# Trends und Erkenntnisse zur Konsumerisierung mobiler Geräte

# Befragung von IT-Verantwortlichen und CEOs

## ABSCHLUSSBERICHT

**VERGLEICHE: PHASE 1 UND 2**

AUFBEREITET FÜR:

TREND MICRO, INC.

AUFBEREITET VON:

DECISIVE ANALYTICS, LLC


Cheryl Harris, Ph.D.

Chief Research Officer

Decisive Analytics, LLC

575 Madison Ave, 10th Floor

New York, NY 10022

917.628.6167

INHALT

# ÜBERBLICK

## Überblick und Ziele

Das Hauptziel dieses Projekts ist es, das Problembewusstsein im Hinblick auf die Konsumerisierung von IT/Computing im Unternehmen auszuwerten und mehr über folgende Aspekte zu erfahren:

- **Einstellungen**
- **Wahrnehmungen**
- **Entwicklung interner Richtlinien zur Konsumerisierung**
- **Weitere aufkommende Bedenken**

Die sogenannte ***Consumer-IT*** hat sich zu einem bedeutenden und branchenübergreifenden Trend entwickelt. Das belegt eine aktuelle Studie (DELL/KACE, *CIO Magazine*, 15. Sept. 2011), in der 87 % der Führungskräfte angeben, dass ihre Mitarbeiter private Geräte am Arbeitsplatz nutzen. Der Aufgabenbereich reicht dabei vom Lesen und Schreiben von E-Mails über die Nutzung der Kalenderfunktion bis hin zum Arbeiten mit ERP- und CRM-Anwendungen. Dadurch wächst der Druck auf die Führungsetagen, wirksame Richtlinien zur Einbindung privater Geräte, Cloud-Services und anderer Erscheinungsformen der Consumer-IT am Arbeitsplatz zu entwickeln.

Um besser zu verstehen, wie sich der neue Trend auf die IT-Umgebung im Unternehmen auswirkt und wie Führungskräfte die Konsumerisierung sinnvoll nutzen können, wurden Führungskräfte zu den ergriffenen Maßnahmen in Bezug auf die Auswirkungen der Konsumerisierung im Unternehmen und/oder zu den damit verbundenen Richtlinienentscheidungen befragt.

## Verfahren

Es wurde eine Online-Befragung unter IT-Führungskräften und CEOs großer Unternehmen (500 Mitarbeiter oder mehr) mit Standort in den USA, dem Vereinigten Königreich und Deutschland durchgeführt. Die erste Interview-Phase wurde zwischen dem 3. und 11. Januar 2012 durchgeführt, die zweite Umfrage zwischen dem 10. und 20. April 2012. In der zweiten Interview-Phase wurden Personen befragt, die an der ersten Umfrage nicht teilgenommen hatten. Dabei wurden die meisten Fragen aus der ersten Phase beibehalten und um einige ausgewählte neue Fragen ergänzt.

**Die Interview-Phasen im Vergleich – befragte Gruppen**

| | *Phase 1 N=* | *Phase 2 N=* |
|---|---|---|
| **CEO** | **26** | **21** |
| **IT-Führungskraft** | **410** | **415** |
| **Gesamt** | **436** | **436** |

**Phase 1** ***(Januar 2012)***
Insgesamt wurden 436 Führungskräfte befragt. Dabei wurden 410 Interviews mit IT-Leitern durchgeführt (50 % aus den USA, 25 % aus dem Vereinigten Königreich, 25 % aus Deutschland); weitere 26 Interviews richteten sich ausschließlich an die CEOs großer Unternehmen aus diesen drei Ländern.

**Phase 2** ***(April 2012)***
Insgesamt wurden 436 Führungskräfte befragt. Dabei wurden 415 Interviews mit IT-Leitern durchgeführt (50 % aus den USA, 25 % aus dem Vereinigten Königreich, 25 % aus Deutschland); weitere 21 Interviews richteten sich ausschließlich an die CEOs großer Unternehmen aus diesen drei Ländern.

**Profil: Aggregierte Phasen**

Zu den Befragten zählten Mitarbeiter aus amerikanischen, britischen und deutschen Unternehmen mit 500 bis über 20.000 Mitarbeitern. Die Hauptaktivitäten dieser Unternehmen liegen in den Bereichen Buchhaltung, Unternehmensdienstleistungen, Ingenieurswesen, Behörden, Logistik und Energieversorgung. 15,5 % aller Befragten gaben an, dass der Unternehmensschwerpunkt in der Herstellung liegt, weitere 15,9 % nannten als zentrale Aktivität IT-Beratung oder Systemintegration.

825 Teilnehmer waren leitende IT-Administratoren, 47 waren Geschäftsführer in ihrem jeweiligen Unternehmen. Die häufigsten IT-Rollen waren IT-Manager/ Administrator (30,6 %), CIO/CSO/CTO (20,9 %) sowie Vice President/Director of IS/IT Security (20,3 %).

Die Teilnehmer mussten zumindest in einem gewissen Maße an der Entscheidung beteiligt sein, ob Mitarbeiter mit ihren Geräten auf das Unternehmensnetzwerk zugreifen dürfen oder nicht. Die meisten IT-Führungskräfte (62,3 %) gaben an, die Hauptverantwortung für derartige Entscheidungen zu tragen. Wenig überraschend erklärten fast alle CEOs (93,6 %), bei diesem Thema der Hauptentscheidungsträger zu sein.

## Bring Your Own Device (BYOD) – Praktiken und Motivation

Fast alle Unternehmen (76,7 %) in dieser Studie erlauben ihren Mitarbeitern, private Geräte wie Laptops, Netbooks, Smartphones und Tablets für berufliche Zwecke zu nutzen.

Tendenziell erklärten mehr US-amerikanische Führungskräfte, dass ihr Unternehmen BYOD erlaubt (80 %). Im Vereinigten Königreich und Deutschland waren es 70,8 % bzw. 75,4 %. Interessanterweise gaben eher Führungskräfte unter 45 Jahren an, dass die Mitarbeiter in ihrem Unternehmen private Geräte am Arbeitsplatz nutzen dürfen.

In nahezu allen befragten Unternehmen gilt eine IT-Sicherheitsrichtlinie für Geräte von Mitarbeitern, die auf das Unternehmensnetzwerk zugreifen (89,7 %). Zur Voraussetzung wird auch gemacht, dass Geräte entweder auf einer im Vorfeld genehmigten Liste aufgeführt und/oder mit entsprechender Sicherheitssoftware ausgestattet sind (53,7 %). Darüber hinaus ist geplant, Unternehmensanwendungen und/oder -daten zu isolieren, wenn private Geräte zu beruflichen Zwecken genutzt werden (71,2 %). Und über 80 % der Unternehmen machen das Installieren einer Sicherheitssoftware auf den privaten Geräten zur Pflicht.

CEOs sind selbst begeisterte Nutzer unterschiedlicher mobiler Geräte: So geben 84,8 % an, Smartphones bei der Arbeit zu nutzen. Bei den IT-Führungskräften liegt dieser Anteil bei 73,7 %. Das am zweithäufigsten genannte Gerät ist der Laptop (CEOs: 78 %, IT-Führungskräfte: 68 %), gefolgt vom iPad oder Tablet (CEOs: 82,6 %, IT-Führungskräfte: 45,2 %). Rund ein Drittel erklärte, mobile Software oder Apps zu verwenden. Etwa genauso viele Teilnehmer nutzen nach eigenen Angaben Online-Datenspeicher oder Cloud-Lösungen. Ebenfalls etwa ein Drittel nutzt Facebook (32,4 %), LinkedIn (20,4 %), Twitter (18,8 %) oder YouTube (13,1 %). Dabei gaben etwa doppelt so viele CEOs wie IT-Führungskräfte an, YouTube zu nutzen.

Von den zahlreichen Betriebssystemen für mobile Geräte lassen viele Unternehmen nur bestimmte im Unternehmensnetzwerk zu. Zu den am häufigsten erlaubten Geräten zählen Android (69,3 %) und BlackBerry (69,2 %), gefolgt von iOS (53,6 %), Windows (50 %) und Symbian (24 %).

Nach der Sicherheit und Verwaltbarkeit der genannten Betriebssysteme gefragt, erstellten die Teilnehmer folgendes Ranking: BlackBerry und iOS belegten die Plätze 1 und 2, dicht gefolgt von Android. Windows kam auf den vierten Platz, Symbian bildete das Schlusslicht.

Nur sehr wenige Unternehmen erklärten, dass es sich bei den unternehmensweit genutzten Geräten ausschließlich um die privaten Geräte von Mitarbeitern handelt, und schätzten den Anteil dieser Geräte auf höchstens ein Drittel. Laptops, Tablets, Netbooks, tragbare Speichermedien und mobile Software/Apps gehören den Angaben zufolge meist den Unternehmen, nicht den Mitarbeitern. Smartphones allerdings bilden die Ausnahme: Sie gehören häufiger den Mitarbeitern, wobei die Quote nur leicht höher lag.

Fast 80 % der Unternehmen haben eine VDI (Virtual Desktop Infrastructure) im clientgehosteten oder Remote-Synchronisationsmodus implementiert. Lediglich 15 % stellen noch keine VDI bereit.

Die weitaus meisten Unternehmen setzen Windows (77,7 %) als Betriebssystem für stationäre Computer (Server/Desktops) ein. Nur wenige nutzen Mac OS als Hauptbetriebssystem (13,5 %) bzw. Linux (7,6 %) oder Unix (1 %).

Die **Hauptmotive**, die Führungskräfte für die Nutzung von privaten Geräten im Unternehmen angeben, sind:

- Verbesserte Mobilität (Möglichkeit zum mobilen Arbeiten unterwegs oder an anderen Standorten): 43,1 %
- Reduzierung der Anzahl mitzuführender bzw. zu wartender Geräte: 13,6 %
- Die Ansicht, dass BYOD vorteilhaft für Mitarbeiter ist: 10,5 %

**Erfahrungen mit Sicherheitslücken**

Fast die Hälfte der Unternehmen, die BYOD zulassen, berichteten von einem Datenverlust oder einer Sicherheitslücke infolge des Netzwerkzugriffs durch ein privates Mitarbeitergerät (46,5 %).

Die Reaktionen auf Sicherheitslücken, die durch Mitarbeitergeräte verursacht wurden, variierten. Am häufigsten aber wurden die Datenzugriffsberechtigungen eingeschränkt (45 %), gefolgt von der sofortigen Installation von Sicherheits-software (42,9 %). 11,6 % der Befragten entzogen den Mitarbeitern die BYOD-Berechtigungen. Deutsche Unternehmen bestehen den eigenen Aussagen zufolge nach einem Sicherheitsvorfall stärker auf der Installation von Sicherheitssoftware. US-amerikanische Unternehmen dagegen verbieten ihren Mitarbeitern eher den Netzwerkzugriff mit privaten Geräten.

Einige Unternehmen gaben an, eine Richtlinie implementiert zu haben, nach der die Daten auf mobilen Geräten nach einem Geräteverlust und nach Beendigung des Arbeitsverhältnisses vollständig gelöscht werden (35,5 %). In anderen Unternehmen werden die Daten nur im Falle eines Geräteverlusts gelöscht

(23,3 %). Einige wenige Unternehmen erklärten, bei Bedarf ganz gezielt Unternehmensdaten und -anwendungen von den Geräten zu löschen (10,1 %).

**Sicherheitssoftware**

Die meisten Unternehmen (83 %) fordern von ihren Mitarbeitern, Software zur Sicherung und Verwaltung der zu beruflichen Zwecken genutzten privaten Geräte zu installieren. Wir fragten die Unternehmen, die *keine* Sicherheitssoftware voraussetzen, nach den Gründen. Überraschenderweise lauteten die häufigsten Antworten „Wir erlauben nur vertrauenswürdigen Nutzern, auf unser Unternehmensnetzwerk zuzugreifen“ (25,7 %) und „Wir machen uns über die Sicherheit auf diesen Geräten keine Sorgen“ (15,6 %). Einige erklären, keine Softwarelösung zu haben (13,8 %) oder noch auf der Suche nach einer passenden Lösung zu sein (12,8 %). Ablehnung durch die Mitarbeiter (11 %), hohe Kosten (10 %) und Komplexität (3,7 %) wurden seltener als Grund angegeben.

Im Hinblick auf die Sicherheit von Daten auf Smartphones äußerten fast alle Teilnehmer (89,5 %) Bedenken.

**Nutzungsrichtlinien**

Die meisten Unternehmen (79,7 %) erklärten, dass sie für die Mitarbeiter eine Nutzungsrichtlinie ausgegeben haben, die die Verantwortlichkeiten des Unternehmens bzw. der Mitarbeiter in Hinblick auf private Geräte, Sicherheit und Haftung klärt.

Danach gefragt, welche Komponenten in diese Richtlinie aufgenommen wurden, gaben die Unternehmen Folgendes an:

- 12,2 % erklärten, ihre Richtlinie besage, dass Daten im Falle eines Geräteverlusts vom Unternehmen per Fernzugriff gelöscht werden können.
- Etwa 10 % erklären in ihrer Richtlinie, dass die unternehmenseigene IT-Abteilung Daten, Downloads und andere Aktivitäten auf den mobilen Geräten routinemäßig überwacht, und/oder dass Daten auf dem Gerät im Falle eines Rechtsstreits offengelegt oder die Geräte selbst beschlagnahmt werden können.
- 9,7 % erklären in ihrer Richtlinie, dass nach fehlgeschlagenen Anmeldeversuchen Daten gelöscht werden können, dass der Standort des Geräts überwacht werden kann oder dass das Unternehmen für Daten auf dem Gerät haftet.

**Auswirkungen von BYOD auf die Kosten**

Die Einführung privater Mitarbeitergeräte kann sich auf die Kosten, die mit der Unterstützung des BYOD-Trends verbunden sind, auswirken. Dabei sind einige Unternehmen der Ansicht, dass die Gesamtkosten steigen; andere wiederum beobachten eine Kostensenkung. Die Gründe für diese Positionen sind sehr vielfältig.

Interessanterweise erklärten fast 40 % der Unternehmen, dass die **Kosten** nach der Einführung von BYOD **sinken** (39,3 %). Zusammen mit dem Anteil derjenigen, die aussagten, die Kosten blieben unverändert (23,3 %), ist der Großteil der Unternehmen der Meinung, dass der BYOD-Trend insgesamt entweder zu einer Kostensenkung führt oder keinerlei Auswirkungen auf die Kosten hat.

Auffällig war, dass in der zweiten Interview-Phase (April 2012) weniger Teilnehmer von einer generellen Kostensteigerung durch BYOD berichteten. In dieser Phase gaben deutlich mehr Befragte als in der ersten Interview-Phase im Januar 2012 an, dass die Kosten entweder unverändert geblieben sind oder sogar reduziert wurden. Möglicherweise hat sich die Bewertung der Kostenauswirkungen durch die gestiegene Erfahrung mit BYOD verbessert oder die mit BYOD verbundenen Gesamtkosten haben sich in den Folgemonaten schlicht reduziert.

Gründe für die beobachtete Kostensenkung waren zu fast gleichen Teilen niedrigere IT-Ausgaben, da Mitarbeiter die Geräte selbst anschaffen (37,9 %), niedrigere Support-Kosten im Desktopbereich (31,3 %) und eine höhere Mitarbeiterproduktivität (29,6 %).

Unter den Teilnehmern, die im Zusammenhang mit BYOD einen Kostenanstieg beobachteten, lag der Hauptgrund in den erhöhten Support-Kosten (41,2 %) bzw. höheren Kapitalausgaben für VDI (31,5 %). Seltener wurden höhere Kosten für Software oder Softwarevirtualisierung genannt (27 %).

Bei der Frage nach den Gesamtauswirkungen von privaten Mitarbeitergeräten im Unternehmen wurde deutlich, dass BYOD einerseits Übergangskosten mit sich bringt, andererseits aber auch Vorteile, die diese Kosten relativieren können. Beispiele hierfür sind eine höhere Produktivität und Zufriedenheit der Mitarbeiter sowie eine höhere Kundenzufriedenheit.

### Zusätzliche Auswirkungen von BYOD

Die wichtigste Auswirkung des BYOD-Trends hat also möglicherweise mit der Unternehmenskultur und -philosophie zu tun. Als wir die Teilnehmer dazu befragten, wie weit sie den Aussagen zu den Auswirkungen von BYOD zustimmten, erhielten wir eine Reihe interessanter Ergebnisse.

Die Führungskräfte stimmten zu, dass die Einbindung von BYOD dem Unternehmen einen Wettbewerbsvorteil verschafft, vorteilhaft für die Mitarbeiter selbst sowie für die Gewinnung und Bindung von Mitarbeitern ist und dass Mitarbeiter de facto ein „Anrecht darauf haben, private Geräte zu beruflichen Zwecken zu nutzen“. Mitarbeiter, die ihre eigenen Geräte nutzen, sind deutlich kreativer und innovativer. Außerdem verbessert sich die Work-Life-Balance.

Die CEOs zeigten eine positivere Haltung gegenüber den Auswirkungen von BYOD als die IT-Führungskräfte. Interessanterweise schätzen IT-Führungskräfte die Meinung ihres Unternehmens zu den einzelnen Aussagen anders ein als von den CEOs tatsächlich geäußert. Dies führt zu der Annahme, dass IT-Führungskräfte nicht in dem Maße über die Ansichten der CEOs aufgeklärt sind, wie man es vielleicht erwarten würde.

Der Großteil der Befragten (62,9 %) erklärte, dass die Einbeziehung von privaten Mitarbeitergeräten am Arbeitsplatz die Sichtweise der Mitarbeiter auf das Unternehmen positiv beeinflusst. Fast die Hälfte (47,5 %) sagte, dass durch BYOD auch Kunden das Unternehmen positiver wahrnehmen.

**Die Zukunft von BYOD**

Die meisten befragten Unternehmen halten die Zunahme und Ausweitung des BYOD-Trends für unvermeidlich. Tatsächlich sind viele der Meinung, dass die Konsumerisierung zukünftig unter allen Nutzern in einem Unternehmen zunehmen wird. Etwa ein Fünftel denkt, dass private Mitarbeitergeräte in vielen Fällen die herkömmlichen PCs ersetzen werden (17 %), obwohl einige Teilnehmer glauben, dass diese Geräte in erster Linie zu Kommunikations- und Messaging-Zwecken genutzt werden (14,7 %).

Unternehmen planen aktiv die weitere Einbindung von BYOD in ihre Unternehmensstruktur. Zu den geplanten Veränderungen zählen der Kauf neuer Software oder Technologien zur Verwaltung von Sicherheitsproblemen (21,4 %), die Umstrukturierung der IT-Abteilung (20,3 % – allerdings häufiger bei CEOs, von denen zwei Drittel eine solche Umstrukturierung anstreben), der Umstieg auf eine schlanke Architekturplattform oder die Neudefinition der Geräteunterstützung generell (14,6 % bzw. 16,2 %).

Über ein Viertel erwartet eine Umstrukturierung des Budgets, da weniger Computing-Geräte gekauft werden müssen, und einige wenige würden auch das Softwarebudget neu ausgestalten (8 %).

Daneben haben wir die Teilnehmer gebeten, ihre Ansichten zu den neuen Herausforderungen im Zusammenhang mit BYOD in ihrem Unternehmen

zusammenzufassen. Während einige BYOD grundsätzlich als ungeeignet für ihre Branche und/oder ihr Unternehmen ablehnten (z. B. Mitarbeiter von Behörden), **erklärten die meisten: „BYOD ist die Zukunft“.**

## FAZIT

1. **BYOD ist schon jetzt Usus.** Mehr als drei Viertel (76,7 %) erklären, dass Mitarbeiter private Geräte wie Laptops, Smartphones und Tablets am Arbeitsplatz nutzen dürfen. Dies ist bei Unternehmen in den USA häufiger der Fall als bei Unternehmen im Vereinigten Königreich oder in Deutschland.

2. **Fast alle Unternehmen, die BYOD erlauben, setzen die Installation von Sicherheitssoftware auf privaten Geräten voraus.** Es gibt eine Vielzahl von Anbietern auf diesem Markt. 4,3 % der Befragten geben an, Sicherheitslösungen von Trend Micro zu verwenden. Marktführend in dieser Stichprobe sind McAfee (16 %), Kaspersky (12,6 %) und Symantec Norton (14,9 %). Es gibt unterschiedliche Gründe, weshalb ein Unternehmen auf Sicherheitssoftware verzichtet. Dennoch machen sich fast alle Befragten Gedanken über die Datensicherheit auf Smartphones (85,9 %).

3. **In fast der Hälfte aller Unternehmen, die BYOD erlauben, ist es bereits zu Sicherheitslücken gekommen.** Umgehende Änderungen der Sicherheits-protokolle sind typische Folgen solcher Sicherheitslücken. Dazu zählen vor allem die Einschränkung der Zugriffsberechtigungen (45 %) und die Installation von Sicherheitssoftware (42,9 %). Nur wenige Teilnehmer verbieten BYOD infolge einer Sicherheitslücke ganz.

4. **CEOs sind grundsätzlich überzeugter von BYOD als IT-Führungskräfte.** Letztere sind sich zu sehr der Sicherheitsherausforderungen und Support-Probleme im Zusammenhang mit BYOD bewusst. CEOs nutzen selbst die unterschiedlichsten mobilen Geräte und empfinden dies als förderlich für die eigene Produktivität und die der Mitarbeiter.

5. **BYOD schafft Wettbewerbsvorteile.** Fast die Hälfte der CEOs gab an, dass BYOD ihrem Unternehmen einen Wettbewerbsvorteil verschafft. Und nur gering-fügig weniger IT-Führungskräfte waren derselben Meinung.

6. **BYOD ist ein Instrument zur Gewinnung und Bindung von Mitarbeitern.** 46 % der CEOs und 42,5 % der IT-Führungskräfte stimmten zu, dass BYOD einen Vorteil für die Mitarbeiter bedeutet und eingesetzt wird, um Mitarbeiter zu gewinnen bzw. zu halten.

7. **BYOD fördert Innovation, Kreativität und Produktivität.** In den Augen der Befragten verbessert BYOD die Mitarbeiterproduktivität (47 % der CEOs und 46 % der IT-Führungskräfte sind dieser Ansicht) sowie die Innovationskraft und Kreativität von Mitarbeitern (50,7 % der CEOs und 48 % der IT-Führungskräfte).

8. **Mitarbeiter wie auch Kunden bevorzugen Unternehmen, die BYOD erlauben.** Der Großteil der Befragten (62,9 %) erklärte, dass die Einbeziehung von privaten Mitarbeitergeräten am Arbeitsplatz die Sichtweise der Mitarbeiter auf das Unternehmen positiv beeinflusst. Fast die Hälfte (47,5 %) sagte, dass durch BYOD auch Kunden das Unternehmen positiver wahrnehmen.

9. **BYOD *senkt* die Kosten bzw. hat keinerlei Kostenauswirkungen.** Während nach Angabe der meisten Unternehmen, die BYOD erlauben, zwar Investitionen in Sicherheitssoftware und Support getätigt werden müssen, wirkt sich BYOD im Großen und Ganzen positiv bzw. neutral auf die Gesamtkosten aus. Dieses wichtige Ergebnis sollte Unternehmen, die an der Einführung von Richtlinien zur Nutzung privater Mitarbeitergeräte interessiert sind, vor Augen geführt werden. Denn mehr als die Hälfte der Befragten gab an, dass die Kosten entweder abnahmen (36 %) oder unverändert blieben (20,1 %).

10. **Haben Mitarbeiter ein Recht auf BYOD?** Fast die Hälfte der CEOs war dieser Ansicht. Diese durchaus provokative Frage sollte unbedingt weiter untersucht werden.

11. **Fast alle Unternehmen, die BYOD erlauben, haben Nutzungsrichtlinien implementiert.** Zu den Komponenten, die in diese Richtlinie einfließen, gehört die Möglichkeit, Daten auf Geräten per Fernzugriff zu löschen. Diese Bestimmung wird am häufigsten genannt, gefolgt von der Befugnis, Aktivitäten zu überwachen, der Möglichkeit, Daten im Falle eines Rechtsstreits offenzulegen, sowie der Datenlöschung nach fehlgeschlagenen Anmeldeversuchen.

12. **Die Zunahme von BYOD am Arbeitsplatz gilt als unvermeidlich.** Dennoch sind sich die oberen Führungsetagen der möglichen Risiken durchaus bewusst und bereit, die für eine reibungslose Bereitstellung erforderlichen Investitionen zu tätigen.