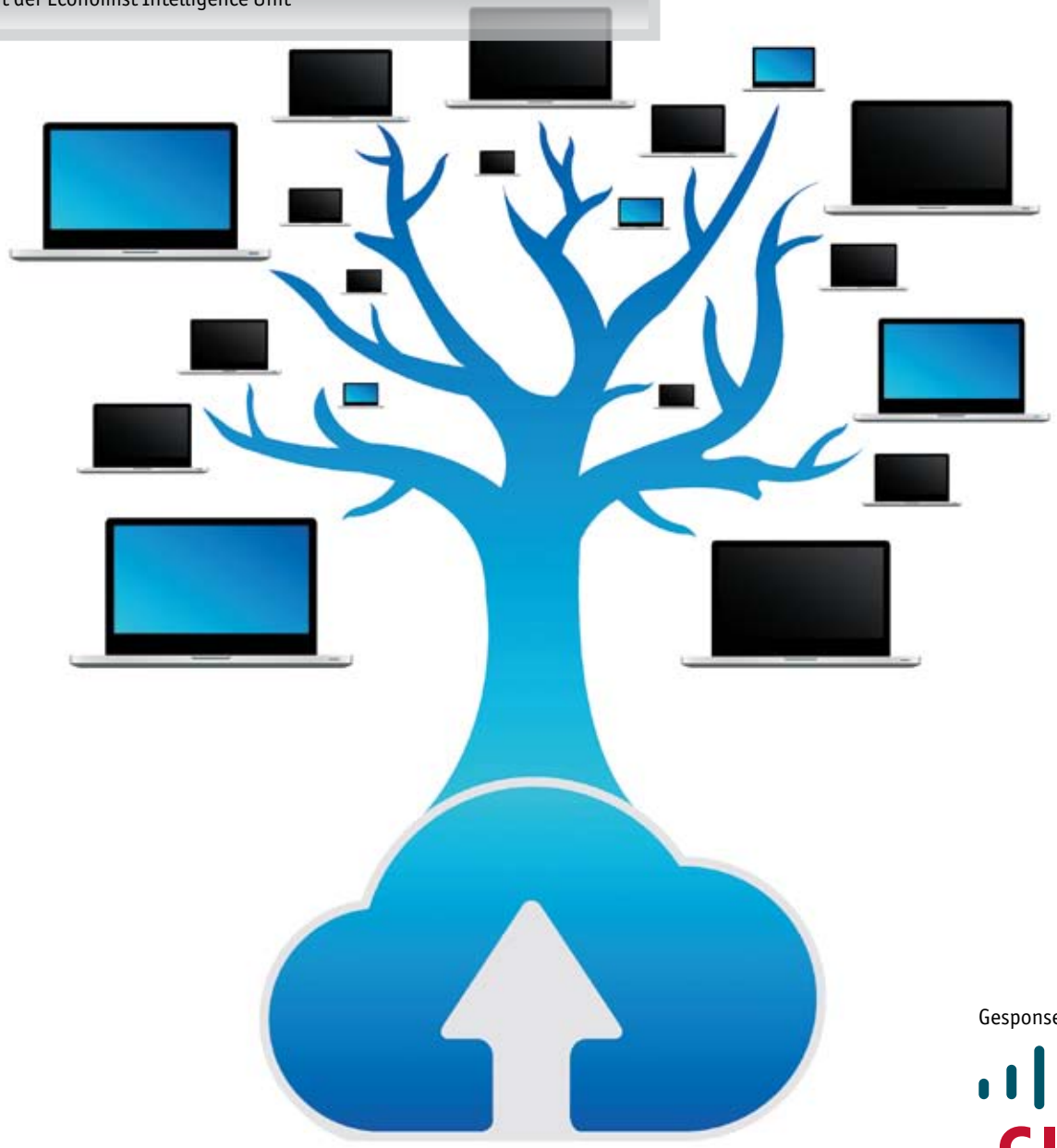
Economist Intelligence Unit

The Economist

Sicherer Datenzugriff in einer mobilen Welt

Ein Report der Economist Intelligence Unit



Gesponsert von

CISCO

Inhalt

	Vorwort	2
	Zusammenfassung	3
	Einführung	5
1	Moderne Mobilität: der Stand der Dinge	6
2	Verlust, Diebstahl und schlechte Angewohnheiten: wie Unternehmen die Herausforderungen bewältigen	9
3	Immer mehr Daten „zum Mitnehmen“: aktuelle Entwicklungen	12
4	Wie können Unternehmen effektive Richtlinien für mobile Geräte gewährleisten?	15
5	Fazit	17
	Anhang: Umfrageergebnisse	18

Vorwort

Die zunehmende Nutzung privater Endgeräte am Arbeitsplatz und das Erfordernis, die Produktivität von Führungskräften und Mitarbeitern auch unterwegs zu steigern, zwingen Unternehmen zu einer Reaktion. Dieser Bericht namens *Sicherer Datenzugriff in einer mobilen Welt* befasst sich mit der Frage, wie Unternehmen die steigende Nachfrage nach dem mobilen Zugriff auf Geschäftsdaten bedienen können, ohne vertrauliche Informationen größeren Sicherheitsrisiken auszusetzen. Als Grundlage für diese Untersuchung führte die Economist Intelligence Unit im Juni 2012 eine weltweite Umfrage unter 578 Führungskräften durch. Hierbei wurde untersucht, wie Unternehmen auf aktuelle wie neue Herausforderungen reagieren – oder reagieren sollten –, die dem unaufhaltsamen BYOD-Trend (Bring Your Own Device) entspringen, und allgemeiner, wie sie die zunehmende Mobilität ihrer Mitarbeiter bewältigen. Ergänzend haben wir eine Reihe eingehender Interviews geführt. Die in diesem Bericht enthaltenen Ergebnisse und geäußerten Ansichten spiegeln nicht zwingend die Ansichten des Sponsors wider. Autor dieses Berichts ist Lynn Greiner. Herausgeber dieses Berichts sind Michael Singer und Justine Thody: Mike Kenny war für das Layout zuständig. Wir bedanken uns bei allen Führungskräften, die an der Umfrage und den Interviews teilgenommen haben – auch jenen, die uns zwar ihre Ansichten mitgeteilt haben, aber nicht namentlich genannt werden wollten –, für ihre Zeit und Mühe.

Interviewte Führungskräfte

Lucy Burrow, Director of IT Governance, King's College London

Mike Cordy, Global Chief Technology Officer, OnX Enterprise Solutions

Steve Ellis, Executive Vice President, Wells Fargo

Jay Leek, Chief Information Security Officer, Blackstone Group

Arturo Medina, Information Technology Director, Ipsos Mexico

Bill Murphy, Chief Technology Officer, Blackstone Group

Al Raymond, Vice President, Aramark

Ashwani Tikoo, Chief Information Officer, CSC India

Zusammenfassung

Ende der 1990er Jahre brachte der Markt mobile Geräte wie Laptops und Smartphones hervor, welche es Führungskräften ermöglichten, auch außerhalb ihrer Büros produktiv zu bleiben. Geräte wie das ThinkPad von IBM oder der BlackBerry von RIM leiteten das Zeitalter multifunktionaler mobiler Geräte ein, deren Reiz sich die Führungsebene nicht entziehen konnte. Heutige mobile Erwerbstätige haben die Zwänge ihrer Eckbüros längst verlassen und dürften laut dem Marktforschungsunternehmen IDC bis 2015 mit 1,3 Milliarden Menschen beinahe 38 Prozent der Erwerbsbevölkerung stellen. Manchen Schätzungen zufolge unterstützen aktuell 76 Prozent aller Unternehmen BYOD und drängen demzufolge ihre Mitarbeiter mit der Aufgabe, den Zugriff auf Daten zu sichern, die auf möglicherweise nicht unternehmenseigenen Geräten gespeichert sind. Als Gründe führen die meisten Unternehmen an, ihre Mitarbeiter könnten durch die Nutzung privater Geräte effektiver Entscheidungen treffen, mehr Chancen wahrnehmen und effizienter mit ihren Partnern und Kunden zusammenarbeiten. Aus denselben Gründen sehen sich Unternehmen dazu veranlasst, den mobilen Datenzugriff über unternehmenseigene Geräte zu gestatten.

Im Juni 2012 führte die Economist Intelligence Unit eine von Cisco gesponserte Umfrage unter 578

Die Teilnehmer dieser Umfrage

Für diese Studie wurden 578 Führungskräfte aus aller Welt befragt. Die Teilnehmer stammten vorrangig aus Nordamerika (29 Prozent), Westeuropa (25 Prozent) und dem Asien-Pazifik-Raum (27 Prozent): die übrigen 19 Prozent kamen aus dem Nahen Osten und Afrika, Lateinamerika sowie Osteuropa. Dabei stammten insgesamt 23 Prozent aus den USA, 10 Prozent aus Indien, 7 Prozent aus Kanada und 6 Prozent aus Großbritannien. Bei 27 Prozent der Befragten handelte es sich um Führungskräfte auf höchster Ebene (CEOs), 17 Prozent stammten aus der zweiten Führungsebene (Senior Vice Presidents) und 15 Prozent aus der Managerebene. 55 Prozent der Befragten sind in Unternehmen mit einem jährlichen Umsatz von mindestens 500 Millionen US-Dollar beschäftigt, und 22 Prozent hiervon wiederum in Unternehmen mit einem Jahresumsatz von mindestens 10 Milliarden US-Dollar. Die Teilnehmer kamen aus einer Vielzahl von Branchen, vornehmlich aus der IT- und Technologiebranche (13 Prozent), dem Finanzdienstleistungssektor (11 Prozent), dem Unternehmensdienstleistungssektor (11 Prozent) und dem Bereich Energie und Rohstoffe (9 Prozent). Auf ihre Funktion im Unternehmen hin befragt gaben die Teilnehmer an, ihre Aufgaben lägen vorwiegend in den Gebieten Geschäftsführung, Geschäftsentwicklung, Finanzen sowie Vertrieb und Marketing. ■

Führungskräften durch, um ihre Meinungen und Standpunkte zur Sicherung von Daten auf mobilen Geräten in Erfahrung zu bringen. Die Untersuchung förderte folgende zentrale Erkenntnisse zutage:

- **Den meisten Führungskräften bereiten die Richtlinien ihrer Unternehmen zum mobilen Datenzugriff Unbehagen**. Obwohl 42 Prozent der Befragten angaben, für eine optimale Produktivität sicheren und zeitnahen Zugriff auf strategische Planungsdaten zu benötigen, hielten es nur 28 Prozent für angemessen, diese Daten auf mobilen Geräten verfügbar zu machen. Fast die Hälfte aller Befragten (49 Prozent) erachteten die Komplexität der Sicherung verschiedener Datenquellen und mangelndes Wissen über die Sicherheit und die Risiken beim mobilen Zugriff (48 Prozent) als größte Herausforderungen für ihre Unternehmen.

- **Größere Unternehmen sind am ehesten bereit, den mobilen Zugriff auf kritische Daten zu gestatten, stellen hierfür jedoch auch strengere Vorschriften auf**. Über 90 Prozent aller Unternehmen mit einem Umsatz von mehr als 1 Milliarde US-Dollar erlauben den Zugriff auf Daten über private oder unternehmenseigene Geräte. Allerdings gestatten mehr als die Hälfte aller Unternehmen mit einem Umsatz von mehr als 5 Milliarden US-Dollar ausschließlich den Zugriff über Unternehmensgeräte, während ein Drittel auch den Zugriff über private Endgeräte erlaubt. Dagegen bestehen nur 37 Prozent aller Unternehmen mit einem Umsatz von weniger als 500 Millionen US-Dollar auf die alleinige Nutzung unternehmenseigener Geräte, während 47 Prozent auch den Zugriff über private Geräte zulassen. In größeren Unternehmen sind mobile Anwender in ihrer Wahl indes auf genehmigte Geräte beschränkt, für deren Nutzung zahlreiche Unterschriften unter den Richtlinien ihrer Unternehmen erforderlich sind.

- **Richtlinien für mobile Geräte dürfen soziale Netzwerke nicht außer Acht lassen**. Während 56 Prozent aller Umfrageteilnehmer angaben, Richtlinien zur zulässigen Nutzung sozialer Netzwerke über mobile Geräte zu unterliegen, ist es 33 Prozent der Führungskräfte untersagt, sich auf Social-Media-Plattformen über ihre Arbeit auszutauschen. Unternehmen, die ein besonderes Augenmerk auf Richtlinien zur Nutzung sozialer Netzwerke legen, können eine effektive Interaktion ermöglichen und gleichzeitig Unternehmensdaten schützen und Haftungsrisiken vermeiden.

- **Die verfügbare Infrastruktur übt einen entscheidenden Einfluss auf Unternehmensrichtlinien für den mobilen Zugriff aus**. Zwar nannten 44 Prozent aller Befragten Druck aus der Führungsebene als wichtigsten Einflussfaktor auf Richtlinien, doch ganze 60 Prozent sehen den größten Einfluss in den Anforderungen an die IT-Infrastruktur. Dies zeigt Chancen für Unternehmen auf, die Dienste zur Sicherung und Verwaltung des mobilen Datenzugriffs anbieten.

Ist der Trend des mobilen Datenzugriffs unaufhaltbar? Die Antwort lautet kurz und bündig: ja. Technisch immer weiterentwickelte Geräte, die ein besseres Benutzererlebnis bieten, beschleunigen diesen Trend zusätzlich. Dies bedeutet zugleich, dass Richtlinien keine Option mehr sind, sondern eine Notwendigkeit. Laut den befragten Führungskräften erhöhe die Einbindung von Mitarbeitern in die Gestaltung dieser Richtlinien zudem die Wahrscheinlichkeit, dass sie die Regeln ihres Unternehmens auch befolgen. ■

Einführung

Das Erfordernis angemessener Richtlinien für den mobilen Datenzugriff gewinnt in der Unternehmenswelt immer stärker an Bedeutung. Leitende Mitarbeiter wie auch Nachwuchskräfte fordern einen orts- und zeitunabhängigen Zugriff auf Unternehmensdaten sowohl über mobile als auch über kabelgebundene Geräte. Dabei erkennen zahlreiche Unternehmen, dass die Gestattung der Nutzung mobiler Geräte sich in Form gesteigerten Engagements und höherer Produktivität bezahlt machen kann. Hierzu zählt auch die gesteigerte Bereitschaft ihrer Mitarbeiter, außerhalb der Arbeitszeit erreichbar zu sein. Unternehmen, die private Geräte in ihren Umgebungen zulassen, sind überdies attraktiver für technikaffine Arbeitnehmer, die in der Regel als Innovationstreiber gelten.

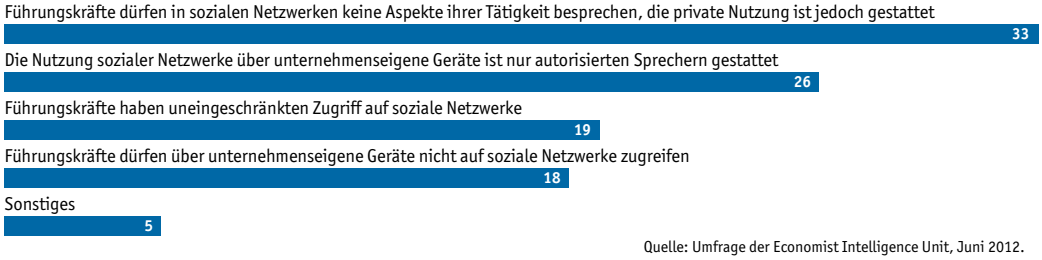
Doch mit der zunehmenden Verbreitung mobiler Geräte und den verschwimmenden Grenzen zwischen Consumer- und Unternehmens-IT wird es auch für Unternehmen immer schwieriger, mit diesem Paradigmenwechsel Schritt zu halten. Der Zugriff auf Geschäftsdaten über mobile Geräte stellt Unternehmen nicht nur vor technologische Herausforderungen, sondern auch unübersehbare Geschäftsrisiken dar. Denn zum einen können tragbare Geräte verloren gehen und gestohlen werden. Zum anderen ist es nicht unwahrscheinlich, dass Mitarbeiter ihre Geräte in die Hände von Freunden oder Verwandten und somit vertrauliche Daten in unbefugte Hände geben. Schließlich erfolgt der Zugriff auf diese Daten oftmals über Anwendungen, die vom Unternehmen nicht genehmigt wurden. Die Bemühungen von IT-Abteilungen, private Geräte und deren Nutzung inner- wie außerhalb des Unternehmens zu kontrollieren, verlaufen unterdessen immer öfter im Sande. Die wachsenden Schwachstellen in Unternehmensnetzwerken müssen jedoch durch effektive Schutzmaßnahmen abgesichert werden, um sowohl geschäftskritische Daten zu schützen als auch die rechtlichen Anforderungen aller Regionen zu erfüllen, in denen ein Unternehmen tätig ist. ■

1 Moderne Mobilität: der Stand der Dinge

Laut Schätzungen der Marktforscher von IDC wurden 2011 weltweit fast eine Milliarde sogenannte Smart Connected Devices verkauft, bis 2016 soll sich diese Zahl gar verdoppeln. Zu diesen Geräten zählen neben Laptops und Netbooks auch Smartphones und Tablets. Wie die Umfrage der Economist Intelligence Unit zeigt, kommen häufig mehrere Geräte gleichzeitig zum Einsatz, wobei es sich meist um eine Kombination aus Laptop und Smartphone handelt. Doch auch Tablets gewinnen zunehmend an Bedeutung. So stieg der weltweite Absatz von Tablets den Schätzungen von IDC zufolge zwischen dem ersten und dem zweiten Quartal 2012 um 33,6 Prozent und gegenüber dem Vorjahresquartal sogar um 66,2 Prozent. Infolge der Veröffentlichung der nächsten Generation von Betriebssystemen dürfte bei den Tablets weiterhin ein rasantes Wachstum zu verzeichnen sein. Da neuere Tablets zudem auch neue Funktionen zur Zusammenarbeit und Kommunikation mitbringen und damit mehr Möglichkeiten zum Datenzugriff bieten als Smartphones, gewinnen sie für Führungskräfte zusätzlich an Attraktivität.

„Indem Führungskräfte unterwegs Zugriff auf wichtige Informationen erhalten, können sie schnell fundierte Entscheidungen treffen – insbesondere in kritischen Situationen wie etwa Geschäftsverhandlungen," so Ashwani Tikoo, Chief Technology Officer des IT-Dienstleisters CSC India. Tikoo ist in der zweitgrößten Betriebszentrale von CSC Global für Sicherheitsrichtlinien zum Schutz geschäftlicher Daten auf mobilen Geräten verantwortlich. „Dank der sofortigen Verfügbarkeit von Daten können unsere Vertriebsmitarbeiter an Ort und Stelle die richtigen Entscheidungen treffen und müssen ihre Kunden nicht warten lassen", erklärt Tikoo. Zur Vermeidung eines Datenverlusts schreiben die Sicherheitsrichtlinien von CSC eine Datenverschlüsselung auf allen mobilen Geräten vor, also auch auf privaten Geräten, die im Rahmen von BYOD in die Unternehmensumgebung gelangen.

Richtlinien für Führungskräfte zur mobilen Nutzung sozialer Netzwerke
Welche Richtlinien bestehen in Ihrem Unternehmen bezüglich der Nutzung sozialer Netzwerke über unternehmenseigene Geräte?
(% der Befragten)



Quelle: Umfrage der Economist Intelligence Unit, Juni 2012.

Fallstudie Der hybride Ansatz bei Ipsos

In Regionen wie Lateinamerika, in denen Marktforschung vorzugsweise in persönlichem Kontakt betrieben wird, lösen Smartphones und Tablets Stift und Papier als bevorzugte Befragungsinstrumente ab. Dementsprechend setzt auch das weltweit tätige Marktforschungsinstitut Ipsos unter anderem in Mexiko zunehmend auf mobile Geräte. Das Unternehmen ist zurzeit in 84 Ländern tätig und beschäftigt 16.000 fest angestellte Mitarbeiter. Für seine Forschungsarbeiten nutzt Ipsos verschiedene Methoden wie Online-Umfragen und persönliche Befragungen und erhebt auf diese Weise weltweit jährlich Daten von über 70 Millionen Personen.

Derzeit stellt Ipsos seinen Interviewern noch die benötigten Geräte zur Verfügung, arbeitet unterdessen jedoch an einem neuen Ansatz, berichtet Arturo Medina, IT-Leiter bei Ipsos Mexiko. „Da mobile Geräte mit recht hohen Kosten verbunden sind, führen wir ein hybrides Modell mit BYOD ein“, erklärt Medina.

Im Rahmen dieses in der Entwicklung stehenden Modells erhalten Interviewer die Wahl zwischen drei Smartphone-Modellen, auf denen die Interview-Software von Ipsos ausgeführt werden kann. Die Kosten für das eigene Gerät werden dabei schrittweise vom Gehalt der Mitarbeiter abgezogen. „In der Regel geht das Gerät auf diese Weise innerhalb von zwei bis drei Wochen vollständig in den Besitz des Mitarbeiters über,“ rechnet Medina vor.

Ipsos stellt bei diesem Modell lediglich eine VPN-Verbindung für den Zugriff auf Unternehmensdaten bereit; alle weiteren Kosten, die durch die Nutzung der Smartphone-Funktionen entstehen, trägt der Mitarbeiter. Da Ipsos die Geräte seiner Mitarbeiter verwaltet, kann das Unternehmen bei Bedarf sämtliche Geschäftsdaten aus der Ferne löschen. Zusätzlich werden die Daten vor der Übertragung auf das Smartphone verschlüsselt, wodurch sich deren Verlust in vielen Fällen verhindern lässt. Als letzte Sicherungsmaßnahme sind die Interviewer zur Einhaltung der Nutzungsrichtlinien des Unternehmens verpflichtet. „Unsere Mitarbeiter können überall dasselbe Gerät verwenden, gleichzeitig besitzen wir genügend Kontrolle, um unsere Daten schützen zu können“, fasst Medina die Vorteile des Modells zusammen. ■

Eine andere Strategie besteht darin, die Speicherung von Daten auf mobilen Geräten zu verhindern. Al Raymond, Vice President Privacy and Records Management bei Aramark, zufolge greifen autorisierte Benutzer über ein sicheres Virtual Private Network (VPN) unterwegs von ihren mobilen Geräten auf Unternehmensdaten des Catering-Anbieters zu. Da außer E-Mails keinerlei Daten auf den Geräten gespeichert werden, lassen sich Unternehmensdaten so vergleichsweise einfach schützen, falls ein Mitarbeiter das Unternehmen verlässt oder sein Gerät verliert.

Ähnliche Herausforderungen schafft die Nutzung sozialer Netzwerke über mobile Geräte außerhalb des Büros, obschon sie Führungskräften oftmals durch Unternehmensrichtlinien untersagt ist. So gaben 33 Prozent der befragten Führungskräfte an, die Besprechung von Aspekten ihrer Tätigkeit in sozialen Netzwerken sei ihnen nicht gestattet, während einem weiteren Viertel der Befragten zufolge nur autorisierten Sprechern ihres Unternehmens die Nutzung sozialer Netzwerke mittels unternehmenseigener Geräte erlaubt ist. Wie unsere Untersuchungen ergaben, wird die Nutzung sozialer Netzwerke durch Führungskräfte auch künftig durch Richtlinien oder Absprache eingeschränkt werden, um Unternehmensdaten zu schützen und die entsprechende Haftung zu beschränken.

Außer Frage steht natürlich, dass Mitarbeiter auf unterschiedlichen Ebenen auch Zugriff auf unterschiedliche Arten von Daten benötigen. Und doch sorgte unsere Umfrage hier für einige Überraschungen. Unter den Führungskräften auf höchster Ebene nannten 60 Prozent den Zugriff auf Finanzinformationen und 42 Prozent den Zugriff

auf strategische Planungsdaten als wichtigste Faktoren für die Steigerung ihrer (mobilen) Produktivität. Manager dagegen benötigen in erster Linie Zugriff auf betriebliche Daten (44 Prozent) sowie Vertriebs- und Marketingdaten (43 Prozent), während für Mitarbeiter auf niedrigeren Stufen mit jeweils 42 Prozent der Zugriff auf Kundendaten und betriebliche Daten am wichtigsten ist. Das Treffen effektiver Entscheidungen (52 Prozent) und die Wahrnehmung zusätzlicher Chancen (42 Prozent) sind unserer Umfrage zufolge die wichtigsten Gründe, aus denen Führungskräfte über mobile Geräte Zugriff auf kritische Unternehmensdaten benötigen. Beziehungen mit Dritten – wie etwa Lieferanten – nehmen in diesem Zusammenhang insbesondere bei kleineren Unternehmen eine wichtige Rolle ein: Für 42 Prozent der Befragten aus Unternehmen mit einem Umsatz von unter 500 Millionen US-Dollar zählt die Pflege dieser Beziehungen zu den drei wichtigsten Gründen für den mobilen Datenzugriff. Im Gesamtdurchschnitt fand sich dieser Aspekt lediglich bei 37 Prozent unter den drei wichtigsten Gründen. Durch die Notwendigkeit, ständig in Verbindung bleiben zu müssen, wurden E-Mails zu einer unverzichtbaren Anwendung auf mobilen Geräten und sind folgerichtig für 81 Prozent aller befragten Führungskräfte das wichtigste Mittel zum Fernzugriff auf Geschäftsdaten. ■

2 Verlust, Diebstahl und schlechte Angewohnheiten: wie Unternehmen die Herausforderungen bewältigen

Die Implementierung von Systemen zum Schutz von Unternehmensdaten, auf die über eine Vielzahl unterschiedlicher Plattformen zugegriffen wird, kostet Geld. Vor diesem Hintergrund überrascht es wenig, dass lediglich die Umfrageteilnehmer aus den größten Unternehmen Vertrauen in die Datensicherheitsmaßnahmen ihrer Arbeitgeber setzen. Während uns 45 Prozent der Befragten aus Unternehmen mit einem Jahresumsatz von mindestens 10 Milliarden US-Dollar mitteilten, ihre Firmen verfügten über Datensicherheitsmaßnahmen auf dem Stand der Technik, kam dieselbe Aussage nur von 10 Prozent der Befragten aus Unternehmen mit einem Jahresumsatz von höchstens 500 Millionen US-Dollar. Doch selbst bei den Unternehmen mit Umsätzen zwischen 500 Millionen und 5 Milliarden US-Dollar beschrieben 33 Prozent aller Befragten die Richtlinien ihres Arbeitgebers als unzureichend oder völlig unzureichend.

Im Großen und Ganzen akzeptieren die befragten Führungskräfte die Tatsache, dass Investitionen erforderlich sind, wobei für 69 Prozent Ausgaben für Sicherheitsdienste eine Priorität darstellen. Allerdings deuten unsere Untersuchungen darauf hin, dass in der Aufklärung von Führungskräften über Sicherheitsrisiken noch Handlungsbedarf besteht. So zeigte sich, dass einige Unternehmen, die über ihrer Ansicht nach umfassende Sicherheitsmaßnahmen verfügen, riskanten Praktiken stattgeben. Unter den Führungskräften, die angaben, ihre Unternehmen verfügten über branchenführende Sicherheitsvorkehrungen (20 Prozent), gaben uns 13 Prozent zu verstehen, ihre Aktivitäten in sozialen Netzwerken unterlägen keinen Beschränkungen. Eine solche Praxis birgt selbstverständlich das Risiko, dass vertrauliche Unternehmensinformationen versehentlich an die Öffentlichkeit gelangen. Wie unsere Untersuchungen weiter ergaben, lassen sich durch Richtlinien für die Nutzung sozialer Netzwerke sowohl eine effektive Interaktion ermöglichen als auch Unternehmensdaten schützen und Haftungsrisiken vermeiden.

Kleinere Unternehmen können auf weniger Ressourcen zurückgreifen als ihre größeren Pendants, woraus sich ihre Herausforderungen im Schutz mobiler Daten noch einmal verschärfen. Daher verwundert es kaum, dass fast 40 Prozent der Befragten aus Unternehmen mit einem jährlichen Umsatz von höchsten 500 Millionen US-Dollar die Richtlinien ihrer Unternehmen zum Schutz mobiler Daten als unzureichend oder völlig unzureichend beschrieben. Doch große wie kleine Unternehmen, die über durchgesetzte, schriftliche Richtlinien verfügen, können mit relativ geringem finanziellen Aufwand viel zum Schutz ihrer Daten beitragen. Denn viele Geräte, die in den letzten Jahren auf den Markt kamen, besitzen integrierte Verschlüsselungsfunktionen, die einfach nur aktiviert werden müssen. Zur Automatisierung von Sicherheitsprozessen sind jedoch oftmals zusätzliche Verwaltungstools erforderlich. Kleinere Firmen müssen daher abwägen, ob sie in Schutztechnologien investieren oder lieber auf

BYOD in den Griff bekommen

Da das Modell Bring Your Own Device noch vergleichsweise neu ist, gibt es bislang nur wenige bewährte Branchenstandards für BYOD-Richtlinien. Verlässt ein Mitarbeiter das Unternehmen – freiwillig oder nicht –, müssen die Unternehmensdaten auf seinen Geräten in der Regel schnell entfernt werden, und dies vorzugsweise ohne auf seine privaten Daten zugreifen zu müssen. BYOD-Richtlinien enthalten für gewöhnlich eine Bestimmung, welche dies zulässt. Laut einer Empfehlung der Zeitschrift National Law Review vom Juni 2012 können Unternehmen sich dabei durch eine Anpassung ihrer bestehenden Richtlinien für mobile Geräte auch rechtlich absichern. Richtlinien zu Belästigung und Diskriminierung, zu gleichen Beschäftigungschancen, zu Vertraulichkeit und zum Schutz von Geschäftsgeheimnissen sowie Compliance- und Ethik-Richtlinien können so aktualisiert werden, dass Unternehmen vor dem Missbrauch mobiler Geräte durch ihre Mitarbeiter geschützt sind.

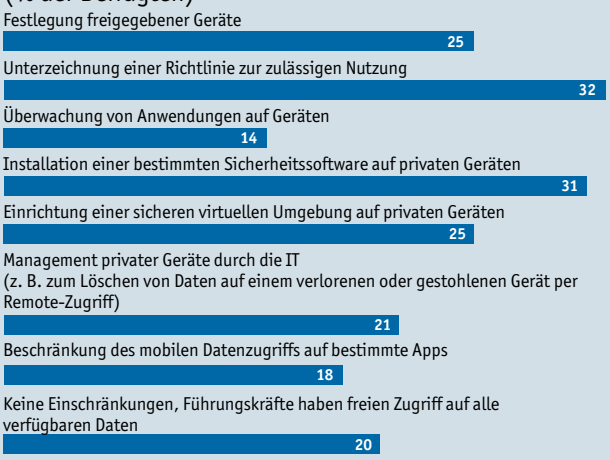
Als Schutzmaßnahme gegen riskante Praktiken installieren viele Unternehmen außerdem spezielle Software auf den Geräten ihrer Mitarbeiter. Hiermit können die Geräte abgeriegelt, Daten verschlüsselt und weitere Verwaltungsfunktionen wie die Aktualisierung von Kalenderdaten und das Einspielen von Sicherheitsupdates durchgeführt werden. Der Mitarbeiter mag dies als unangemessenen Eingriff empfinden, doch die meisten Richtlinien für mobile Geräte sehen eine solche Form der Fernüberwachung und -steuerung vor. Einige Unternehmen mit BYOD-Programmen erwarten von ihren Führungskräften und Mitarbeitern, dass sie auf eigene Kosten die erforderliche Software auf ihren Geräten installieren. Andere wiederum erstatten die Kosten für Software, die für die geschäftliche Nutzung des Geräts erforderlich ist, teilweise oder vollständig. „Die richtige Konfiguration und die Einhaltung von Nutzungsbedingungen müssen zentral überwacht und durchgesetzt werden“, weiß Al Raymond von Aramark. Zusätzlich lasse sich durch regelmäßige Schulungen zum Sicherheitsbewusstsein gewährleisten, dass das Thema sicherer Datenzugriff bei Mitarbeitern nicht in Vergessenheit gerät.

Laut Raymond verfolgt sein Unternehmen jedoch einen anderen Ansatz zur Verwaltung mobiler Geräte und zum Schutz der darauf gespeicherten Daten. Die Mitarbeiter nutzen ihre Geräte lediglich zur Darstellung der Daten, die auf den Servern des Unternehmens bleiben. Die Server wiederum gewährleisten einen sicheren Zugriff und entlasten die mobilen Geräte zusätzlich, da sie die Rechenarbeit übernehmen. Die hierzu erforderlichen Mittel, wie Desktopvirtualisierung und Datenzugriff über webbasierte Dienste wie Salesforce.com, finden immer breitere Anwendung, da Unternehmen beim mobilen Zugriff auf sichere Netzwerke Verschlüsselung, Authentifizierung und Verwaltung steuern können.

Arturo Medina von Ipsos, wo sich ähnliche netzwerkbasierte Kontrollen finden, empfiehlt einen ständigen Dialog mit Mitarbeitern, um die Einhaltung von Richtlinien sicherzustellen und das unbefugte Herunterladen von Unternehmensdaten zu verhindern. „Man muss eine klare Grenze zwischen sensiblen Unternehmensdaten und Benutzerdaten ziehen und klarstellen, welche Daten auf den Servern des Unternehmens gesichert werden und welche Daten als privat gelten“, lautet Medinas Rat.

F

BYOD-Richtlinien
Welche Bestimmungen enthalten die BYOD-Richtlinien Ihres Unternehmens für den Zugriff auf kritische Daten? Wählen Sie alle zutreffenden Antworten aus.
(% der Befragten)



Quelle: Umfrage der Economist Intelligence Unit, Juni 2012.

kostengünstigere Methoden setzen sollten, indem sie etwa ihren Mitarbeitern Sicherheitsrichtlinien auferlegen.

Im selben Maße wie die Leistungsfähigkeit selbst kleinster mobiler Geräte steigt unterdessen das Risiko, Daten aus Gründen zu verlieren, die wenig mit Technologie zu tun haben. Laut dem PC-Zubehörhersteller Kensington gehen jährlich mehr als 70 Millionen Smartphones verloren, von denen nur 7 Prozent wieder zu ihrem Besitzer finden. Und auch Laptops kommen zuweilen abhanden – den Recherchen von Kensington

zufolge werden 10 Prozent aller Geräte verloren oder gestohlen. Drei Viertel aller Geräte verschwinden dabei während der Übergabe zwischen Mitarbeitern oder außerhalb des Unternehmens. Erschwert wird der Verlust in vielen Fällen durch die Tatsache, dass mit dem Gerät auch Unternehmensdaten in fremde Hände gelangen.

Die durchschnittlichen Kosten eines Datenlecks in einem Unternehmen beliefen sich 2010 laut dem Beratungsunternehmen Ponemon Institute auf 7,2 Millionen US-Dollar – pro Fall. 2005 betrugen die durchschnittlichen Kosten nicht einmal die Hälfte. Al Raymond von Aramark hält diese Zahlen angesichts der Anzahl und Arten von Datenverlusten für glaubhaft. Neben hunderten kleineren Vorfällen jährlich komme es zudem immer wieder zu einigen schweren Vorfällen, deren Kosten sich auf 25 bis 500 Millionen US-Dollar summieren könnten.

Besondere Sorge bereitet Unternehmen, die Verletzungen der Datensicherheit durch Mitarbeiter verhindern wollen, der Umstand, dass Daten auf mobilen Geräten häufig durch Unachtsamkeit abhandenkommen. Wie die Ponemon-Studie *Cost of Data Breach* vom 2011 belegt, sind 30 bis 40 Prozent aller Datenpannen auf Fahrlässigkeit zurückzuführen, während böswillige Angriffe mit 43 Prozent kaum häufiger die Ursache sind. Weiter lässt sich laut der Studie die Hälfte aller Sicherheitsverletzungen in italienischen Unternehmen auf den Diebstahl oder Verlust mobiler Geräte zurückführen. Nur in Deutschland (42 Prozent), Frankreich (43 Prozent) und Australien (36 Prozent) stellten böswillige Angriffe eine größere Gefahr dar als Fahrlässigkeit. Indien stellte sich als einziges Land heraus, in dem Systemstörungen oder -ausfälle häufiger die Ursache von Datenverlusten sind als Fahrlässigkeit und Böswilligkeit.

Einige nennenswerte Fälle des Verlusts eines mobilen Geräts veranschaulichen, wie schnell es zu einer Sicherheitsverletzung kommen kann. Der Krebsklinik Cancer Care Group in Indianapolis kamen im Juli 2012 personenbezogene Daten von mehr als 55.000 Patienten sowie ihrer Mitarbeiter abhanden, als der Laptop eines Angestellten mit Backup-Dateien des Servers aus einem abgeschlossenen Fahrzeug entwendet wurde. Entgegen der allgemein empfohlenen Vorgehensweise waren die Daten nicht verschlüsselt. Das MD Anderson Cancer Center der Universität Texas erlitt in Juni und Juli 2012 gleich zwei Sicherheitsverletzungen. Während beim ersten Vorfall ein USB-Stick mit unverschlüsselt gespeicherten Daten in einem Bus verloren ging, wurde beim zweiten Mal der Laptop – ebenfalls mit unverschlüsselten Daten – aus dem Haus einer Lehrkraft entwendet. Bei diesen beiden Datenpannen gerieten Informationen zu mehr als 30.000 Patienten in fremde Hände. Nach dem zweiten Datenverlust begann die Einrichtung, aus den Vorfällen eine Lehre zu ziehen und ihren kompletten Datenbestand zu verschlüsseln.

Unternehmen können dem Verlust von Daten in vielen Fällen vorbeugen, indem sie mobile Geräte – egal, ob Laptops, Smartphones oder tragbare Speichermedien – mit einem Passwortschutz versehen und Datenträger vollständig verschlüsseln.

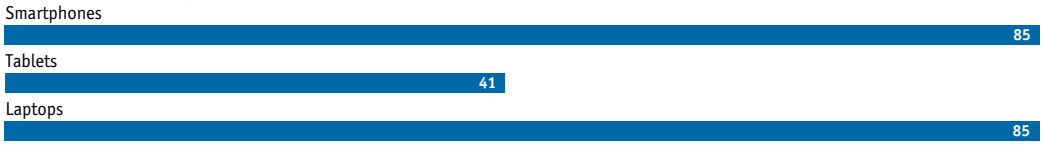
Zusätzliche sollten Geräte physisch gesichert werden. So sollten Geräte beispielsweise niemals in unbeaufsichtigt abgestellten Fahrzeugen zurückgelassen werden, selbst wenn diese abgeschlossen wurden. Smartphones sowie Laptops mit der VPro-Technik von Intel lassen sich zudem im Falle eines Verlusts aus der Ferne sperren, wobei auch darauf gespeicherte Daten gelöscht werden können. Je sensibler die Daten auf einem Gerät sind, desto wichtiger ist die Einrichtung eines solchen Mechanismus, da eine Verschlüsselung geknackt werden kann und somit allein keinen ausreichenden Schutz darstellt. ■

3 Immer mehr Daten „zum Mitnehmen“: aktuelle Entwicklungen

Fast 90 Prozent aller Unternehmen weltweit gestatten laut der Internationalen Fernmeldeunion (ITU), einer Sonderorganisation der Vereinten Nationen, den Zugriff auf kritische Daten über mobile Geräte. Von den in der Umfrage des Economist vertretenen Unternehmen, die über keine formellen BYOD-Richtlinien verfügen, planen 25 Prozent die Einrichtung eines entsprechenden Programms in den kommenden 12 bis 18 Monaten. Als Hauptgrund führen sie an, BYOD sorge für motiviertere Mitarbeiter – eine Beobachtung, die auch von unabhängigen Studien bestätigt wird. Einer im August 2012 von iPass, einem Anbieter von Software für Mobilgeräte, durchgeführten Studie zufolge machen viele Mitarbeiter, die stets online sind, bis zu 20 unbezahlte Überstunden pro Woche. Beinahe 90 Prozent der von iPass befragten Arbeitnehmer gaben an, eine mobile Internetverbindung sei ein ebenso wichtiger Bestandteil ihres Lebens wie Strom und fließend Wasser.

Doch obwohl immer mehr Arbeitskräfte auch außerhalb des Büros tätig sind, stellt der mobile Zugriff auf geschäftliche Daten im Rahmen von BYOD für einige Unternehmen keine Option dar. Stark regulierte Einrichtungen wie Banken und Finanzgesellschaften etwa besitzen strenge Richtlinien, die Führungskräften den Zugriff auf Geschäftsdaten über private Geräte verbieten. Steve Ellis, Executive Vice President von Wells Fargo, bemerkt in diesem Zusammenhang, sein Unternehmen nähere sich dem Thema BYOD mit Vorsicht und werte derzeit verschiedene Optionen aus. „Bis wir ein formelles Programm haben, kann noch ein Jahr vergehen“, blickt Ellis in die Zukunft. Andere Unternehmen ohne formelle BYOD-Richtlinien berichten unterdessen, private Geräte schlichen sich unterhalb des Radars bei ihnen ein. Bevor Aramark vor zehn Monaten seine Richtlinien für mobile Geräte einführte, gab es keine feste Regelung darüber, welche Geräte und Betriebssysteme mit dem Unternehmensnetzwerk verbunden werden durften. Mit den neuen Richtlinien dagegen, die rollenbasierten Zugriff und bestimmte genehmigte Geräte und

Unternehmenseigene Geräte für Führungskräfte
Welche Arten von Geräten stellt Ihr Unternehmen seinen Führungskräften für den Zugriff auf kritische Daten zur Verfügung?
Wählen Sie alle zutreffenden Antworten aus.
(% der Befragten)



Quelle: Umfrage der Economist Intelligence Unit, Juni 2012.

Fallstudie US-Behörde für Chancengleichheit am Arbeitsplatz startet BYOD-Pilotprojekt

Das Budget der Equal Employment Opportunity Commission (EEOC) der US-Regierung wurde im Geschäftsjahr 2012 um fast 15 Prozent von 17,6 auf 15 Millionen US-Dollar gekürzt. Chief Information Officer Kimberly Hancher sah sich daher gezwungen, die Betriebskosten zu senken, und entschied sich, das Budget der Behörde für mobile Geräte um die Hälfte zu reduzieren. Um die hierdurch entstandene Lücke zu füllen, startete die Behörde ein BYOD-Pilotprojekt. Im Mittelpunkt stand dabei, Mitarbeitern den Zugriff auf E-Mail-Konten, Kalenderdaten sowie Kontakt- und Aufgabenlisten der Behörde zu ermöglichen. Ausgewählte Führungskräfte erhielten im Rahmen des Projekts zudem privilegierten Zugriff auf die internen Systeme der Behörde.

In der ersten Testphase gaben 40 freiwillige Mitarbeiter ihre von der Regierung bereitgestellten BlackBerrys zurück und verwendeten stattdessen ihre eigenen Smartphones. Die Mitarbeiter aus der Informationssicherheit, die Rechtsabteilung und die Gewerkschaft erstellten Regeln, um die Anforderungen an die Privatsphäre der Mitarbeiter (Social-Media- und Überwachungsrichtlinien) mit den Sicherheitsbestimmungen der Regierung in Einklang zu bringen, darunter etwa die Sonderveröffentlichung SP 800-53 zu empfohlenen Sicherheitskontrollen für Bundesinformationssysteme und -organisationen des National Institute of Standards and Technology (NIST). Die zweite Phase des Projekts startete im Juni 2012. Dabei richtete die EEOC zusammen mit ihren Auftragnehmern den Zugriff auf die E-Mail-Konten der Behörde für Mitarbeiter ein, die an der zweiten Testphase teilnahmen. Den übrigen 468 Mitarbeitern, die bis dahin weiter BlackBerrys der EEOC genutzt hatten, wurden drei Optionen angeboten:

1. Sie konnten ihren BlackBerry freiwillig zurückgeben und stattdessen ein privates Android-, Apple- oder BlackBerry-Smartphone oder -Tablet zum Arbeiten verwenden.

2. Sie konnten ihren BlackBerry zurückgeben und dafür ein Mobiltelefon von der Regierung erhalten, das lediglich Telefonfunktionen besitzt.

3. Sie konnten ihren BlackBerry behalten und mussten anerkennen, dass die EEOC ihnen bei Bedarf kein Ersatzgerät zur Verfügung stellen kann.

Laut den Direktoren der EEOC erwies sich das Pilotprojekt bislang als Erfolg. Die Mitarbeiter tragen die Kosten für die Nutzung von Sprach- und Datendiensten selbst, während die Behörde die Lizenzkosten für die Verwaltungssoftware übernimmt. Kimberly Hancher zufolge könnten sich die Kosten für einige Mitarbeiter jedoch als Problem erweisen, weshalb auch noch die Frage zu klären sei, ob die Behörde nicht zumindest einen Teil der Kosten für die Sprach- und Datendienste erstatten könne. Die frühzeitige Einbindung von Mitarbeitern, Gewerkschaft und Rechtsabteilung, so Hancher, sei der Erfolgsgarant für dieses Projekt gewesen. ■

Konfigurationen vorsehen, weiß das Unternehmen heute genau, wer auf welche Daten zugreifen kann. „Damit hat das Augenzudrücken ein Ende“, begrüßt Al Raymond die Neuerung. Und schließlich gilt: Je transparenter Richtlinien sind, desto eher werden sie auch befolgt.

Neben Richtlinien haben auch neue Arten von Geräten Einzug in die Unternehmenswelt erhalten. Gemäß unserer Umfrage erfolgt der Zugriff auf kritische Daten in mehr als einem Viertel aller Fälle (27 Prozent) über Smartphones. Die Teilnehmer unserer Umfrage erwarten in den nächsten 12 bis 18 Monaten einen Anstieg der Smartphone-Nutzung auf 35 Prozent, während der Zugriff auf kritische Daten ihren Vermutungen zufolge zu 30 Prozent über andere mobile Geräte erfolgen wird (zurzeit 20 Prozent). Im Zuge des Aufkommens neuer Software und dazugehöriger Geräte sind auch Tablets prädestiniert, Führungskräften immer häufiger als Fenster zur Welt der Unternehmensdaten zu dienen. Laut einem Artikel im *Economist* (Oktober 2011) könnten sie eines Tages womöglich sogar das Smartphone ersetzen. Dank ihrer größeren Displays lassen sich mehr Daten anzeigen, und mit einer externen Tastatur ausgestattet ermöglichen sie auch eine einfachere Interaktion mit Apps.

Obwohl 42 Prozent der Befragten angaben, für eine optimale Produktivität von Führungskräften sei ein sicherer und zeitnaher Zugriff auf strategische Planungsdaten nötig, hielten es interessanterweise nur 28 Prozent für angemessen, diese Daten auf mobilen Geräten verfügbar zu machen. Als größtes Hindernis auf dem Weg zu BYOD stellte sich wenig überraschend die Besorgnis über Sicherheits- und andere Risiken heraus. Dessen ungeachtet gaben uns nur 11 Prozent der Befragten zu verstehen, ihre Unternehmen gestatteten den Zugriff auf kritische Daten außerhalb des Büros nicht. ■

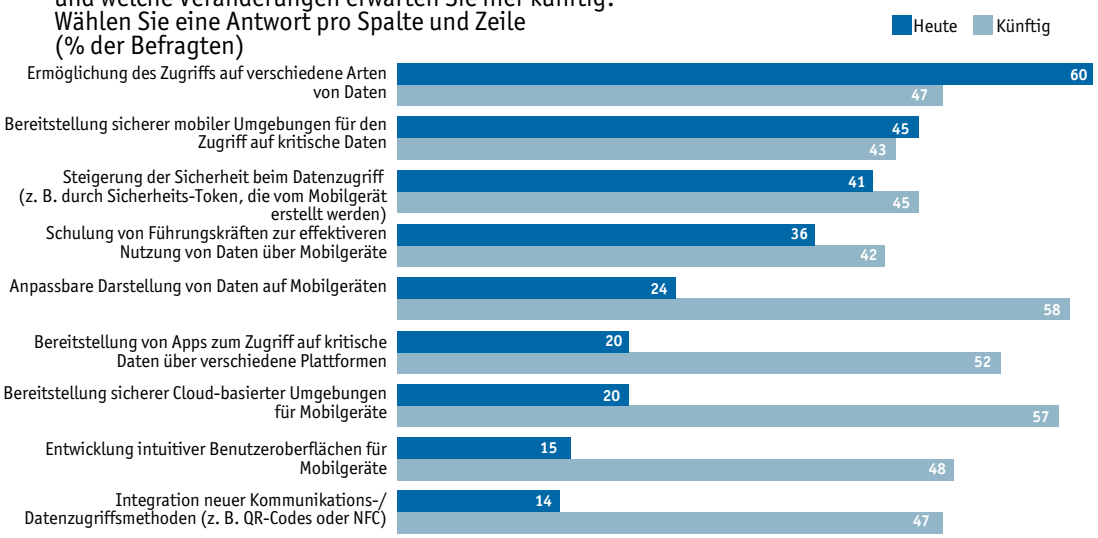
4 Wie können Unternehmen effektive Richtlinien für mobile Geräte gewährleisten?

Die Teilnehmer unserer Umfrage haben die Vorteile des mobilen Datenzugriffs klar erkannt und wissen um die hierfür notwendigen Investitionen und Maßnahmen. Einige der Maßnahmen, die zum Schutz von Unternehmensdaten beim Zugriff über mobile Geräte erforderlich sind, lassen sich aus der Ferne treffen. Schon heute können IT-Verantwortliche oftmals mit vorhandenen Verwaltungstools Laptops, Smartphones und Tablets mit Sicherheitsfunktionen ausstatten. Zusätzlich können sie private Daten von Unternehmensdaten trennen und letztere in Unternehmensnetzwerken duplizieren und speichern. Virtuelle Desktops ermöglichen zu guter Letzt den sicheren mobilen Zugriff auf Daten über private Laptops. All diese Schutzmaßnahmen gestatten es mobilen Mitarbeitern, Daten mit relativ geringem Aufwand wiederherzustellen, falls ihr Gerät verloren geht oder beschädigt wird. Unsere Umfrageteilnehmer sind sich einig, dass diese Maßnahmen es künftig immer mehr Führungskräften ermöglichen werden, von jedem beliebigen Computer aus sicher auf Unternehmensdaten zuzugreifen.

Führungskräfte, die weniger Zeit für die Aktualisierung von Sicherheitsprotokollen

F

Mobilitätsmaßnahmen
Auf welche Weise unterstützt Ihr Unternehmen heute den Zugriff auf kritische Daten und welche Veränderungen erwarten Sie hier künftig?
Wählen Sie eine Antwort pro Spalte und Zeile
(% der Befragten)



Quelle: Umfrage der Economist Intelligence Unit, Juni 2012.

aufwenden müssen, haben auf Geschäftsreisen mehr Zeit für ihre eigentliche Arbeit. Laut Ashwani Tikoo von CSC wird die Datensicherheit in Zukunft durch neue Technologien verstärkt, die direkt in Anwendungen integriert sind und die Daten selbst schützen. Das Abfangen und der Missbrauch von Daten werde auf diese Weise zusätzlich erschwert. „Eine Anwendung sollte in der Lage sein, zu erkennen, ob ich ein iPad oder ein kleines Fünf-Zoll-Display vor mir habe, und mir die Daten entsprechend aufbereiten", führt Tikoo seine Erwartungen an die Zukunft weiter aus.

Obschon sein Unternehmen es nicht vorschreibe, hält Al Raymond getrennte Umgebungen für die geschäftliche und private Nutzung für wichtig. Würden die Richtlinien oder sonstigen Sicherheitsmaßnahmen für diese Umgebungen allerdings nicht durchgesetzt, bliebe dies nicht ohne Folgen. In Gesprächen mit Kollegen aus anderen Firmen, berichtete uns Raymond, sei er immer wieder überrascht, wie viele der vermeintlichen Sicherheitsmaßnahmen in großen Unternehmen sich als „Schall und Rauch" herausstellten. Viel mehr als ein Lippenbekenntnis sei oftmals nicht auszumachen.

Beim weltweit tätigen Marktforschungsinstitut Ipsos ist jeder Mitarbeiter verpflichtet, über das Intranet an einer Schulung zum Sicherheitsbewusstsein teilzunehmen – ein kostengünstiger Weg, alle Mitarbeiter in 84 Ländern zu erreichen. Für die interne Entwicklung des Schulungsprogramms wurden kommerziell verfügbare Lösungen zum Sicherheitsbewusstsein verschiedener Anbieter wie dem National Security Institute (NSI) eingesetzt, die sich an die lokalen Anforderungen anpassen ließen. Zusätzlich sind die Mitarbeiter von Ipsos verpflichtet, eine Richtlinie zur zulässigen Nutzung von Mobilgeräten zu unterzeichnen, in der unter anderem dargelegt wird, auf welche Arten von Daten über die Geräte zugegriffen werden darf und welche Passwortstärke erforderlich ist.

Sicherheitsmaßnahmen wie die Einrichtung von Passwörtern erfordern eine zuverlässige Mitwirkung seitens der Benutzer. Schätzungen der Prüfungsgesellschaft Coalfire zufolge ist jedoch nur die Hälfte aller privaten Geräte tatsächlich mit einem Passwort geschützt. Als weitere Sicherheitsmaßnahme im Rahmen eines BYOD-Programms müssen Mitarbeiter zustimmen, dass ihre IT-Abteilung im Falle eines Verlusts oder Diebstahls des privaten Geräts befugt ist, zum Schutz der Unternehmensdaten sämtliche auf dem Gerät gespeicherten Informationen aus der Ferne zu löschen.

Die meisten Unternehmen haben offensichtlich noch einen weiten Weg vor sich, bis alle Mitarbeiter über die Sicherheitsfragen aufgeklärt sind, die der mobile Zugriff auf Unternehmensdaten aufwirft. Wie aus unserer Umfrage hervorging, treffen Datensicherheitsrichtlinien für private Geräte bei Führungskräften außerhalb Europas und Nordamerikas noch am ehesten auf Widerstand. Dabei darf nicht vergessen werden, dass sich Sicherheitslücken in einem Teil unserer zunehmend vernetzten Geschäftswelt schnell auf Unternehmen mit durchgesetzten Richtlinien sowie deren Kunden in anderen Teilen der Welt auswirken können. ■

5 Fazit

Dieser Bericht konnte unmissverständlich aufzeigen, dass der mobile Datenzugriff nicht nur immer weiterwächst, sondern dass der Trend geradezu unaufhaltbar ist. Nicht verwaltete und ungesicherte mobile Geräte haben sich in der Zwischenzeit längst in die Geschäftswelt eingeschlichen. Einmal kompromittiert öffnen sie Angriffen Tür und Tor und bringen Unternehmensdaten in Gefahr. Fast ein Drittel aller für diesen Bericht befragten Führungskräfte gab zudem an, ihr Unternehmen verfüge nur über unzureichende Richtlinien für mobile Geräte. Dabei ist die Festlegung sinnvoller, praxistauglicher Richtlinien nur der erste Schritt in Richtung eines tragfähigen BYOD-Programms, das den Datenzugriff über das eigene mobile Gerät gestattet.

Diejenigen Führungskräfte, welche die Geräterichtlinien ihres Unternehmens als „branchenführend" einstuften, führten an, sie könnten mithilfe des mobilen Datenzugriffs Entscheidungen effektiver und koordinierter treffen, mehr Chancen wahrnehmen und effizienter mit ihren Geschäftspartnern und Kunden zusammenarbeiten. Damit dieser mobile Zugriff nicht zu einer Gefahr für Geschäftsdaten wird, sollten Führungskräfte jedoch Programmen zur Risikominimierung Priorität einräumen und Investitionen in Daten- und Sicherheitsdienste unterstützen.

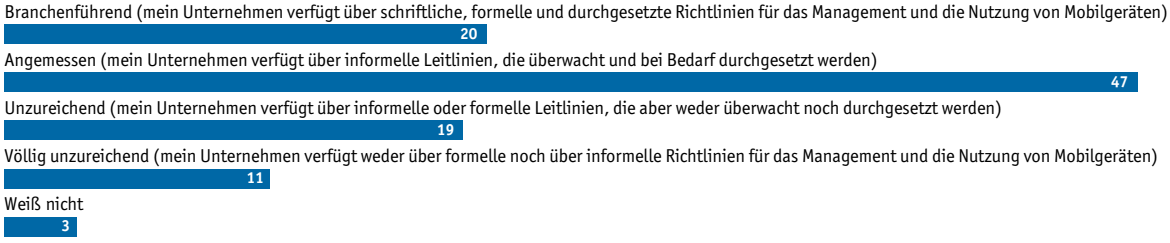
Vernetzte Geräte sind in der modernen globalen Geschäftswelt nicht mehr wegzudenken. Derweil zeichnet sich insbesondere aufgrund des wachsenden Segments der Tablets ein Umbruch in der mobilen Unternehmenslandschaft ab. Infolge der Veröffentlichung der nächsten Generation von Betriebssystemen dürfte bei den Tablets weiterhin ein rasantes Wachstum zu verzeichnen sein, da neuere Softwareversionen zusätzliche Optionen für den Datenzugriff mitbringen, die Smartphones oftmals vorenthalten bleiben. Analysten sehen hierin jedoch einen zweifelhaften Segen, da Tablets vorhandene Systeme ergänzen und nicht ersetzen werden, wodurch der zu verwaltende und zu sichernde Gerätepark weiterhin wächst.

Für den Schutz kritischer Daten könnten somit künftig noch strengere Zugriffsrichtlinien erforderlich sein. So wird denn auch das Tablet als neuerdings bevorzugtes Gerät für berufliche Angelegenheiten außerhalb des Büros ganz neue Herausforderungen mit sich bringen, da Führungskräfte über ihre neuen mobilen Begleiter auf eine größere Bandbreite an Daten zugreifen wollen. Viele Unternehmen werden daher gezwungen sein, sich mit dem Thema des mobilen Datenzugriffs erneut auseinanderzusetzen – angefangen bei den Geräten und ihren Schwachstellen über die verfügbare Infrastruktur bis hin zu den Benutzern selbst. ■

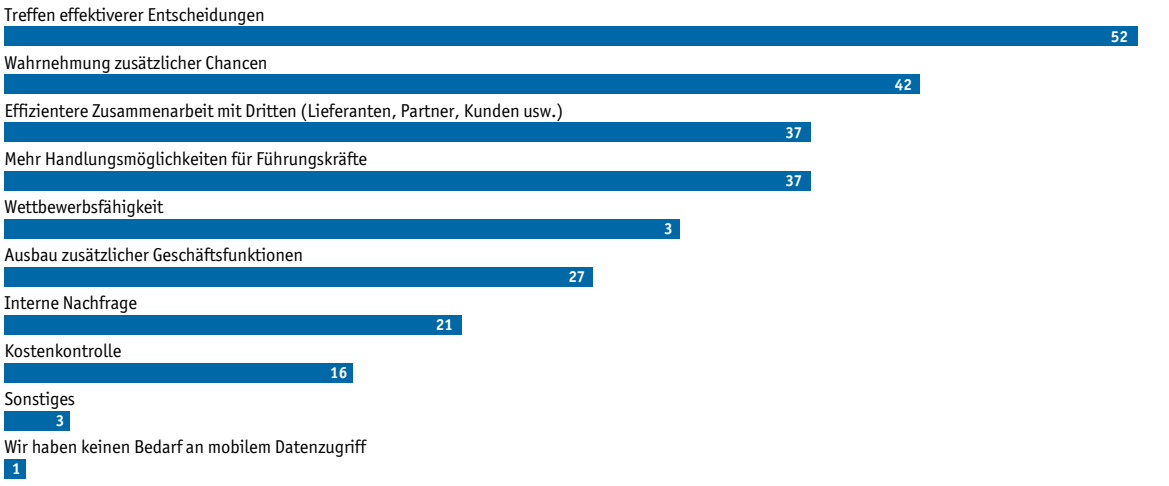
Anhang: Umfrageergebnisse

Aufgrund von Rundungen und der Möglichkeit mehrerer Antworten summieren sich die Prozentangaben ggf. nicht auf 100 Prozent.

Wie würden Sie die Richtlinien Ihres Unternehmens für Mobilgeräte im Vergleich zu jenen brancheninterner Wettbewerber beurteilen?
(% der Befragten)

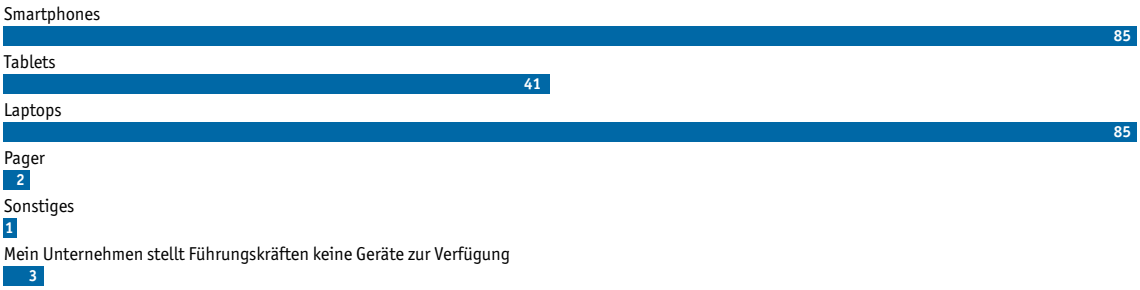


Welche maßgeblichen Geschäftsfaktoren steigern den Bedarf am Zugriff auf kritische Daten über Mobilgeräte?
Wählen Sie maximal drei.
(% der Befragten)



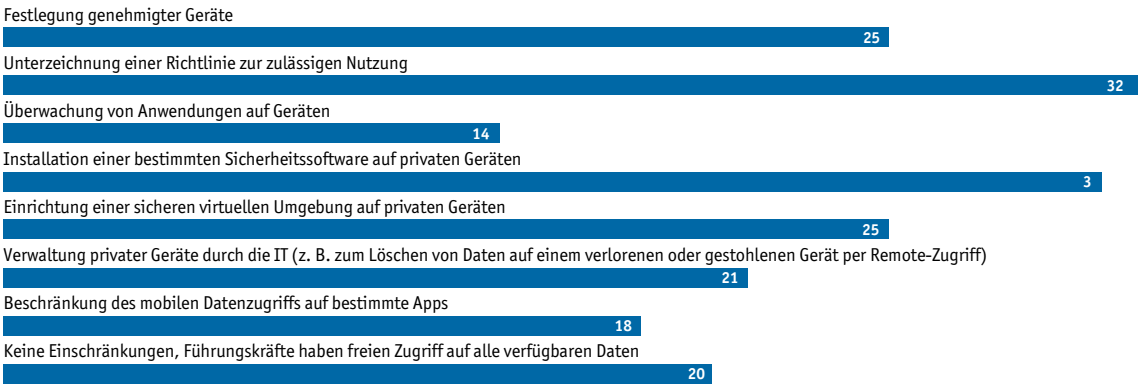
Gestattet Ihr Unternehmen außerhalb des Büros den Zugriff auf kritische Daten?
(% der Befragten)

Welche Arten von Geräten stellt Ihr Unternehmen seinen Führungskräften für den Zugriff auf kritische Daten zur Verfügung? Wählen Sie alle zutreffenden Antworten aus.
(% der Befragten)

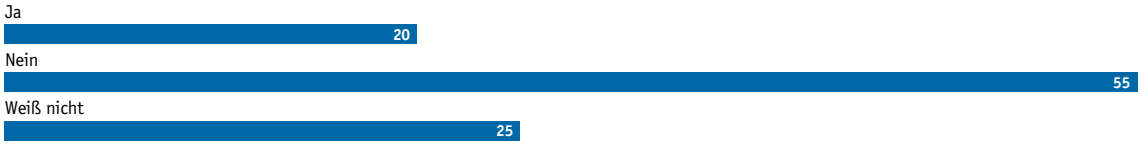


Gestattet Ihr Unternehmen seinen Führungskräften, statt unternehmenseigener Geräte private Geräte für den Zugriff auf kritische Daten zu verwenden?
(% der Befragten)

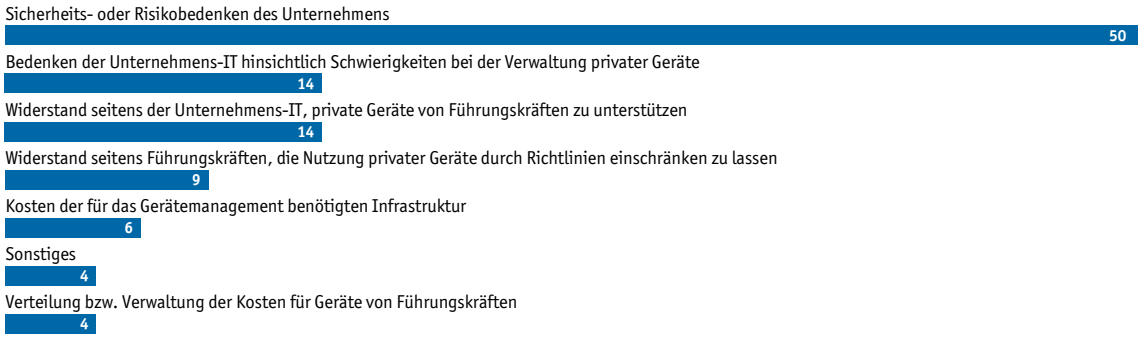
Welche Bestimmungen enthalten die BYOD-Richtlinien Ihres Unternehmens für den Zugriff auf kritische Daten?
Wählen Sie alle zutreffenden Antworten aus.
(% der Befragten)



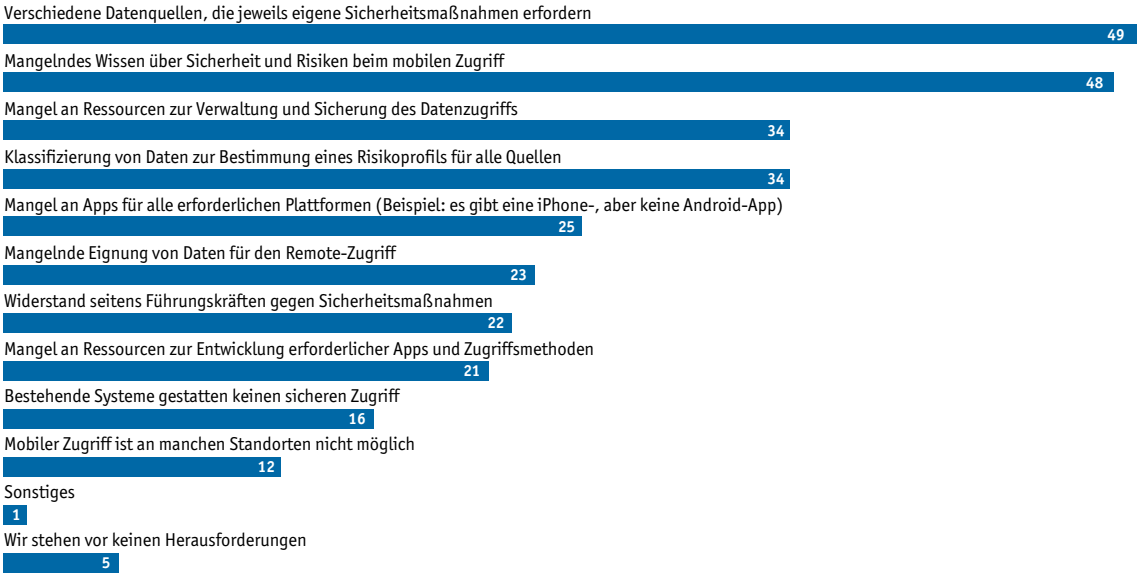
Beabsichtigt Ihr Unternehmen die Einführung eines BYOD-Programms für den Zugriff auf kritische Daten?
(% der Befragten)



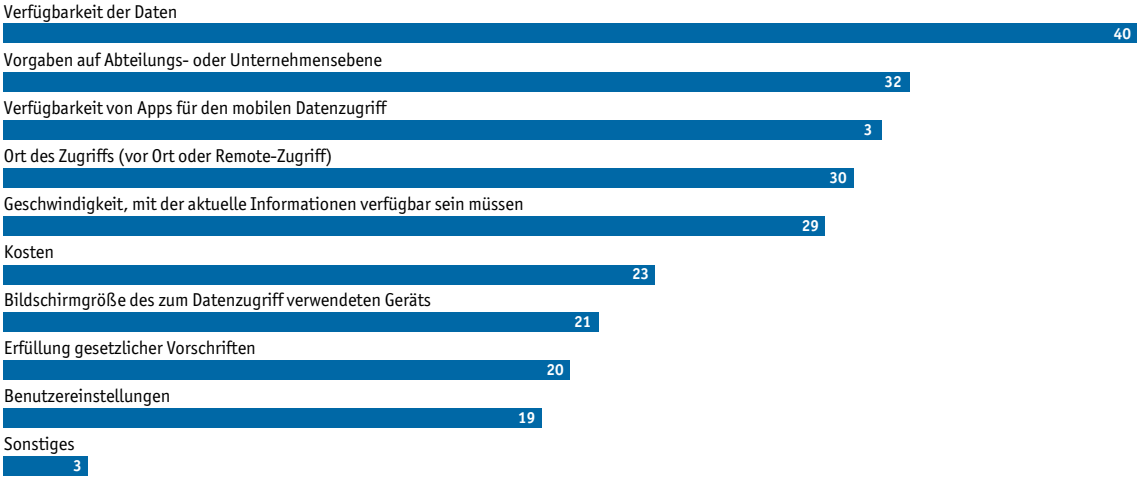
Worin besteht Ihrer Meinung nach das größte Hindernis für die Einführung eines BYOD-Programms für den Zugriff auf kritische Daten?
(% der Befragten)



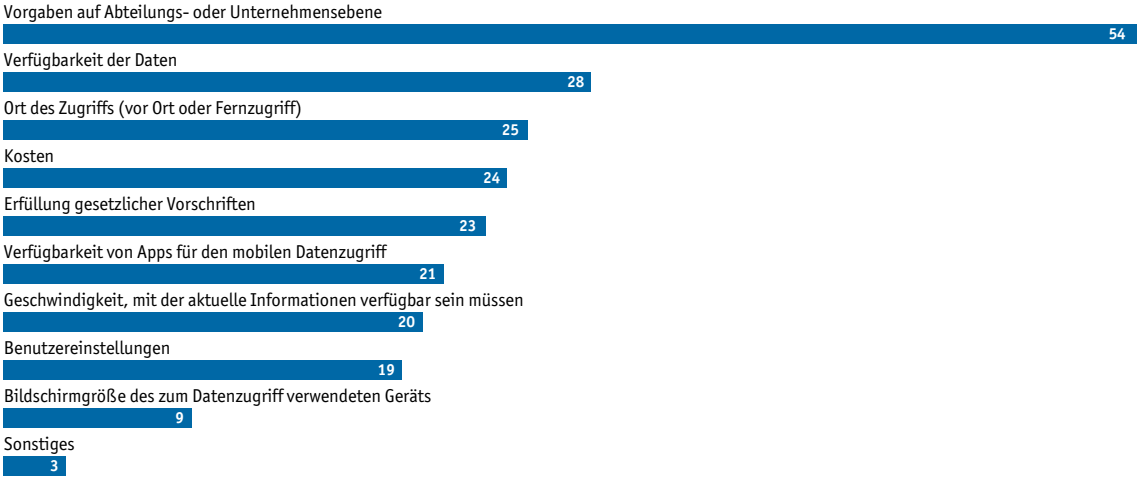
Worin bestehen Ihrer Meinung nach die größten Herausforderungen für Ihr Unternehmen bei der Gewährleistung eines sicheren Zugriffs auf kritische Daten über unternehmenseigene oder private Mobilgeräte?
Wählen Sie maximal vier.
(% der Befragten)



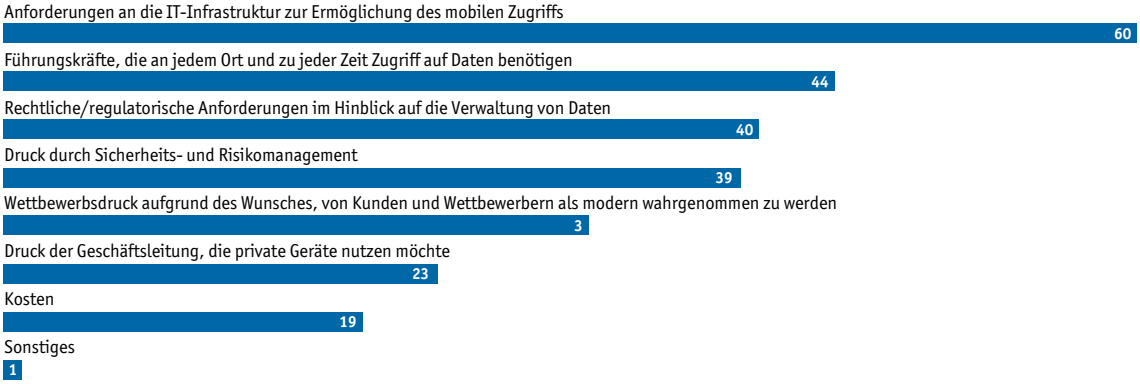
Welche Faktoren neben Ihrer Position bestimmen, auf welche Daten Sie heute bzw. künftig über Mobilgeräte zugreifen können?
Wählen Sie maximal drei.
(% der Befragten)



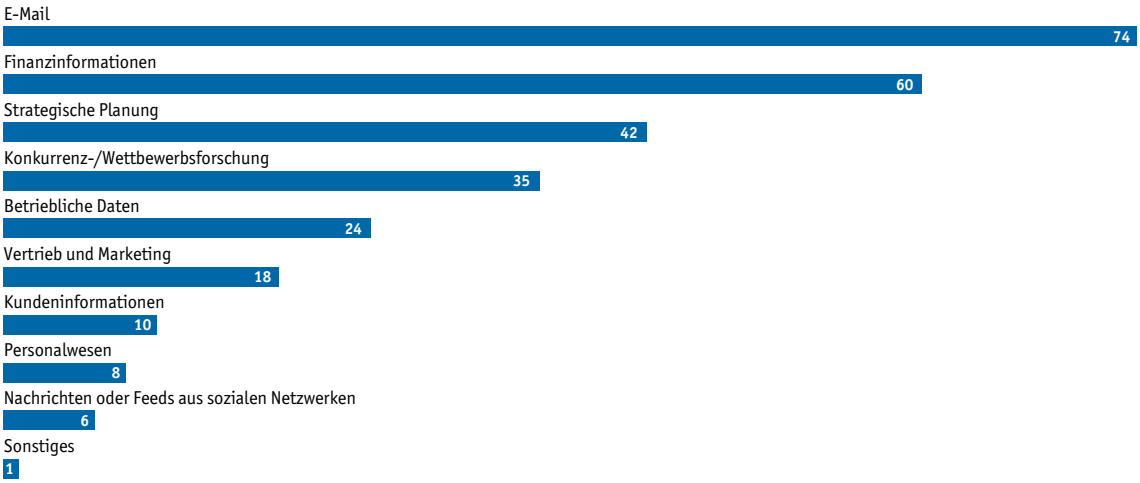
Welche Faktoren bestimmen, wer heute bzw. künftig über Mobilgeräte auf kritische Daten zugreifen darf?
Wählen Sie maximal drei.
(% der Befragten)



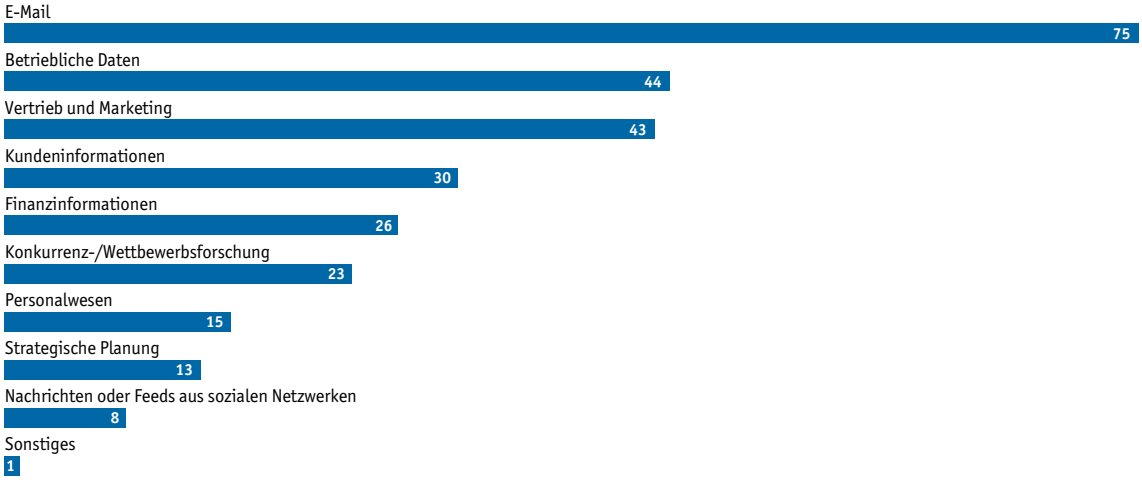
Welche Faktoren üben den größten Einfluss auf die Richtlinien Ihres Unternehmens und die Entwicklung einer Strategie für Mobilgeräte und Anwendungen aus?
Wählen Sie maximal drei.
(% der Befragten)



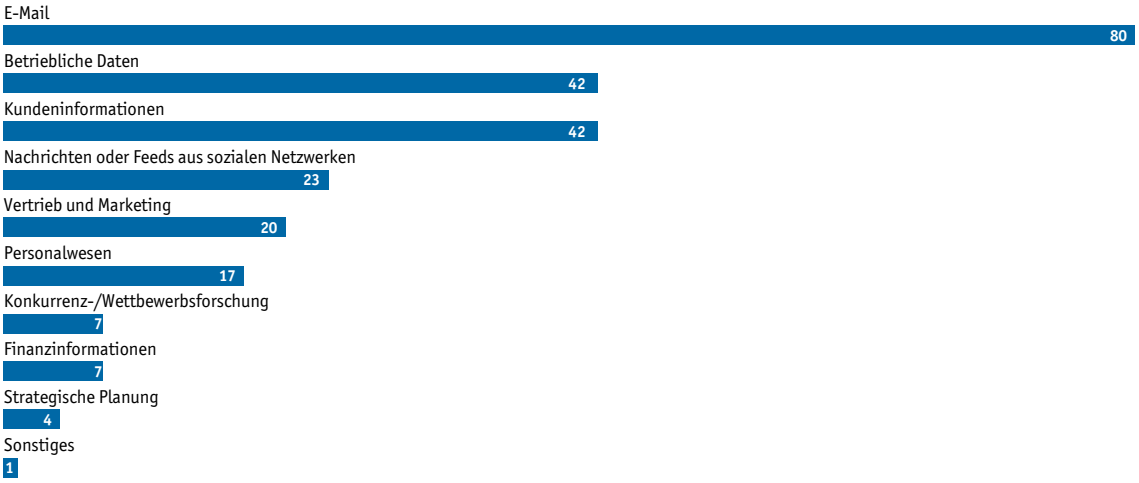
Welche der hier aufgeführten Informationen müssen den folgenden Funktionen für eine optimale Produktivität sicher und zeitnah bereitgestellt werden?
– Führungskräfte auf höchster Ebene
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



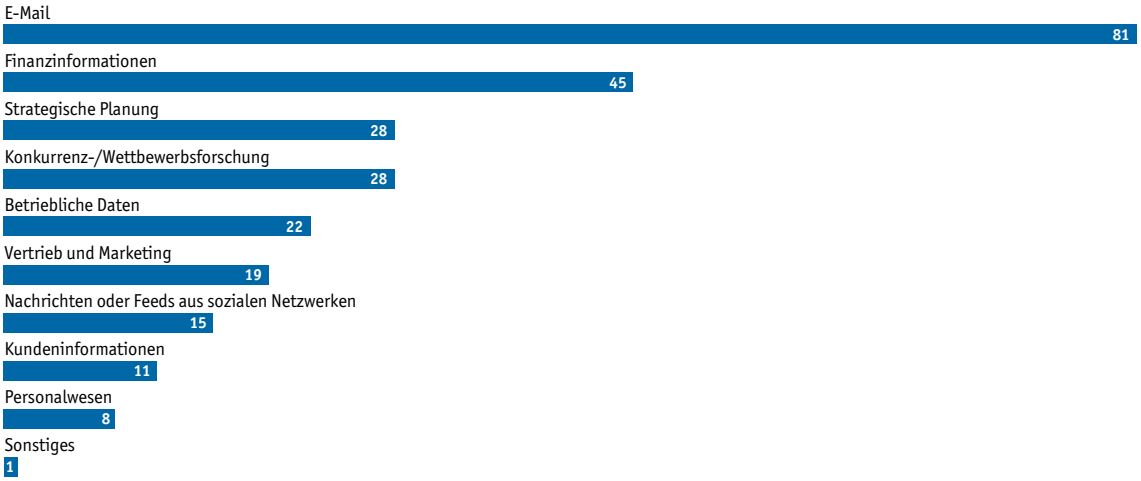
Welche der hier aufgeführten Informationen müssen den folgenden Funktionen für eine optimale Produktivität sicher und zeitnah bereitgestellt werden?
– Managerebene
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



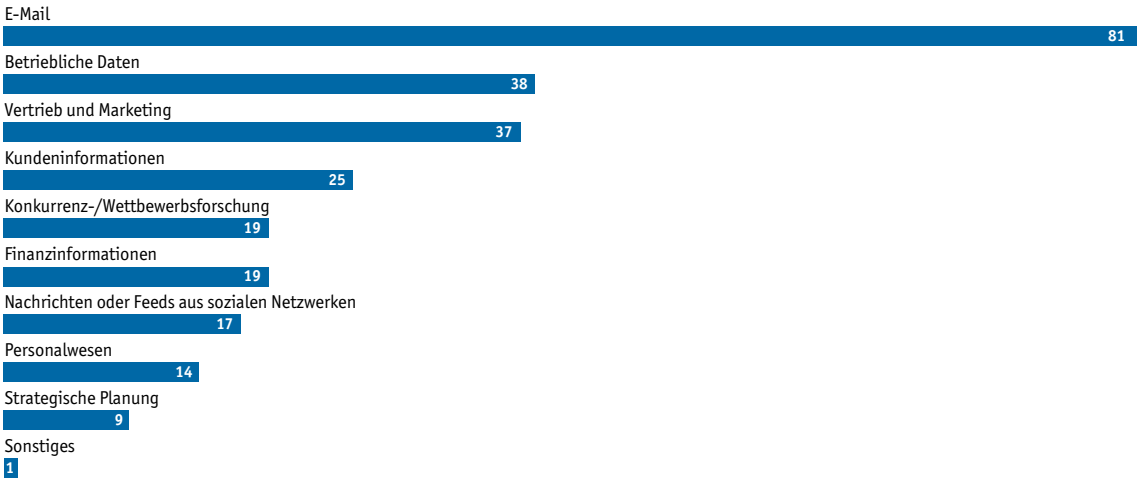
Welche der hier aufgeführten Informationen müssen den folgenden Funktionen für eine optimale Produktivität sicher und zeitnah bereitgestellt werden?
– Mitarbeiter
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



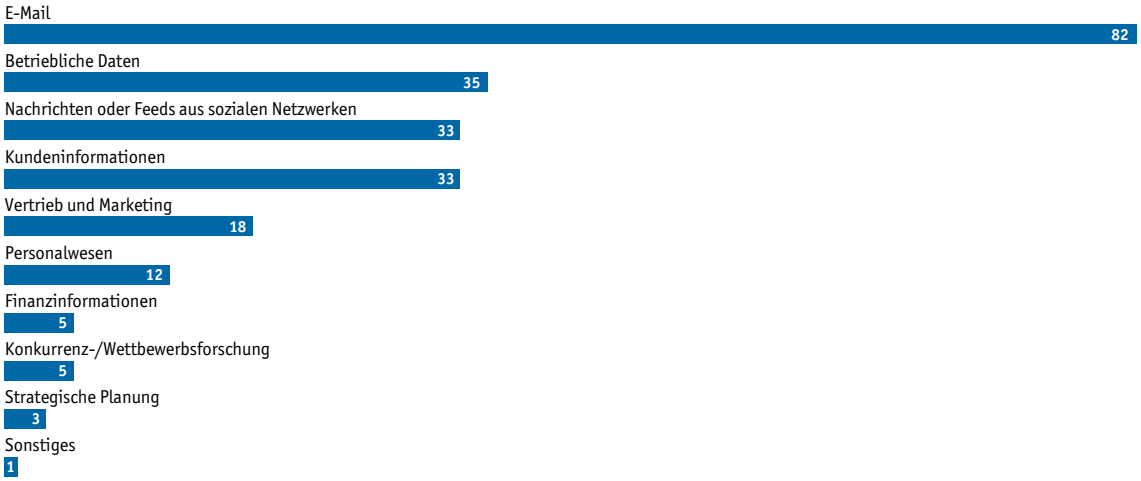
Für welche der folgenden Arten von Informationen/Medien ist der Zugriff über Mobilgeräte angemessen? – Führungskräfte auf höchster Ebene
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



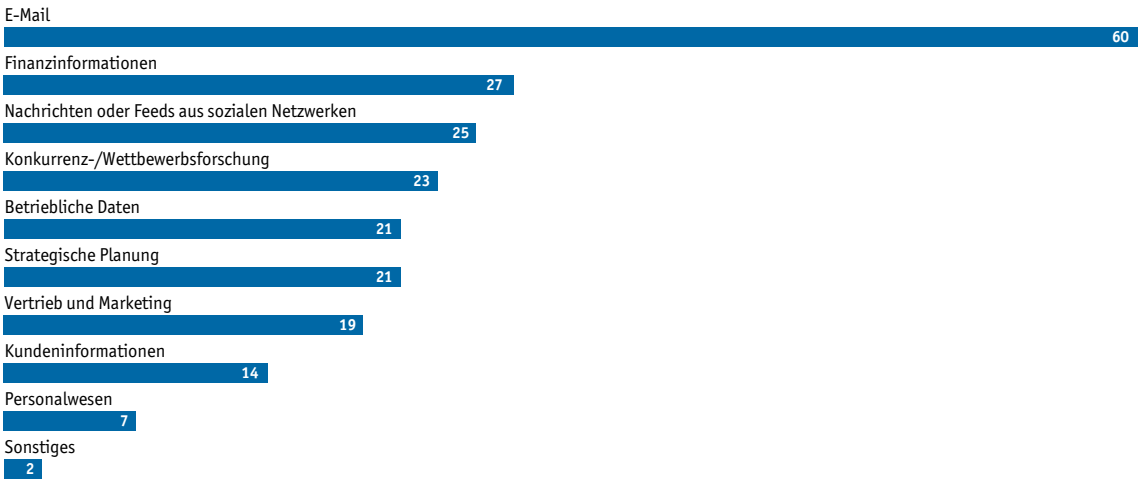
Für welche der folgenden Arten von Informationen/Medien ist der Zugriff über Mobilgeräte angemessen? – Managerebene
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



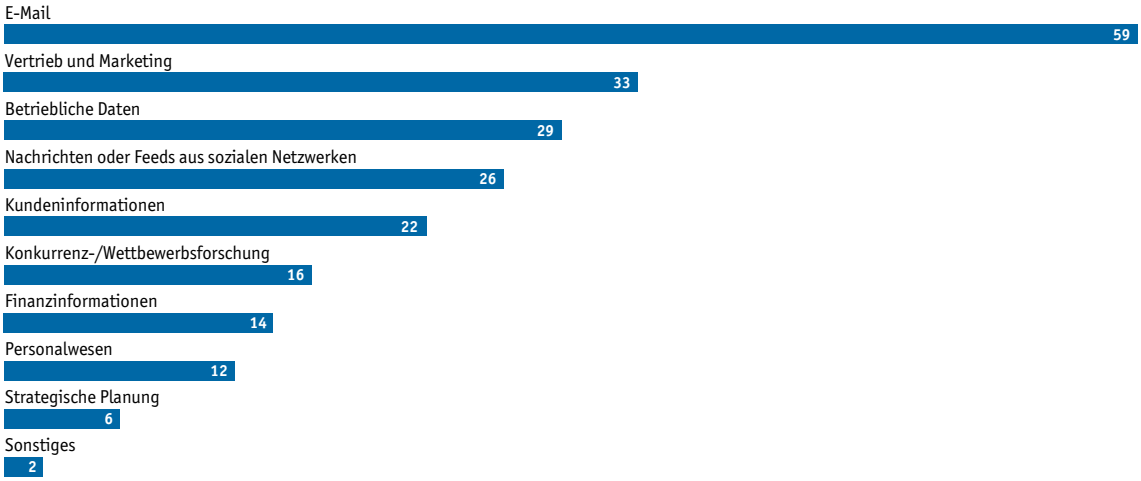
Für welche der folgenden Arten von Informationen/Medien ist der Zugriff über Mobilgeräte angemessen? – Mitarbeiter
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



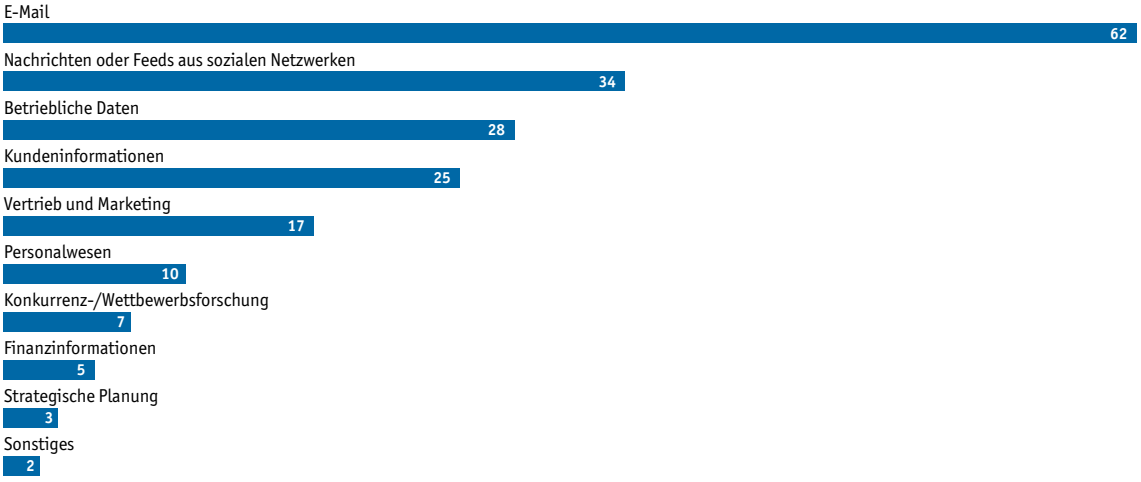
Für welche der folgenden Arten von Informationen/Medien ist der Zugriff über Mobilgeräte angemessen, wenn diese in Cloud-basierten Datenspeichern residieren bzw. ausgeführt werden? – Führungskräfte auf höchster Ebene
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



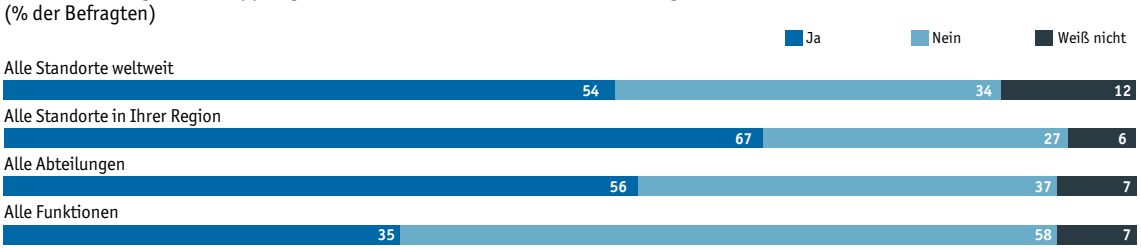
Für welche der folgenden Arten von Informationen/Medien ist der Zugriff über Mobilgeräte angemessen, wenn diese in Cloud-basierten Datenspeichern residieren bzw. ausgeführt werden?
– Managerebene
Wählen Sie maximal drei pro Funktion.
(% der Befragten)



Für welche der folgenden Arten von Informationen/Medien ist der Zugriff über Mobilgeräte angemessen, wenn diese in Cloud-basierten Datenspeichern residieren bzw. ausgeführt werden?
– Mitarbeiter
Wählen Sie maximal drei pro Funktion.
(% der Befragten)

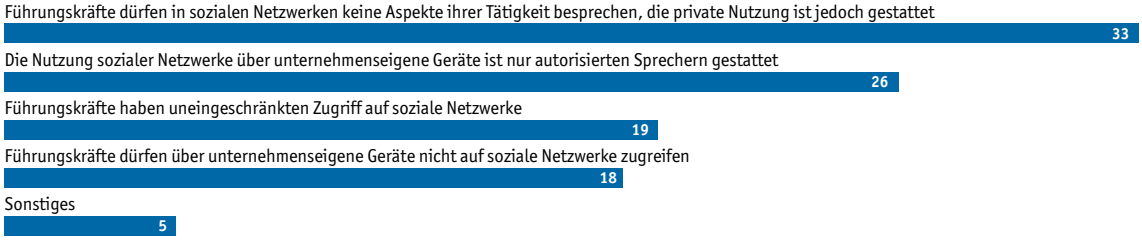


Welchen der folgenden Gruppen gestattet Ihr Unternehmen den mobilen Zugriff auf Daten?
(% der Befragten)

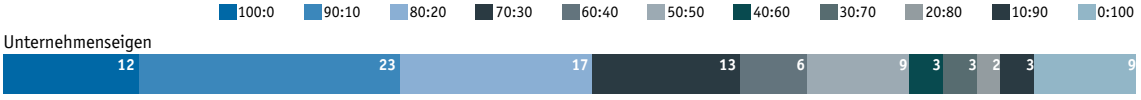


Gibt es in Ihrem Unternehmen Richtlinien zur zulässigen Nutzung sozialer Netzwerke (z. B. Facebook oder Twitter) über unternehmenseigene Geräte?
(% der Befragten)

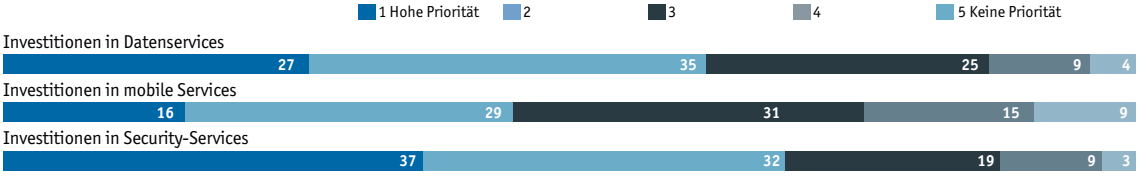
Welche Richtlinien bestehen in Ihrem Unternehmen bezüglich der Nutzung sozialer Netzwerke über unternehmenseigene Geräte?
(% der Befragten)



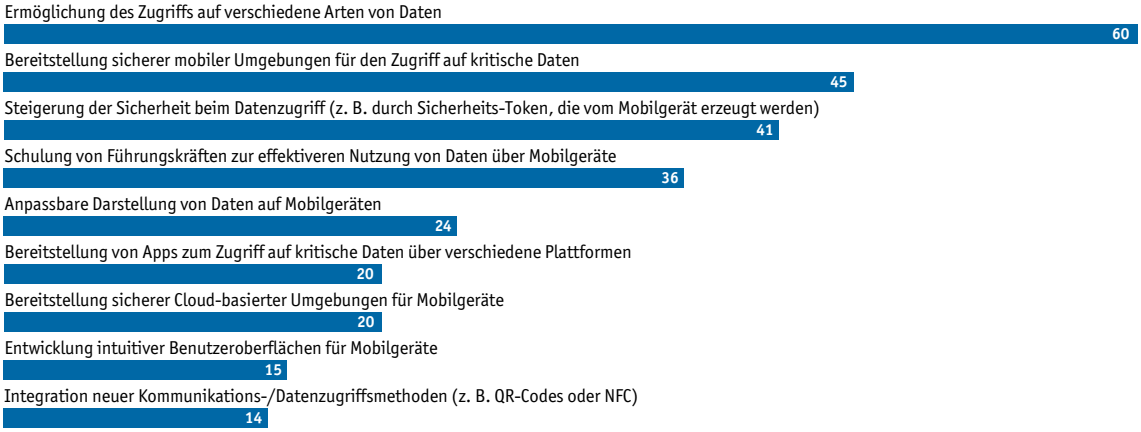
In welchem Verhältnis verwenden Sie unternehmenseigene und private Mobilgeräte für Ihre Tätigkeit?
Ziehen Sie den Schieberegler auf die prozentuale Verteilung, die Ihrem Nutzungsverhalten entspricht (z. B. 60 % zu 40 %).
(% der Befragten)



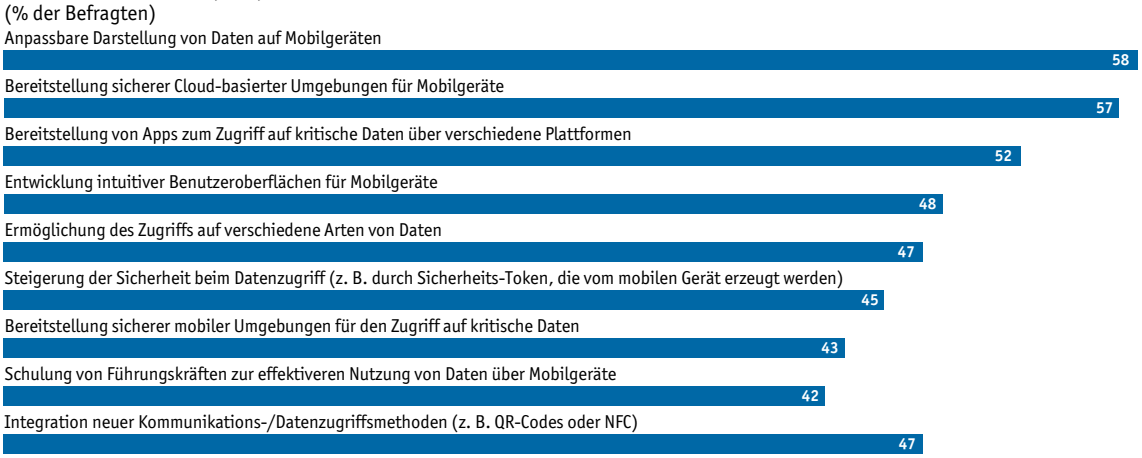
Welche Priorität misst Ihr Unternehmen den folgenden Strategien zu?
Bewerten Sie auf einer Skala von 1 bis 5, wobei 1 „hohe Priorität" bedeutet und 5 „keine Priorität"
(% der Befragten)



Auf welche Weise unterstützt Ihr Unternehmen heute den Zugriff auf kritische Daten und welche Veränderungen erwarten Sie hier künftig?
– heute
Wählen Sie eine Antwort pro Spalte und Zeile
(% der Befragten)



Auf welche Weise unterstützt Ihr Unternehmen heute den Zugriff auf kritische Daten und welche Veränderungen erwarten Sie hier künftig?
– künftig
Wählen Sie eine Antwort pro Spalte und Zeile
(% der Befragten)



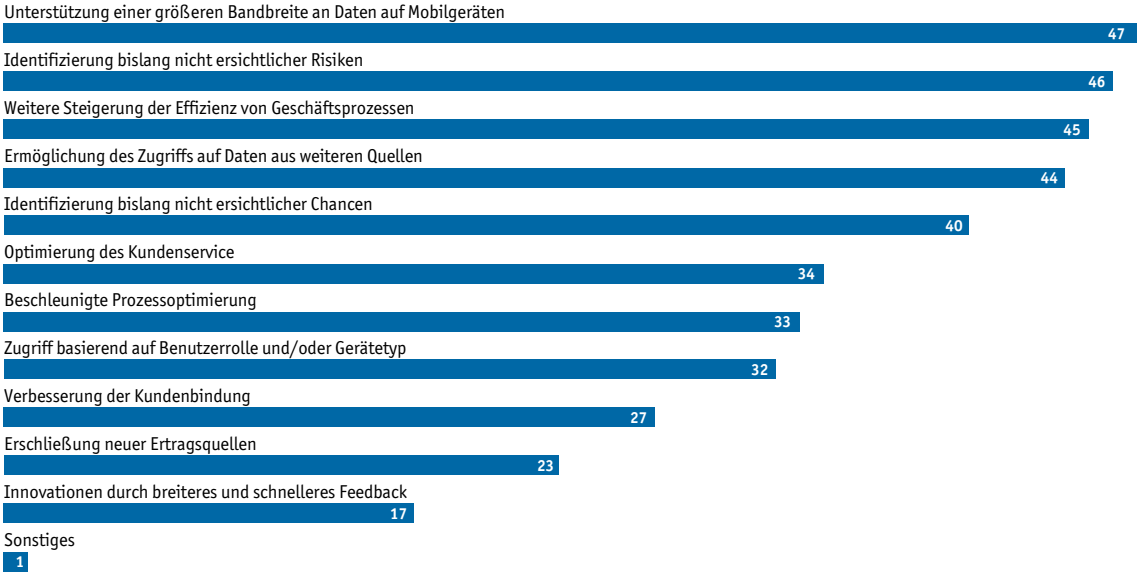
Wie hoch ist der Anteil kritischer Daten, auf die Sie heute über mobile Geräte zugreifen?
Die Summe aller Prozentangaben sollte 100 Prozent betragen.

	Durchschnitt
Mobil (Smartphone)	26,9
Mobil (sonstige Geräte, z. B. Tablets)	21,7
Nicht mobil	59,8

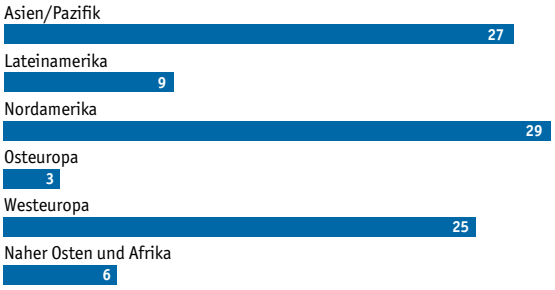
Wie hoch wird der Anteil kritischer Daten, auf die Sie über mobile Geräte zugreifen, in den kommenden 12 bis 18 Monaten sein?
Die Summe aller Prozentangaben sollte 100 Prozent betragen.

	Durchschnitt
Mobil (Smartphone)	34,5
Mobil (sonstige Geräte, z. B. Tablets)	30,2
Nicht mobil	42,8

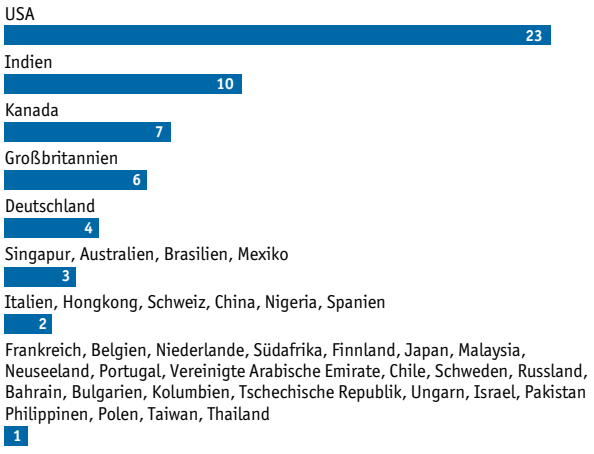
Welche neuen Möglichkeiten verspricht sich Ihr Unternehmen im Hinblick auf den Zugriff auf kritische Daten in den kommenden 12 bis 18 Monaten?
Wählen Sie alle zutreffenden Antworten aus.



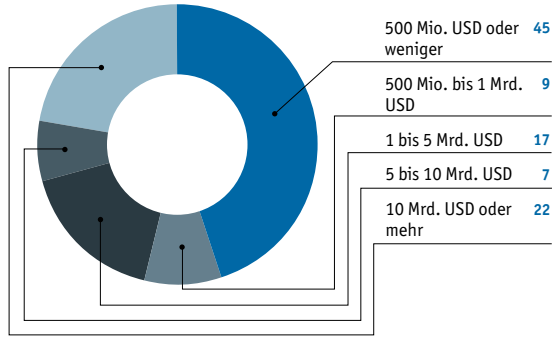
In welchem geografischen Gebiet leben/arbeiten Sie?
(% der Befragten)



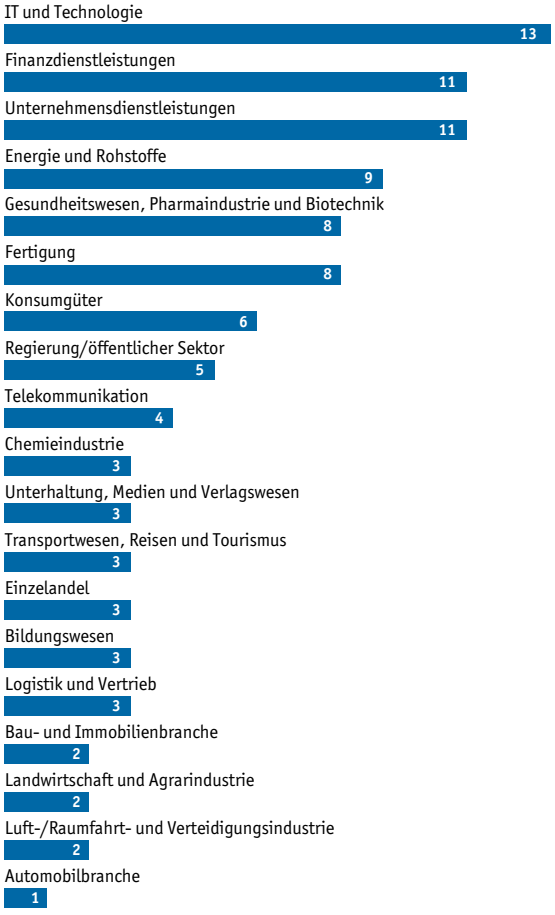
In welchem Land leben/arbeiten Sie?
(% der Befragten)



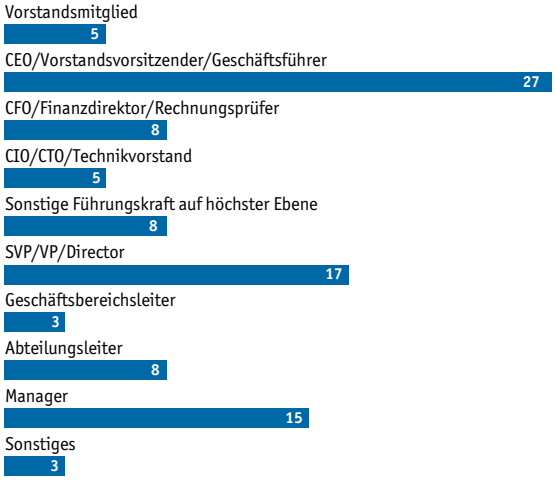
Wie hoch ist der weltweite Jahresumsatz Ihres Unternehmens in US-Dollar?
(% der Befragten)



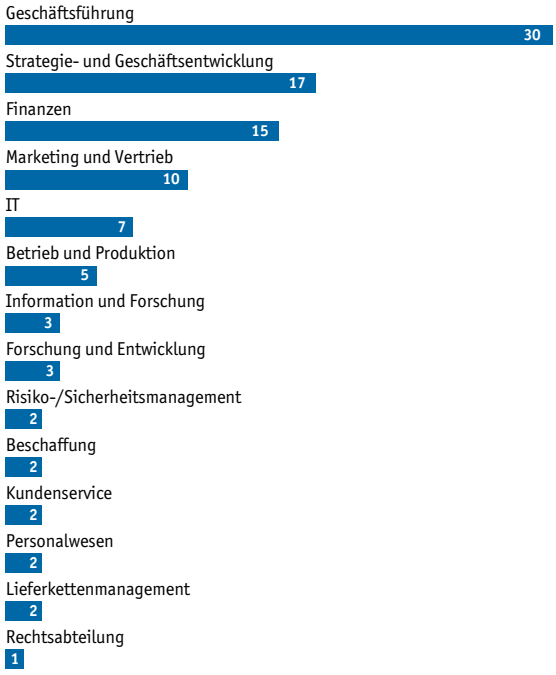
In welcher Branche ist Ihr Unternehmen vorwiegend tätig?
(% der Befragten)



Welche der folgenden Angaben beschreibt Ihre Position am besten?
(% der Befragten)



In welchem Bereich sind Sie vorwiegend tätig?
(% der Befragten)



Cover: Shutterstock

London
26 Red Lion Square
London
WC1R 4HQ
Großbritannien
Tel.: +44 20 7576 8000
Fax: +44 20 7576 8476
E-Mail: london@eiu.com

New York
750 Third Avenue
5th Floor
New York, NY 10017
USA
Tel.: +1 212 554 0600
Fax: +1 212 586 0248
E-Mail: newyork@eiu.com

Hongkong
6001, Central Plaza
18 Harbour Road
Wanchai
Hongkong
Tel.: +852 2585-3888
Fax: +852 2802 7638
E-Mail: hongkong@eiu.com

Genf
Boulevard des
Tranchées 16
1206 Genf
Schweiz
Tel.: +41 22 566 2470
Fax: +41 22 346 93 47
E-Mail: geneva@eiu.com