einer Fragebogengestützten Umfrage durchgeführt.

Um Zeit und Kosten zu sparen wurde für die Studie das Online-Umfragewerkzeug LimeSurvey⁷ eingesetzt. Neben der Wahl des Verfahrens und dessen Werkzeug zur Durchführung, ist die Entscheidung über die Art der Fragen wesentlich für das Forschungsdesign von Fragebögen⁸: Offene Fragen bieten die Möglichkeit, Antworten zu formulieren und zu beschreiben, während geschlossene Fragen Antwortmöglichkeiten vorgeben. Halboffene Fragen geben dem Befragten die Möglichkeit, zu den vorgegebenen Antworten neue Hinzuzufügen. Vorgegebene Antworten können beispielsweise Ja/Nein oder klassische Antwortsätze, welche zu der gestellten Frage passen, sein.

Eine besondere Form der Antworten bieten sogenannte Skalen. Ziel von Skalen ist es, den Befragten dahingehend zu beeinflussen, dass er sich für eine Richtung entscheidet (geradzahlige Skalen). Soll dem Befragten eine Möglichkeit gegeben werden, sich neutral zu einer Frage zu äußern, wird eine neutrale Antwort eingefügt (ungeradzahlige Skalen). Eine zusätzliche Unterscheidung nach direkten und indirekten Fragen wird an dieser Stelle nicht

⁴Vgl. Liebold, Trinczek (2002).

⁵Vgl. Bortz, Döring (2006).

⁶Vgl. Meuser, Nagel (2005).

⁷Vgl. LimeSurvey (2013).

⁸Vgl. Bortz, Döring (2006).

vorgenommen, da nur Hypothesen bewertet werden sollen. Die zu jeder These offen gestellten Fragen wurden als direkte Fragen formuliert.

In der durchgeführten Studie wird die geschlossene als auch die offene Fragetechnik verwendet. Damit lassen sich einerseits leichter Aussagen über Zustimmung und Ablehnung zu den Hypothesen treffen und andererseits haben die Befragten die Möglichkeit, sich individuell zu äußern. In den geschlossenen Fragen kommen Likert-Skalen⁹ zum Einsatz, welche persönliche Einstellungen messen.

3. Empirische Untersuchung der Organisationsrichtlinie Bring your own Device

3.1 Konzeption der Untersuchung

Wie in Abschnitt eins beschrieben, soll diese Untersuchung es ermöglichen, einen Trend der Bring your own Device Nutzung zu erfassen. Weiterhin ist es von Interesse, ob Unternehmen, welche ByoD bisher nicht im Einsatz haben, die Einführung in Betracht ziehen. Auch sind die Gründe interessant, warum ByoD (noch) nicht eingeführt worden ist. Abschließend wird eine Auswertung der getroffenen Aussagen vorgenommen, um zu prüfen, welchen Status ByoD in deutschen Unternehmen hat. Nachdem die Technik der Umfrage in diesem Fall rein den quantitativen Methoden zugeordnet werden kann, steht die Menge der Daten im Vordergrund.

In den Vorbereitungen für diese Untersuchung wurden Überlegungen angestellt, mit welchen Methoden die oben genannten Ziele am besten erreicht werden können. Auch wenn das Interview als qualitative Methode einen tieferen Informationsgehalt und gleichzeitig eine erhöhte Subjektivität der Ergebnisse bietet¹⁰, sind die Nachteile ausschlaggebend gewesen. Innerhalb des gegebenen Zeitraumes, wären Interviews nur mit einer sehr begrenzten Auswahl von Personen möglich gewesen. Auch der Kostenfaktor ist bei dieser Methode deutlich größer als bei der gewählten Umfragetechnik. Die Studie enthält fünf Thesen, welche durch einzelne Aussagen bewertet wurden. In diesem Beitrag werden nur die Thesen betrachtet und in Summe der Einzelaussagen bewertet.

Die Umfrage ist, je nachdem ob ByoD im Einsatz ist, vom Fragenumfang unterschiedlich. Damit unterscheidet sich auch der benötigte zeitliche Aufwand der Beantwortung. Es wurde

⁹Vgl. Bortz, Döring (2006).

¹⁰Vgl. Winter (2000).

davon abgesehen, ausschließlich Unternehmen direkt zu konsultieren und so auf die Umfrage hinzuweisen, da viele Firmen Aufforderungen zu Umfragen nicht beachten oder zu wenig freie Ressourcen besitzen. Die Alternative zur direkten Ansprache ist der Weg über soziale Netzwerke. Das wichtigste soziale Netzwerk, welches für diese Untersuchung genutzt wurde ist XING. XING hat gegenüber LinkedIn und Facebook den Vorteil, dass die Mehrheit der Nutzer aus dem Deutschsprachigen Raum kommt, was für diese Studie sehr wichtig ist. Nur so konnte ein Trend innerhalb Deutschlands ermittelt werden. Des Weiteren ist XING (wie LinkedIn auch) ein Netzwerk für berufliche Kontakte, welches vor allem im B2B Bereich genutzt wird.¹¹ Um die „richtigen“ Ansprechpartner zu finden, wurde der Kontakt zu Gruppen gesucht, dessen Mitglieder vermehrt CIOs oder Technikspezialisten sind. Dadurch konnten 51 Teilnehmer für diese Studie gewonnen werden.

3.2 Thesen der empirischen Untersuchung

In der einschlägigen Literatur finden sich verschiedene positive und negative Aussagen zu ByoD. Die gefunden Aussagen lassen sich zu den folgenden fünf Hypothesen verdichten, die in einer näheren Untersuchung unterzogen werden sollen:

1. Die IT-Sicherheit im Unternehmen wird durch ByoD gefährdet.¹²
2. Der Aufwand (Administration) für den Support von IT-Geräten steigt durch ByoD.¹³
3. ByoD ist ein Technologietreiber für die Unternehmensinfrastruktur.¹⁴
4. ByoD wirft ungeklärte juristische Fragestellungen auf.¹⁵
5. ByoD hilft (junge) Absolventen zu rekrutieren (HR-Sicht).¹⁶

Die erste These bezieht sich auf die IT-Sicherheit in Unternehmen: Die IT-Sicherheit im Unternehmen wird durch ByoD gefährdet. Eine zentrale Versorgung der Mitarbeiter durch das eigene Unternehmen hat den Vorteil, dass die Sicherheit der IT-Systeme, durch den Einsatz von vorkonfigurierten Geräten, weitestgehend gewährleistet werden kann. Bei ByoD ist dies anders gelagert: der Nutzer hat bereits ein Gerät, welches „von außen“ in bestehende IT-

¹¹ Vgl. Arns (2013).

¹² Vgl. Ballagas et al. (2004).

¹³ Vgl. Dufft, Flug, Niemann (2011).

¹⁴ Vgl. Arns (2013). sowie Burnham (2012).

¹⁵ Vgl. Dufft, Flug, Niemann (2011).

¹⁶ Vgl. Werle (2012).

Systeme eingeschleust wird und Zugriff auf das Intranet bekommen soll. Inwieweit das Gerät zuverlässig vor Schadsoftware und Kompromittierung geschützt ist, ist von Nutzer zu Nutzer unterschiedlich. Dies stellt ein grundlegendes Problem dar, denn bereits auf dem externen Gerät vorhandene Schadsoftware kann sich so leicht im Unternehmensnetzwerk verbreiten. Hierfür müssen Lösungen erarbeitet werden, um solche Gefahren auszuschließen. Diese Lösungen müssen, wenn möglich, auch plattformübergreifend und auf Smartphones/Tablets verfügbar sein. Eine Möglichkeit, um die Sicherheit für das Unternehmensnetzwerk und die Unternehmensdaten zu gewährleisten, wäre unter anderem das Einschränken des Nutzerkontos, was jedoch von den meisten Mitarbeiter in der Regel abgelehnt werden würde. Eine andere Möglichkeit wäre die Überwachung des Geräts mittels einer Mobile Device Management Lösung. Damit lassen sich installierte Anwendungen überprüfen um z. B. bei alten Versionsständen Updates zu veranlassen. Dies erhöht die Sicherheit, da Sicherheitslücken alter Versionen nicht zur Gefahr werden können.

Die zweite These bezieht sich auf den Arbeitsaufwand in der IT-Abteilung: Der Aufwand (Administration) für den Support von IT-Geräten steigt durch ByoD. Neben den Aufwänden für die IT-Sicherheit, muss die IT-Abteilung zusätzliche Ressourcen für die Administration und den Support von ByoD-Geräten vorhalten. Aufgrund der fehlenden zentralen Versorgung mit von der IT genehmigter Hardware, entsteht eine heterogene Gerätelandschaft. Diese Heterogenität hat zur Folge, dass grundlegende Techniken, wie das Erstellen einer VPN Verbindung zum Unternehmensnetzwerk, individuell betreut und konfiguriert werden müssen. Ein ähnliches Problem ergibt sich, wenn unternehmensinterne Anwendungen für mehrere Plattformen bereitgestellt werden müssen, die es den Mitarbeitern ermöglichen, mit ihren präferierten Systemen zu arbeiten. Ein weiterer Punkt, an dem der Administrationsaufwand deutlich wird, ist die Durchführung von Best-Practice Handlungen. Ein allumfassendes, zentrales Backup von allen Daten ist beispielsweise nur dann möglich, wenn Veränderungen an Datenbeständen von vornherein nicht lokal gespeichert werden können. Sollte dies nicht möglich sein, sind zusätzliche Schritte zur Absicherung der Geräte unabdingbar. Allerdings ist bei wichtigen Bereichen, wie Firewall und Virens Scanner, eine Betriebssystemfragmentierung nicht von Vorteil. Das Problem hierbei sind oft voneinander abweichende Sicherheitseinstellungen für jede Version eines Betriebssystems.

Die dritte These bezieht sich auf den technologischen Fortschritt innerhalb des Unternehmens: ByoD ist ein Technologietreiber für die Unternehmensinfrastruktur. Technologische

Trends bei Hard- und Software können durch die in der Regel kurzen Produktlebenszyklen bei den von den Mitarbeitern ins Unternehmen eingebrachten Smartphones und Tablets schneller verfügbar sein. Beispielsweise lassen sich Technologien, wie Near Field Communication (NFC), auch im Unternehmensumfeld produktiv einsetzen. So kann beispielsweise die Zeiterfassung von Mitarbeitern oder auch das Beziehen der Einstellungen für das WLAN Netzwerk kontaktlos durch NFC vereinfacht werden. Neben dem Einsatz von neuen Technologien ist aber auch der Ausbau der bereits etablierten Techniken nötig. Viele der Geräte, die als ByoD auftreten, können zwar auch über das Mobilfunknetzwerk mit dem Internet und so mit dem Unternehmensnetzwerk kommunizieren, jedoch nicht unbegrenzt mit voller UMTS/LTE Geschwindigkeit. Abhängig vom Transfervolumen kann dies zudem ein Kostenfaktor sein. Des Weiteren ist es bei zunehmender Verbreitung von Smartphones und Tablets im Unternehmenseinsatz notwendig, künftige Anwendungen speziell auf mobile Geräte auszurichten. Dies wird durch den Einsatz von plattformübergreifenden Techniken wie z. B. HTML5 und CSS3 möglich.

Die vierte These bezieht sich auf juristische Einschätzungen im Zusammenhang mit ByoD: ByoD wirft ungeklärte juristische Fragestellungen auf. Auch außerhalb der technischen Aspekte gibt es für das Unternehmen Chancen und Risiken. Mitarbeiter, welche ByoD nutzen und auch Zugriff auf das Unternehmensnetzwerk haben, sehen sich konfrontiert mit dem Arbeitszeitgesetz, welches die maximale werktägliche Arbeitszeit auf acht Stunden festsetzt.¹⁷ Des Weiteren können Unternehmensdaten z. B. personenbezogene Daten, welche auf mobilen Geräten gespeichert sind, leichter durch Dritte (Personen/Software) gelesen werden. Ein Unternehmen, welches ByoD für seine Mitarbeiter ermöglicht, muss prüfen, inwieweit eine Trennung von Unternehmensdaten und privaten Daten auf dem Gerät/den Geräten des Mitarbeiters Zugriff möglich ist. Daraufhin können Zugriffsberechtigungen angepasst werden. Des Weiteren müssen mit der IT-Abteilungen rechtlich einwandfreie Lösungen gefunden werden, damit weder Einsicht in private Daten genommen werden kann, noch dass unternehmensinterne Daten nach außen dringen können.

Die fünfte These bezieht sich auf das eventuell veränderte Recruitment mit ByoD: ByoD hilft (junge) Absolventen zu rekrutieren (HR-Sicht). Von Soziologen werden diverse Begriffe wie Generation Y, Millennials oder Digital Natives für die aktuelle Absolventen Generation (Jahrgänge von 1980 bis 1995) verwendet. Dies ist die erste Generation, welche als Kinder die

¹⁷ Vgl. Bundesamt für Justiz (1994).

Möglichkeit hatte, das Internet zu nutzen und so als besonders technologieaffin gelten. In unterschiedlichen Interviews mit Personalverantwortlichen ist zu lesen, dass diese Generation der neuen Mitarbeiter eine andere Arbeitsweise an den Tag legt. Ihnen geht es mehr um die Selbstverwirklichung in der Arbeit und auf die Work-Life-Balance, die Möglichkeiten des Aufstiegs sind nicht primär im Vordergrund.¹⁸ Durch den Einsatz von ByoD ist es für Unternehmen leichter geworden, diese Anforderungen an die Work-Life-Balance der neuen Generation anzupassen. In dem „Kampf um Talente“¹⁹, welcher aktuell auf dem Arbeitsmarkt herrscht, müssen die Unternehmen alle Register bei der Personalsuche ziehen. Dabei ist es gerade für die kleinen und mittleren Unternehmen wichtig sich positiv zu positionieren. ByoD kann ein Schritt sein, sich als Arbeitgeber von anderen abzuheben.

4 Bewertung der Thesen

4.1 Bewertung der ersten These

Die IT-Sicherheit von Unternehmen ist ständig in Gefahr, einerseits durch Bedrohungen von außen aber andererseits auch Bedrohungen von innen. Eine Einführung von ByoD sorgt in der Regel für neue Probleme, welche sonst mit Unternehmenseigenen Geräten überschaubar sind. Dass die IT-Sicherheit in Unternehmen durch ByoD zusätzlich gefährdet wird, haben die Teilnehmer der Studie mit den Bewertungen einzelner Aussagen, welche sich auf die These beziehen bestätigt. Eine der größten Bedrohungen im Alltag sind Drive-By-Downloads.²⁰ Diese stellen eine Gefahr für alle Arten von mobilen Geräten dar²¹, wobei es wichtig ist, gerade Anwender von ByoD Geräten zu schulen, da das Unternehmen nicht ständig Zugriff auf den aktuellen Stand der Sicherheitssoftware haben kann. Auch sollten Mitarbeiter über den richtigen Umgang mit Unternehmensdaten unterrichtet werden – unabhängig vom ByoD Einsatz. Dass das Bewusstsein der Mitarbeiter für einen sensiblen Umgang mit Unternehmensdaten gestärkt werden muss, bestätigten 55% der Teilnehmer. Dass die Sicherheit von IT-Systemen durch ByoD in Gefahr gerät, kann nicht pauschal ausgesprochen werden. Im Einzelnen kann dies aber vorkommen, wenn neue Geräte ohne Überprüfung und ohne entsprechende Sicherheitsmaßnahmen in das Unternehmensnetzwerk integriert werden.

¹⁸Vgl. Werle (2012).

¹⁹Gatermann(2011).

²⁰ Vgl. Neugebauer (2013).

²¹ Vgl. Eikenberg(2012).

Die Auswertungen der Aussagen der ersten These können folgend entnommen werden:

Die Ergebnisse der Aussage „Bei privaten Daten legen Angestellte nicht genügend Wert auf Sicherheit (privates Surfen auf unsicheren Webseiten).“ können der Abbildung 1 entnommen werden. Auffällig ist, dass diese Aussage von 85% der Befragten bestätigt wird.

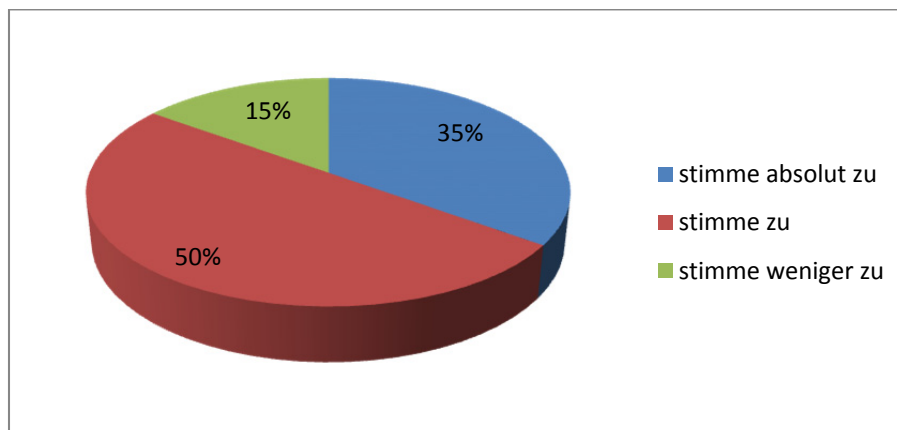


Abbildung 1: Auswertung These 1 Aussage 1

Die Auswertung der Aussage „Durch BYOD gehen Anwender nicht sorgsam genug mit Unternehmensdaten um.“ ist aus der nachstehenden Abbildung ersichtlich. 45% der Befragten stimmen dieser Aussage weniger oder gar nicht zu. Wenn BYOD-Nutzer extra geschult werden, wie mit Unternehmensdaten umgegangen werden soll, ist dieses Ergebnis nicht überraschend. Das dies wohl nicht die Regel ist, stimmten 40% dieser Aussage zu und 15% absolut zu.

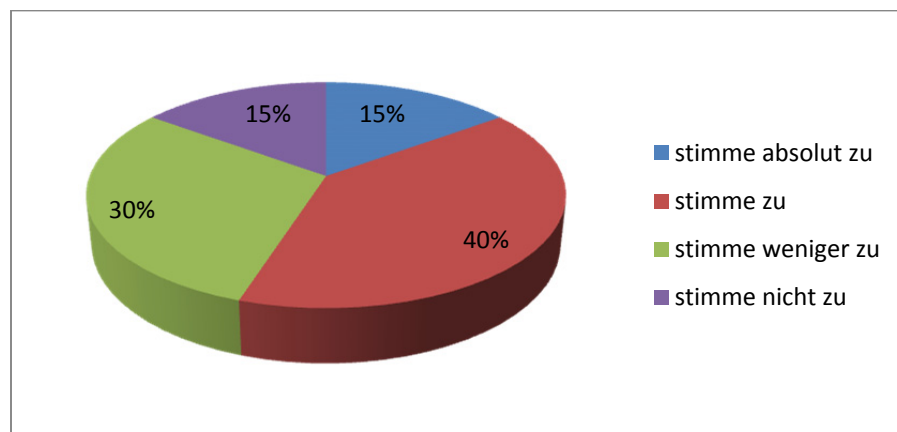


Abbildung 2: Auswertung These 1 Aussage 2

Die folgende Abbildung stellt die Ergebnisse der Aussage „Die Durchführung von regelmäßigen Backups wird durch BYOD erschwert.“ dar. Ihr kann entnommen werden, dass BYOD für den Großteil der Befragten keinen Einschnitt in bestehende Backup Pläne aufzeigt. 40% der Befragten gaben an, dass Backups durch BYOD erschwert werden.

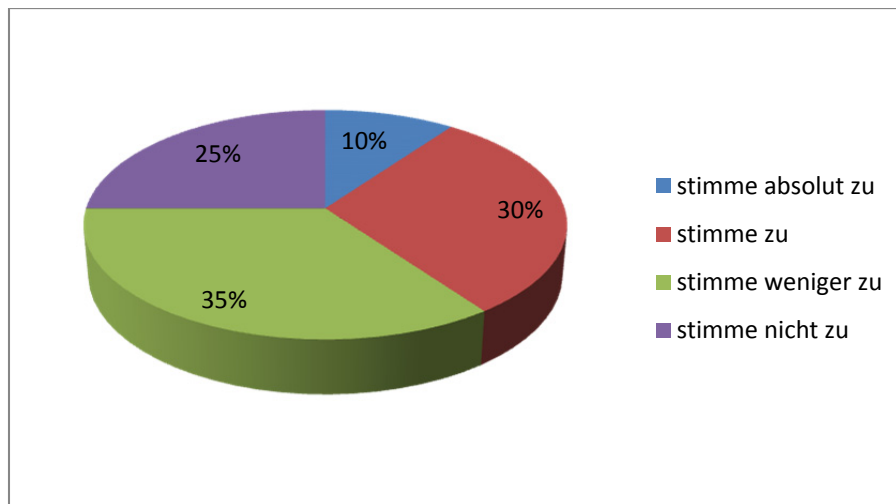


Abbildung 3: Auswertung These 1 Aussage 3

Die Resultate der Aussage „Trotz Einschränkungen in den privaten Geräten kann keine umfassende Sicherheit gewährleistet werden.“ zeigen, dass die Befragten BYOD nicht als „offenes Tor“ in das Unternehmensnetzwerk sehen. Nur 35% sind der Meinung, dass private Geräte trotz Einschränkungen ein Risiko darstellen.

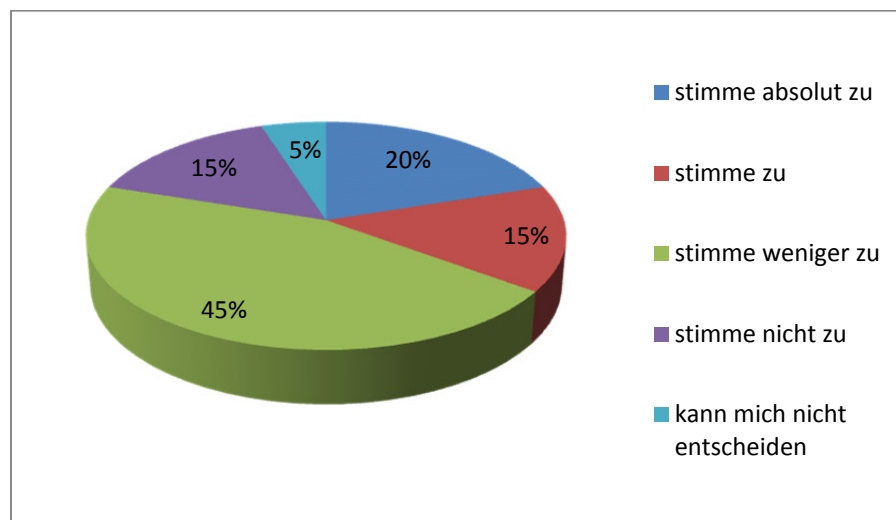


Abbildung 4: Auswertung These 1 Aussage 4

Aus den Ergebnissen der Aussage „Durch nicht hinreichend geschützte private Geräte wird die Sicherheit der IT Infrastruktur gefährdet.“ geht hervor, dass private IT-Geräte besonders gemanagt werden müssen, um kein Risiko darzustellen.

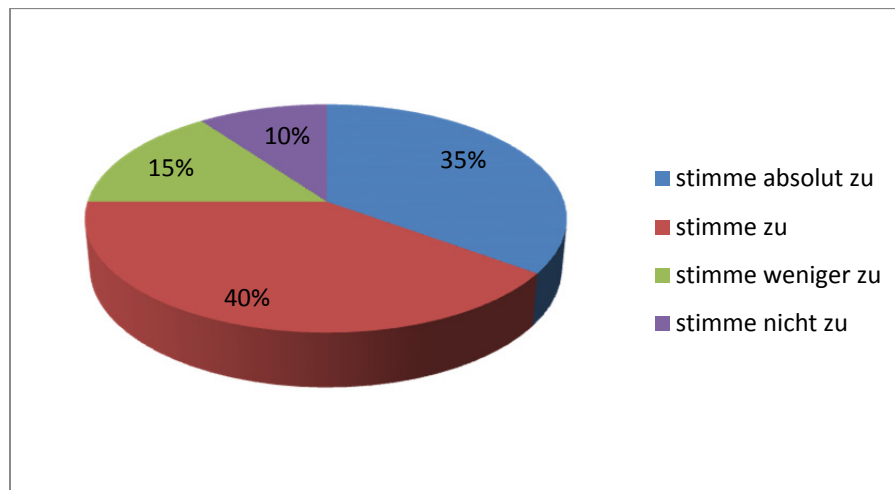


Abbildung 5: Auswertung These 1 Aussage 5

Die Abbildung 6 visualisiert die Ergebnisse der Aussage „Die bereits auf privaten Geräten vorhandene Schadsoftware stellt im BYOD Einsatz eine besondere Herausforderung für IT-Sicherheitsmaßnahmen dar.“. 60% der Teilnehmer sind der Meinung, dass die im Unternehmen vorhandene IT-Sicherheit mit zusätzlichen Maßnahmen gegen auf mobilen Geräten vorhandene Schadsoftware gerüstet werden muss.

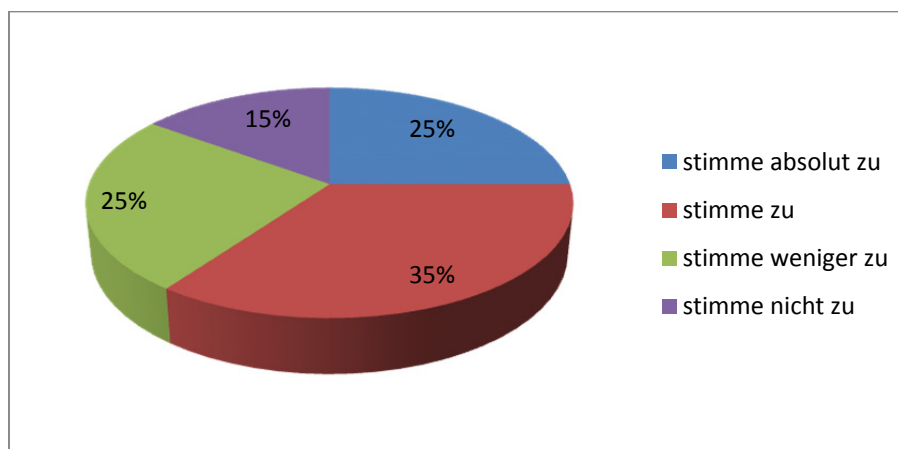


Abbildung 6: Auswertung These 1 Aussage 6

Die letzte Aussage der ersten These „Sicherheitsvorschriften können nicht wie auf unternehmenseigenen Geräten durchgesetzt werden.“ bekommt 60% Zustimmung der Befragten. Lediglich 20% stimmen dieser Aussage nicht und weitere 20% eher nicht zu. Daraus kann gefolgert werden, dass es in dem Bereich der mobilen Sicherheit viel Potential gibt. An dieser Stelle dienen Mobile Device Management Lösungen als Hilfsmittel, Sicherheitsvorschriften in mobilen Systemen umzusetzen.

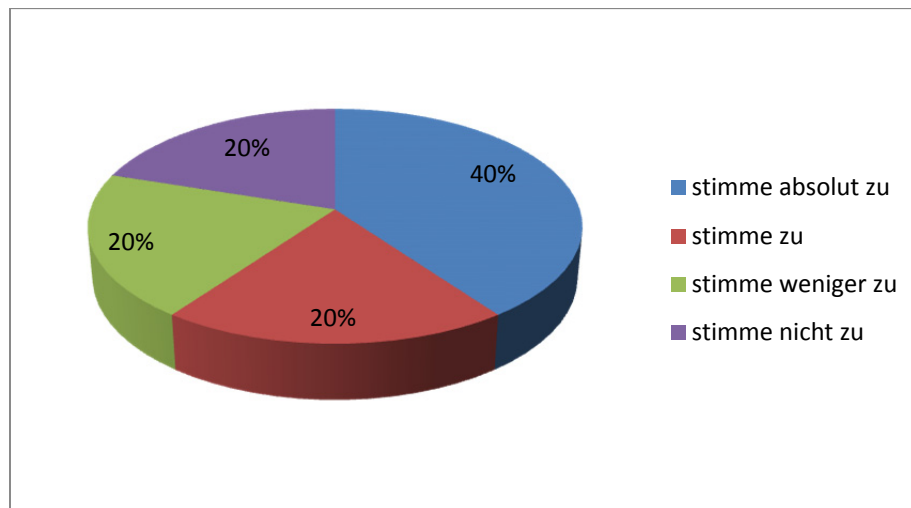


Abbildung 7: Auswertung These 1 Aussage 7

4.2 Bewertung der zweiten These

Dass durch ByoD auch der Administrationsaufwand für den Support der IT-Geräte steigt, ist an der mehrheitlichen Zustimmung der einzelnen Aussagen zu dieser These erkennbar. Dabei ist nicht nur der Einführungsaufwand, sondern auch laufende Aufwände gemeint, wie beispielsweise der Support der im Unternehmen vorhandenen Geräte. Der Supportaufwand wird nach Ansicht von 65% der Teilnehmer durch die Heterogenität ansteigen. Außerdem sind die meisten unternehmensinternen Anwendungen auf ein Betriebssystem zugeschnitten und nicht für die neue Technikgeneration der Tablets und Smartphones vorgesehen. Damit Anwendungen, welche sich auch auf z. B. Tablets produktiv einsetzen lassen, auch auf unterschiedlichen Gerätetypen und unterschiedlichen Betriebssystemen funktionieren, ist eine Portierung notwendig. Dieser ressourcenintensive Aufwand wird nur dann getätigt, wenn das Unternehmen einen Mehrwert und eine Steigerung der Produktivität erwarten kann. Die Berücksichtigung unterschiedlicher Gerätetypen ist ebenso wichtig, wie die Beachtung der Betriebssystemversionen. Hier bietet sich eine Möglichkeit an, mittels einer Blacklist nur bestimmte Geräte zu erlauben. Durch Einschränkungen können so Supportanfragen schneller bearbeitet werden, da die Lösungssuche vereinfacht wird, wenn eine beschränkte Heterogenität in der IT-Landschaft vorhanden ist.

Die Auswertungen der Aussagen der zweiten These können folgend entnommen werden:

Die Auswertung der ersten Aussage „Der Aufwand jede Software auf jedem Geräts aktuell zu halten steigt durch BYOD.“ zeigt, dass in Summe 71% der Befragten dem so nicht zustimmen. Nur 29% sind der Meinung, dass der Aufwand steigt.

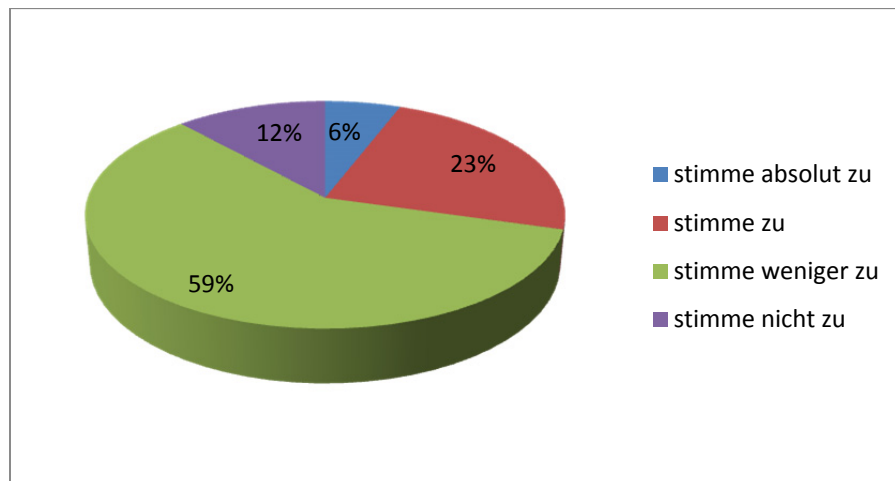


Abbildung 8: Auswertung These 2 Aussage 1

Die Abbildung 9 zeigt auf, dass eine Mehrheit von 53% der Aussage „Unternehmensinterne Anwendungen müssen wegen BYOD für unterschiedliche Plattformen bereit gestellt werden.“ zustimmen. Nur 12% der Teilnehmer widersprechen dieser Aussage. Hier wird deutlich, dass eine Vielzahl von Plattformen in einem Unternehmen aufwendiger zu verwalten ist.

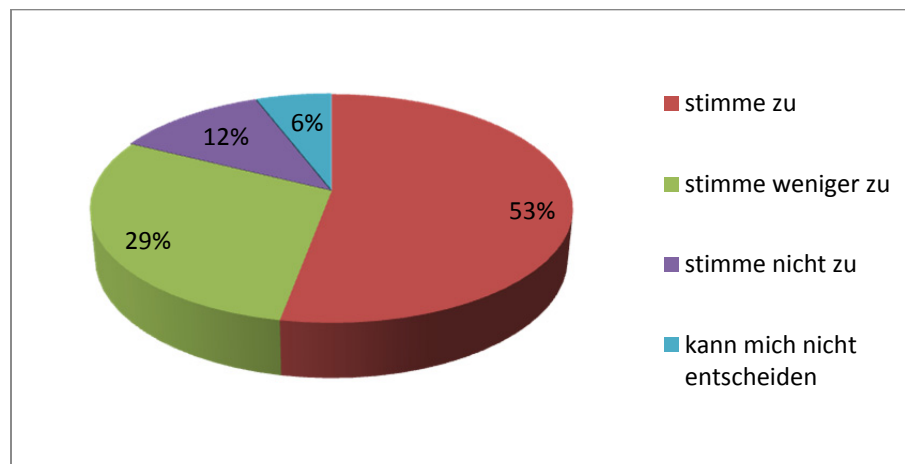


Abbildung 9: Auswertung These 2 Aussage 2

Auch wird aus der folgenden Abbildung, welche sich auf die Behauptung „Der unterschiedliche Funktionsumfang der BYOD Geräte führt zu Insellösungen (Bsp. Implementierung einer VPN Verbindung).“ stützt, ersichtlich, dass 76% der Meinung sind, Insellösungen werden mit BYOD nicht im Unternehmen eingeführt. Nur 24% der Befragten halten Insellösungen durch BYOD für möglich.

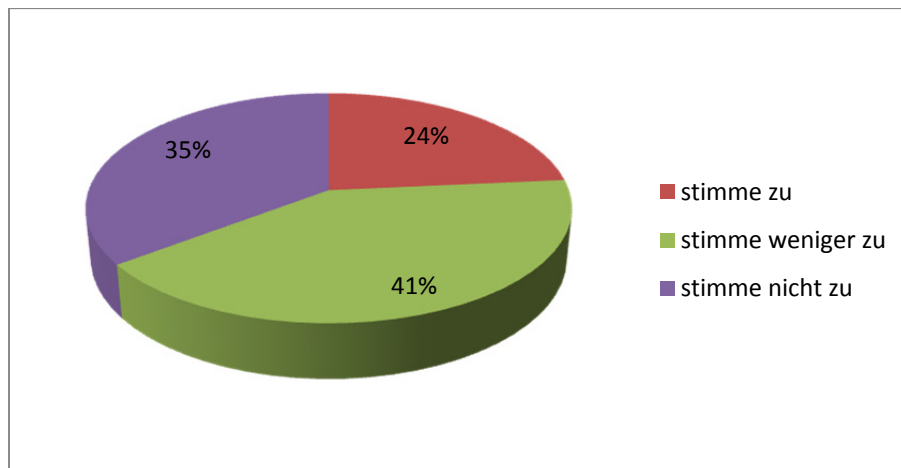


Abbildung 10: Auswertung These 2 Aussage 3

Die Resultate der vierten Aussage „Best-Practice Handlungen könnten nur schwer durchgeführt werden (z. B. Backup).“ zeigen, dass BYOD Best-Practice Vorgänge, laut der Umfrageteilnehmer, nicht beeinflusst.

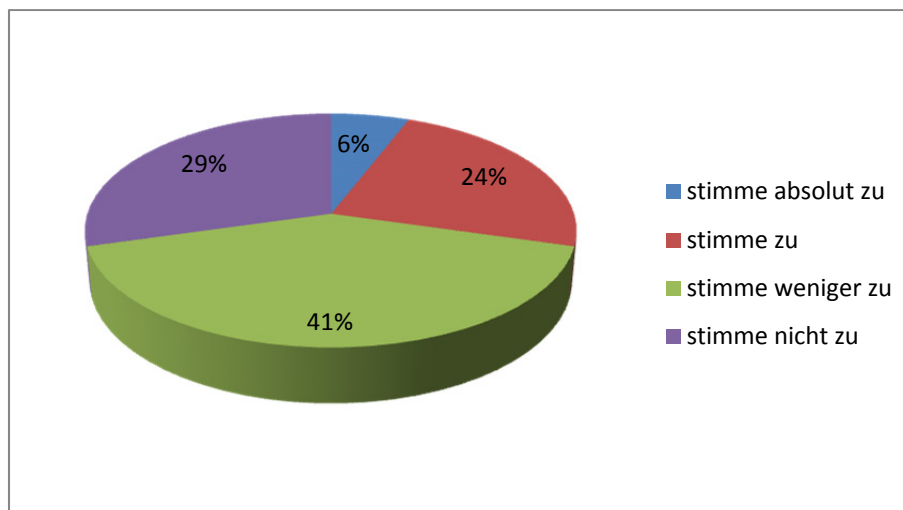


Abbildung 11: Auswertung These 2 Aussage 4

65% der Befragten stimmten der Aussage „Verschiedene Geräte erfordern unterschiedliche Administration (z. B. Sicherheitseinstellungen (z. B. aktueller Virens Scanner) müssen für jedes Gerät vorgenommen werden).“ voll zu. Die Gesamte Zustimmung liegt bei deutlichen 71%.

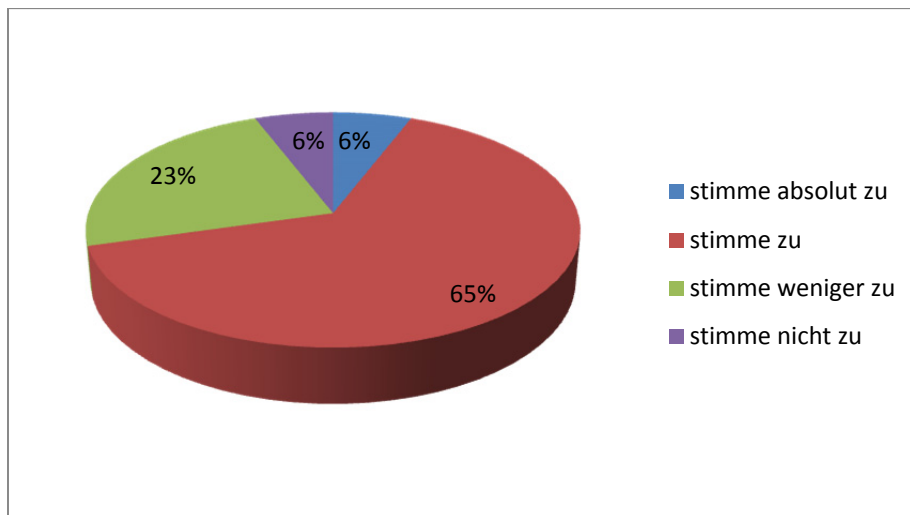


Abbildung 12: Auswertung These 2 Aussage 5

Die Auswertung der vorletzten Aussage „Im Fehlerfall (Supportanfragen) müssen produktindividuelle Lösungen gefunden werden.“ zeigt sehr deutlich, dass eine heterogene IT-Landschaft durch BYOD einen Mehraufwand mit sich bringt. Dem stimmen 65% der Teilnehmer zu.

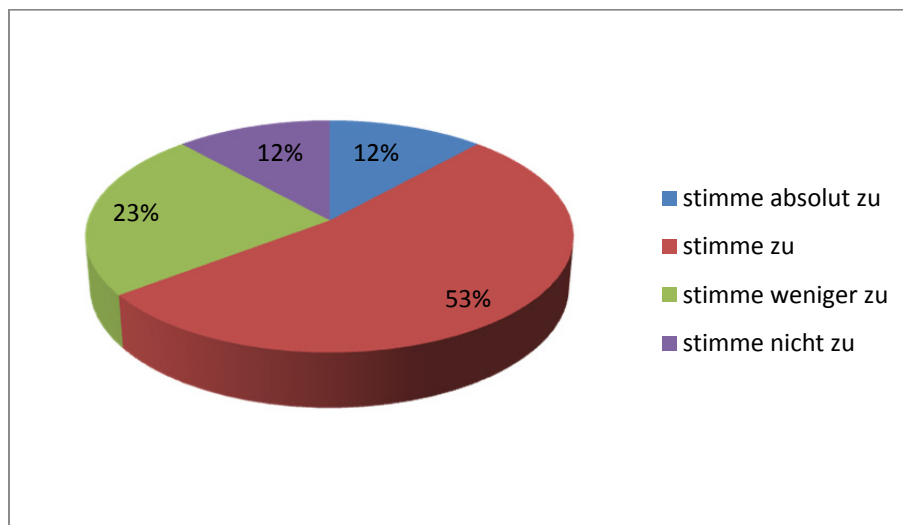


Abbildung 13: Auswertung These 2 Aussage 6

Aus der Abbildung 14 wird das Ergebnis der Aussage „Durch den Einsatz von unterschiedlichen Mobilgeräten muss die Absicherung des Firmennetzwerks (z. B. eigene DMZ für BYOD Geräte) neu geplant werden.“ deutlich. In Summe stimmten 71% der Befragten dieser Aussage zu.

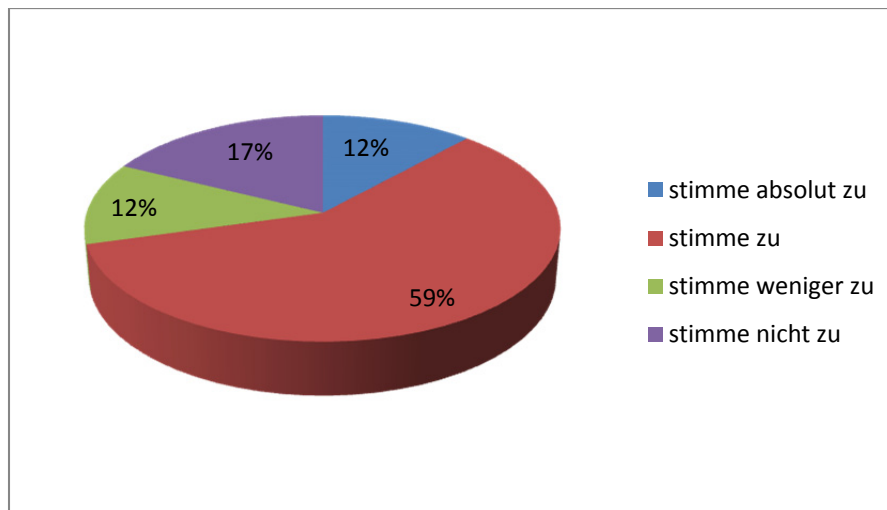


Abbildung 14: Auswertung These 2 Aussage 7

4.3 Bewertung der dritten These

Die Mehrheit der Befragten ist der Meinung, dass ByoD im Unternehmensumfeld nicht als Technologietreiber fungiert. Ein Punkt, der durch den vermehrten Einsatz von Smartphones und Tablets in der Unternehmensinfrastruktur eine Rolle spielt, ist der Ausbau von WLANs. Nur mit WLAN können auf ByoD Geräten praktikabel Anwendungen und Informationen schnell abgerufen werden. Das dennoch weniger Zustimmung bei dieser These vorhanden ist (41% der Befragten), liegt eventuell daran, dass viele Unternehmen ohnehin bereits ein WLAN im Einsatz haben. Dadurch ist eine wichtige Grundlage gegeben. Auch ist der Zugriff via VPN auf das Unternehmensnetzwerk in vielen Unternehmen bereits Standard und somit sind keine zusätzlichen Investitionen zu tätigen, denn die nötige Konfiguration der Client Geräte stellt keine besonderen Anforderungen an die Infrastruktur dar. Der Nutzen von neuen Technologien wie NFC ist bisher noch nicht in der Breite angekommen, weswegen an dieser Stelle weniger investiert wird.

Die Auswertungen der Aussagen der dritten These können folgend entnommen werden:

Die erste Aussage „Die IT-Infrastruktur wird durch die Anforderung an den Einsatz von BYOD flexibler.“ wurde in Summe von 47% der Teilnehmer abgelehnt. Nur 12% stimmten der Aussage absolut zu.

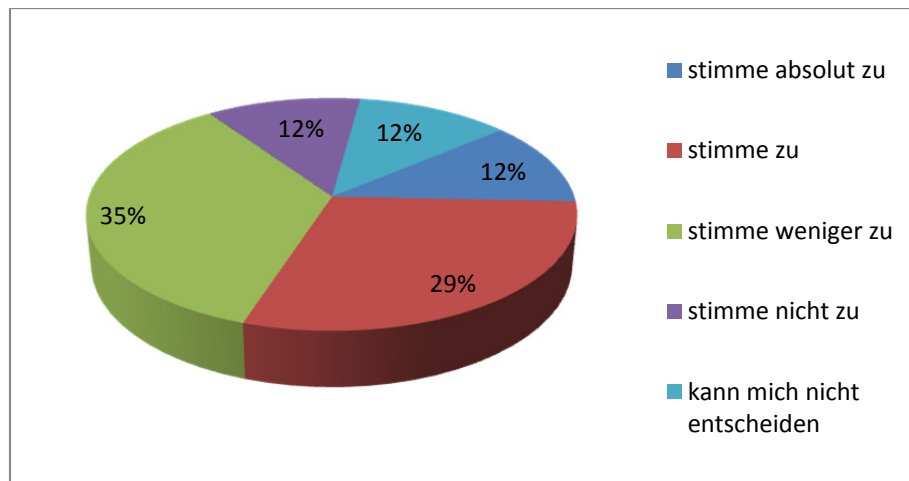


Abbildung 15: Auswertung These 3 Aussage 1

Die Abbildung 16 zeigt die Auswertung der Aussage „BYOD ist ein Grund, den Fernzugriff (VPN) in das Unternehmensnetzwerk zu ermöglichen.“. Es ist deutlich erkennbar, dass die Mehrheit (71%) der Umfrageteilnehmer dieser Aussage zustimmen.

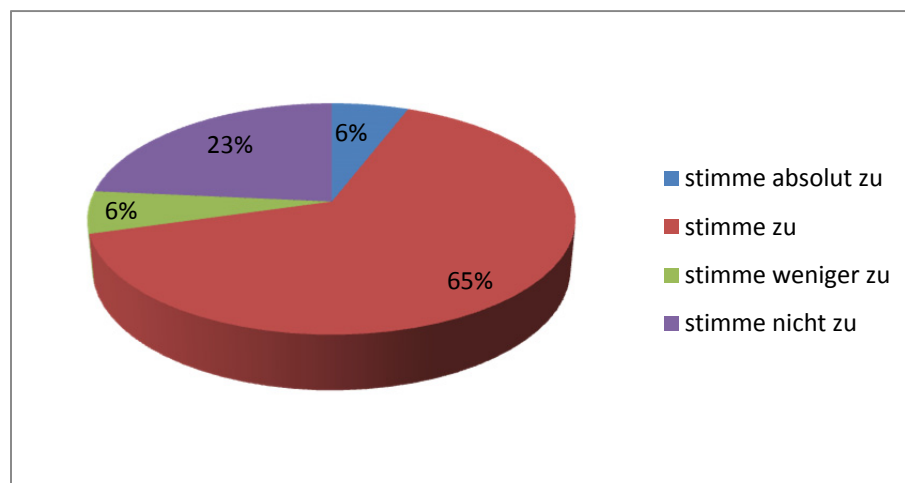


Abbildung 16: Auswertung These 3 Aussage 2

Die Aussage „Neue Technologien (z. B. Einsatz von NFC) können durch BYOD schneller in bestehende Strukturen eingebettet werden.“ wurde in Summe mit 58% abgelehnt. Dies könnte ein Indiz dafür sein, dass bestehende Geschäftsprozesse, auch wenn neue Technologien durch BYOD vorhanden sind, nicht flexibel genug sind diese mit Einzubinden.

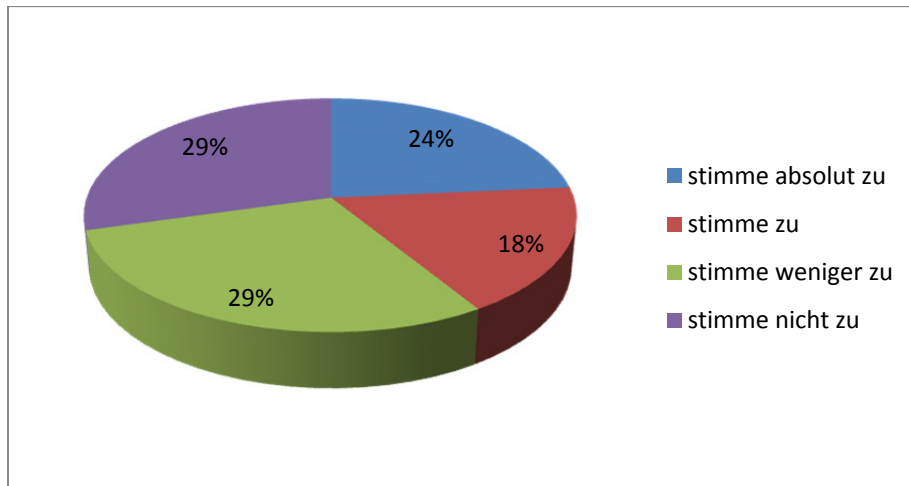


Abbildung 17: Auswertung These 3 Aussage 3

Bei der letzten Aussage der dritten These „Durch die Einführung von BYOD steigen die Investitionen in aktuelle Hard- und Software (z. B. WLAN Infrastruktur).“ konnten 12% der Befragten sich nicht entscheiden. 41% stimmten der Aussage zu, während 47% keine Zustimmung signalisieren konnten.

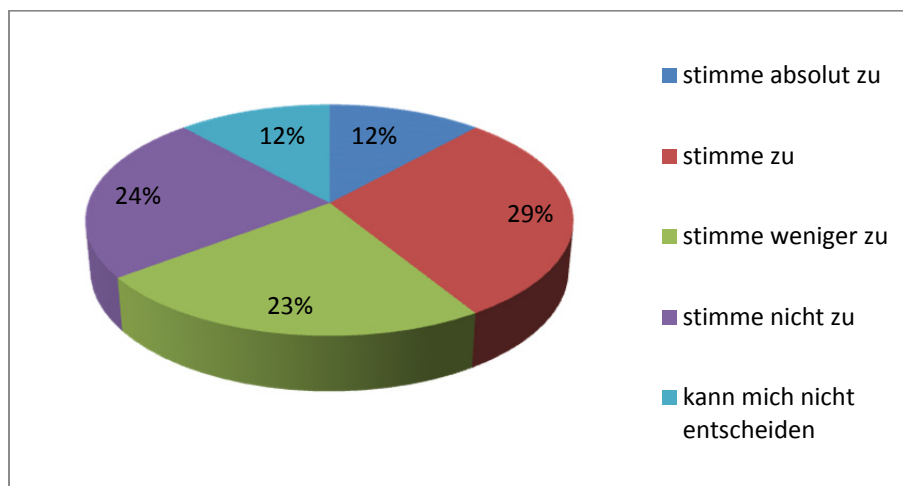


Abbildung 18: Auswertung These 3 Aussage 4

4.4 Bewertung der vierten These

Bei vielen Entscheidungen im Unternehmen, müssen diverse rechtliche Vorschriften beachtet werden. Auch die Nutzung von ByoD muss geprüft werden, damit keine rechtlichen Konsequenzen zu erwarten sind. Dies wird auch von den Studienteilnehmern so gesehen. Von einem Zugriff auf ein ByoD Gerät durch Dritte (z. B. Familienangehörigen) ist auszugehen, weswegen immer die Gefahr besteht, dass Einsicht in Firmendaten genommen werden kann. Des Weiteren besteht die Gefahr, dass Anwendungen, welche im Hintergrund aktiv sind, Informationen auslesen. Eine Speicherung von Daten in der Cloud sollte unbedingt nach den

Vorgaben des Bundesdatenschutzgesetzes (BDSG) geschehen. Bei lokaler Speicherung ist eine Trennung von privaten und Unternehmensdaten von Vorteil. Neben der Trennung der Daten ist es auch wichtig, die Arbeitszeit von der Freizeit zu trennen. Beispielsweise bei der Nutzung eines Mobiltelefons lässt es die Konfiguration für gewöhnlich nicht zu, bei der Zustellung zwischen dienstlichen und privaten Anrufen und E-Mails nach einer bestimmten Uhrzeit zu unterscheiden. Hier ist ByoD ein Nachteil für den Mitarbeiter, welcher außerhalb der Dienstzeit leichter für das Unternehmen tätig werden kann, ohne dass er dafür extra vergütet wird. 52% der Teilnehmer stimmen zu, dass es schwer ist, eine klare Trennung von privater und dienstlicher Nutzung festzulegen. Wichtig sind verbindliche Vereinbarungen zwischen Arbeitgeber und Arbeitnehmer, um juristische Probleme auszuschließen.

Die Auswertungen der Aussagen der vierten These können folgend entnommen werden:

Wie aus der Abbildung 19 ersichtlich, stimmen 29% der Befragten der Aussage „Durch BYOD besteht die Gefahr, dass unberechtigte Dritte Zugriff auf interne Informationen erhalten.“ absolut zu. Weitere Zustimmung kommt von 47% der Befragten. Nur 18% sind der Meinung, dass interne Informationen vor dem Zugriff Dritter geschützt sind.

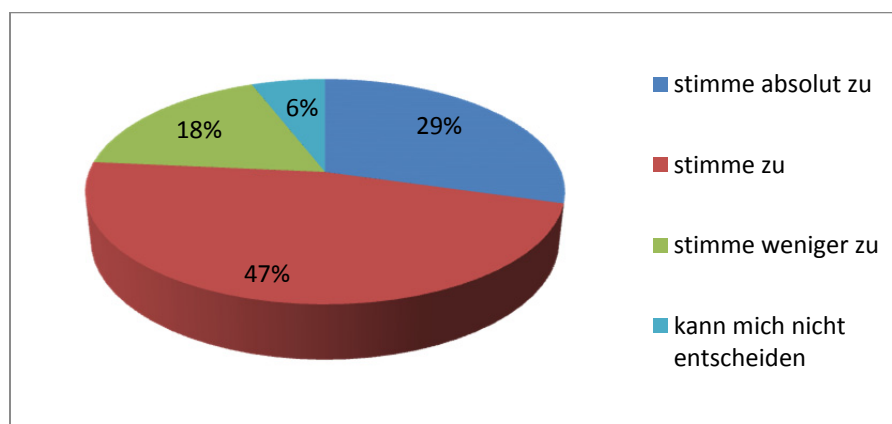


Abbildung 19: Auswertung These 4 Aussage 1

Die Resultate der Aussage „Eine Fernlöschung bei Verlust des privaten Gerätes, ist aufgrund des BDSG nicht zulässig.“ sind eindeutig. Summiert sprechen sich 53% gegen die Aussage aus. Nur 35% der Befragten stimmen zu.

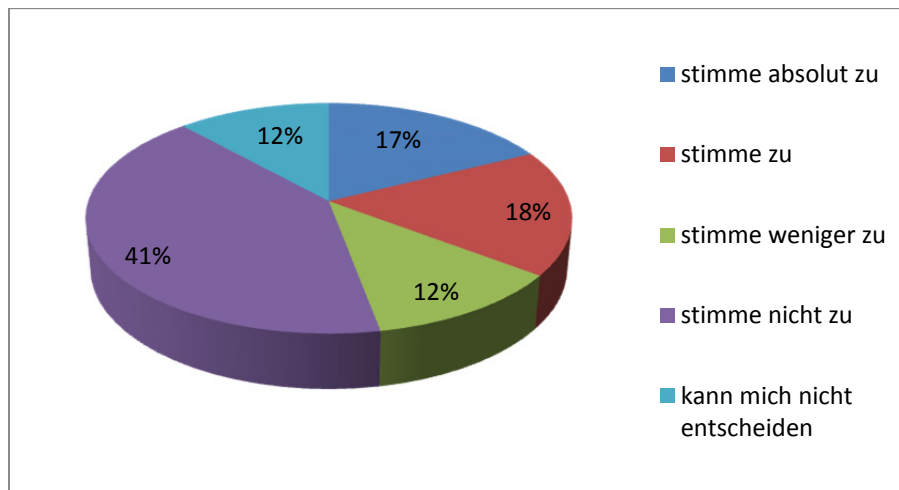


Abbildung 20: Auswertung These 4 Aussage 2

Die Auswertung der Aussage „Durch die ständige Erreichbarkeit des Mitarbeiters auf dem beruflich genutzten privaten Gerät wird die Einhaltung des Arbeitszeitgesetzes erschwert.“ zeigt, dass nur eine knappe Mehrheit von 52% die Gefahr eines Arbeitszeitverstoßes ernst nimmt. 32% sehen keine Kollisionen mit dem Arbeitszeitgesetz. Die Gründe hierfür können beispielsweise bereits getroffene Regelungen mit dem Mitarbeiter sein.

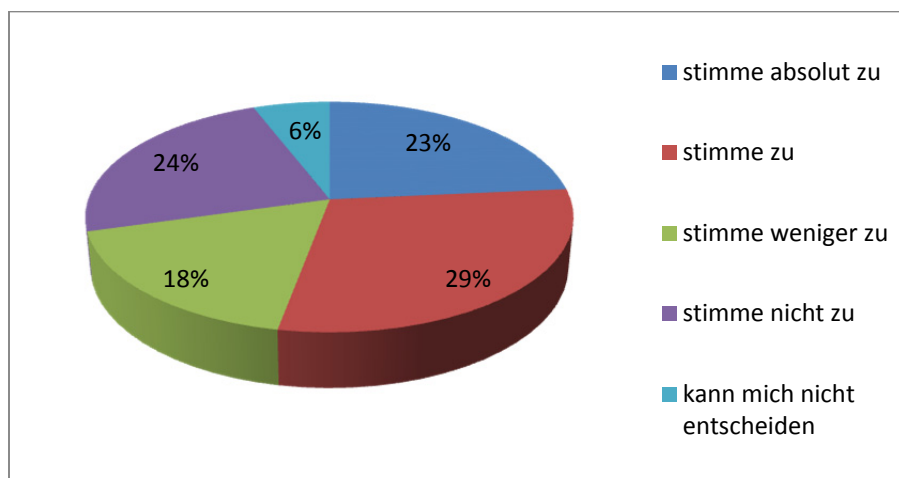


Abbildung 21: Auswertung These 4 Aussage 3

Aus der folgenden Abbildung, welche die Ergebnisse der Aussage „Informationen können von privaten Anwendungen (Apps) ausgelesen und entgegen bestehender Verträge (z. B. NDA) verbreitet werden.“ darstellt, kann entnommen werden, dass nur 30% der Aussage widersprechen. 64% hingegen stimmten der Aussage zu.

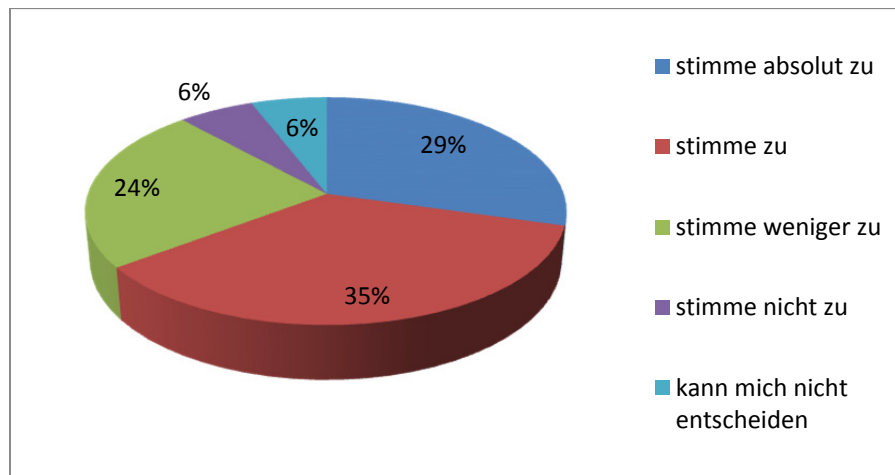


Abbildung 22: Auswertung These 4 Aussage 4

Die Ergebnisse der fünften Aussage dieser These, „Wenn Daten außerhalb von Deutschland gespeichert und verarbeitet werden, müssen besondere gesetzliche Vorschriften beachtet werden.“, sind einheitlich. Eine Zustimmung von insgesamt 88% ist zu vernehmen.

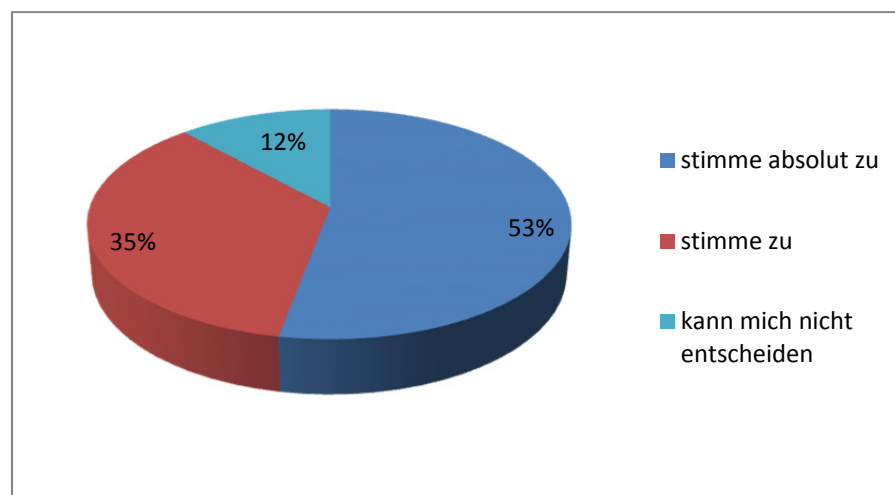


Abbildung 23: Auswertung These 4 Aussage 5

Bei der vorletzten Behauptung, „Die strikte Trennung von Unternehmensdaten und privaten Daten ist gesetzlich erforderlich.“ sind die Befragten zu 24% unentschlossen. 52% stimmten zu, dass eine Trennung der Daten gesetzlich sinnvoll wäre. Um eine einheitliche Trennung der Daten zu gewährleisten, ist eine Plattformüberprüfung von mobilen Geräten erforderlich.

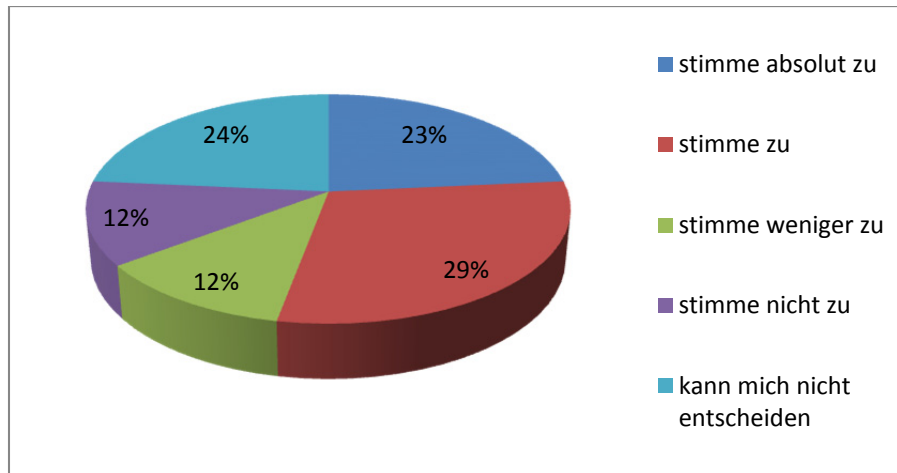


Abbildung 24: Auswertung These 4 Aussage 6

Die letzte Aussage dieser These, „Die Kontrolle durch das Unternehmen, ob ein BYOD-Nutzer die Governance und Compliance Standards einhält, ist nicht möglich.“ erhält eine Zustimmung von 47%. 53% hingegen denken, dass die Governance und Compliance Standards im Unternehmen nicht eingehalten werden können.

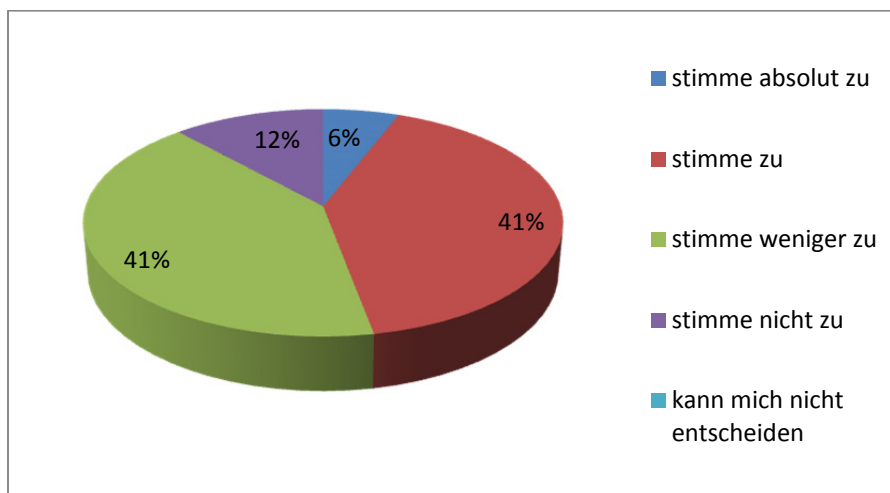


Abbildung 25: Auswertung These 4 Aussage 7

4.5 Bewertung der fünften These

Nachdem es in der ITK-Branche einen Mangel an qualifiziertem Personal gibt²², müssen Unternehmen Möglichkeiten eruieren, Fachkräfte für sich zu gewinnen. Eine dieser Möglichkeiten ist das Werben mit ByoD als zusätzlichen Anreiz. ByoD soll Interessierten zeigen, dass sich das Unternehmen mit aktuellen Trends beschäftigt und diese den Mitarbeitern auch zur Nutzung frei gibt. Dass ByoD zumindest einen Beitrag zum Recruitment liefert, wurde auch von den Umfrageteilnehmern bestätigt. Während des Recruitingprozesses können die Vor-

²² Vgl. Handelsblatt (2013).

teile für den künftigen Mitarbeiter dargestellt werden, wie z. B. das private Gerät auch dienstlich weiter zu nutzen um einer Umgewöhnung zu entgehen, was 64% der Befragten positiv aufnehmen. Der Arbeitgeber hat hier den Vorteil, dass er keine Arbeitszeitverluste verbuchen muss. Für den Mitarbeiter können auch monetäre Gründe für ByoD sprechen, wobei für den Einzelfall zu klären ist, ob es eine Einmalzahlung oder eine fortlaufende Zahlung gibt. Eine faire Beteiligung ist für das Arbeitsverhältnis förderlich und verbessert gleichzeitig das Image des Unternehmens. Auf diesem Weg entsteht eine Win-Win-Situation für beide Seiten. Viele, gerade junge Absolventen, besitzen hochwertige und teure Technik. Dies ist ein Punkt, an dem ByoD ansetzen kann, denn das private Gerät wäre redundant zu einem geschäftlichen und die ursprüngliche Investition vergebens. Dass ByoD im Recruitment hilft, Talente anzuwerben sehen nur 24% der Studienteilnehmer.

Die Auswertungen der Aussagen der fünften These können folgend entnommen werden:

Aus den Ergebnissen der Aussage „Das bekannte und vertraute Gerät im betrieblichen Umfeld zu nutzen, schafft einen zusätzlichen Anreiz.“ kann abgelesen werden, dass 64% der Befragten gerne mit der individuell bekannten Plattform arbeiten.

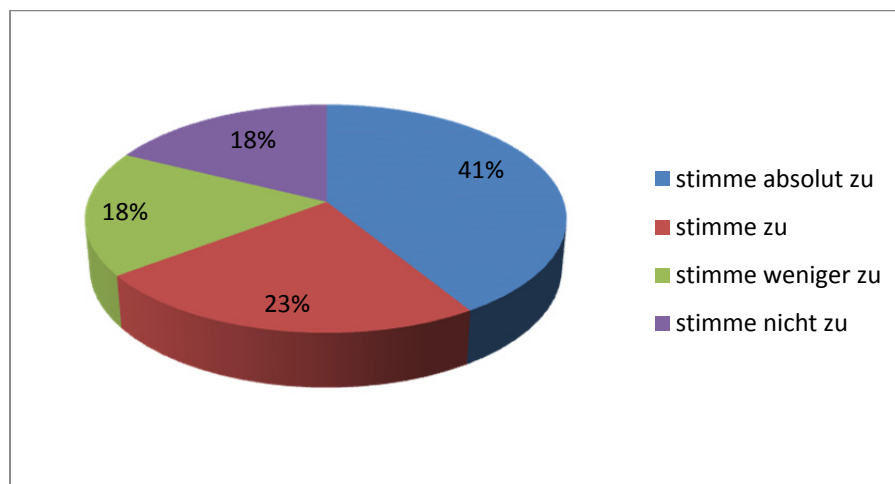


Abbildung 26: Auswertung These 5 Aussage 1

Aus der Abbildung 27 wird ersichtlich, wie die Ergebnisse der Aussage „Mitarbeiter, welche mit ihrem gewohnten Gerät(en) arbeiten, sind produktiver.“ Ausfallen. Es wird sichtbar, dass 59% dieser Aussage zustimmen.

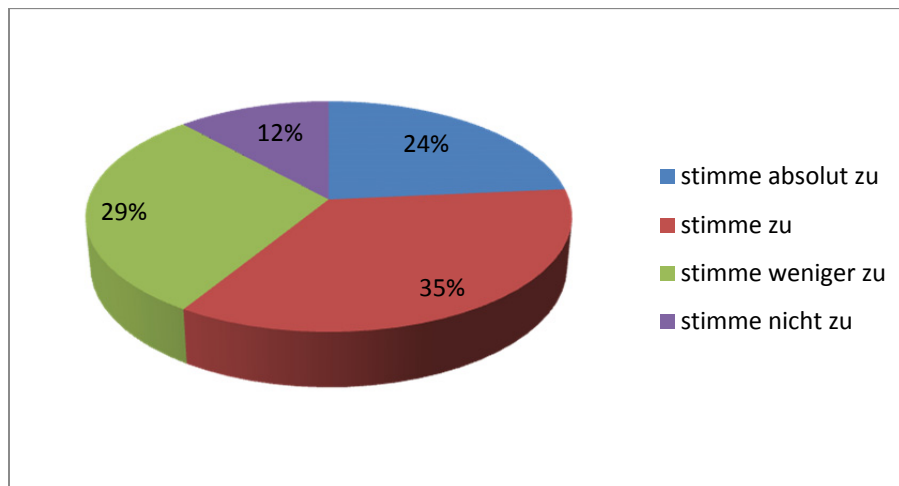


Abbildung 27: Auswertung These 5 Aussage 2

Die Auswertung der Aussage, „Eine Beteiligung seitens des Unternehmens an den monatlichen Gebühren (Handy-Vertrag, Ratenzahlung bei Laptops) bietet einen Anreiz, sich für das Unternehmen als Arbeitgeber zu entscheiden.“ zeigt, dass 58% eine finanzielle Beteiligung an monatlichen oder einmaligen Kosten für richtig befinden, um neue Mitarbeiter für das Unternehmen anzuwerben.

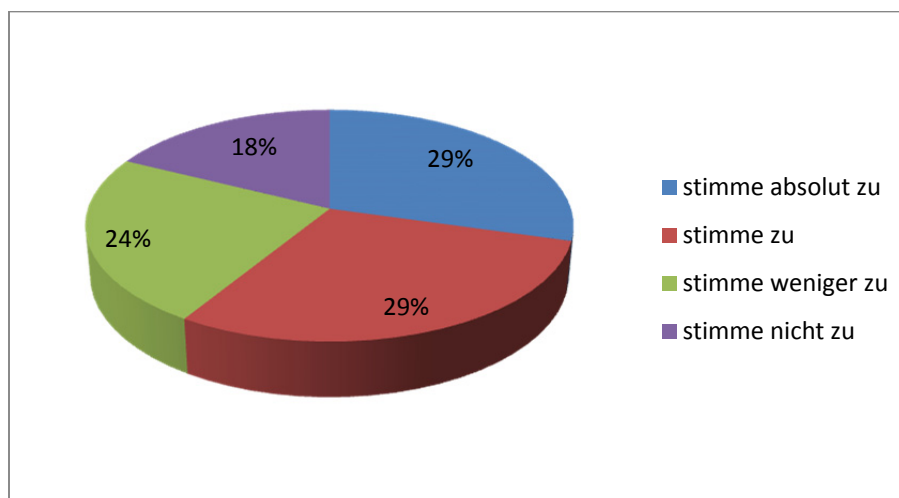


Abbildung 28: Auswertung These 5 Aussage 3

Die Ergebnisse der Aussage „BYOD hilft dem Unternehmen, das eigene Image und die Employer Brand zu verbessern.“ zeigen, dass mit 59% die Mehrheit der Meinung ist, dass die Employer Brand durch BYOD gesteigert wird.

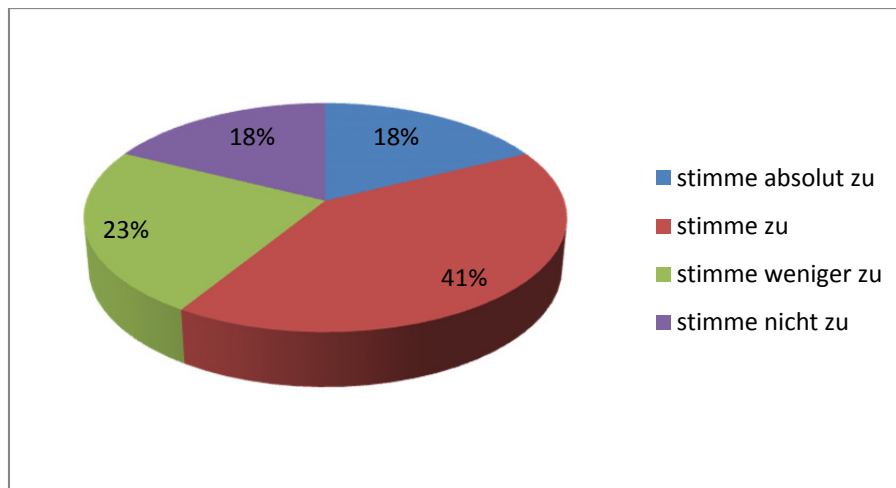


Abbildung 29: Auswertung These 5 Aussage 4

Die Abbildung 30 zeigt die Auswertung der Aussage „Durch BYOD wird das Interesse am Unternehmen von High Potentials gesteigert.“. Die Umfrageteilnehmer glauben zu 59% nicht, dass Unternehmen mit BYOD gefragte Mitarbeiter rekrutieren können.

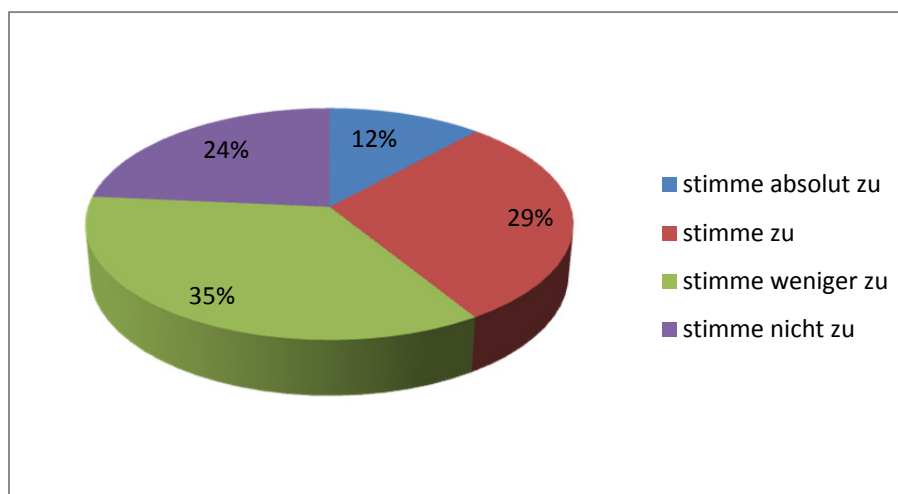


Abbildung 30: Auswertung These 5 Aussage 5

Der letzten Aussage „BYOD ist ein entscheidender Punkt im "war for talents".“ konnte die Mehrheit mit 70% nicht zustimmen. Lediglich 24% stimmten der Aussage zu.

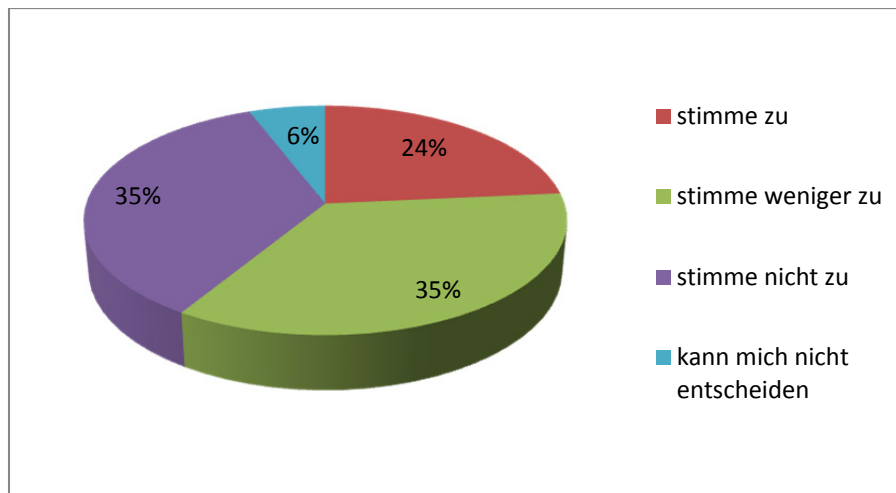


Abbildung 31: Auswertung These 5 Aussage 6

5. Zusammenfassung und Ausblick

Das Ziel des vorliegenden Beitrags war es, mit Hilfe einer empirischen Untersuchung den Einsatz und die Vor- und Nachteile von ByoD in deutschen Unternehmen zu erfassen. Darüber hinaus wurde der Fragestellung nachgegangen, warum der Einsatz von ByoD auf Zustimmung oder Ablehnung stößt. Dabei hat sich gezeigt, dass Bring your own Device in deutschen Unternehmen angewendet wird. Jedoch ist die Einführung und Nutzung von der Lösung sowohl individueller als auch allgemeiner Probleme abhängig. Es hat sich jedoch gezeigt, dass ByoD trotz vorhandener und wahrgenommener Risiken eingesetzt wird.

Von einer flächendeckenden Nutzung ist trotzdem nicht zu sprechen, denn 49% der befragten Personen verneinten die Frage nach der ByoD Nutzung. Die Gründe hierfür sind unter anderem IT-Sicherheit, rechtliche Fragestellungen oder Lizenz Probleme. Die Ergebnisse der Umfrage zeigen, dass ByoD in den Unternehmen nicht als Technologietreiber für die Unternehmensinfrastruktur angesehen wird. Dem gegenüber wird die IT-Sicherheit als gefährdet angesehen. Des Weiteren sehen die Unternehmen einen erhöhten Aufwand im Support der IT-Geräte, welche zusätzlich in die IT-Infrastruktur eingebunden werden müssen. Zwar können durchaus juristische Probleme bei dem Einsatz von ByoD auftreten, allerdings ergeben sich Vorteile bei der Rekrutierungsunterstützung. Generell hängt der Nutzen von ByoD für das Unternehmen von den Regelungen ab, welche in diesem Zusammenhang getroffen werden.

Weiterer Forschungsbedarf zu ByoD besteht, zum Beispiel um die Einstellung der Mitarbeiter gegenüber ByoD zu untersuchen. So sind die Gründe, welche für oder gegen eine Entschei-

dung zur Nutzung von Bring Your own Device bei Mitarbeitern sprechen, nicht hinreichend untersucht. Eine branchenfokussierte Betrachtung kann Hinweise liefern, in welchen Branchen Unternehmen eher bereit sind, Trends und Neuerungen in die Geschäftsabläufe zu integrieren. Abschließend lässt sich festhalten, dass ByoD, in Verbindung mit Mobile Device Management, für das Unternehmen Vorteile bieten kann. Um den Support zu erleichtern kann es langfristig von Vorteil sein, nur bestimmte Geräte für ByoD zuzulassen. Außerdem ist das Alter der Geräte ein entscheidender Faktor, damit keine Sicherheitslücken entstehen. Ein weiterer maßgeblicher Punkt für den Erfolg von ByoD ist die Akzeptanz der Mitarbeiter. Diese sollten selbst und ohne Beeinflussung entscheiden, ob sie ByoD nutzen oder auf ein firmeneigenes Gerät zurückgreifen wollen.

Abbildungsverzeichnis

Abbildung 1: Auswertung These 1 Aussage 1	10
Abbildung 2: Auswertung These 1 Aussage 2	10
Abbildung 3: Auswertung These 1 Aussage 3	11
Abbildung 4: Auswertung These 1 Aussage 4	11
Abbildung 5: Auswertung These 1 Aussage 5	12
Abbildung 6: Auswertung These 1 Aussage 6	12
Abbildung 7: Auswertung These 1 Aussage 7	13
Abbildung 8: Auswertung These 2 Aussage 1	14
Abbildung 9: Auswertung These 2 Aussage 2	14
Abbildung 10: Auswertung These 2 Aussage 3	15
Abbildung 11: Auswertung These 2 Aussage 4	15
Abbildung 12: Auswertung These 2 Aussage 5	16
Abbildung 13: Auswertung These 2 Aussage 6	16
Abbildung 14: Auswertung These 2 Aussage 7	17
Abbildung 15: Auswertung These 3 Aussage 1	18
Abbildung 16: Auswertung These 3 Aussage 2	18
Abbildung 17: Auswertung These 3 Aussage 3	19
Abbildung 18: Auswertung These 3 Aussage 4	19
Abbildung 19: Auswertung These 4 Aussage 1	20
Abbildung 20: Auswertung These 4 Aussage 2	21
Abbildung 21: Auswertung These 4 Aussage 3	21
Abbildung 22: Auswertung These 4 Aussage 4	22
Abbildung 23: Auswertung These 4 Aussage 5	22
Abbildung 24: Auswertung These 4 Aussage 6	23
Abbildung 25: Auswertung These 4 Aussage 7	23
Abbildung 26: Auswertung These 5 Aussage 1	24
Abbildung 27: Auswertung These 5 Aussage 2	25
Abbildung 28: Auswertung These 5 Aussage 3	25
Abbildung 29: Auswertung These 5 Aussage 4	26
Abbildung 30: Auswertung These 5 Aussage 5	26
Abbildung 31: Auswertung These 5 Aussage 6	27

Literaturverzeichnis

- Arns, T. (2013): Leitfaden Social Media. <http://www.bitkom.org/files/documents/leitfadensocialmedia2012%281%29.pdf> (Abgerufen am 21.03.2013).
- Bortz, J.; Döring, N. (2006): Forschungsmethoden und Evaluation : für Human- und Sozialwissenschaftler. 4., überarb. Aufl. Berlin; Heidelberg : Springer (Springer-Lehrbuch), 2006
- Ballagas, R.; Rohs, M.; Sheridan, J.; Borchers, J. (2004):BYOD: Bring Your own Device. In: Proceedings of the Workshop on Ubiquitous Display Environments, Ubicomp, 2004.
- Burnham, K. (2012): 4 Personas of the Next-Generation CIO. URL: http://www.cio.com/article/671573/4_Personas_of_the_Next_Generation_CIO. Abrufdatum: 28.03.2012.
- Bundesamt für Justiz (1994): Arbeitszeitgesetz 21.07.2012. http://www.gesetze-im-internet.de/arbzg/___3.html (Abgerufen am 22.03.2013).
- Dufft, N.; Flug, M.; Niemann, F.: Enterprise(2001): Mobility 2011 – Bestandsaufnahme und Investitionspläne in deutschen Unternehmen, www.berlecon.de/studien/downloads/PAC_Berlecon_EnterpriseMobility2011.pdf. Abrufdatum: 28.03.2013.
- Eikenberg, R.(2012): Android-Malware öffnet Hintertür ins Intranet. heise Security. 03.05.2012. <http://heise.de/-1566356> (Abgerufen am 22.03.2013).
- Gartner(2013) IT-Glossary. <http://www.gartner.com/it-glossary/bring-your-own-device-byod> (Abgerufen am 27.05.2013).
- Gatermann, M. (2011): Was Arbeitgeber Bewerbern bieten müssen. In: managermagazin online. 22.11.2011. <http://www.manager-magazin.de/magazin/artikel/0,2828,796972,00.html> (Abgerufen am 22.03.2013).
- Gertz, W. (2007): Millennials - was der Nachwuchs wirklich will. In: COMPUTERWOCHE. 28.02.2007. <http://www.computerwoche.de/a/millennials-was-der-nachwuchs-wirklich-will,588806> (Abgerufen am 27.05.2013).
- Handelsblatt (2013): Warnung vor Fachkräftemangel. In: Handelsblatt 04.03.2013. <http://www.handelsblatt.com/politik/deutschland/it-branche-ist-job-motor-warnung-vor-fachkraeftemangel/7874984.html> (Abgerufen am 21.03.2013).
- LimeSurvey (2013): LimeSurvey. <https://www.limesurvey.org/de/> (Abgerufen am 27.05.2013).
- Liebold, R.; Trinczek, R. (2002): Experteninterviews. In: Kühl, S.; Strodtholz, P. (Hrsg.): Methoden der Organisationsforschung : Ein Handbuch. Hamburg : Rowolt Taschenbuch Verlag, 2002, S. 33-71
- Meuser, M.; Nagel, U. (2005): ExpertInneninterview - vielfach erprobt, wenig bedacht : Ein Beitrag zur qualitativen Methodendiskussion. In: Bogner, A.; Littig, B.; Menz, W. (Hrsg.): Das Experteninterview : Theorie, Methode und Anwendung. 2. Aufl. Wiesbaden : Verlag für Sozialwissenschaften, 2005, S. 71-94
- Neugebauer, L. (2013): Die zehn größten Gefahren im Internet. 04.03.2013. https://www.bitkom.org/de/presse/8477_74922.aspx (Abgerufen am 22.03.2013).

- Werle, K. (2012): Die Generation Y ändert die Unternehmen. In: KarriereSPIEGEL. 09.08.2012. <http://www.spiegel.de/karriere/berufsstart/generation-y-audi-personalvorstand-thomas-sigi-im-interview-a-848764.html> (Abgerufen am 22.03.2013).
- Winter, S. (2000): Quantitative vs. Qualitative Methoden. 15.05.2000. https://imihome.imi.uni-karlsruhe.de/nquantitative_vs_qualitative_methoden_b.html (Abgerufen am 22.03.2013).

Anhang: Rohdaten der Umfrage (bereinigt von Leereinträgen)

id	Wie viele Mitarbeiter hat Ihr Unternehmen?	In welcher Branche ist Ihr Unternehmen tätig?	Wie hoch ist der Jahresumsatz Ihres Unternehmens?	Wie ist Ihr Unternehmen geografisch aufgestellt?	Nutzen Sie BYOD in Ihrem Unternehmen?	Ist die Einführung von BYOD in Ihrem Unternehmen geplant?
1	<50	Informationstechnologie	Unbekannt	Regional	Ja	N/A
2	<50	Sonstige	< 2 Mio. €	National	Ja	N/A
3	<250	Finanzen	< 10 Mio. €	Global	Nein	Ja
4	<5000	Informationstechnologie	> 50 Mio. €	Global	Ja	N/A
5	>5000	Informationstechnologie	> 50 Mio. €	Global	Ja	N/A
6	<250	Informationstechnologie	< 50 Mio. €	Regional	Ja	N/A
7	<250	Informationstechnologie	Unbekannt	Global	Ja	N/A
8	<250	Informationstechnologie	< 10 Mio. €		Ja	N/A
9	<250	Automobil	< 10 Mio. €	National	Ja	N/A
10	<500	Finanzen	> 50 Mio. €	Global	Nein	Nein
11	<50	Informationstechnologie	< 2 Mio. €	National	Nein	Ja
12	<500	Informationstechnologie	> 50 Mio. €	National	Nein	Nein
13	<50	Informationstechnologie	Unbekannt	National	Ja	N/A
14	<1000	Informationstechnologie	> 50 Mio. €	National	Ja	N/A
15	<50	Sonstige	< 2 Mio. €	National	Ja	N/A
16	>5000	Informationstechnologie	Unbekannt	Global	Ja	N/A
17	>5000	Elektroindustrie	> 50 Mio. €	Global	Nein	Ja
18	<500	Informationstechnologie	> 50 Mio. €	Global	Ja	N/A
19	>5000	Sonstige	> 50 Mio. €	Global	Nein	Nein
20	>5000	Informationstechnologie	> 50 Mio. €	Global	Nein	Nein
21	<50	Informationstechnologie	< 10 Mio. €	National	Ja	N/A
22	>5000	Informationstechnologie	> 50 Mio. €	Global	Nein	Nein
23	<50	Informationstechnologie	< 2 Mio. €	National	Ja	N/A
24	<5000	Informationstechnologie	> 50 Mio. €	Global	Nein	Nein

25	<50	Sonstige	< 10 Mio. €	Regional	Nein	Nein
26	<5000	Gesundheit	> 50 Mio. €	Global	Ja	N/A
27	<5000	Sonstige	Unbekannt	Global	Nein	Nein
28	<500	Finanzen	< 50 Mio. €	Global	Nein	Nein
29	>5000	Informationstechnologie	> 50 Mio. €	Global	Ja	N/A
30	<1000	Finanzen	> 50 Mio. €	Regional	Nein	Ja
31	<50	Informationstechnologie	< 10 Mio. €	Global	Ja	N/A
32	<50	Informationstechnologie	< 10 Mio. €	National	Ja	N/A
33	<1000	Informationstechnologie	< 50 Mio. €	National	Ja	N/A
34	<5000	Sonstige	> 50 Mio. €	Regional	Nein	Ja
35	>5000	Automobil	> 50 Mio. €	Global	Nein	Ja
36	>5000	Sonstige	> 50 Mio. €	Global	Nein	Nein
37	<5000	Informationstechnologie	> 50 Mio. €	Global	Nein	Nein
38	>5000	Automobil	> 50 Mio. €	Global	Nein	Nein
39	>5000	Automobil	> 50 Mio. €	Global	Nein	Ja
40	<50	Sonstige	< 2 Mio. €	Regional	Nein	Ja
41	<250	Informationstechnologie	< 50 Mio. €	National	Nein	Nein
42	<500	Informationstechnologie	> 50 Mio. €	Global	Ja	N/A
43	>5000	Informationstechnologie	> 50 Mio. €	Global	Ja	N/A
44	<250	Elektroindustrie	< 50 Mio. €	National	Ja	N/A
45	<50	Informationstechnologie	< 2 Mio. €	Global	Ja	N/A
46	<250	Informationstechnologie	< 50 Mio. €	National	Nein	Ja
47	<250	Sonstige	< 50 Mio. €	National	Nein	Nein
48	<250	Gesundheit	< 10 Mio. €	Regional	Nein	Nein
49	<1000	Informationstechnologie	> 50 Mio. €	Global	Ja	N/A
50	<5000	Finanzen	> 50 Mio. €	National	Nein	Ja
51	<5000	Finanzen	< 10 Mio. €	National	Ja	N/A

id	Wie lange ist BYOD in Ihrem Unternehmen im Einsatz?	Nutzen Sie die Mobile Device Management Lösungen Ihres ERP-Systems?	Welches ERP-System nutzen Sie?	In welchem Unternehmen sind Sie tätig?
1	seit einem bis zwei Jahren	Nein		selbstständig
2	seit unter einem Jahr	Nein		
3		N/A		nicht genannt
4	seit einem bis zwei Jahren	Nein		
5	seit zwei bis drei Jahren	Nein		
6	seit über drei Jahren	Nein		
7	seit über drei Jahren	Nein		
8	seit unter einem Jahr	Nein		
9	seit unter einem Jahr	Nein		
10		N/A		
11		N/A		
12		N/A		
13	seit über drei Jahren	Nein		
14	seit einem bis zwei Jahren	Nein		
15	seit unter einem Jahr	Nein		
16	seit einem bis zwei Jahren	Ja		
17		N/A		
18	seit zwei bis drei Jahren	Nein		
19		N/A		
20		N/A		
21	seit einem bis zwei Jahren	Nein		
22		N/A		
23	seit über drei Jahren	Nein		
24		N/A		

25		N/A		
26	seit einem bis zwei Jahren	Nein		
27		N/A		Forschungseinrichtung
28		N/A		
29	seit einem bis zwei Jahren	Nein		
30		N/A		
31	seit einem bis zwei Jahren	Nein		
32	seit über drei Jahren	Nein		
33	seit über drei Jahren	Nein		
34		N/A		öffentlicher Dienst, Gebietskörperschaft
35		N/A		
36		N/A		
37		N/A		
38		N/A		
39		N/A		
40		N/A		
41		N/A		
42	seit über drei Jahren	Nein		
43	seit einem bis zwei Jahren	Nein		
44	seit unter einem Jahr	Ja		
45	seit über drei Jahren	Nein		
46		N/A		
47		N/A		
48		N/A		
49	seit einem bis zwei Jahren	Nein		
50		N/A		
51	seit einem bis zwei Jahren	Nein		

id	Warum wird BYOD in Ihrem Unternehmen nicht eingesetzt?	These 1: Aussage 1	These 1: Aussage 2
1		stimme absolut zu	stimme absolut zu
2			
3	machen uns gedanken darüber		
4		stimme zu	stimme zu
5		stimme zu	stimme zu
6		stimme absolut zu	stimme weniger zu
7		stimme zu	stimme zu
8		stimme zu	stimme nicht zu
9			
10	Sicherheits- und Rechts-Problematik		
11	Wir sind dabei BYOD zu erörtern und zukünftig bei uns einzuführen. Es geht hier vor allem noch um Fragen der Sicherheit		
12			
13		stimme absolut zu	stimme zu
14		stimme absolut zu	stimme absolut zu
15		stimme weniger zu	stimme zu
16			
17			
18			
19	zu hoher Verwaltungsaufwand, IT-Sicherheits-relevante Probleme		
20	datensicherheit - automatisierte softwareupdates		
21		stimme weniger zu	stimme nicht zu
22	Weiß nicht		
23		stimme zu	stimme zu
24			

25	Unwissenheit		
26		stimme zu	stimme weniger zu
27	Geräte werden vom AG gestellt, d.h. es besteht kein Bedarf		
28	Aus datenschutz- und lizenzrechtlichen Gründen. Der Aufwand, entsprechende organisatorische Policies einzuführen, diese immer wieder zu prüfen und durchzusetzen, ist gemessen am Nutzen zu hoch. Vielmehr ist es weitaus kostengünstiger, einem Mitarbeiter ein Pad oder Mobiltelefon im Rahmen der (ausschließlich) betrieblichen Nutzung zu überlassen, als dessen privates Gerät zu kontrollieren und hierbei der Gefahr zu begegnen, unlizenzierte Software sowie Schadsoftware ins Haus zu holen. Viel Erfolg weiterhin mit ihrer Studie.		
29		stimme absolut zu	stimme zu
30	Sicherheitsbedenken, Kosten		
31		stimme absolut zu	stimme weniger zu
32		stimme zu	stimme zu
33			
34	derzeit Marktbeobachtung in Wirtschaft und ÖffDienst, rechtliche Entwicklung und Integration in die Arbeitsabläufe unter Berücksichtigung der Auswirkungen auf die IT-Fachabteilung		
35	Sicherheitstechnisch nicht vorbereitet...		
36	U		
37	Aktuell erfolgt die Ausstattung von Mitarbeitern mit Firmengeräten. Zum Teil setzen aber Mitarbeiter aber inoffiziell private Geräte, z.B. für das Abrufen von Emails ein, ohne, dass es eine Absprache mit der IT gibt.		
38			
39			
40	Bisher noch kein Mobile Device Management im Einsatz		
41	Unternehmen in der IT Sicherheitsberatung tätig und durch strikte Vorgaben kein BYOD möglich.		
42		stimme zu	stimme weniger zu
43		stimme zu	stimme nicht zu
44		stimme absolut zu	stimme absolut zu
45		stimme weniger zu	stimme weniger zu
46	Es ist eine gewisse Verunsicherung zu erkennen die sich aber in nächster Zeit abbauen wird, da bin ich mir sicher.		
47			
48	Weil die Sicherheit in den privat verwalteten Geräten nicht hoch genug ist		
49			
50			
51		stimme zu	stimme weniger zu

id	These 1: Aussage 3	These 1: Aussage 4	These 1: Aussage 5	These 1: Aussage 6	These 1: Aussage 7
1	stimme zu	stimme zu	stimme absolut zu	stimme absolut zu	stimme zu
2					
3					
4	stimme weniger zu	stimme absolut zu	stimme zu	stimme absolut zu	stimme weniger zu
5	stimme weniger zu	stimme weniger zu	stimme weniger zu	stimme weniger zu	stimme nicht zu
6	stimme zu	stimme absolut zu	stimme zu	stimme absolut zu	stimme absolut zu
7	stimme weniger zu	stimme zu	stimme zu	stimme zu	stimme nicht zu
8	stimme weniger zu	stimme weniger zu	stimme zu	stimme zu	stimme weniger zu
9					
10					
11					
12					
13	stimme absolut zu	stimme weniger zu	stimme zu	stimme absolut zu	stimme absolut zu
14	stimme nicht zu	stimme nicht zu	stimme absolut zu	stimme weniger zu	stimme absolut zu
15	stimme weniger zu	stimme weniger zu	stimme weniger zu	stimme weniger zu	stimme zu
16					
17					
18					
19					
20					
21	stimme nicht zu	stimme absolut zu	stimme nicht zu	stimme weniger zu	stimme zu
22					
23	stimme weniger zu	kann mich nicht entscheiden	stimme absolut zu	stimme absolut zu	stimme absolut zu
24					

25				
26	stimme weniger zu	stimme weniger zu	stimme absolut zu	stimme nicht zu
27				
28				
29	stimme zu	stimme absolut zu	stimme absolut zu	stimme weniger zu
30				
31	stimme nicht zu	stimme weniger zu	stimme absolut zu	stimme zu
32	stimme absolut zu	stimme weniger zu	stimme zu	stimme zu
33				
34				
35				
36				
37				
38				
39				
40				
41				
42	stimme zu	stimme zu	stimme absolut zu	stimme zu
43	stimme nicht zu	stimme nicht zu	stimme nicht zu	stimme nicht zu
44	stimme zu	stimme weniger zu	stimme weniger zu	stimme nicht zu
45	stimme nicht zu	stimme weniger zu	stimme zu	stimme zu
46				
47				
48				
49				
50				
51	stimme zu	stimme nicht zu	stimme zu	stimme zu

id	Welche (neuen) Probleme in der IT-Sicherheit sehen Sie, wenn BYOD eingesetzt wird?	These 2: Aussage 1	These 2: Aussage 2	These 2: Aussage 3	These 2: Aussage 4
1		stimme weniger zu	stimme zu	stimme weniger zu	stimme zu
2					
3					
4	Fehlende Trennung von Privat- und Firmennutzung, Probleme bei Ausfall des BYOD-Devices, Probleme bei der OS-Unterstützung.....	stimme weniger zu	stimme zu	stimme weniger zu	stimme weniger zu
5	Linzenzmanagement	stimme weniger zu	stimme weniger zu	stimme nicht zu	stimme weniger zu
6	zu heterogenes Umfeld. Nicht-Wartbarkeit. zu viele Betriebssysteme und damit Lücken in der Sicherheit	stimme weniger zu	stimme weniger zu	stimme nicht zu	stimme zu
7		stimme nicht zu	stimme zu	stimme nicht zu	stimme nicht zu
8		stimme nicht zu	stimme zu	stimme weniger zu	stimme weniger zu
9					
10					
11					
12					
13					
14	Datenschutz Datenverlust Saubere Trennung von privat Daten und Geschäftsdaten Saubere rechtliche Vereinbarungen mit dem Mitarbeiter Lizenzen auf den privateb Geräten	stimme weniger zu	stimme nicht zu	stimme nicht zu	stimme nicht zu
15					
16					
17					
18					
19					
20					
21	Verlust vertraulicher Daten, Zugriff auf Unternehmensinterna über verlorene oder gestohlene Geräte	stimme weniger zu	stimme nicht zu	stimme weniger zu	stimme weniger zu
22					
23		stimme weniger zu	stimme zu	stimme zu	stimme weniger zu
24					

25					
26		stimme absolut zu	stimme zu	stimme nicht zu	stimme nicht zu
27					
28					
29		stimme zu	kann mich nicht entscheiden	stimme zu	stimme absolut zu
30					
31		stimme weniger zu	stimme zu	stimme zu	stimme nicht zu
32		stimme weniger zu	stimme weniger zu	stimme nicht zu	stimme nicht zu
33					
34					
35					
36					
37					
38					
39					
40					
41					
42	Verlust von Unternehmensdaten bei lokaler Speicherung; höherer Aufwand der IT bei Wartung, damit höhere Kosten	stimme zu	stimme zu	stimme zu	stimme zu
43					
44		stimme zu	stimme weniger zu	stimme weniger zu	stimme weniger zu
45		stimme weniger zu	stimme zu	stimme weniger zu	stimme weniger zu
46					
47					
48					
49					
50					
51		stimme zu	stimme weniger zu	stimme weniger zu	stimme zu

id	These 2: Aussage 5	These 2: Aussage 6	These 2: Aussage 7	In welchen Bereichen ist der Aufwand durch BYOD in Ihrem Unternehmen gestiegen?
1	stimme zu	stimme zu	stimme zu	
2				
3				
4	stimme zu	stimme absolut zu	stimme absolut zu	Anfragen unerfahrener Nutzer zur Integration ihrer BYOD-Devices, Troubleshooting verschiedenster Plattformen, Erklärungsbedarf für nicht unterstützte Plattformen (Gründe dafür)
5	stimme weniger zu	stimme weniger zu	stimme weniger zu	
6	stimme weniger zu	stimme nicht zu	stimme zu	Bei Ausfällen ist kein Ersatz vorhanden -> Arbeitsausfall. BYOD bedeutet doch eigentlich nur, daß die Firma den Mitarbeiter dazu zwingt, sich selber sein Equipment zu besorgen, das er zum arbeiten braucht.
7	stimme zu	stimme zu	stimme zu	
8	stimme zu	stimme zu	stimme zu	
9				
10				
11				
12				
13				
14	stimme zu	stimme zu	stimme zu	Fehlersuche, Sicherheitsthemen
15				
16				
17				
18				
19				
20				
21	stimme weniger zu	stimme zu	stimme nicht zu	Support für mobilen Zugriff über Smartphones auf die Groupware des Unternehmens
22				
23	stimme zu	stimme weniger zu	stimme zu	
24				

25				
26	stimme nicht zu	stimme nicht zu	stimme zu	
27				
28				
29	stimme zu	stimme weniger zu	stimme weniger zu	
30				
31	stimme weniger zu	stimme weniger zu	stimme nicht zu	
32	stimme zu	stimme zu	stimme nicht zu	
33				
34				
35				
36				
37				
38				
39				
40				
41				
42	stimme zu	stimme zu	stimme zu	
43				
44	stimme zu	stimme zu	stimme absolut zu	
45	stimme zu	stimme zu	stimme zu	
46				
47				
48				
49				
50				
51	stimme absolut zu	stimme absolut zu	stimme zu	

id	These 3: Aussage 1	These 3: Aussage 2	These 3: Aussage 3	These 3: Aussage 4
1	stimme zu	stimme absolut zu	stimme absolut zu	kann mich nicht entscheiden
2				
3				
4	stimme weniger zu	stimme nicht zu	stimme weniger zu	stimme weniger zu
5	stimme weniger zu	stimme zu	stimme weniger zu	stimme nicht zu
6	stimme nicht zu	stimme zu	stimme nicht zu	stimme nicht zu
7	stimme zu	stimme zu	stimme zu	stimme nicht zu
8	stimme zu	stimme zu	stimme weniger zu	kann mich nicht entscheiden
9				
10				
11				
12				
13				
14	stimme nicht zu	stimme nicht zu	stimme nicht zu	stimme absolut zu
15				
16				
17				
18				
19				
20				
21	stimme zu	stimme zu	stimme weniger zu	stimme weniger zu
22				
23	stimme weniger zu	stimme zu	stimme nicht zu	stimme weniger zu
24				

25				
26	stimme weniger zu	stimme nicht zu	stimme weniger zu	stimme zu
27				
28				
29	kann mich nicht entscheiden	stimme zu	stimme absolut zu	stimme zu
30				
31	stimme weniger zu	stimme zu	stimme nicht zu	stimme zu
32	stimme zu	stimme nicht zu	stimme zu	stimme nicht zu
33				
34				
35				
36				
37				
38				
39				
40				
41				
42	stimme weniger zu	stimme zu	stimme nicht zu	stimme weniger zu
43				
44	stimme absolut zu	stimme zu	stimme absolut zu	stimme zu
45	stimme absolut zu	stimme zu	stimme absolut zu	stimme zu
46				
47				
48				
49				
50				
51	kann mich nicht entscheiden	stimme weniger zu	stimme zu	stimme absolut zu

id	In welchen Bereichen der Unternehmensinfrastruktur wurde aufgrund von BYOD investiert?	These 4: Aussage 1	These 4: Aussage 2
1		kann mich nicht entscheiden	stimme weniger zu
2			
3			
4		stimme absolut zu	stimme nicht zu
5	WLAN, Policy& Device Management	stimme zu	stimme nicht zu
6		stimme absolut zu	stimme absolut zu
7		stimme weniger zu	stimme nicht zu
8		stimme weniger zu	stimme nicht zu
9			
10			
11			
12			
13			
14	WLAN	stimme absolut zu	stimme absolut zu
15			
16			
17			
18			
19			
20			
21	Für den sicheren Groupware-Zugang aus Mobilfunknetzen wurde ein SSL-Reverse-Proxy in Betrieb genommen und eine entsprechende Zertifikat-Infrastruktur geschaffen.	stimme zu	stimme nicht zu
22			
23		stimme absolut zu	kann mich nicht entscheiden
24			

25			
26		stimme weniger zu	stimme nicht zu
27			
28			
29		stimme zu	stimme absolut zu
30			
31		stimme zu	stimme nicht zu
32		stimme zu	stimme zu
33			
34			
35			
36			
37			
38			
39			
40			
41			
42		stimme absolut zu	stimme zu
43			
44		stimme zu	stimme weniger zu
45		stimme zu	kann mich nicht entscheiden
46			
47			
48			
49			
50			
51		stimme zu	stimme zu

id	These 4: Aussage 3	These 4: Aussage 4	These 4: Aussage 5	These 4: Aussage 6	These 4: Aussage 7
1	stimme weniger zu	stimme zu	stimme zu	stimme absolut zu	stimme zu
2					
3					
4	stimme zu	stimme absolut zu	stimme absolut zu	stimme zu	stimme nicht zu
5	kann mich nicht entscheiden	stimme zu	stimme zu	kann mich nicht entscheiden	stimme weniger zu
6	stimme absolut zu	stimme absolut zu	stimme absolut zu	stimme absolut zu	stimme absolut zu
7	stimme weniger zu	stimme zu	stimme zu	kann mich nicht entscheiden	stimme zu
8	stimme zu	stimme weniger zu	stimme zu	stimme absolut zu	stimme weniger zu
9					
10					
11					
12					
13					
14	stimme absolut zu	stimme zu	stimme absolut zu	stimme absolut zu	stimme weniger zu
15					
16					
17					
18					
19					
20					
21	stimme nicht zu	stimme weniger zu	kann mich nicht entscheiden	stimme weniger zu	stimme weniger zu
22					
23	stimme absolut zu	stimme absolut zu	stimme absolut zu	stimme nicht zu	stimme zu
24					

25					
26	stimme nicht zu	stimme nicht zu	stimme absolut zu	stimme zu	stimme nicht zu
27					
28					
29	stimme absolut zu	kann mich nicht entscheiden	stimme absolut zu	stimme weniger zu	stimme zu
30					
31	stimme nicht zu	stimme weniger zu	stimme zu	stimme zu	stimme weniger zu
32	stimme zu	stimme absolut zu	kann mich nicht entscheiden	kann mich nicht entscheiden	stimme weniger zu
33					
34					
35					
36					
37					
38					
39					
40					
41					
42	stimme nicht zu	stimme absolut zu	stimme absolut zu	stimme nicht zu	stimme zu
43					
44	stimme zu	stimme weniger zu	stimme zu	stimme zu	stimme weniger zu
45	stimme weniger zu	stimme zu	stimme absolut zu	kann mich nicht entscheiden	stimme zu
46					
47					
48					
49					
50					
51	stimme zu	stimme zu	stimme absolut zu	stimme zu	stimme zu

id	Welche rechtlichen Probleme hatten oder haben Sie durch den Einsatz von BYOD?	These 5: Aussage 1	These 5: Aussage 2	These 5: Aussage 3	These 5: Aussage 4
1		stimme absolut zu	stimme absolut zu	stimme absolut zu	stimme absolut zu
2					
3					
4	Fernlöschung des Device nach Teilnahme von BYOD, Sicherung des Devices und notwendige Sperren, Differenzierung von Daten welche geheim gehalten werden müssen....	stimme nicht zu	stimme weniger zu	stimme weniger zu	stimme weniger zu
5		stimme absolut zu	stimme weniger zu	stimme zu	stimme zu
6		stimme nicht zu	stimme nicht zu	stimme nicht zu	stimme nicht zu
7		stimme weniger zu	stimme zu	stimme weniger zu	stimme nicht zu
8		stimme zu	stimme zu	stimme weniger zu	stimme absolut zu
9					
10					
11					
12					
13					
14	s.o.	stimme weniger zu	stimme weniger zu	stimme nicht zu	stimme zu
15					
16					
17					
18					
19					
20					
21		stimme absolut zu	stimme absolut zu	stimme absolut zu	stimme zu
22					
23		stimme zu	stimme zu	stimme zu	stimme weniger zu
24					

25					
26		stimme absolut zu	stimme absolut zu	stimme absolut zu	stimme weniger zu
27					
28					
29		stimme absolut zu	stimme zu	stimme zu	stimme weniger zu
30					
31		stimme nicht zu	stimme nicht zu	stimme nicht zu	stimme nicht zu
32		stimme zu	stimme zu	stimme zu	stimme zu
33					
34					
35					
36					
37					
38					
39					
40					
41					
42		stimme zu	stimme weniger zu	stimme zu	stimme zu
43					
44		stimme absolut zu	stimme zu	stimme absolut zu	stimme zu
45		stimme absolut zu	stimme absolut zu	stimme absolut zu	stimme absolut zu
46					
47					
48					
49					
50					
51		stimme weniger zu	stimme weniger zu	stimme weniger zu	stimme zu

id	These 5: Aussage 5	These 5: Aussage 6	Konnten Sie durch BYOD einen Vorteil im "war fortalents" gegenüber ihren Konkurrenten erlangen?
1	stimme zu	kann mich nicht entscheiden	
2			
3			
4	stimme weniger zu	stimme nicht zu	Nein, vorwiegend haben sich Schichten angemeldet, die nicht im War for Talents enthalten sind (einfache Techniker z.B.) Hochkarätige Consultants oder Systemintegratoren haben sich eher gegen BYOD entschieden.
5	stimme zu	stimme weniger zu	
6	stimme nicht zu	stimme nicht zu	BYOD bedeutet doch eigentlich nur, daß die Firma den Mitarbeiter dazu zwingt, sich selber sein Equipment zu besorgen, das er zum arbeiten braucht. Damit spart die Firma, stellt dies aber als "Incentive" für den Mitarbeiter dar. Eine Firma hat die Pflicht, dem Mitarbeiter das Arbeitsgerät zu stellen, das er zum arbeiten braucht.
7	stimme nicht zu	stimme nicht zu	
8	stimme weniger zu	stimme zu	
9			
10			
11			
12			
13			
14	stimme zu	stimme nicht zu	Nein, solange Unternehmensanwendungen auf mobilen Geräten wie Smartphones oder Tablets nicht optimal unterstützt werden ist das BYOD Gerät ein zusätzliches zu den gestellten Firmengeräten. Dieser Mangel wird dann schnell als negativ empfunden und macht den Vorteil BYOD überhaupt zu unterstützen wett.
15			
16			
17			
18			
19			
20			
21	stimme weniger zu	stimme weniger zu	Nein, andere Faktoren waren bisher immer entscheidender.
22			
23	stimme weniger zu	stimme weniger zu	
24			

25			
26	stimme nicht zu	stimme nicht zu	
27			
28			
29	stimme zu	stimme zu	
30			
31	stimme nicht zu	stimme nicht zu	
32	stimme zu	stimme weniger zu	
33			
34			
35			
36			
37			
38			
39			
40			
41			
42	stimme weniger zu	stimme weniger zu	nein
43			
44	stimme absolut zu	stimme zu	
45	stimme absolut zu	stimme zu	
46			
47			
48			
49			
50			
51	stimme weniger zu	stimme weniger zu	