



Die Open Source Groupware Studie: Standpunkte zu Sicherheit und Datenschutz in den USA und EMEA

Unter Mitwirkung von Zimbra

Unabhängige Recherche des Ponemon Institute LLC

Datum der Veröffentlichung: November 2014

Die Open Source Groupware Studie: Standpunkte zur Sicherheit und Datenschutz in den USA und EMEA

Ponemon Institute, November 2014

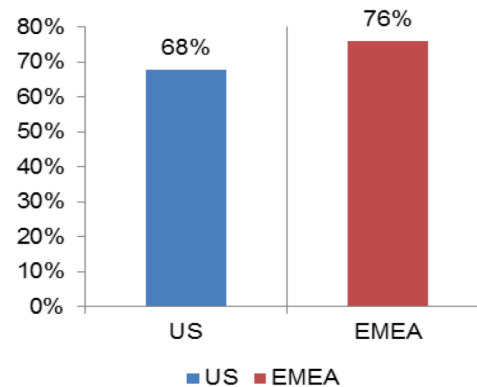
Teil: 1. Einleitung

Das Ponemon Institute freut sich, die Ergebnisse der *Open Source Groupware Studie: Standpunkte zur Sicherheit und Datenschutz in den USA und EMEA* mitzuteilen; diese Studie wurde mit Unterstützung von Zimbra durchgeführt. Im Rahmen dieser Marktforschungsstudie wurden IT-Praktiker und IT-Sicherheitsbeauftragte befragt, inwieweit ihre Unternehmen Open-Source-Groupware nutzen und welche Vorteile diese ihrer Meinung nach haben.

Wir befragten 723 IT-Praktiker und IT-Sicherheitsbeauftragte in den USA und 675 IT-Praktiker und IT-Sicherheitsbeauftragte in folgenden 18 EMEA-Ländern: Großbritannien, Deutschland, Frankreich, Russische Föderation, Spanien, Saudi Arabien, Italien, Niederlande, Türkei, Polen, Vereinigte Arabische Emirate, Südafrika, Irland, Schweiz, Dänemark, Schweden, Israel und Griechenland.

Die Mehrzahl (57%) der Befragten in den USA und den EMEA-Ländern sind entweder sehr vertraut oder vertraut mit den Sicherheits- und Datenschutzrichtlinien bzw. Sicherheits- und Datenschutzanforderungen ihrer Unternehmen. 55% der Antwortgeber aus den USA und 48% der Befragten aus den EMEA-Ländern haben eine Führungs- oder eine höhere Position inne.

Abbildung 1. Kann das Vertrauen in die Anwendung durch die Nutzung von kommerziellen Unternehmen und einer Codetransparenz erhöht werden? (Ja-Antworten)



Wie in Abbildung 1 zu ersehen, sind die Befragten aus den USA und den EMEA-Ländern überzeugt, dass eine Nutzung von kommerziellen Unternehmen und eine Codetransparenz das Vertrauen in eine Anwendung erhöhen. Auf die Frage, inwieweit die IT-Abteilung in die Bewertung bzw. Auswahl von Lösungen für eine Groupware einbezogen sei, gaben 39% der Befragten aus den USA und 30% der Befragten aus den EMEA-Ländern an, dass die Einbeziehung „signifikant“ sei. Nach Angaben von 84% der Befragten aus den USA und 82% der Befragten aus den EMEA-Ländern versuchen ihre Unternehmen den Anteil der Open-Source-Software im Vergleich zu proprietären Unternehmensanwendungen zu beeinflussen. Der durchschnittliche Anteil der Unternehmensanwendungen, wo Open-Source-Software kommerziell eingesetzt wird, liegt in den USA bei 30% und in den EMEA-Ländern bei 25%.

Als Open-Source-Software (OSS) definieren wir im Rahmen dieser Studie Computersoftware, deren Source-Code gegen eine Lizenz verfügbar ist und bei welcher der Copyright-Inhaber das Recht erhält, die Software zu studieren, zu ändern und an andere zu verteilen. Open-Source-Software wird in großem Maße durch gemeinschaftliche Zusammenarbeit entwickelt.

Die wichtigsten Studienerkenntnisse:

An oberster Stelle bei kommerziell eingesetzten Open-Source-Anwendungen steht die Gewissheit, dass die Software weiterentwickelt wird. Die Befragten sind im Großen und Ganzen sehr positiv gegenüber kommerziell eingesetzten Open-Source-Anwendungen eingestellt, insbesondere was die garantierte Weiterentwicklung betrifft.

Trotz der Vorteile zögern Unternehmen bei der Einführung. Der durchschnittliche Anteil von kommerziell eingesetzten Open-Source-Anwendungen sind, liegt bei den Befragten in den USA bei 30% und in EMEA bei 25%.

In EMEA sind die Sicherheits- und Datenschutzrichtlinien oft strenger. Die Studie ergab, dass die Unternehmen in EMEA in Sachen Groupware mehr Bedenken hinsichtlich Datenschutz haben. Für die US-Unternehmen spielt die Sicherheit eine größere Rolle.

Sicherheit, Datenschutz und Vertrauen in Anwendungen werden gleichermaßen durch eine kommerzielle Unterstützung und Codetransparenz erhöht. Die Befragten stimmen zu, dass kommerziell eingesetzte Open-Source-Groupware Lösungen, die bereits bei kommerziellen Unternehmen eingesetzt werden und Codetransparenz gewährleisten, besser sind. Die Befragten aus den EMEA-Ländern sind meist positiv eingestellt, insbesondere was die geringeren Risiken im Datenschutzbereich anbelangt (66% der EMEA-Befragten sowie 52% der US-Befragten).

Welche Faktoren sind bei Groupware Lösungen ausschlaggebend? Nach Angaben der US-Befragten ist die Benutzerfreundlichkeit wichtig, während nach Angaben der Befragten aus den EMEA-Ländern die Anbieter Unterstützung bei der Auswahl einer Groupware Lösung die wichtigste Rolle spielt.

Teil: 2. Hauptkenntnisse

In diesem Abschnitt analysieren wir die Ergebnisse der Marktforschungsstudie. Die vollständigen, auditierten Ergebnisse finden Sie im Anhang dieses Berichts. Der Bericht ist nach den folgenden Themen gegliedert:

- Positive Wahrnehmung von Open-Source-Anwendungen im kommerziellen Einsatz
- Sicherheits- und Datenschutzrisiken von Groupware
- Bedeutung der Funktionen von Groupware
- Prognose für die Akzeptanz solcher Lösungen

Positive Wahrnehmung von Open-Source-Anwendungen im kommerziellen Einsatz

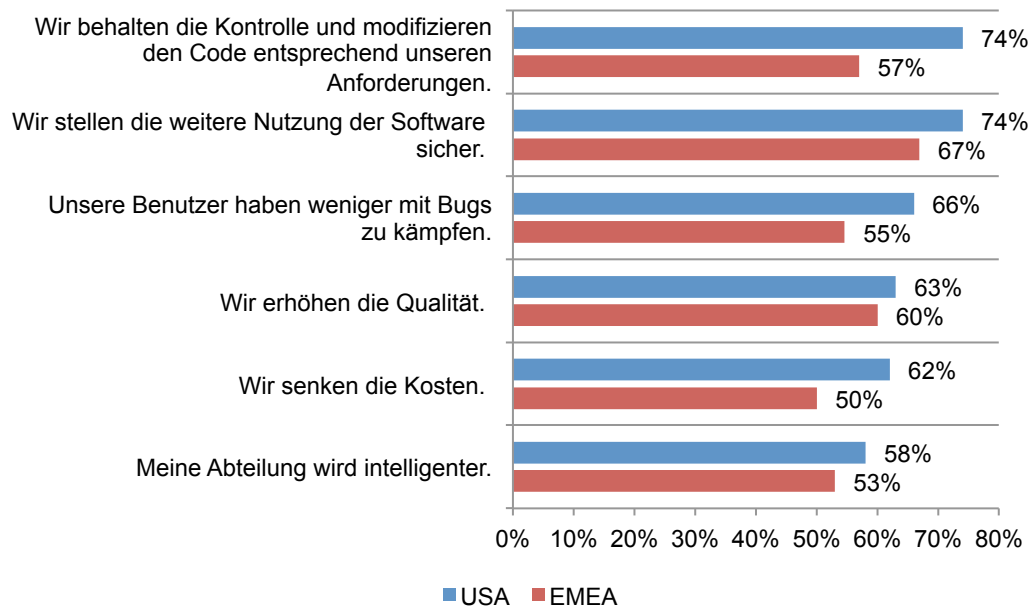
In dieser Studie wird unter kommerzieller Open-Source-Software ein Open-Source-Projekt verstanden, das in einem kommerziellen Unternehmen eingesetzt wird. Ein „Community-Open-Source-Projekt“ wird hingegen nicht in einem kommerzielles Unternehmen genutzt. Kommerzielle Open-Source-Software unterscheidet sich auch von kommerziell zur Verfügung gestellter proprietärer Software, d. h. einem geschlossenen Standardsystem mit proprietären Methoden, welches in einem kommerziellen Unternehmen zum Einsatz kommt.

Als wichtigster Vorteil bei kommerziell eingesetzten Open-Source-Anwendungen steht die Gewissheit, dass die Software weiterentwickelt wird. Die Antwortgeber sind gegenüber kommerziell eingesetzten Open-Source-Anwendungen im Allgemeinen sehr positiv eingestellt, insbesondere was die Sicherheit der Weiterentwicklung betrifft. Wie in Abbildung 2 zu erkennen ist, trifft dies auf US-Befragte sogar noch mehr zu. Insbesondere sind die US-Befragten eher der Ansicht, dass deren Abteilungen innerhalb der Open-Source-Communities, übers Internet und einem besseres Verständnis von IT-Praktiken, Ressourcen und Tools der Technikerteams (74% der US-Befragten und 57% der Befragten aus den EMEA-Ländern), effizienter arbeiten können.

Deutlich unterscheiden sich auch die Meinungen der Befragten aus den USA und den EMEA-Ländern hinsichtlich Kosteneinsparungen, da Open-Source-Software im Vergleich zu proprietärer Software flexibel ist (62% der US-Befragten bzw. 50% der EMEA-Befragten) und weniger Softwarefehler aufweist. Viele Mitglieder der Community prüfen akribisch und permanent den Programmierungscode, um Bugs zu ermitteln und diese schnell und effizient zu beseitigen (66% der Befragten aus den USA und 55% der Befragten aus den EMEA-Ländern).

Abbildung 2. Warum ist kommerzielle Open-Source-Software besser als kommerzielle proprietäre Software?

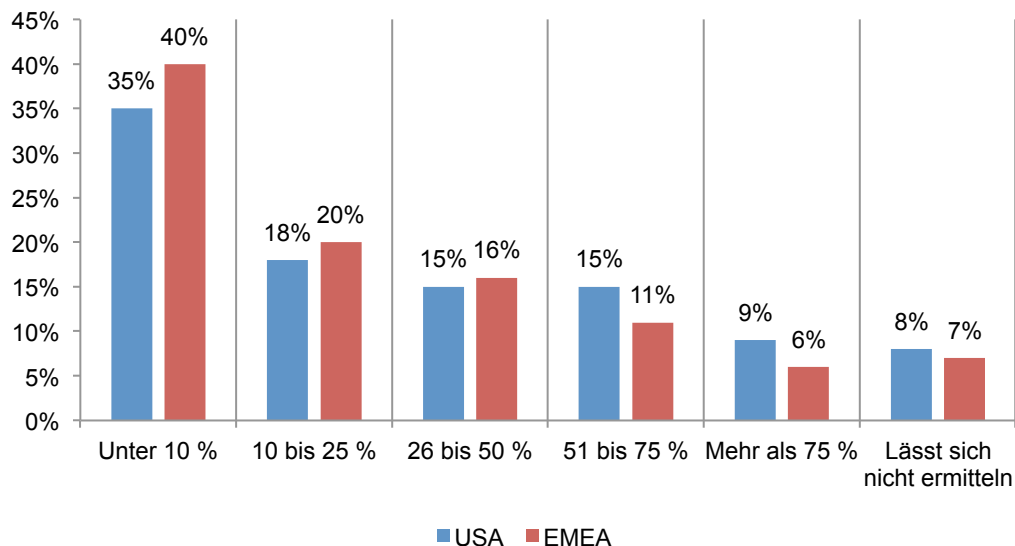
Zusammenfassung der Bewertungen „stimme in vollem Umfang zu“ und „stimme zu“



Trotz der Vorteile zögern Unternehmen bei der Einführung. Nach Abbildung 3 liegt der durchschnittliche Anteil der Unternehmensanwendungen, die auf kommerzieller Open Source Software basiert, bei den Befragten in den USA bei 30% und den Befragten in den EMEA-Ländern bei 25%. 39% der US-Befragten und 30% der EMEA-Befragten geben an, dass die IT-Abteilung ihres Unternehmens in die Bewertung bzw. Auswahl der Groupware Lösungen einbezogen sei.

Abbildung 3. Anteil der Unternehmensanwendungen basierend auf kommerzieller Open-Source-Software:

Hochgerechneter Wert: US = 30%, EMEA-Länder = 25%

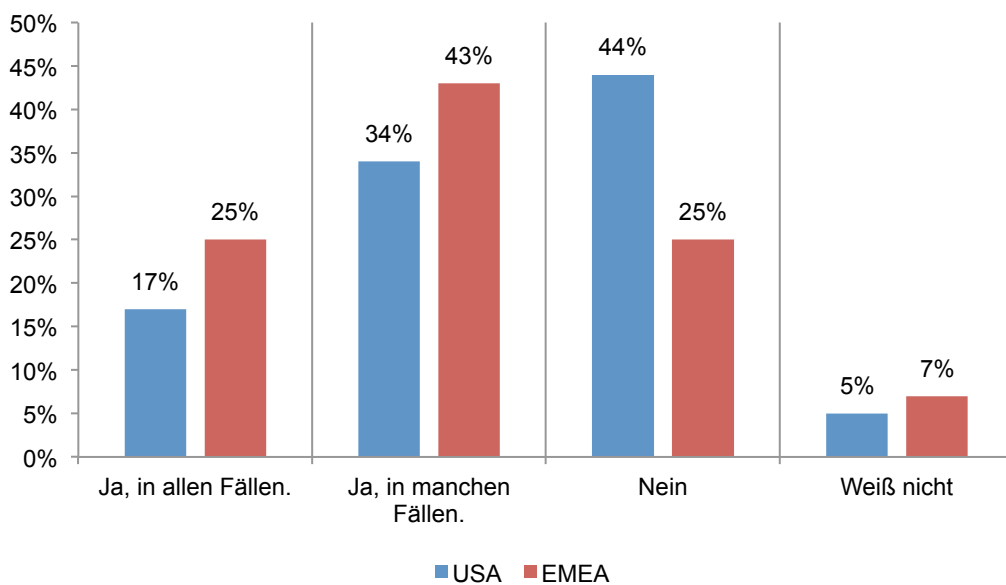


Sicherheits- und Datenschutzrisiken bei Groupware Lösungen

In EMEA sind die Sicherheits- und Datenschutzrichtlinien in Unternehmen oft strenger. Die Studie ergab, dass die EMEA-Unternehmen bei der Auswahl von Groupware Lösungen mehr Bedenken hinsichtlich Datenschutz haben. Für die US-Unternehmen spielt die Sicherheit eine stärkere Rolle.

Nach den Ergebnissen der Recherche sind 57% der Befragten in den USA und den EMEA-Ländern „sehr vertraut“ bzw. „vertraut“ mit den allgemeinen Sicherheits- und Datenschutzrichtlinien bzw. Anforderungen ihrer Unternehmen. Wie in Abbildung 4 dargestellt, geben mehr Befragte in der USA an, dass das Unternehmen seine Sicherheits- und Datenschutzrichtlinien nicht durchsetze, als bei den entsprechenden EMEA-Unternehmen (44% bzw. 25%).

Abbildung 4. Setzt Ihr Unternehmen seine Sicherheits- und Datenschutzrichtlinien durch?



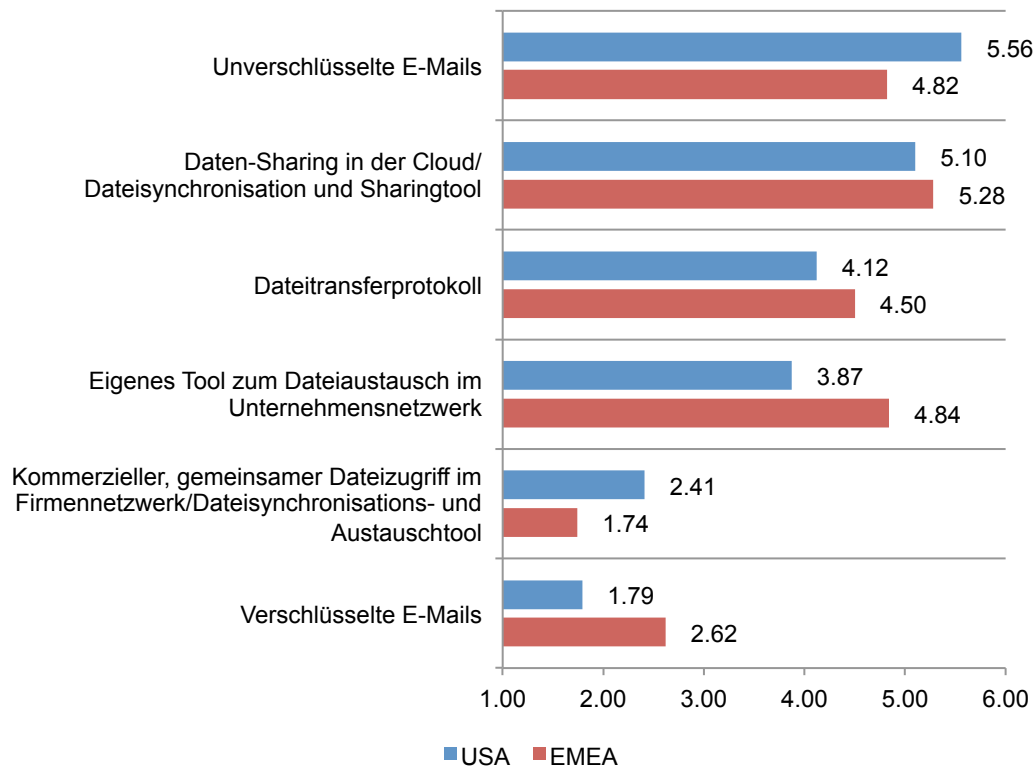
Unverschlüsselte E-Mails gelten als riskantestes Verfahren zum Austausch von Dateien.

Sowohl Befragte in den USA als auch in den EMEA-Ländern sind der Ansicht, dass unverschlüsselte E-Mails die riskanteste Art und Weise des Austauschs von Dokumenten sind, gefolgt vom Austausch von Dateien in der Cloud sowie Tools zur Daten-Synchronisation und zum Datenaustausch (siehe Abbildung 5).

Am wenigsten riskant sind verschlüsselte E-Mails. Ein interessanter Unterschied ist beispielsweise, dass in den Augen der US-Befragten die Verwendung von unverschlüsselten E-Mails riskanter ist. Die Befragten in den EMEA-Ländern dagegen haben größere Bedenken hinsichtlich der Verwendung von eigenen Tools zum Dateiaustausch oder hinsichtlich der privaten Tools der Anwender.

Abbildung 5. Verfahren zum Datenaustausch mit dem höchsten Risiko

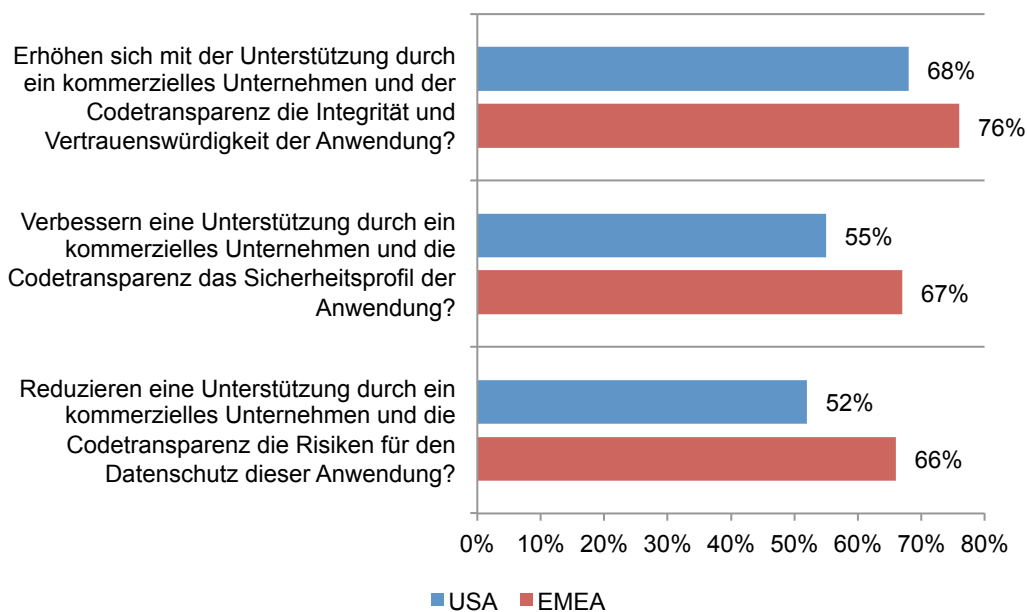
6 = höchstes Risiko, 1 = niedrigstes Risiko



Sicherheit, Datenschutz und Vertrauen in Anwendungen werden gleichermaßen durch eine bereits vorhandene kommerzielle Nutzung sowie Codetransparenz erhöht. Nach Abbildung 6 stimmen die Befragten darin überein, dass kommerziell eingesetzte Open-Source-Groupware, die bereits eine kommerzielle Nutzung von Unternehmen erfährt und Codetransparenz hat, besser ist. Die Befragten in EMEA sind meist positiv eingestellt, insbesondere was die geringeren Risiken hinsichtlich Datenschutz anbelangt (66% der EMEA-Befragten und 52% der US-Befragten).

Darüber hinaus geben 67 % der Befragten aus EMEA und 55% aus den USA an, dass dadurch die Sicherheit der Anwendung erhöht und die Risiken gesenkt werden. 76% der Befragten aus den EMEA-Ländern und 68 % der Befragten aus den USA verweisen darauf, dass damit die Integrität und das Vertrauen in die Anwendungen steigen.

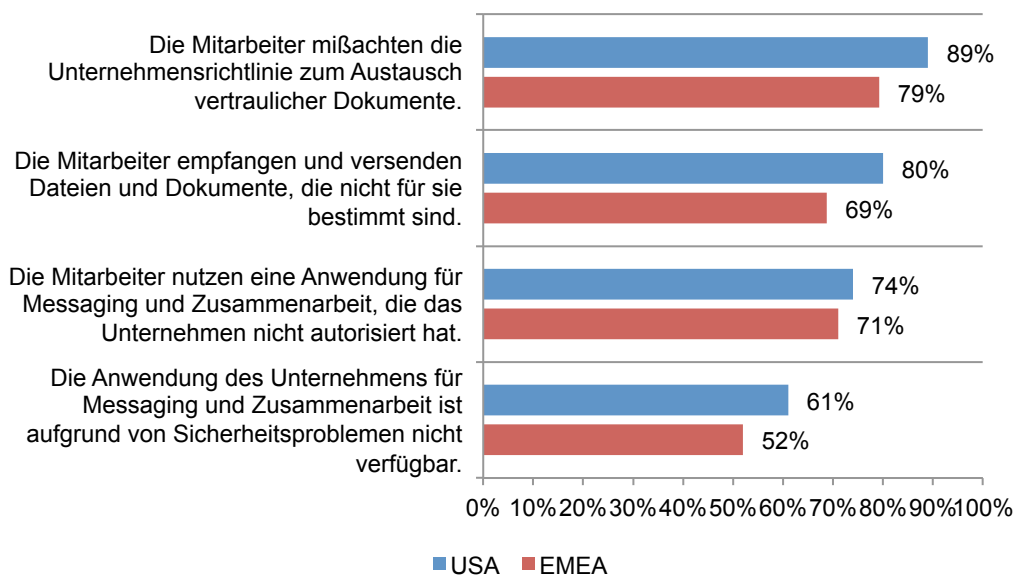
Abbildung 6. Wird durch die kommerzielle Nutzung und Codetransparenz die Sicherheit und das Vertrauen erhöht und reduzieren sich somit die Risiken für den Datenschutz?
Ja-Antworten



Mitarbeiter gefährden die Sicherheit und Datenschutz im Unternehmen. Die Mitarbeiter in den USA neigen mehr dazu, die Groupware Lösungen ihrer Unternehmen zu gefährden, als die Mitarbeiter in den EMEA-Ländern. Abbildung 7 zeigt vier Praktiken, die Bedrohungen für vertrauliche Unterlagen eines Unternehmens darstellen. Mehr US-Befragte sind der Ansicht, dass ihre Unternehmen ein Problem mit Mitarbeitern haben.

Nach Aussagen der Befragten aus beiden Regionen jedoch bestünde ein hohes Risiko, dass Mitarbeiter die Richtlinien des Unternehmens zum Austausch vertraulicher Unterlagen missachten und Dateien versenden und empfangen, die nicht für sie bestimmt waren bzw. eine Groupware Anwendung einsetzen, die vom Unternehmen nicht genehmigt wurde. 61% der Befragten in den USA und 52 % der Befragten in den EMEA-Ländern bestätigen, dass die Groupware Anwendungen ihrer Unternehmen aufgrund von Sicherheitsproblemen in der Vergangenheit nicht zur Verfügung gestellt wurden.

Abbildung 7. Mitarbeiter gefährden die Sicherheit und den Datenschutz
Zusammenfassung der Antworten „oft“ und „regelmäßig“



Bedeutung der Funktionen von Groupware Lösungen

Weltweit nutzen mehr als 200.000 Unternehmen Zimbra, davon 100 Mio. Nutzer die kommerzielle Version und 500 Mio. User die kostenfreie Variante. Die Befragten wurden gebeten, die Funktionen zu bewerten, die für ihr Unternehmen am wichtigsten seien.

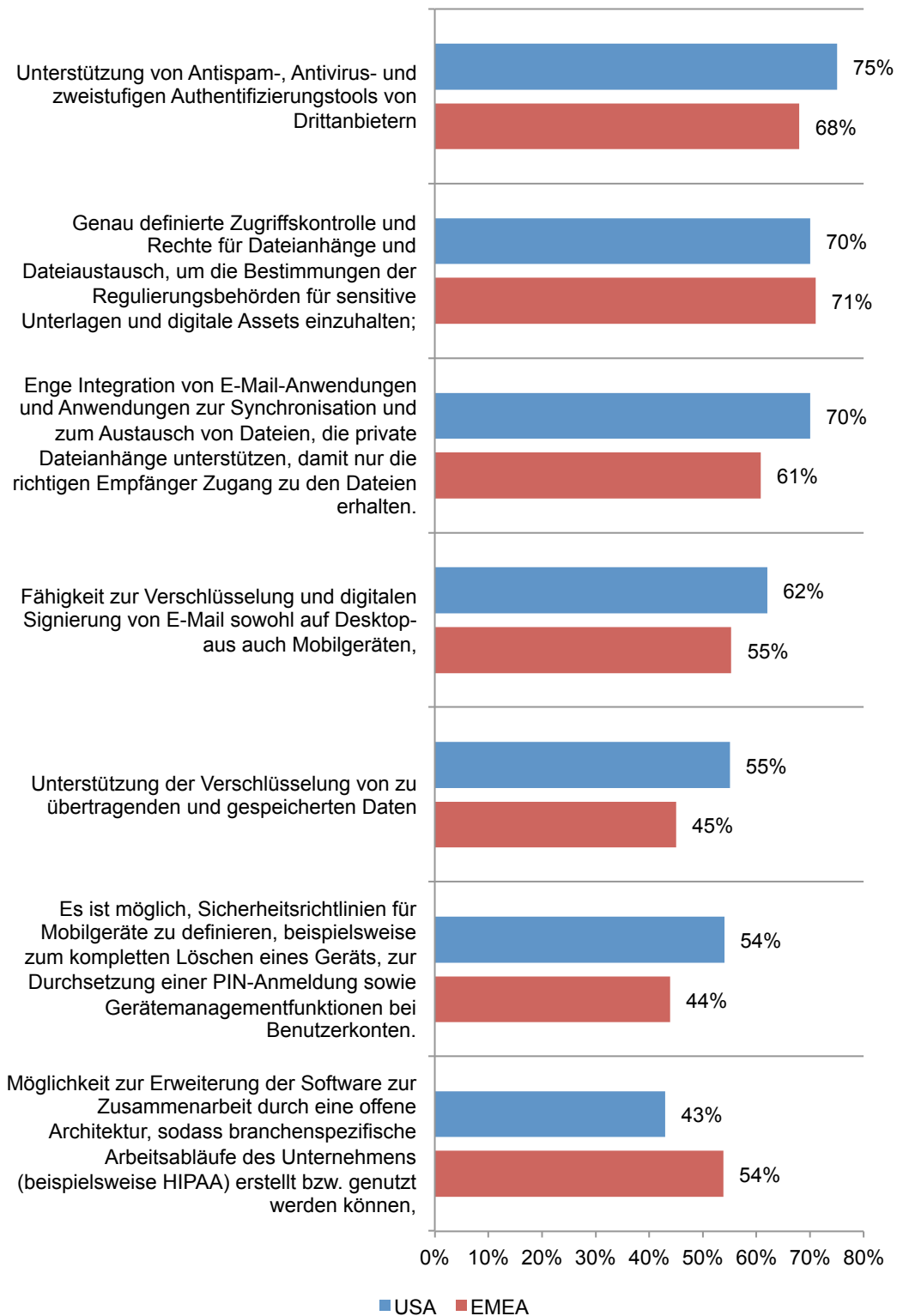
Sicherheit und Datenschutz waren die Prioritäten der Befragten in den USA und EMEA.

Wie in Abbildung 8 zu erkennen, stimmen die Antwortgeber aus den USA und den EMEA-Ländern darin überein, dass die Unterstützung von fremden Antispam-, Antivirus- und zweistufigen Authentifizierungstools genauso wichtig ist, wie die Fähigkeit der Kontrolle der Unternehmensdaten zur Sicherung des Verbleibs der Unternehmensdaten innerhalb definierter Rechtsgebiete sowie die Einhaltung des Datenschutzrechtes.

Wesentliche Unterschiede zwischen den Aussagen der Befragten aus den USA und EMEA-Ländern betreffen die Erweiterung der Groupware mit einer offenen Architektur, sodass firmen- und branchenspezifische Arbeitsabläufe (beispielsweise HIPAA) erstellt oder genutzt werden können. Befragte aus den USA sind eher der Ansicht, dass die Unterstützung der Verschlüsselung zu übertragender sowie gespeicherter Daten und die Fähigkeit zur Definition von Sicherheitsrichtlinien für Mobilgeräte unternehmenskritische Funktionen sind.

Abbildung 8. Die häufigsten Sicherheits- und Datenschutzfunktionen für Groupware-Lösungen

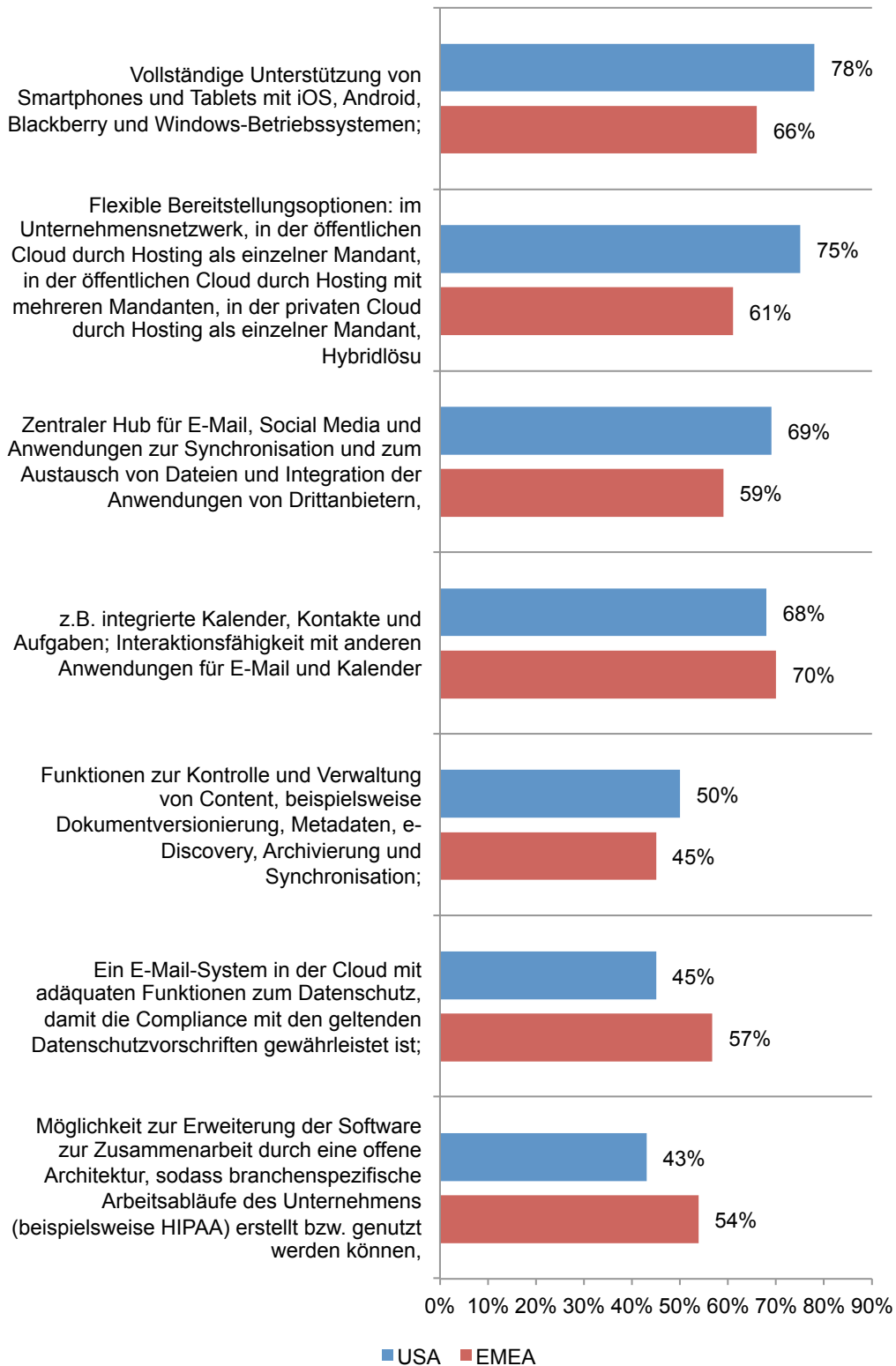
Zusammenfassung der Antworten „sehr wichtig“ und „wichtig“



Unterschiedliche Prioritäten hinsichtlich Groupware bei den Befragten in den USA und den EMEA-Ländern. Für die Anwender der USA ist die Unterstützung von Smartphones und Tablets mit iOS, Android, Blackberry und Windows, die Unterstützung von fremden Antispam-, Antivirus- und zweistufigen Authentifizierungstools sowie flexible Installationsoptionen für die Cloud, am wichtigsten. Nach Ansicht der Befragten der EMEA-Länder ist ein integrierter Kalender, Kontakte und Aufgaben sowie die Interoperabilität mit anderen E-Mail- und Kalenderanwendungen wichtig. Abbildung 9 verdeutlicht die größten Unterschiede zwischen den Antworten aus den USA und den Antworten aus den EMEA-Ländern.

Abbildung 9. Die wichtigsten Groupware Funktionen

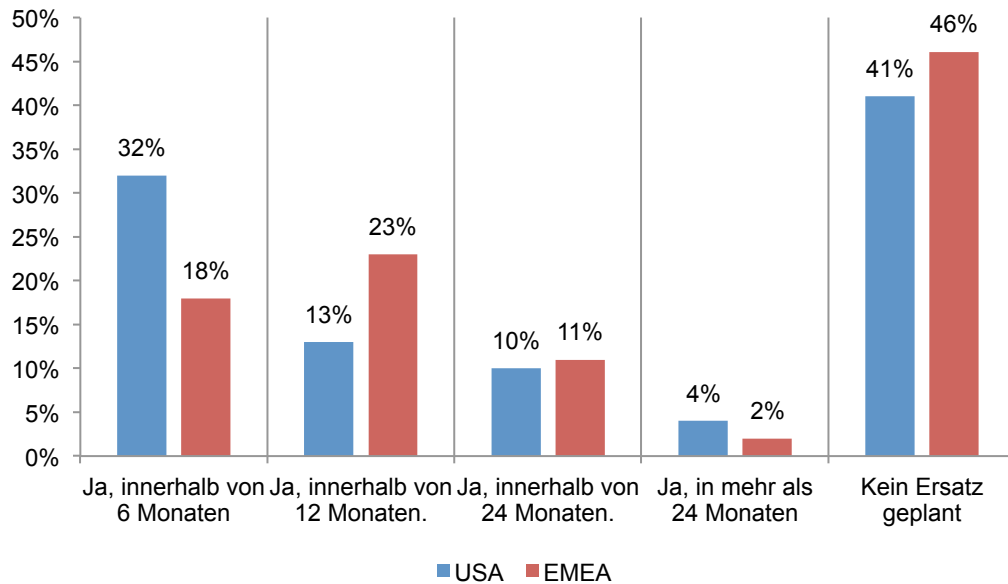
Zusammenfassung der Antworten "sehr wichtig" und "wichtig"



Prognose für die Akzeptanz

Die meisten Befragten sind nicht oder weniger zufrieden mit ihrer jetzigen Groupware. Wie in Abbildung 10 zu erkennen, geben 55% der Befragten aus den USA und 52% der Befragten aus den EMEA-Ländern an, dass deren Unternehmen ihre Groupware innerhalb von zwei Jahren erneuern wollen. In den EMEA-Ländern plant ein etwas höherer Anteil der Befragten (46%) als in den USA (41%), die existierende Groupware beizubehalten.

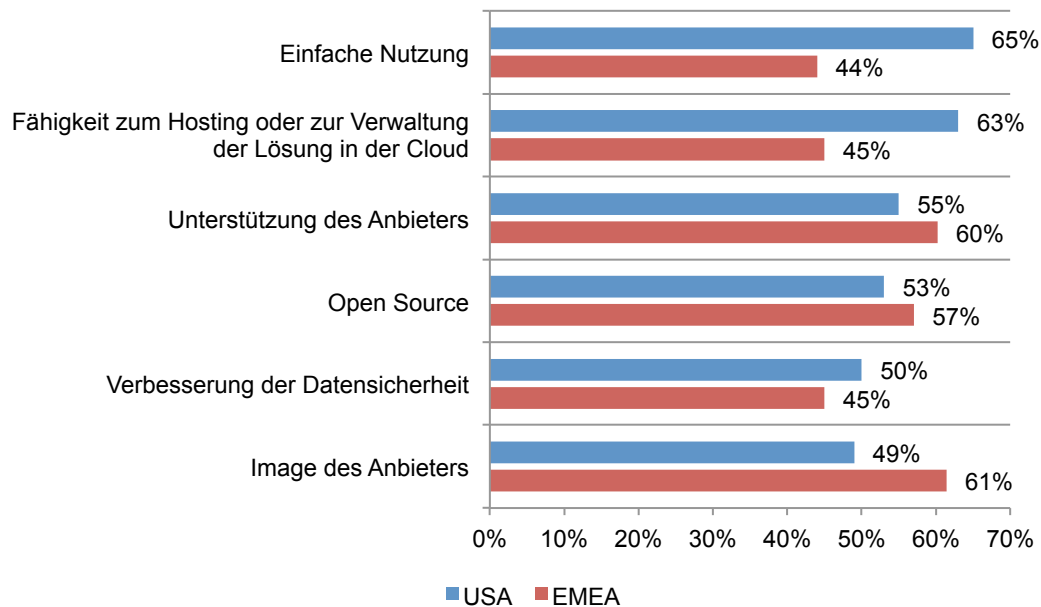
Abbildung 10. Wann soll die existierende Groupware ersetzt werden?



Welche Faktoren sind bei Groupware Lösungen ausschlaggebend? Für die Befragten aus den USA steht die Benutzerfreundlichkeit an erster Stelle, während für die Befragten aus den EMEA-Ländern vor allem das Image des Anbieters bei der Auswahl einer neuen Groupware entscheidend ist. Die größten Unterschiede zwischen den Antworten aus den USA und den EMEA-Ländern bestehen in Punkto Benutzerfreundlichkeit sowie die Fähigkeit, Lösungen in der Cloud zu hosten bzw. zu verwalten.

Abbildung 11. Die wichtigsten Faktoren bei der Groupware Auswahl

Fünf Antworten zulässig



Teil: 3. Fazit

Im Wesentlichen ist die Einstellung der IT-Profis zu kommerzieller Open-Source-Groupware positiver als deren Meinung zu proprietärer Software. Die IT-Profis in den USA und den EMEA-Ländern sind gleichermaßen unzufrieden mit ihrer existierenden Groupware, die meist proprietär sind. Zwar haben IT-Profis in den USA und den EMEA-Ländern unterschiedliche Ansichten hinsichtlich den Auswirkungen von Datensicherheit bzw. Datenschutz. Es besteht jedoch Einklang unter den IT-Profis, dass kommerzielle Open-Source-Software Vorteile durch geringere Kosten, bessere Kontrolle, Qualität und Weiterentwicklung gegenüber proprietärer Software habe.

Teil: 4. Methoden

Die Stichprobe umfasst 17.680 erfahrene IT-Praktiker und IT-Sicherheitsbeauftragte aus den USA sowie 16.700 erfahrene IT-Praktikern und IT-Sicherheitsbeauftragte aus EMEA und liefert den Inhalt für diese Studie. Tabelle 1 zeigt, dass insgesamt 1.584 Antworten eingingen. Nach umfassendem Screening und Zuverlässigkeitsprüfungen mussten 186 Antworten ausgesondert werden. Die endgültige Stichprobe bestand aus 1.398 Antworten, d. h. es gab eine Antwortquote von 4,1 % für die USA und 4,0 % für die EMEA-Länder.

Tabelle 1 Antworten auf die Umfrage					
Regionale Cluster	Stichproben- größen	Gesamtzahl der Antworten	Ausgeson- derte oder abgelehnte Antworten	Endgültige Stichprobe	Antwort- quote
USA	17.680	821	98	723	4,1 %
EMEA	16.700	763	88	675	4,0 %

Abbildung 12 zeigt die Position der Befragten in der Hierarchie der entsprechenden Unternehmen. 79% der US-Befragten und 74% der Befragten aus den EMEA-Ländern sind Vorgesetzte oder Führungskräfte.

Abbildung 12. Aktuelle Position im Unternehmen

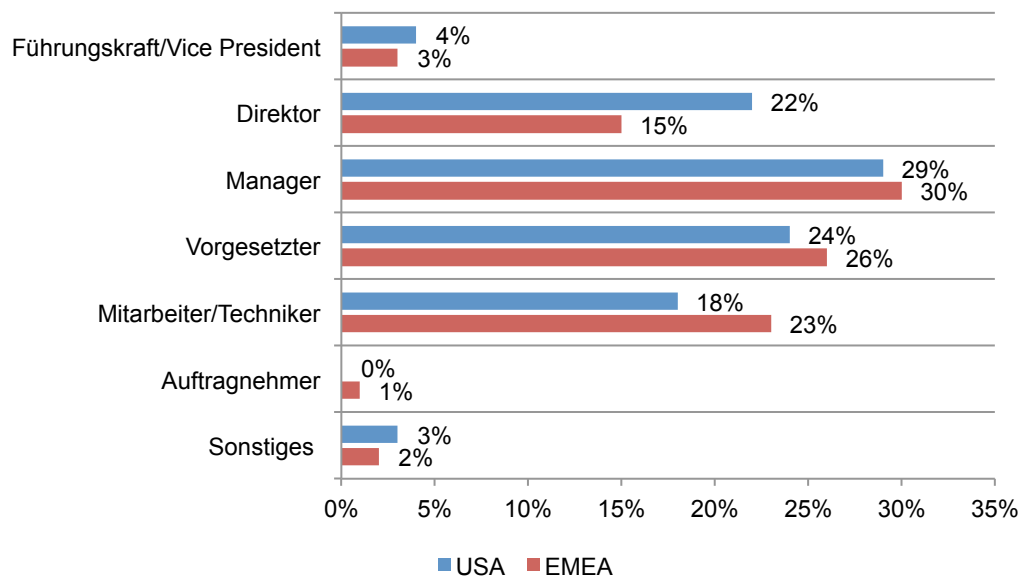


Abbildung 13 zeigt die Anzahl der Länder, in denen die Unternehmen der Befragten tätig sind. Der hochgerechnete Wert für die USA ergibt 7.93 Länder und für die EMEA-Länder liegt der Wert bei 9.49 Ländern.

Abbildung 13. In wie vielen Ländern ist Ihr Unternehmen geschäftlich tätig?

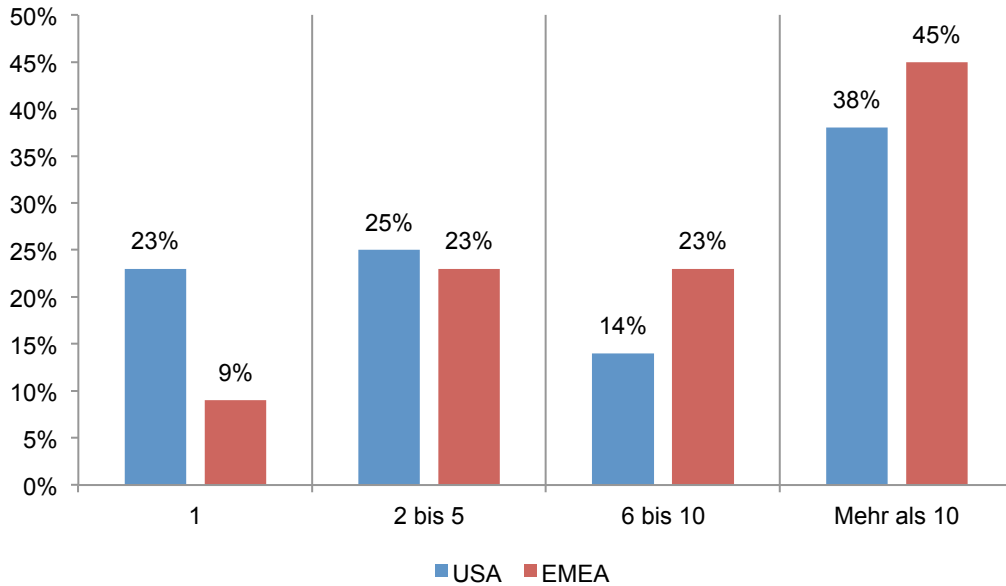


Abbildung 14 zeigt die Gesamtzahl der Vollzeitmitarbeiter im weltweit tätigen Unternehmen des Befragten. Der hochgerechnete Wert für die USA beträgt 8.458 Mitarbeiter, in den EMEA-Ländern liegt der Wert bei 7.317 Mitarbeitern.

Abbildung 14. Wie viele Vollzeitmitarbeiter beschäftigt Ihr weltweit tätiges Unternehmen insgesamt?

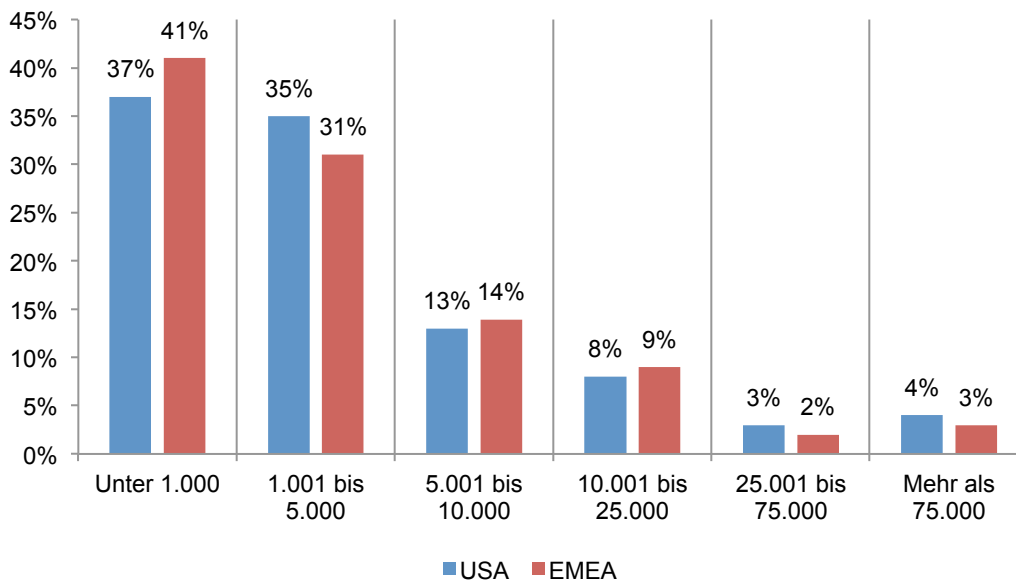
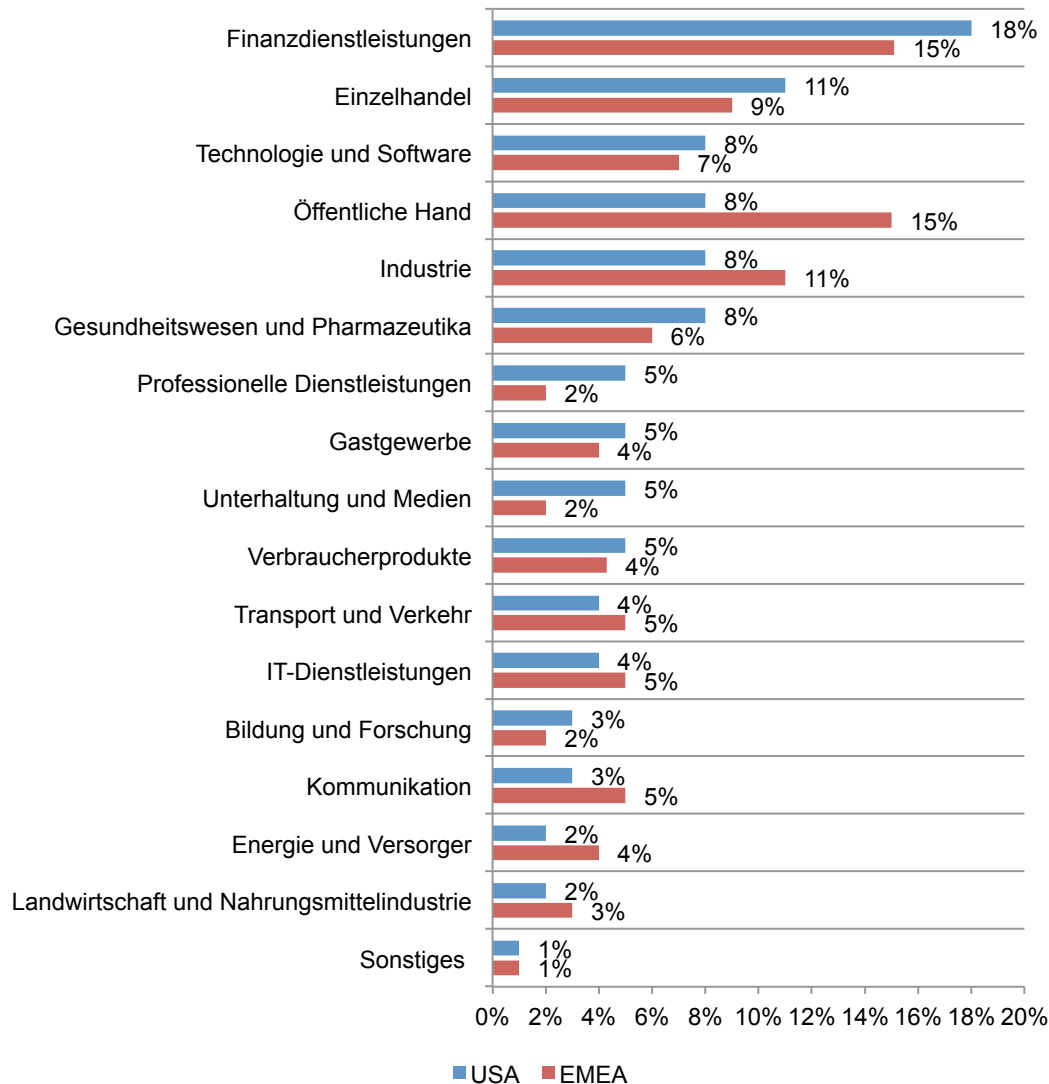


Abbildung 15 zeigt die Aufschlüsselung der Unternehmen der Befragten geordnet nach Branchen. Dieses Diagramm zeigt, dass das größte Segment sowohl in den USA (18 %) als auch in den EMEA-Ländern (15 %) die Finanzdienstleistungsbranche ist.

Abbildung 15. Aufschlüsselung nach Unternehmensbranche



Teil: 4. Gewährleistungsausschluss

Umfragen sind Richtlinien unterworfen, die sorgfältig eingehalten werden müssen, bevor Schlussfolgerungen aus den Ergebnissen gezogen werden. Die folgenden Punkte sind spezifische Einschränkungen, die für die meisten einschlägigen Umfragen zutreffen.

Verfälschung durch Enthaltungen: Die aktuellen Umfragen basieren auf einer Stichprobe der beantworteten Umfragen. Wir haben Umfragen an eine repräsentative Gruppe von Einzelpersonen in zwei globalen Regionen gesandt. Dadurch ergibt sich eine hohe Zahl verwertbarer Rückantworten. Trotz Enthaltungs-Tests besteht immer die Möglichkeit, dass Einzelpersonen, die an der Umfrage nicht teilnahmen, eine ganz andere Einstellung haben als diejenigen, die an der Umfrage teilnahmen.

Verfälschung durch die Größe der Stichprobe: Die Genauigkeit der Studie basiert auf den Kontaktangaben der Befragten und hängt zudem davon ab, inwieweit die Liste repräsentativ für Personen ist, die IT-Praktiker oder IT-Sicherheitsbeauftragte sind. Uns ist auch bewusst, dass die Ergebnisse durch externe Ereignisse, beispielsweise Berichte in den Medien, verfälscht werden können. Bewusst ist uns außerdem, dass die Ergebnisse insofern verfälscht werden können, indem die Befragten für das Ausfüllen der Umfrage innerhalb einer bestimmten Frist, eine Vergütung erhielten.

Verfälschte Ergebnisse: Die Qualität der Studie hängt ab von der Authentizität der von den Befragten gelieferten Antworten ab. Trotz Qualitätsprüfungen und Anpassungen, kann es vorkommen, dass ein Befragter eine falsche Antwort gab.

Anhang: Detaillierte Ergebnisse der Umfrage

Die folgenden Tabellen enthalten die Häufigkeit der Antworten bezüglich aller gestellten Fragen, (global) konsolidiert für vier regionale Cluster. Alle Antworten wurden im Oktober 2014 erfasst.

Antworten auf die Umfrage	Häufigkeit	USA	Häufigkeit	EMEA
Gesamtzahl der Befragten	17.680	100,0 %	16.700	100,0 %
Gesamtzahl der Antworten	821	4,6 %	763	4,6 %
Ausgesonderte oder abgelehnte Antworten	98	0,6 %	88	0,5 %
Endgültige Stichprobe	723	4,1 %	675	4,0 %

S1. Versucht Ihr Unternehmen den Anteil der Open-Source-Software gegenüber proprietären Unternehmensanwendungen zu kontrollieren?	Häufigkeit	USA	Häufigkeit	EMEA
Ja	609	84 %	556	82 %
Nein	114	16 %	119	18 %
Gesamt	723	100 %	675	100 %

S2. Welche Aussage beschreibt am besten, wie vertraut Sie im Allgemeinen mit den Richtlinien und Anforderungen Ihres Unternehmens zur Datensicherheit und zum Datenschutz sind?	Häufigkeit	USA	Häufigkeit	EMEA
Sehr vertraut	175	29 %	156	28 %
Vertraut	168	28 %	159	29 %
Etwas vertraut	156	26 %	160	29 %
Nicht vertraut	78	13 %	57	10 %
Keine Ahnung	32	5 %	24	4 %
Gesamt	609	100 %	556	100 %

Verwandte Anzahl für die Analyse der Stichprobe	577	532
-------------------------------------------------	-----	-----

Teil: 2. Rolle und Funktion im Unternehmen

D1. Welche Bezeichnung beschreibt Ihre Position in Ihrem Unternehmen am besten?	USA	EMEA
Führungskraft/Vice President	4 %	3 %
Direktor	22 %	15 %
Manager	29 %	30 %
Vorgesetzter	24 %	26 %
Mitarbeiter/Techniker	18 %	23 %
Auftragnehmer	0 %	1 %
Andere (bitte angeben)	3 %	2 %
Gesamt	100 %	100 %

D2. In wie vielen Ländern ist Ihr Unternehmen in etwa tätig?	USA	EMEA
1	23 %	9 %
2 bis 5	25 %	23 %
6 bis 10	14 %	23 %
Mehr als 10	38 %	45 %
Gesamt	100 %	100 %
Hochgerechneter Wert	7,93	9,49

D3. In welchem Bereich liegt in Ihrem weltweit agierenden Unternehmen die Gesamtzahl der Vollzeitmitarbeiter?	USA
Unter 1.000	37 %
1.001 bis 5.000	35 %
5.001 bis 10.000	13 %
10.001 bis 25.000	8 %
25.001 bis 75.000	3 %
Mehr als 75.000	4 %
Gesamt	100 %
Hochgerechneter Wert	8.458

EMEA
41 %
31 %
14 %
9 %
2 %
3 %
100 %
7.317

D4. Bitte geben Sie an, wie groß der Anteil der kommerziellen Open-Source-Anwendungen Ihrer Unternehmensanwendungen in Ihrem Unternehmen ist.	USA
Unter 10 %	35 %
10 bis 25 %	18 %
26 bis 50 %	15 %
51 bis 75 %	15 %
Mehr als 75 %	9 %
Lässt sich nicht ermitteln	8 %
Gesamt	100 %
Hochgerechneter Wert	30 %

EMEA
40 %
20 %
16 %
11 %
6 %
7 %
100 %
25 %

D5. Welche Aussage beschreibt am besten das primäre Betriebssystem Ihres Unternehmens? Bitte wählen Sie nur eines aus.	USA
Linux	36 %
Windows	43 %
Mac	16 %
Andere (bitte angeben)	5 %
Gesamt	100 %

EMEA
39 %
41 %
14 %
6 %
100 %

D6. Setzt Ihr Unternehmen seine Sicherheits- und Datenschutzrichtlinien durch?	USA
Ja, in allen Fällen.	17 %
Ja, in manchen Fällen.	34 %
Nein	44 %
Weiß nicht	5 %
Gesamt	100 %

EMEA
25 %
43 %
25 %
7 %
100 %

D7. Welche Aussage beschreibt am besten die Branche Ihres Unternehmens?	USA
Landwirtschaft und Nahrungsmittelindustrie	2 %
Kommunikation	3 %
Verbraucherprodukte	5 %
Wehrtechnik sowie Luft- und Raumfahrt	0 %
Bildung und Forschung	3 %
Energie und Versorgungsindustrie	2 %
Unterhaltung und Medien	5 %
Finanzdienstleistungen	18 %
Gesundheitswesen und Pharmaindustrie	8 %
Gastronomie	5 %
Industrie	8 %
IT-Dienstleistungen	4 %
Professionelle Dienstleistungen	5 %
Öffentliche Hand	8 %
Einzelhandel	11 %
Technologie und Software	8 %
Transport und Verkehr	4 %
Andere (bitte angeben)	1 %
Gesamt	100 %

EMEA
3 %
5 %
4 %
1 %
2 %
4 %
2 %
15 %
6 %
4 %
11 %
5 %
2 %
15 %
9 %
7 %
5 %
0 %
100 %

Teil: 3. Eigenschaften kommerzieller Open-Source-Anwendungen:
 Nachfolgend sehen Sie 6 Vorteile kommerzieller Open-Source-Software, die in einem kürzlich veröffentlichten Artikel diskutiert wurden (Quelle: CIO Insight). Bitte bewerten Sie jede Aussage mit Hilfe der folgenden Bewertungsskala.

Q1a. Sie können Kosten senken, da Open-Source-Software flexibler ist als proprietäre Software.	USA
Stimme in vollem Umfang zu	26 %
Stimme zu	36 %
Weiß nicht	28 %
Stimme nicht zu	8 %
Stimme keinesfalls zu	2 %
Gesamt	100 %

EMEA
20 %
30 %
30 %
15 %
5 %
100 %

Q1b. Die Qualität wird durch kommerzielle gesteigert, da Open-Source-Software für Zusammenarbeit prädestiniert ist und laufend verbessert wird.	USA
Stimme in vollem Umfang zu	31 %
Stimme zu	32 %
Weiß nicht	24 %
Stimme nicht zu	10 %
Stimme keinesfalls zu	3 %
Gesamt	100 %

EMEA
30 %
30 %
24 %
14 %
2 %
100 %

Q1c. Sie sitzen am Steuer. Bei proprietärer Software diktieren die Anbieter den Code und die Preise. Bei kommerzieller Open-Source-Software ändern Sie den Code und können so Ihre Anforderungen im Rahmen Ihres Budgets erfüllen.	USA
Stimme in vollem Umfang zu	26 %
Stimme zu	32 %
Weiß nicht	30 %
Stimme nicht zu	9 %
Stimme keinesfalls zu	3 %
Gesamt	100 %

EMEA
23 %
30 %
28 %
16 %
3 %
100 %

Q1d. Sie bestimmen, wie lange Sie die Software nutzen. Falls ein Anbieter von proprietärer Software bankrott geht oder ein Softwareprodukt nicht mehr unterstützt, haben Sie Pech gehabt. Wenn ein führender Anbieter von kommerzieller Open-Source-Software ein Projekt abbricht oder die Community verlässt, treten andere an seine Stelle.	USA
Stimme in vollem Umfang zu	33 %
Stimme zu	41 %
Weiß nicht	18 %
Stimme nicht zu	6 %
Stimme keinesfalls zu	2 %
Gesamt	100 %

EMEA
29 %
38 %
20 %
11 %
2 %
100 %

Q1e. Ihre Abteilung erweitert Ihr Wissen. Durch den Kontakt mit den Open-Source-Communities und die interne Zusammenarbeit lernt Ihr Technikerteam mehr über allgemeine IT-Praktiken, Ressourcen und Tools, die Sie für Ihr Unternehmen optimal einsetzen können.	USA
Stimme in vollem Umfang zu	39 %
Stimme zu	35 %
Weiß nicht	19 %
Stimme nicht zu	5 %
Stimme keinesfalls zu	2 %
Gesamt	100 %

EMEA
30 %
27 %
23 %
16 %
4 %
100 %

Q1f. Ihre Benutzer haben weniger mit Bugs zu kämpfen. Es gibt eine enorme Anzahl von Community-Mitgliedern, die permanent und akribisch die Codebasis prüfen und sicherstellen, dass Bugs gefunden sowie schnell und effektiv beseitigt werden.	USA
Stimme in vollem Umfang zu	33 %
Stimme zu	33 %
Weiß nicht	21 %
Stimme nicht zu	9 %
Stimme keinesfalls zu	4 %
Gesamt	100 %

EMEA
28 %
27 %
25 %
18 %
3 %
100 %

Teil: 4. Allgemeine Fragen

Q2. Bitte bewerten Sie in der folgenden Liste das Datensicherheitsrisiko jedes Dateiaustauschverfahrens für Ihr Unternehmen. 1 = höchstes Risiko und 6 = niedrigstes Risiko	USA
Unverschlüsselte E-Mails	1,44
Verschlüsselte E-Mails	5,21
Dateitransferprotokoll (FTP)	2,88
Daten-Sharing in der Cloud/Dateisynchronisation und Sharingtool	1,90
Kommerzieller, gemeinsamer Dateizugriff im Firmennetzwerk/Dateisynchronisations- und Austauschtool	4,59
Eigenes Tool zum Dateiaustausch im Unternehmensnetzwerk	3,13
Durchschnitt	3,19

EMEA
2,18
4,38
2,50
1,72
5,26
2,16
3,37

Q3. Welche Aussage beschreibt am besten den Grad der Einbeziehung der IT-Abteilung Ihres Unternehmens in die Bewertung bzw. Auswahl von Groupware Lösungen?	USA
Signifikant einbezogen	39 %
Teilweise einbezogen	43 %
Nicht einbezogen	18 %
Gesamt	100 %

EMEA
30 %
53 %
17 %
100 %

Q4. Wie zufrieden ist Ihr Unternehmen mit seiner existierenden Groupware?	USA
Sehr zufrieden	16 %
Zufrieden	28 %
Etwas zufrieden	20 %
Nicht zufrieden	36 %
Gesamt	100 %

EMEA
11 %
24 %
21 %
44 %
100 %

Q5a. Wie wird Ihre Software zur Zeit betrieben?	USA
Betrieb im eigenen Netzwerk	56 %
Öffentliche Cloud, Hosting als einzelner Mandant	27 %
Öffentliche Cloud, Hosting mit mehreren Mandanten	45 %
Private Cloud, Hosting als einzelner Mandant	17 %
Hybridlösung mit Betrieb in der Cloud und im Unternehmensnetzwerk	45 %
Gesamt	190 %

EMEA
69 %
22 %
40 %
24 %
31 %
186 %

Q5b. Wie zufrieden ist Ihr Unternehmen mit dem aktuellen Softwarebetrieb?	USA
Sehr zufrieden	15 %
Zufrieden	24 %
Etwas zufrieden	24 %
Nicht zufrieden	37 %
Gesamt	100 %

EMEA
12 %
19 %
26 %
43 %
100 %

Q6. Wählen Sie bitte anhand der nachfolgenden Liste die fünf (5) wichtigsten Faktoren bei der Auswahl einer Groupware Lösung aus.	USA
Fähigkeit zum Hosting oder zur Verwaltung der Lösung in der Cloud	63 %
Einfache Installation	28 %
Einfache Verwaltung	37 %
Einfache Nutzung	65 %
Verbesserung des Datenschutzes	9 %
Verbesserung der Datensicherheit	50 %
Open Source	53 %
Unterstützung für den Zugriff auf verschlüsselte E-Mails mit Mobilgeräten.	21 %
Technische Zertifizierungen	15 %
Gesamtnutzungskosten	39 %
Schulungsprogramm für die Benutzer bzw. Schulungsunterlagen	16 %
Image des Anbieters	49 %
Unterstützung des Anbieters	55 %
Gesamt	500 %

EMEA
45 %
26 %
42 %
44 %
38 %
45 %
57 %
17 %
12 %
37 %
15 %
61 %
60 %
500 %

Q7. Beabsichtigt Ihr Unternehmen seine Groupware Lösung zu erneuern?	USA
Ja, innerhalb von 6 Monaten	32 %
Ja, innerhalb von 12 Monaten	13 %
Ja, innerhalb von 24 Monaten	10 %
Ja, in mehr als 24 Monaten	4 %
Keine Erneuerung geplant	41 %
Gesamt	100 %

EMEA
18 %
23 %
11 %
2 %
46 %
100 %

Q8. Verbessert Ihrer Meinung nach eine bereits vorhandene kommerzielle Nutzung und Codetransparenz von kommerzieller Open-Source-Groupware die Sicherheit der Anwendung?	USA
Ja	55 %
Nein	34 %
Weiß nicht	11 %
Gesamt	100 %

EMEA
67 %
24 %
9 %
100 %

Q9. Erhöht Ihrer Meinung nach eine kommerzielle Open-Source-Groupware durch die bereits vorhandene kommerzielle Nutzung und Codetransparenz die Datensicherheit?	USA
Ja	52 %
Nein	37 %
Weiß nicht	11 %
Gesamt	100 %

EMEA
66 %
26 %
8 %
100 %

Q10. Erhöht Ihrer Meinung nach eine kommerzielle Open-Source-Groupware durch die bereits vorhandene kommerzielle Nutzung und Codetransparenz die Integrität und das Vertrauen in die Anwendung?	USA
Ja	68 %
Nein	23 %
Weiß nicht	9 %
Gesamt	100 %

EMEA
76 %
16 %
8 %
100 %

Wie häufig treten die folgenden Szenarien bezüglich Datenschutz und Datensicherheit bei der in Ihrem Unternehmen eingesetzten Groupware auf?	
Q11a. Die Mitarbeiter versenden und empfangen Dateien und Dokumente, die nicht für sie bestimmt sind.	USA
Niemals	8 %
Selten	12 %
Oft	56 %
Häufig	24 %
Gesamt	100 %

EMEA
18 %
13 %
50 %
19 %
100 %

Q11b. Die Mitarbeiter mißachten die Unternehmensrichtlinien zum Austausch vertraulicher Dokumente.	USA
Niemals	5 %
Selten	6 %
Oft	34 %
Häufig	55 %
Gesamt	100 %

EMEA
16 %
5 %
33 %
46 %
100 %

Q11c. Die Mitarbeiter nutzen eine Groupware, die vom Unternehmen nicht autorisiert ist.	USA
Niemals	11 %
Selten	15 %
Oft	38 %
Häufig	36 %
Gesamt	100 %

EMEA
16 %
13 %
31 %
40 %
100 %

Q11d. Die Groupware steht aus Sicherheitsgründen nicht zur Verfügung.	USA
Niemals	13 %
Selten	26 %
Oft	35 %
Häufig	26 %
Gesamt	100 %

EMEA
23 %
25 %
24 %
28 %
100 %

Q12. Nutzen Sie eine der folgenden Groupware Anwendungen? Bitte wählen Sie alle Anwendungen aus, die zutreffen.	USA
Zimbra	41 %
Microsoft Exchange	71 %
Microsoft Office 365	53 %
Google Apps/Gmail	56 %
IBM Domino	27 %
Novell GroupWise	35 %
Andere (bitte angeben)	9 %
Keine der oben genannten	5 %
Gesamt	297 %

EMEA
30 %
61 %
44 %
44 %
29 %
23 %
9 %
17 %
257 %

Q13. Welche der folgenden Anwendungen werden in Ihrem Unternehmen im Rahmen Ihrer Groupware eingesetzt? Bitte wählen Sie alle Anwendungen aus, die zutreffen.	USA
Kostenlose Versionen der Dateisynchronisations- und Datenaustauschanwendungen für Verbraucher (beispielsweise Dropbox und Google)	66 %
Für Verbraucher konzipierte Anwendungen zur Dateispeicherung in einer öffentlichen Cloud (beispielsweise Box und Microsoft)	72 %
Für Unternehmen konzipierte Angebote zum Dateiaustausch in einer privaten Cloud (beispielsweise Syncplicity von EMC, Egnyte)	34 %
Hauseigene Anwendungen zum Dateiaustausch (beispielsweise Accellion, IBM)	49 %
Keine der oben genannten	5 %
Gesamt	226 %

EMEA
37 %
57 %
41 %
65 %
7 %
207 %

Teil: 5. Produkteigenschaften: Mehr als 200.000 Unternehmen mit mehr als 100 Mio. kommerziellen Nutzern und 500 Mio. Usern der kostenfreien Variante nutzten Zimbra zur Zeit weltweit. Bitte bewerten Sie jede Eigenschaft entsprechend ihrer Bedeutung bei der Auswahl dieser Groupware Lösung für Ihr Unternehmen.

Q14a. Zentraler Hub für E-Mail, Social Media und Anwendungen zur Synchronisation und zum Austausch von Dateien und Integration der Anwendungen von Drittanbietern	USA
Sehr wichtig	36 %
Wichtig	33 %
Teilweise wichtig	16 %
Nicht wichtig	8 %
Irrelevant	7 %
Gesamt	100 %

EMEA
28 %
31 %
25 %
11 %
5 %
100 %

Q14b. Integrierter Kalender, Kontakte und Aufgaben; Interaktionsfähigkeit mit anderen Anwendungen für E-Mail und Kalender	USA
Sehr wichtig	36 %
Wichtig	32 %
Teilweise wichtig	19 %
Nicht wichtig	8 %
Irrelevant	5 %
Gesamt	100 %

EMEA
37 %
33 %
22 %
6 %
2 %
100 %

Q14c. Fähigkeit zur Verschlüsselung und digitalen Signatur von E-Mail sowohl auf Desktop- als auch Mobilgeräten	USA
Sehr wichtig	29 %
Wichtig	33 %
Teilweise wichtig	23 %
Nicht wichtig	8 %
Irrelevant	7 %
Gesamt	100 %

EMEA
26 %
29 %
26 %
13 %
5 %
100 %

Q14d. Unterstützung von Antispam-, Antivirus- und zweistufigen Authentifizierungstools von Drittanbietern	USA
Sehr wichtig	41 %
Wichtig	34 %
Teilweise wichtig	16 %
Nicht wichtig	8 %
Irrelevant	1 %
Gesamt	100 %

EMEA
32 %
36 %
21 %
6 %
5 %
100 %

Q14e: Möglichkeit zur Definition von Sicherheitsrichtlinien für Mobilgeräte, beispielsweise zur kompletten Löschung eines Geräts, zur Durchsetzung einer PIN-Eingabe und Geräteverwaltungsfunktionen für Benutzerkonten	USA
Sehr wichtig	25 %
Wichtig	29 %
Teilweise wichtig	23 %
Nicht wichtig	15 %
Irrelevant	8 %
Gesamt	100 %

EMEA
19 %
25 %
29 %
19 %
9 %
100 %

Q14f. Unterstützung der Verschlüsselung von zu übertragenden und gespeicherten Daten	USA
Sehr wichtig	26 %
Wichtig	29 %
Teilweise wichtig	22 %
Nicht wichtig	16 %
Irrelevant	7 %
Gesamt	100 %

EMEA
20 %
25 %
32 %
15 %
8 %
100 %

Q14g. Vollständige Unterstützung von Smartphones und Tablets mit iOS, Android, BlackBerry und Windows-Betriebssystemen	USA
Sehr wichtig	48 %
Wichtig	30 %
Teilweise wichtig	13 %
Nicht wichtig	8 %
Irrelevant	1 %
Gesamt	100 %

EMEA
36 %
30 %
22 %
12 %
0 %
100 %

Q14h. Flexible Bereitstellungsoptionen: im Unternehmensnetzwerk, in der öffentlichen Cloud durch Hosting als einzelner Mandant, in der öffentlichen Cloud durch Hosting mit mehreren Mandanten, in der privaten Cloud durch Hosting als einzelner Mandant, Hybridlösung mit Installation in der Cloud und im Firmennetzwerk	USA
Sehr wichtig	46 %
Wichtig	29 %
Teilweise wichtig	15 %
Nicht wichtig	8 %
Irrelevant	2 %
Gesamt	100 %

EMEA
31 %
30 %
24 %
12 %
3 %
100 %

Q14i. Die Fähigkeit, den Verbleib von Daten zu kontrollieren, sodass die Daten des Unternehmens innerhalb definierter Rechtsgebiete verbleiben und die Einhaltung der Datenschutzgesetze gewährleistet ist	USA
Sehr wichtig	23 %
Wichtig	29 %
Teilweise wichtig	26 %
Nicht wichtig	18 %
Irrelevant	4 %
Gesamt	100 %

EMEA
23 %
27 %
28 %
20 %
2 %
100 %

Q14j. Enge Integration mit E-Mail und Anwendungen zum Dateiaustausch und zur Dateisynchronisation, die private Dateianhänge unterstützen, damit nur der beabsichtigte Empfänger Zugriff auf die Dateien erhält (in Abhängigkeit von der betreffenden E-Mail-Adresse)	USA
Sehr wichtig	39 %
Wichtig	31 %
Teilweise wichtig	19 %
Nicht wichtig	10 %
Irrelevant	1 %
Gesamt	100 %

EMEA
36 %
25 %
19 %
15 %
5 %
100 %

Q14l. Genau definierte Zugriffskontrolle und Rechte für Dateianhänge und Dateiaustausch, um die Bestimmungen der Regulierungsbehörden für hochvertrauliche Unterlagen und digitale Assets einzuhalten	USA
Sehr wichtig	35 %
Wichtig	35 %
Teilweise wichtig	15 %
Nicht wichtig	9 %
Irrelevant	6 %
Gesamt	100 %

EMEA
34 %
37 %
13 %
13 %
3 %
100 %

Q14m. Möglichkeit zur Erweiterung der Software zur Zusammenarbeit durch eine offene Architektur, sodass branchenspezifische Arbeitsabläufe des	USA
------------------------------------------------------------------------------------------------------------------------------------------------	-----

EMEA

Unternehmens (beispielsweise HIPAA) erstellt bzw. genutzt werden können	
Sehr wichtig	23 %
Wichtig	20 %
Teilweise wichtig	29 %
Nicht wichtig	21 %
Irrelevant	7 %
Gesamt	100 %

	25 %
	29 %
	18 %
	22 %
	6 %
	100 %

Q14n. Ein E-Mail-System in der Cloud mit adäquaten Funktionen zum Datenschutz, damit die Einhaltung der geltenden Datenschutzvorschriften gewährleistet ist	USA
Sehr wichtig	24 %
Wichtig	21 %
Teilweise wichtig	30 %
Nicht wichtig	20 %
Irrelevant	5 %
Gesamt	100 %

	EMEA
	28 %
	29 %
	20 %
	21 %
	2 %
	100 %

Q14o. Funktionen zur Kontrolle und Verwaltung von Content, beispielsweise Dokumentversionierung, Metadaten, e-Discovery, Archivierung und Synchronisation	USA
Sehr wichtig	21 %
Wichtig	29 %
Teilweise wichtig	32 %
Nicht wichtig	15 %
Irrelevant	3 %
Gesamt	100 %

	EMEA
	20 %
	25 %
	26 %
	23 %
	6 %
	100 %

Q14p. Funktionen zur Verwaltung, zum Zugriff auf bzw. zur sonstigen Integration mit Backend-Diensten wie Netzwerkdateisystemen, Verzeichnissen, Workflow-Systemen, Repositories und Unternehmensanwendungen	USA
Sehr wichtig	23 %
Wichtig	23 %
Teilweise wichtig	31 %
Nicht wichtig	17 %
Irrelevant	6 %
Gesamt	100 %

	EMEA
	19 %
	25 %
	29 %
	20 %
	7 %
	100 %

Zusammensetzung des EMEA-Clusters nach Ländern	Häufigkeit	Prozent
Dänemark	12	2 %
Frankreich	69	10 %
Deutschland	98	15 %
Griechenland	7	1 %
Irland	22	3 %
Israel	10	1 %
Italien	41	6 %
Niederland	35	5 %
Polen	29	4 %
Russische Föderation	48	7 %

Saudi Arabien	43	6 %
Südafrika	23	3 %
Spanien	48	7 %
Schweden	12	2 %
Schweiz	13	2 %
Türkei	30	4 %
Vereinigte Arabische Emirate	27	4 %
Großbritannien	108	16 %
Gesamt	675	100 %

Weitere Informationen zu dieser Studie erhalten Sie vom Ponemon Institut per E-Mail unter research@ponemon.org. Alternativ können Sie und auch unter unserer gebührenfreien Rufnummer 1 800 887 3118 erreichen.

Ponemon Institut

Advancing Responsible Information Management

Das Ponemon Institute befasst sich mit unabhängiger Recherche und Weiterbildung zur Förderung verantwortungsbewusster Information- und Datenschutzmanagementpraktiken in Unternehmen und Behörden. Unsere Mission sehen wir in der Durchführung hochwertiger empirischer Studien zu kritischen Fragen, die Management und Sicherheit sensibler Informationen von Personen und Unternehmen betreffen.

Als Mitglieder des **Council of American Survey Research Organizations (CASRO)** sind wir strengsten Normen zur Geheimhaltung von Daten zum Datenschutz und zur ethischen Durchführung von Recherchen unterworfen. Wir erfassen keine personenbezogenen Informationen von Einzelpersonen (oder unternehmensbezogene Informationen) in unseren Unternehmensumfragen. Darüber hinaus verfügen wir über strikte Qualitätsnormen, die sicherstellen, dass den befragten Personen keine verletzenden, irrelevanten oder unangemessenen Fragen gestellt werden.