»SICHERE CLOUD«

Sicherheit in Cloud-Computing-Systemen
Umfrage des Fraunhofer IAO, 2011

30 Jahre
Fraunhofer IAO

Fraunhofer
IAO

Cloud Computing und Sicherheit

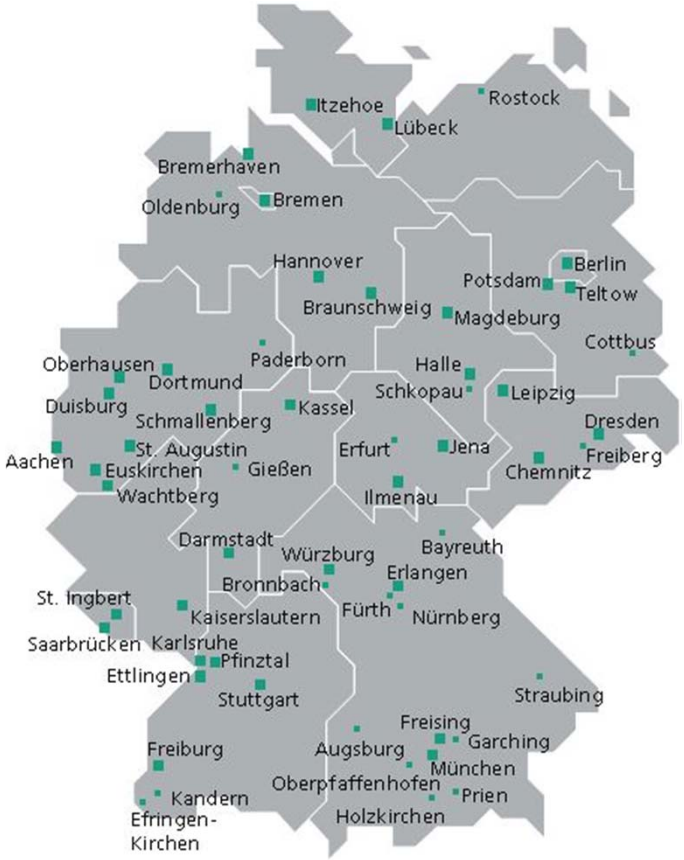
Cloud Computing gilt als eine der wichtigsten Innovationen in der (IKT-) Wirtschaft der vergangenen Jahre. Die Idee ist, dass Speicherplatz, Rechenleistung und konkrete Software-Anwendungen nicht mehr beim Anwender selbst vorgehalten, sondern extern als Dienstleistung eingekauft werden.

Vielversprechend sind die Möglichkeiten, die sich durch das Outsourcing von Rechen-, Speicher- und IT-Dienstleistungen für Unternehmen ergeben. Bevor Unternehmen jedoch in die Wolke ziehen, müssen grundlegende Fragestellungen geklärt werden; speziell die Frage nach der Sicherheit ist vorrangig.

Aus diesem Grund erforscht das Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO in Zusammenarbeit mit der BITKOM, inwiefern Cloud-Anbieter auf die Sicherheitsanforderungen potenzieller Kunden vorbereitet sind. In diesem Zusammenhang wurden ein Stimmungsbild und konkrete Unternehmensanforderungen erhoben.

Fraunhofer IAO

Fraunhofer-Gesellschaft im Profil

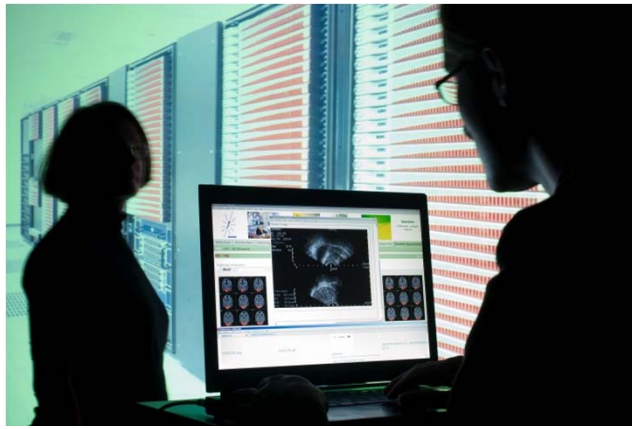


- **Gründungsjahr:** 1949
- 18 000 **Mitarbeiter**
- Mehr als **80 Forschungseinrichtungen**,
  davon 60 Institute als selbständige Profit-Center
- **Fraunhofer International**
  Europa: Brüssel (Belgien), Moskau (Russland),
  Budapest (Ungarn), Jönköping (Schweden),
  Bozen (Italien) u.a.
  USA: Boston (Massachusetts), Pittsburgh (Pennsylvania),
  Plymouth (Michigan), Providence (Rhode Island),
  College Park (Maryland), Peoria (Illinois)
  Asien: Ampang (Malaysia), Beijing (China), Jakarta (Indonesien),
  Koramangala Bangalore (Indien), Seoul (Korea), Singapur, Tokio
  (Japan)
  Naher Osten: Dubai (VAE), Kairo (Ägypten)

Fraunhofer IAO

Fraunhofer IAO im Profil

www.iao.fraunhofer.de



- **Gründungsjahr:** 1981
- **Institutsleiter:** Prof. Dr.-Ing. Dr.-Ing. E.h. Dieter Spath
- **Finanzvolumen:** 31,5 Mio. €, davon 33% im Auftrag der Wirtschaft
- **Mitarbeiter:** 480 Mitarbeiter*

*Daten 2010, inklusive IAT der Universität Stuttgart

Fraunhofer IAO

Cloud-Forschung am Fraunhofer IAO: Die Fraunhofer-Allianz Cloud Computing

www.cloud.fraunhofer.de

Die Fraunhofer-Allianz Cloud Computing ist ein Verbund von derzeit acht Fraunhofer-Instituten, die sich in Forschung und Industrieprojekten mit unterschiedlichen Themenstellungen im Bereich des Cloud Computing – und zuvor bereits mit thematisch verwandten Bereichen wie Grid Computing, Utility Computing und Serviceorientierte Architekturen – befassen.

Im Rahmen der Fraunhofer-Allianz Cloud Computing bündeln die beteiligten Institute ihre Kompetenzen, um Kunden und Forschungspartnern gegenüber eine zentrale Anlaufstelle in Fragen der Vernetzung und optimierten Nutzung verteilter IT-Ressourcen anzubieten. Die Fraunhofer-Allianz Cloud Computing bietet ein breites Leistungsspektrum an, welches das koordinierte Know-how der beteiligten Institute umfasst und für den Kunden als eine Einheit mit einem zentralen Ansprechpartner angeboten werden kann.

Die Kompetenzen der acht Fraunhofer-Institute liegen in den folgenden Bereichen:

- Betriebs- und Geschäftsmodelle
- Prozessmanagement
- Ressourcenplanung
- Anwendungsentwicklung
- Life Cycle Management für Cloud Services und Cloud-Umgebungen

Fraunhofer IAO
Fraunhofer ITWM
Fraunhofer SCAI
Fraunhofer IIS
Fraunhofer AISEC
Fraunhofer FIRST
Fraunhofer ISST
Fraunhofer FOKUS

Sicherheitsbezogene Cloud-Forschung am Fraunhofer IAO: BMWi-geförderte Projekte im Rahmen von Trusted Cloud

Trusted Cloud

Bundesministerium für Wirtschaft und Technologie

Die Fraunhofer-Gesellschaft ist im Rahmen von Trusted Cloud in acht von vierzehn durch das Bundesministerium für Wirtschaft und Technologie geförderten Projekten beteiligt:

- Cloud4E
- CloudCycle
- goBerlin
- HealthCloud
- MIA
- Sealed Cloud
- SkIDentity
- CLOUDwerker

Das Fraunhofer IAO ist an den Projekten **CLOUDwerker** und **SkIDentity** beteiligt.

In dem Projekt **CLOUDwerker** entstehen entsprechend den Anforderungen von Handwerksbetrieben und unter Berücksichtigung vorhandener, Cloud-basierter Lösungen Dienstebündel mit dazugehörigen Geschäftsmodellen auf einer vertrauenswürdigen, offenen Service-Plattform, welche die Geschäftsprozesse in kleinen und mittelständischen Unternehmen sicher unterstützen.

Im Projekt **SkIDentity** wird eine tragfähige Brücke zwischen den sicheren elektronischen Ausweisen (eID) und den heute existierenden bzw. sich entwickelnden Cloud-Computing-Infrastrukturen geschlagen.
Somit können vertrauenswürdige Identitäten für die Cloud bereitgestellt und komplette Prozess- und Wertschöpfungsketten sicher gestaltet werden.

Fraunhofer IAO

»SICHERE CLOUD«

- **Untersuchungsdesign**
- Ergebnisse der Studie
- Ausblick
- Ansprechpartner

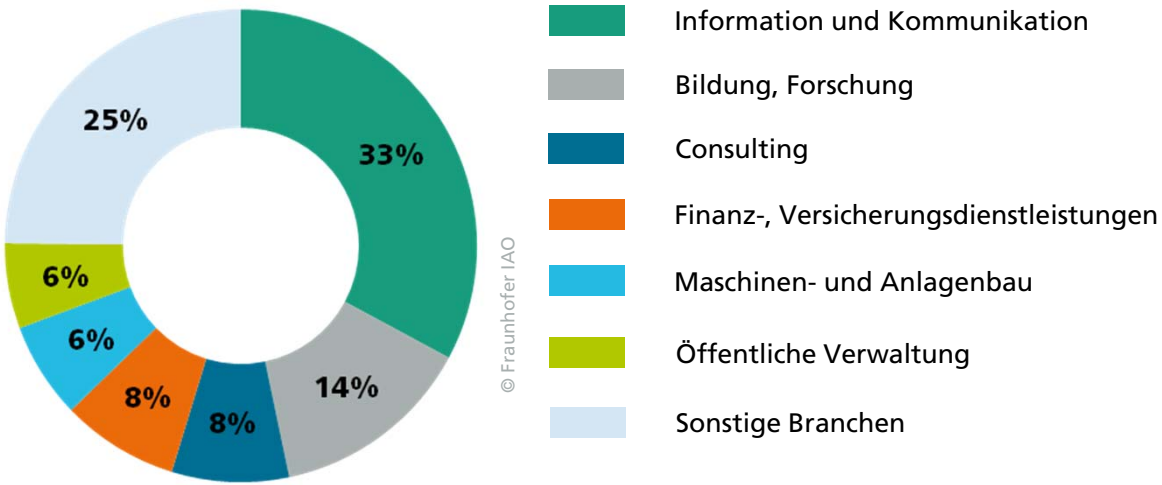
Untersuchungssteckbrief

Untersuchung zu Sicherheit in Cloud-Computing-Systemen	
Zielgruppe	IT-Entscheider und IT-Professionals in Deutschland
Untersuchungs-bereiche	Aktuelle Einschätzung der Sicherheit von Cloud-Angeboten Kriterien für eine »Sichere Cloud« Sicherheitsanforderungen von Anwendern
Untersuchungs-umfang	142 Personen (bei 3.000 angeschriebenen Personen)
Untersuchungs-zeitraum	Juni und Juli 2011

Hinweise

Die vorliegende Foliendokumentation liefert eine Gesamtauswertung der Daten. Die angegebenen Prozentwerte beziehen sich immer auf die gültigen Antworten. Auf- und Abrundungen können dazu führen, dass die Summenwerte leicht von 100 Prozent abweichen. In die Aufbereitung und Dokumentation der Untersuchungsergebnisse flossen nur solche Erkenntnisse ein, die unter statistischen Gesichtspunkten über eine genügend hohe Aussagekraft verfügten.

Verteilung nach Branche



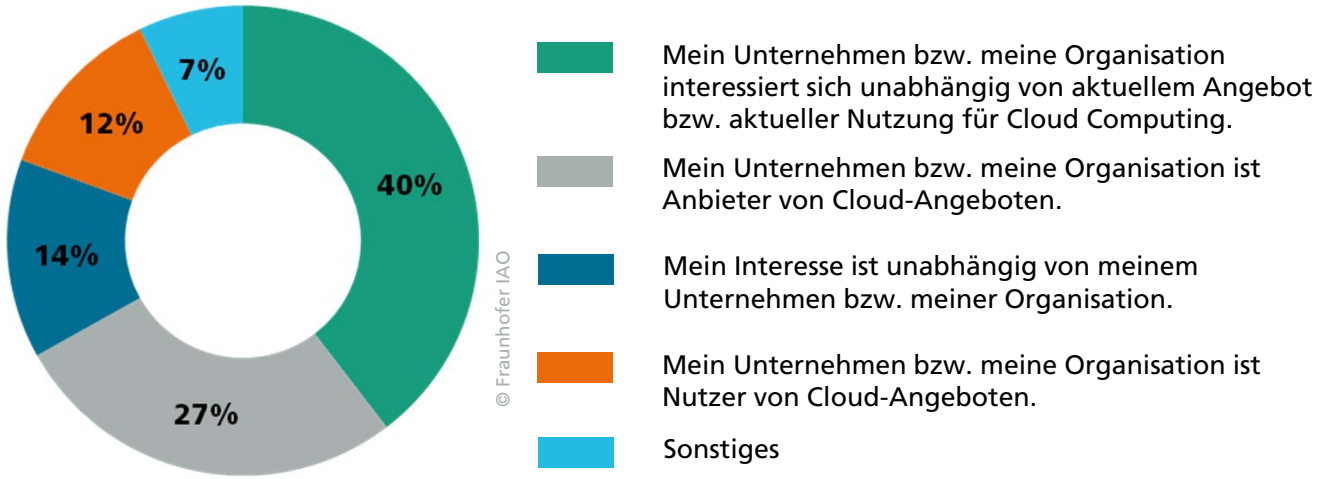
n = 137

Die Branchenverteilung zeigt mit einem Drittel Rückläuferanteil einen Schwerpunkt in der IT-Branche. Mit 14 Prozent Anteil sind IT-Entscheider aus Bildung und Forschung am zweithäufigsten vertreten. Jeweils acht Prozent der Teilnehmer sind im Bereich von Consulting oder Finanz- und Versicherungsdienstleistungen aktiv. Ein relativ kleiner, jedoch auswertbarer Anteil, ist dem Maschinen- und Anlagenbau oder der öffentlichen Verwaltung zuzurechnen (je sechs Prozent). Unter sonstige Branchen (25 Prozent) fielen einzelne Vertreter aus der Automobil-, Luft- und Raumfahrt sowie Konsumgüterindustrie, Handel und Gewerbe oder aus dienstleistungsintensiven Zweigen wie Transport und Logistik, Energie- und Wasserversorgung sowie Gesundheits- und Sozialwesen.

»SICHERE CLOUD«

- Untersuchungsdesign
- **Ergebnisse der Studie**
  - **Aktuell wahrgenommene Cloud Security**
  - Sicherheitsbedarf bei Anwendern
- Ansprechpartner

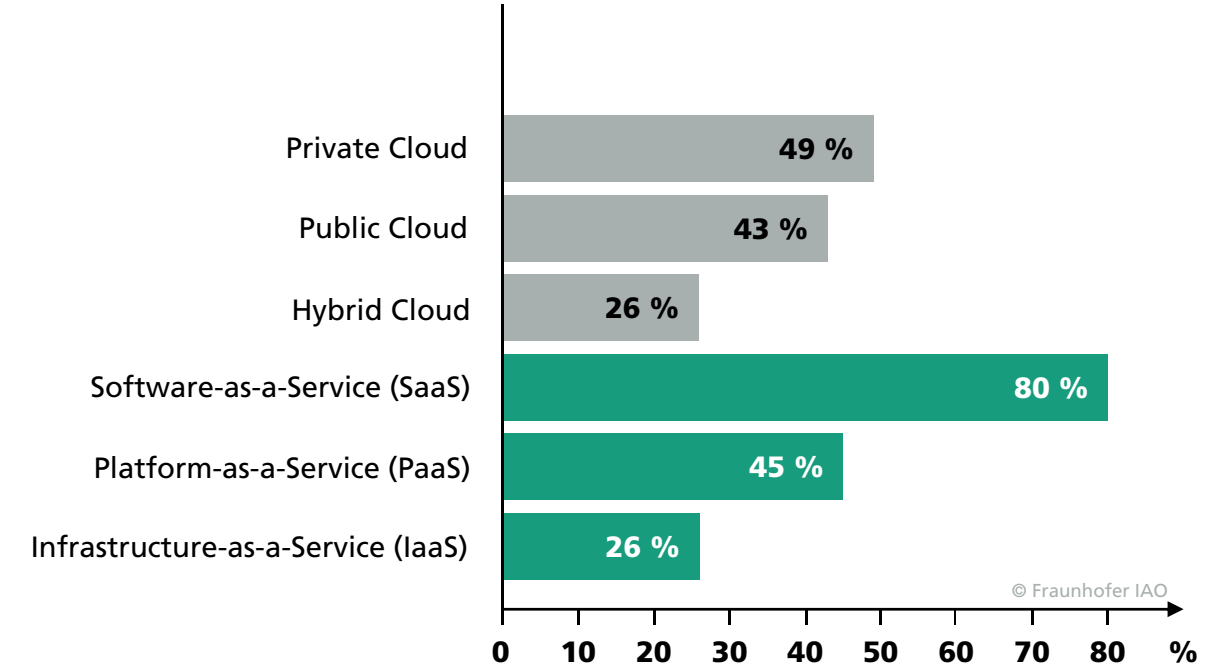
In welchem Rahmen beschäftigen Sie sich mit Cloud Computing?



n = 139

Der Großteil der Teilnehmer interessiert sich unabhängig von der Cloud-Nutzung oder des Cloud-Angebots ihres Arbeitgebers für das Thema Cloud Computing. Ein ähnlich großer Anteil (39 Prozent) der Befragten gab an, dass ihr Arbeitgeber Cloud-Lösungen entweder nutzt oder anbietet. Diese Werte zeigen , dass sich Unternehmen aufteilen in die, die früh neue Technologien benutzen und bewerten und die, die warten und analysieren, wann es sich für sie lohnt, die neue Technologie zu benutzen. Die 14 Prozent der Teilnehmer, die aus einem Eigeninteresse teilnehmen, lassen sich als Privatpersonen interpretieren.

Wo liegen Ihre Schwerpunkte im Zusammenhang mit Cloud Computing?*

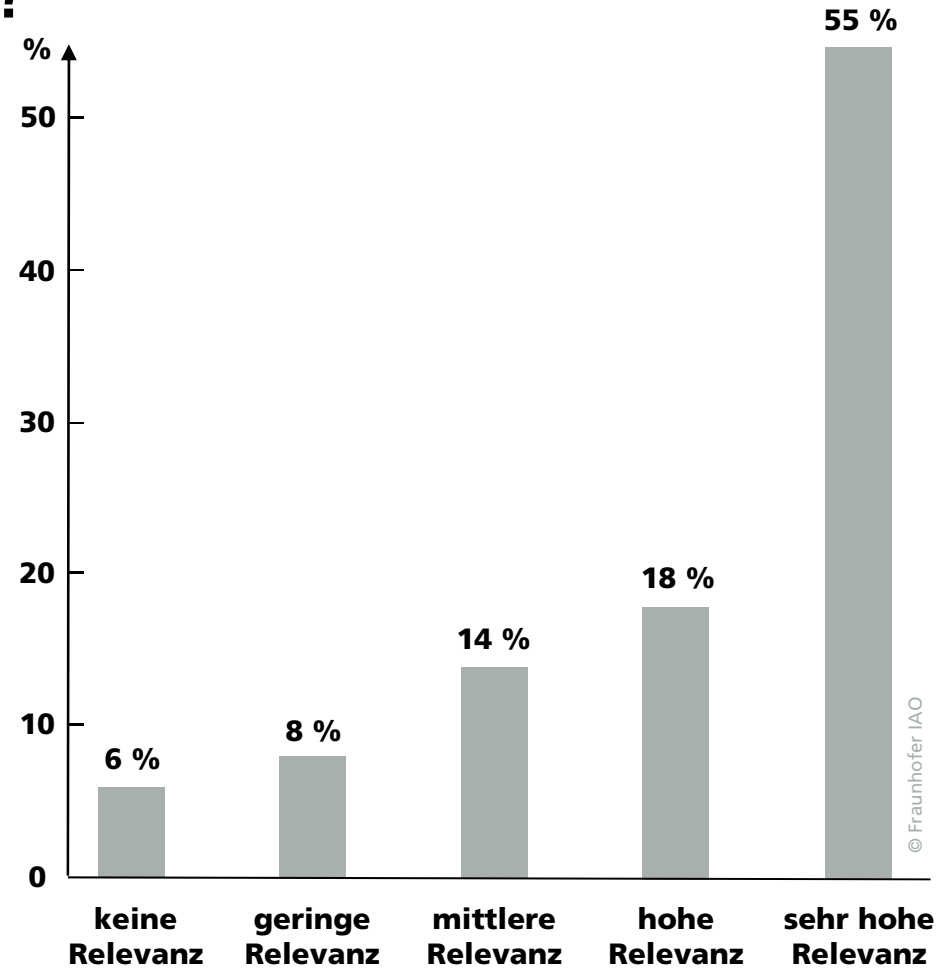


* Mehrfachantworten möglich

n = 53

Diese Frage ist eine Anschlussfrage, die gestellt wurde, falls Teilnehmer in der vorherigen Frage angaben, bereits Cloud-Lösungen zu nutzen bzw. anzubieten. Ein eindeutiger Schwerpunkt liegt hier beim Thema Software-as-a-Service. 80 Prozent der Befragten nutzen bzw. bieten bereits Softwarelösungen aus der Cloud. Die Antworten auf die Frage, wo die jeweiligen Services installiert werden bzw. betrieben werden, sind relativ ausgeglichen zwischen dem Betrieb im eigenen Haus (Private Cloud) und extern (Public Cloud). Es kommt im Einzelfall auf die Daten und Prozesse an, wo diese gespeichert oder verarbeitet werden dürfen. Als weitere Betriebsmodelle wurden genannt: Remote Private Cloud, Provider Cloud und die Unterstützung aller Modelle seitens des Cloud-Betreibers.

Welche Relevanz hat das Thema »Cloud Security« für Sie?



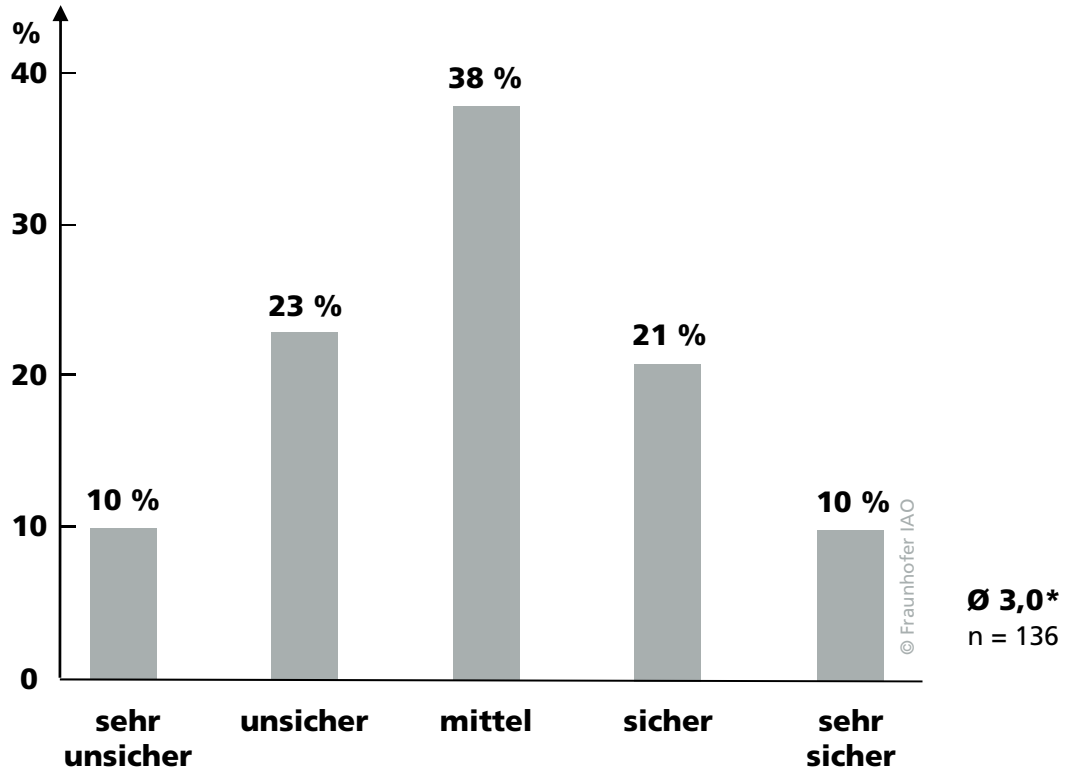
* 1 entspricht »keine Relevanz«,
5 entspricht »sehr hohe Relevanz«

Ø 3,7*
n = 141

Für die Mehrheit der Teilnehmer hat das Thema »Sicheres Cloud Computing« eine sehr hohe Relevanz.

Als wie risikoreich stufen Sie Cloud-Angebote nach heutigem Stand in Bezug auf folgende Grundwerte der IT-Sicherheit ein?

> Integrität
Verfügbarkeit
Vertraulichkeit



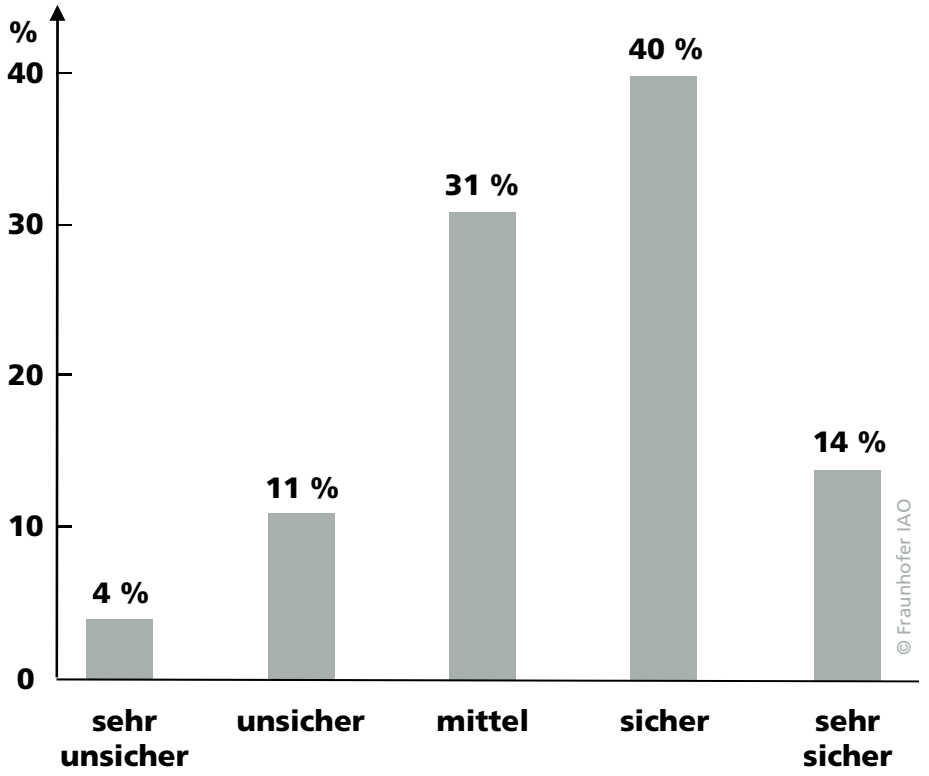
Ø 3,0*
n = 136

* 1 entspricht »sehr unsicher«,
5 entspricht »sehr sicher«

Der IT-Grundwert Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen (Quelle: Glossar des Bundesamts für Sicherheit in der Informationstechnik BSI). Der Inhalt und die Metadaten von Dateien werden unverändert in der Cloud gespeichert und nicht durch den Vorgang verändert.
Die Meinungen über diesen Grundwert sind normalverteilt, was sich als Unsicherheit gegenüber dem Thema interpretieren lässt. Daten-Integrität wurde unter Umständen bislang von den Teilnehmern nicht mit dem Thema IT-Sicherheit in Verbindung gebracht, weswegen das Risiko in diesem Zusammenhang nur schwer eingeschätzt werden kann.

Als wie risikoreich stufen Sie Cloud-Angebote nach heutigem Stand in Bezug auf folgende Grundwerte der IT-Sicherheit ein?

Integrität
> Verfügbarkeit
Vertraulichkeit



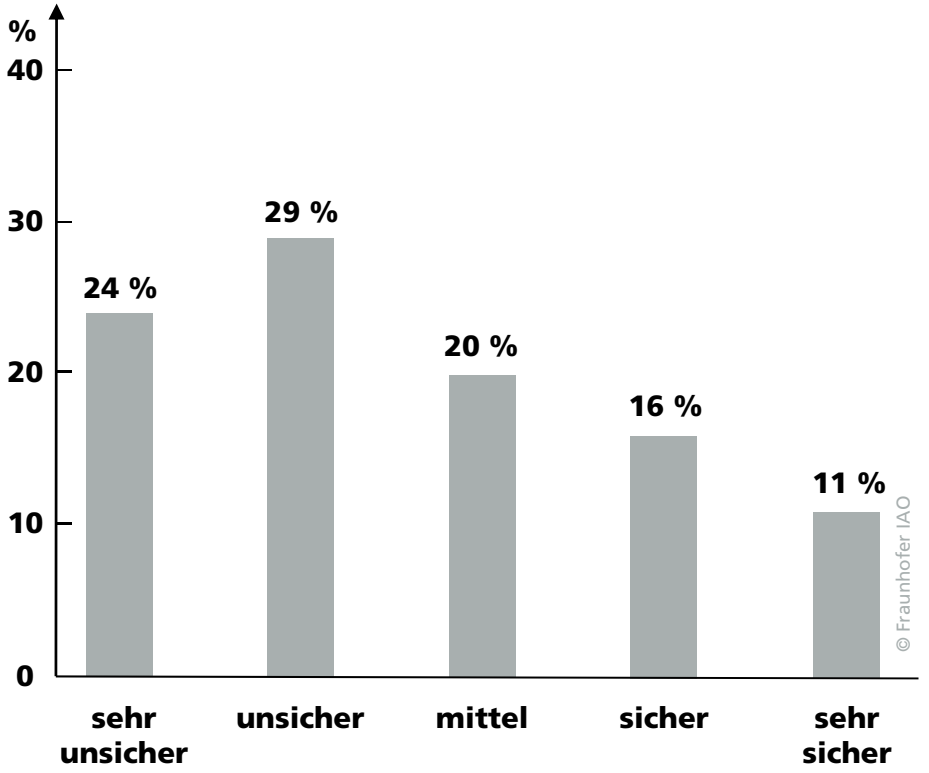
Ø 3,5*
n = 137

* 1 entspricht »sehr unsicher«, 5 entspricht »sehr sicher«

Der IT-Grundwert Verfügbarkeit bezeichnet die Nutzbarkeit von Dienstleistungen, Funktionen eines IT-Systems, von IT-Anwendungen, IT-Netzen oder Informationen durch den Anwender wie vorhergesehen (Quelle: Glossar des Bundesamts für Sicherheit in der Informationstechnik BSI). Über die Hälfte der Befragten (54 Prozent) schätzen das Thema Verfügbarkeit als sicher bis sehr sicher ein. Sie gehen davon aus, dass die Betreiber von Cloud-Lösungen jederzeit in der Lage sind, den Zugriff auf Daten und Prozesse zu gewährleisten. Dieser Grundwert lässt sich im Übrigen auch gut in Service Level Agreements festlegen und während des Betriebs überwachen.

Als wie risikoreich stufen Sie Cloud-Angebote nach heutigem Stand in Bezug auf folgende Grundwerte der IT-Sicherheit ein?

Integrität
Verfügbarkeit
> Vertraulichkeit



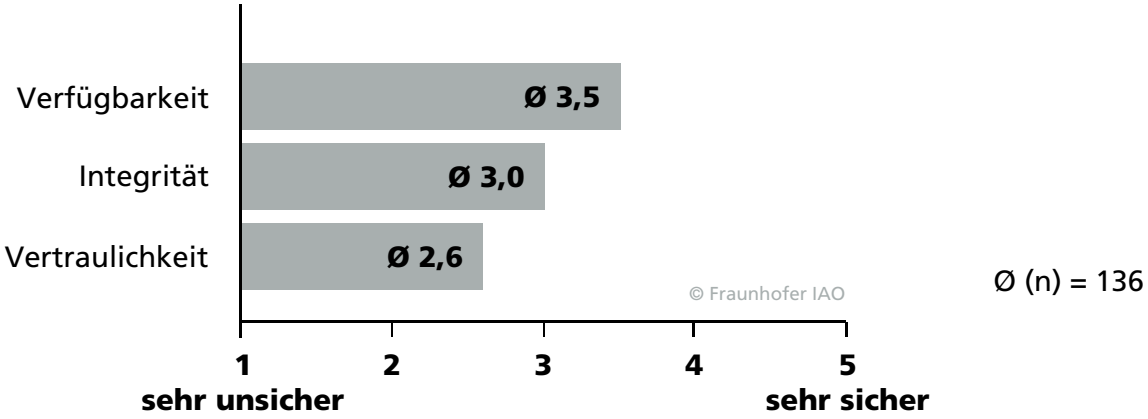
Ø 2,6*
n = 136

* 1 entspricht »sehr unsicher«,
5 entspricht »sehr sicher«

Der IT-Grundwert Vertraulichkeit bezeichnet den Schutz vor unbefugter Preisgabe von Informationen (Quelle: Glossar des Bundesamts für Sicherheit in der Informationstechnik BSI). Der Zugriff auf Daten und Prozesse wird in der Cloud durch Berechtigungen eingeschränkt, und während des Betriebs überwacht und durchgesetzt. Die Antworten auf diese Frage sind sehr pessimistisch: über die Hälfte der Befragten (53 Prozent) hält aktuelle Cloud-Lösungen für unsicher bis sehr unsicher. Hier sind weitere Sicherheitslösungen und Aufklärungsarbeit gefragt, um die technische Sicherheit und das Vertrauen darin zu bestärken.

Als wie risikoreich stufen Sie Cloud-Angebote nach heutigem Stand in Bezug auf folgende Grundwerte der IT-Sicherheit ein?*

Integrität
Verfügbarkeit
Vertraulichkeit



Ø (n) = 136

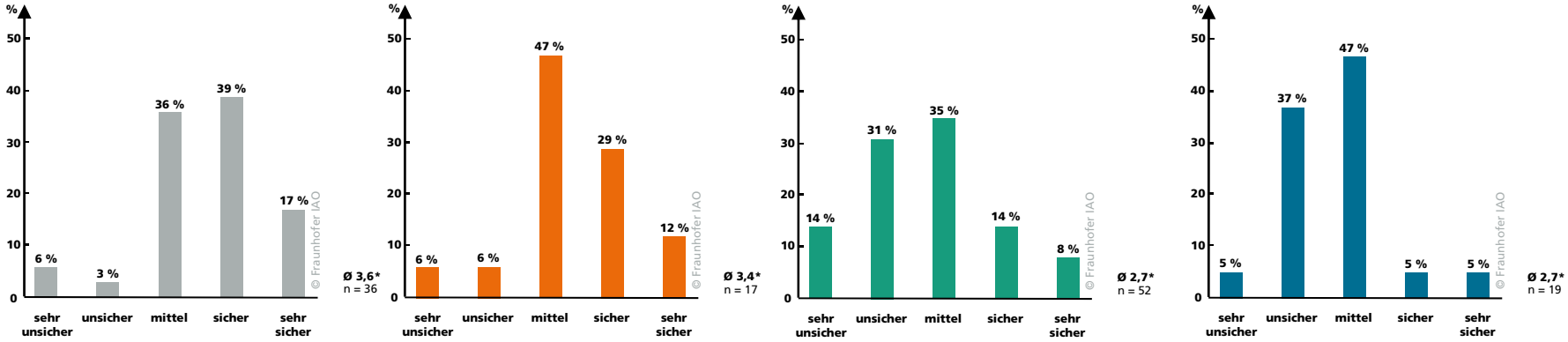
* Mittelwerte

Der direkte Vergleich der Mittelwerte zeigt, wie viel unsicherer die Vertraulichkeit gegenüber den anderen Grundwerten der IT-Sicherheit eingeschätzt wird.

Als wie risikoreich stufen Sie Cloud-Angebote nach heutigem Stand in Bezug auf folgende Grundwerte der IT-Sicherheit ein?

> Integrität
Verfügbarkeit
Vertraulichkeit

- Mein Unternehmen bzw. meine Organisation ist Anbieter von Cloud-Angeboten.
- Mein Unternehmen bzw. meine Organisation ist Nutzer von Cloud-Angeboten.
- Mein Unternehmen bzw. meine Organisation interessiert sich unabhängig von aktuellem Angebot bzw. aktueller Nutzung für Cloud Computing.
- Mein Interesse ist unabhängig von meinem Unternehmen bzw. meiner Organisation.

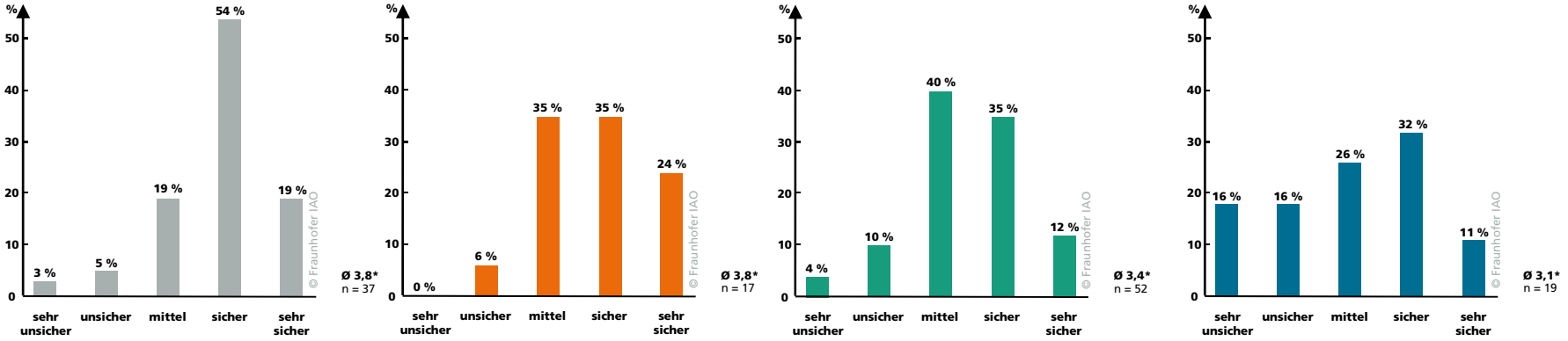


Unterteilt man die Befragten anhand des bisherigen Kontaktes mit dem Thema Cloud Computing in die Gruppen Anbieter, Nutzer, geschäftlich Interessierte und privat Interessierte, so ergeben sich Unterschiede in den Bewertungen der IT-Grundwerte.
Das Risiko bei der Integrität wird von Anbietern und Nutzern geringer eingeschätzt als von Teilnehmern, welche die Cloud noch nicht nutzen. Letztere vermuten unter Umständen fehlende Integritätsmaßnahmen, die in der Realität von Anbietern aber schon zur Verfügung gestellt werden. Das Ergebnis deutet darauf hin, dass erst mit der Erfahrung durch Nutzung oder Angebot von Cloud Computing Vertrauen in Bezug auf diesen Punkt entstehen kann.

Als wie risikoreich stufen Sie Cloud-Angebote nach heutigem Stand in Bezug auf folgende Grundwerte der IT-Sicherheit ein?

Integrität
> Verfügbarkeit
Vertraulichkeit

- Mein Unternehmen bzw. meine Organisation ist Anbieter von Cloud-Angeboten.
- Mein Unternehmen bzw. meine Organisation ist Nutzer von Cloud-Angeboten.
- Mein Unternehmen bzw. meine Organisation interessiert sich unabhängig von aktuellem Angebot bzw. aktueller Nutzung für Cloud Computing.
- Mein Interesse ist unabhängig von meinem Unternehmen bzw. meiner Organisation.

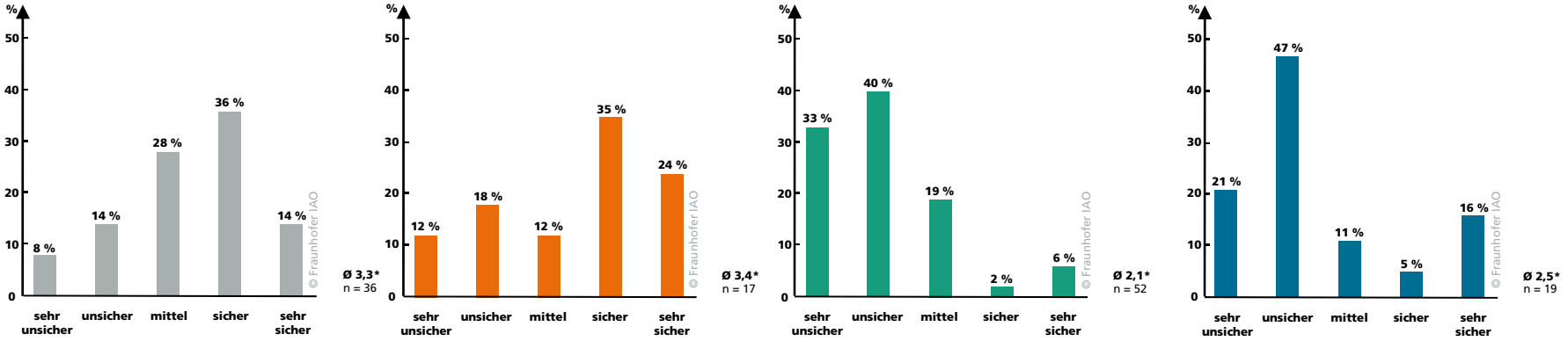


In Bezug auf die Verfügbarkeit ist die Einschätzung der Anbieter und Anwender von Cloud Computing positiver als die der Interessierten-Gruppen. Anbieter und Anwender halten die Verfügbarkeit als gesichert bis sehr gesichert, während die geschäftlich Interessierten dies eher im Mittelmaß verorten und die Einschätzungen der privat Interessierten stark fragmentiert sind.

Als wie risikoreich stufen Sie Cloud-Angebote nach heutigem Stand in Bezug auf folgende Grundwerte der IT-Sicherheit ein?

Integrität
Verfügbarkeit
> Vertraulichkeit

- Mein Unternehmen bzw. meine Organisation ist Anbieter von Cloud-Angeboten.
- Mein Unternehmen bzw. meine Organisation ist Nutzer von Cloud-Angeboten.
- Mein Unternehmen bzw. meine Organisation interessiert sich unabhängig von aktuellem Angebot bzw. aktueller Nutzung für Cloud Computing.
- Mein Interesse ist unabhängig von meinem Unternehmen bzw. meiner Organisation.



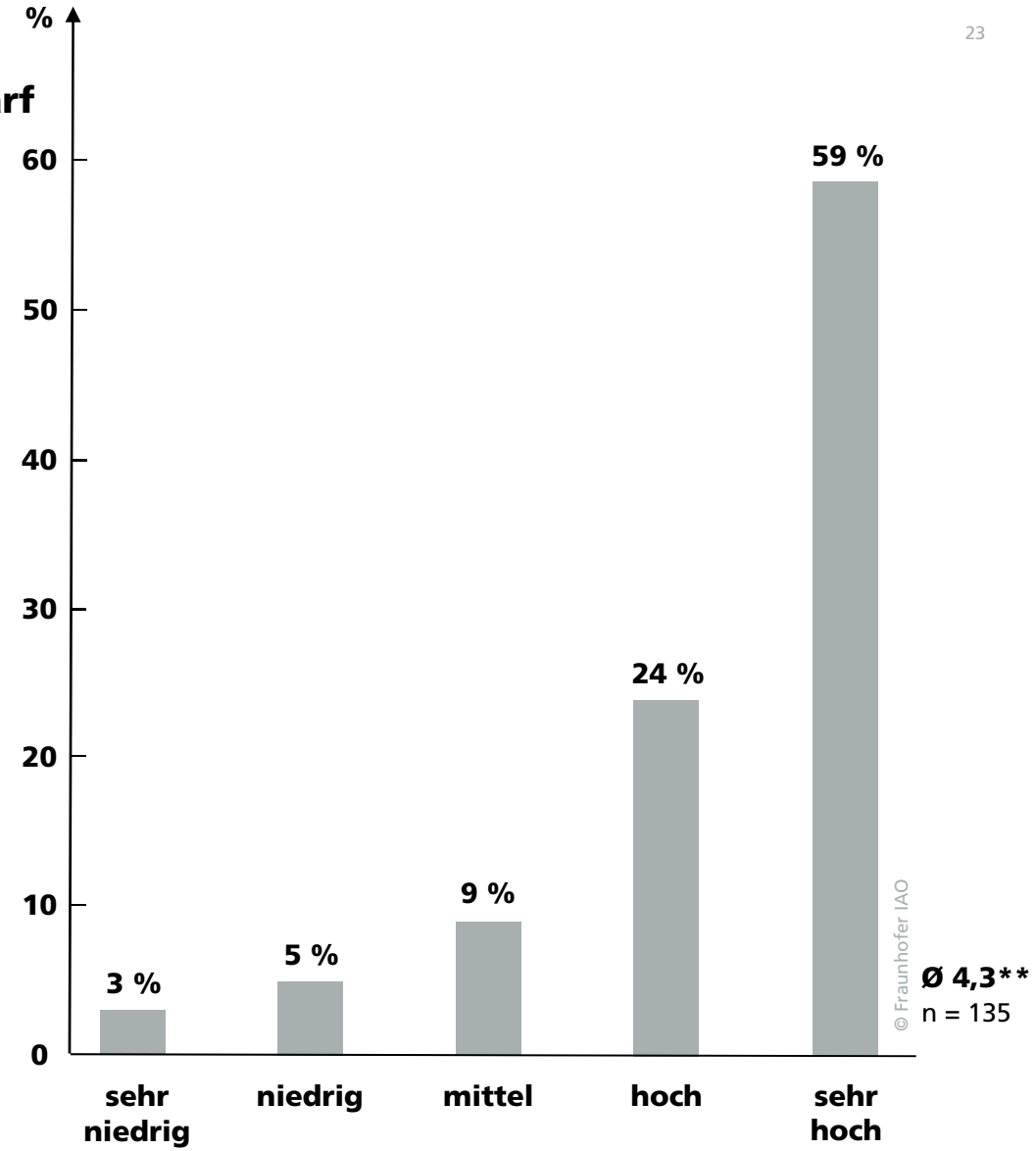
Beim Thema Vertraulichkeit gibt es sehr deutliche Unterschiede bei den Einschätzungen. Anbieter und Anwender bewerten die Cloud als mittelsicher bis sicher, auch wenn ein auffallend hoher Prozentsatz (20 bzw. 30 Prozent) die Cloud für unsicher bis sehr unsicher im Hinblick auf Vertraulichkeit hält. Die Gruppen derjenigen, die bislang noch kein Cloud Computing verwenden, bewerten die Vertraulichkeit in der Mehrheit als unsicher bis sehr unsicher. Hieran lässt sich ein dringender Bedarf ablesen: zum einen nach verbesserten Sicherheitstechnologien und zum anderen nach einer besseren Aufklärung über das, was die Cloud schon jetzt im Bereich Sicherheit leistet.

»SICHERE CLOUD«

- Untersuchungsdesign
- **Ergebnisse der Studie**
  - Aktuell wahrgenommene Cloud Security
  - **Sicherheitsbedarf bei Anwendern**
- Ansprechpartner

Wie schätzen Sie den Sicherheitsbedarf in ihrem Unternehmen in den folgenden Punkten ein?

> Authentisierung*
Datensicherheit / Datenschutz
Datenverfügbarkeit
Externe Kommunikation
Patch-Level
Daten-Integrität

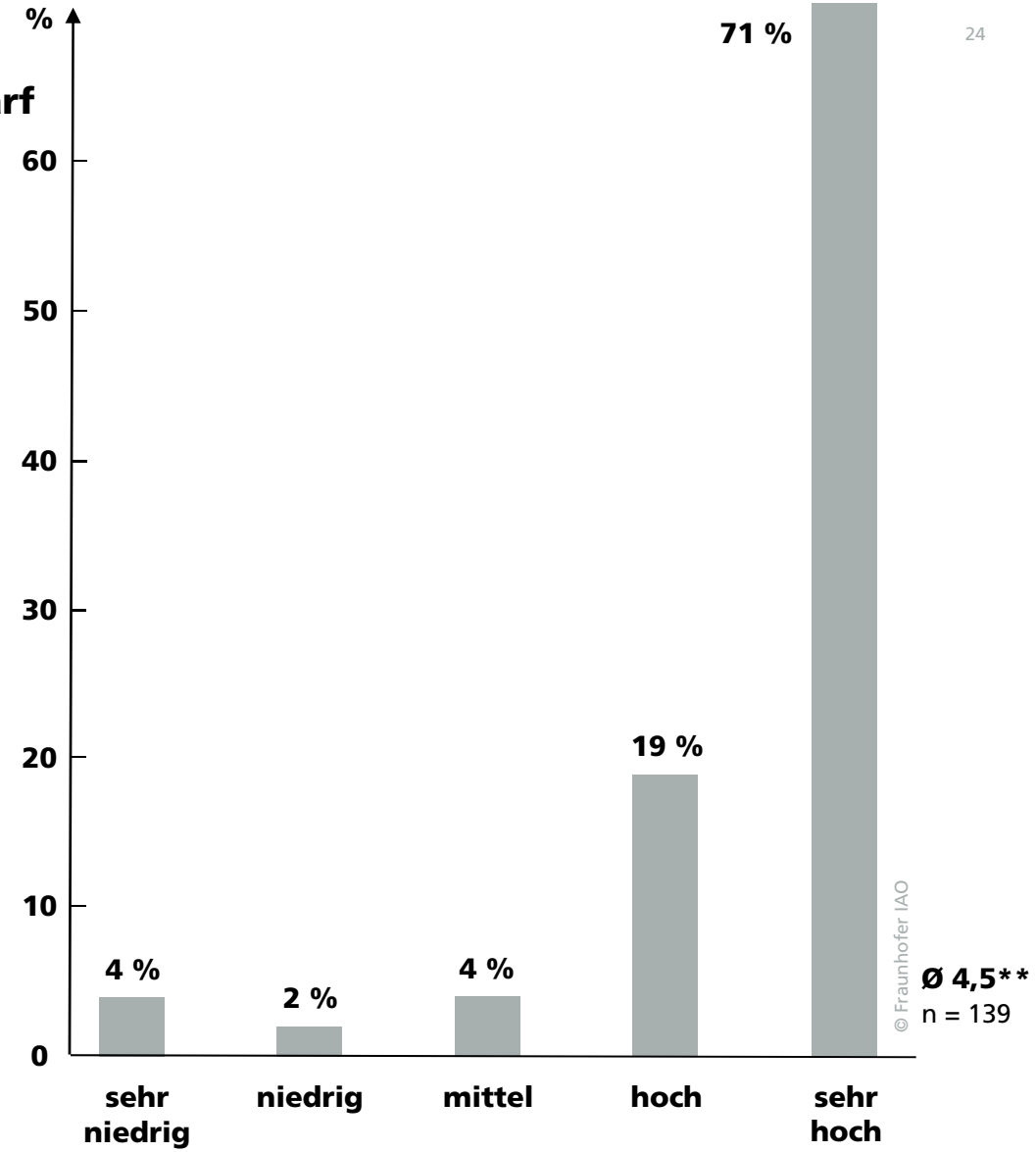


* u.a. Phishing, Pharming, Cross-Site Scripting etc.
** 1 entspricht »sehr niedrig«, 5 entspricht »sehr hoch«

In den folgenden Fragen wurden die Befragten gebeten einzuschätzen, wie hoch der Sicherheitsbedarf für die aufgezählten IT-Bereiche im täglichen Arbeitsalltag ist. Der Sicherheitsbedarf bei der **Authentisierung** schließt den Schutz vor Passwort-Diebstahl, Phishing-Attacken, Cross-Site-Scripting u.ä. ein. Die Befragten gaben für diesen Bereich einen hohen bis sehr hohen Sicherheitsbedarf an. Identitätsdiebstahl ist eine große Sorge im Umgang mit Cloud Computing.

Wie schätzen Sie den Sicherheitsbedarf in ihrem Unternehmen in den folgenden Punkten ein?

Authentisierung
> Datensicherheit / Datenschutz*
Datenverfügbarkeit
Externe Kommunikation
Patch-Level
Daten-Integrität

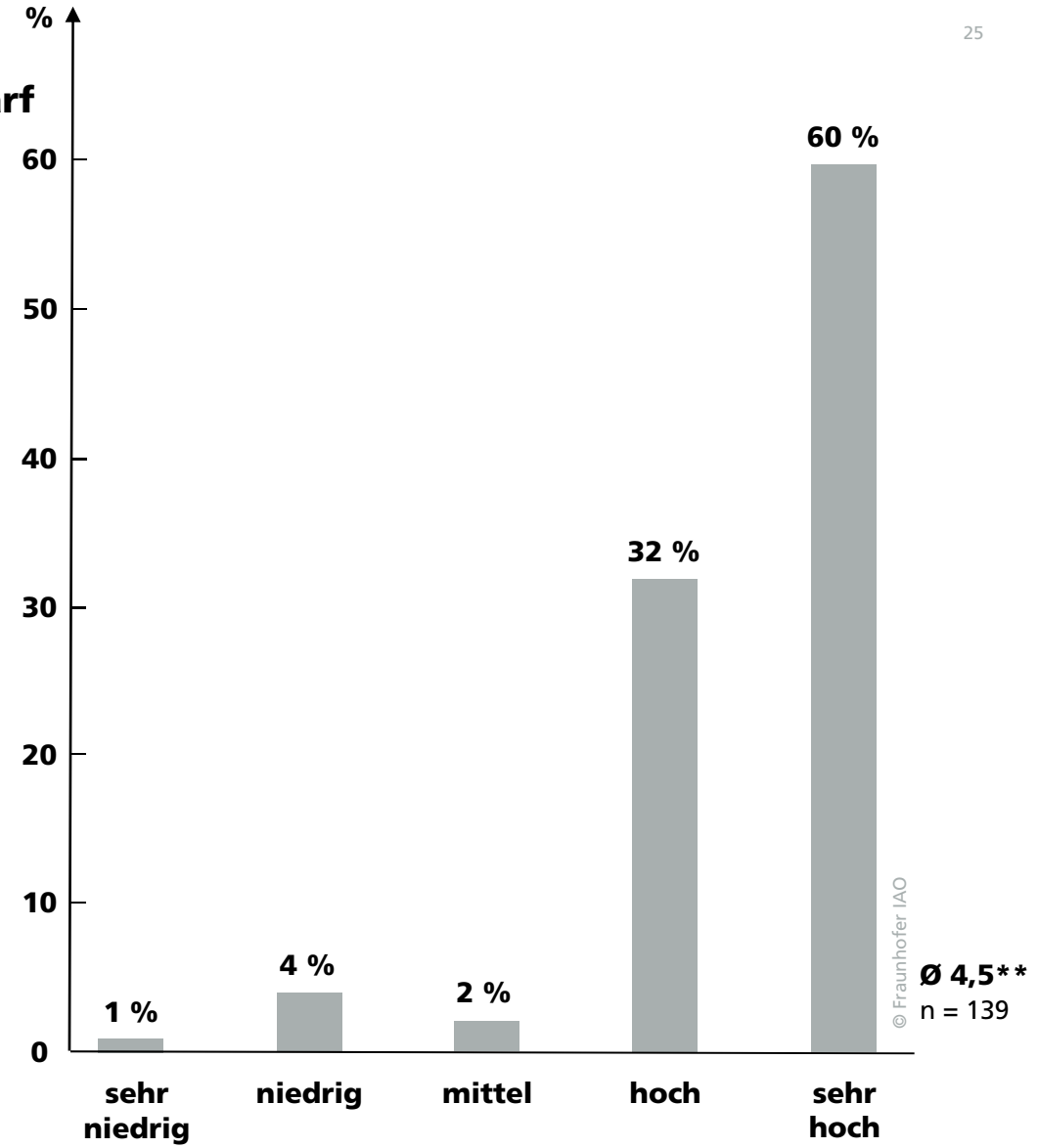


* Wert der Daten, Datenschutzrichtlinien etc.
** 1 entspricht »sehr niedrig«,
5 entspricht »sehr hoch«

Der Sicherheitsbedarf bei der **Datensicherheit** bzw. beim **Datenschutz** betrifft den Zugriff auf die in der Cloud gespeicherten Daten: Niemand soll auf die Daten zugreifen können, dem es nicht erlaubt ist. Eine große Mehrheit der Befragten (71 Prozent) betrachtet die eigenen Daten als sehr schützenswert und legt deswegen einen sehr hohen Wert auf die Datensicherheit.

Wie schätzen Sie den Sicherheitsbedarf in ihrem Unternehmen in den folgenden Punkten ein?

Authentisierung
Datensicherheit / Datenschutz
> Datenverfügbarkeit*
Externe Kommunikation
Patch-Level
Daten-Integrität

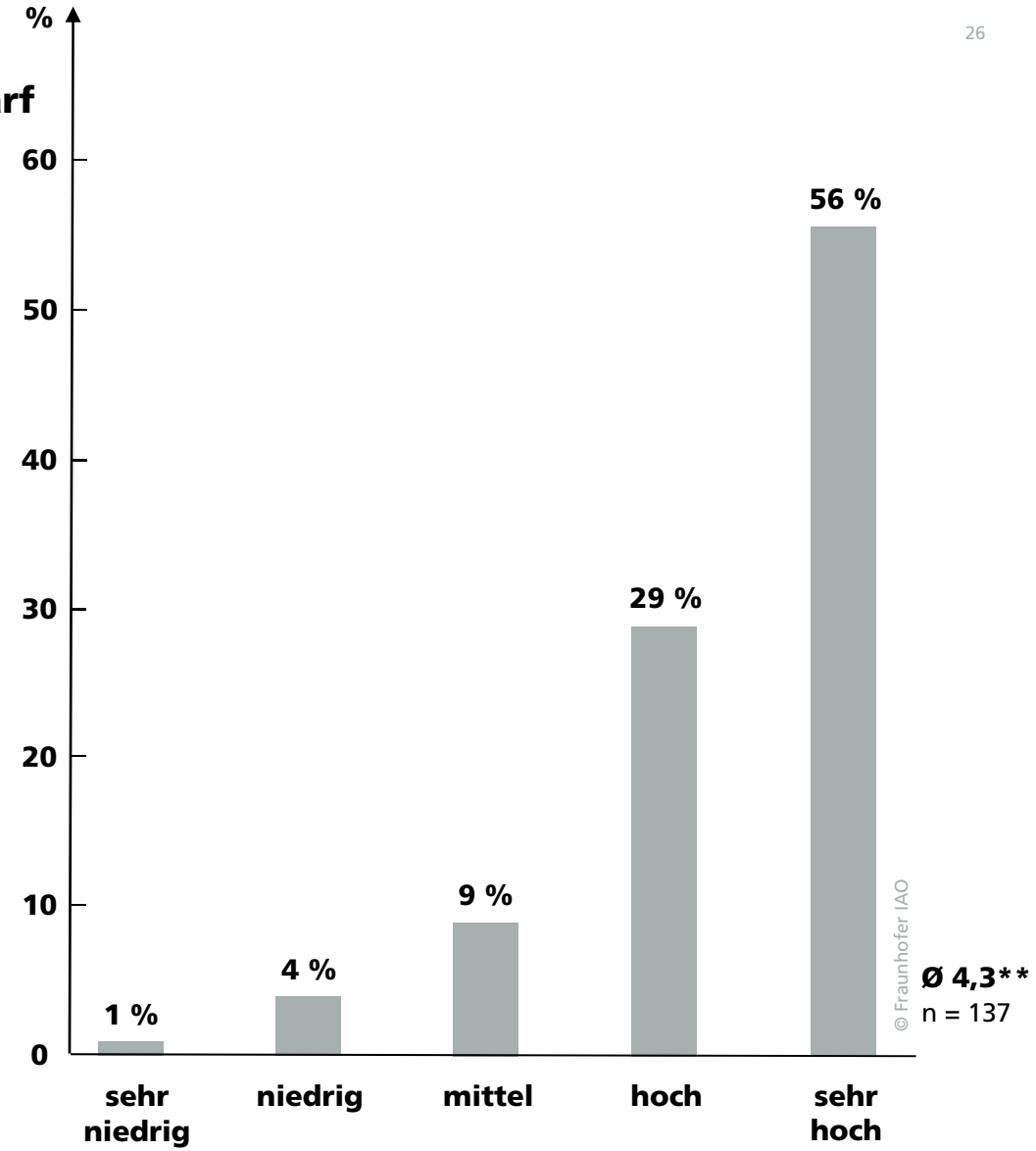


* Failover, Backups, Netzwerkverfügbarkeit etc.
** 1 entspricht »sehr niedrig«, 5 entspricht »sehr hoch«

Der Sicherheitsbedarf bei der **Datenverfügbarkeit** betrifft die Gewährleistung durchgängiger Funktionalität des Dienstes in der Cloud. Cloud-Anbieter verwenden Mechanismen wie Failover-Systeme, Backups und redundante Netzwerkstrukturen, um eine vollständige Verfügbarkeit ihrer Systeme garantieren zu können. Für eine absolute Mehrheit der Befragten (92 Prozent) hat die Verfügbarkeit einen hohen bis sehr hohen Stellenwert. Cloud-Lösungen müssen zu jedem Zeitpunkt Zugriff auf Daten und Prozesse bereitstellen.

Wie schätzen Sie den Sicherheitsbedarf in ihrem Unternehmen in den folgenden Punkten ein?

Authentisierung
Datensicherheit / Datenschutz
Datenverfügbarkeit
> Externe Kommunikation*
Patch-Level
Daten-Integrität

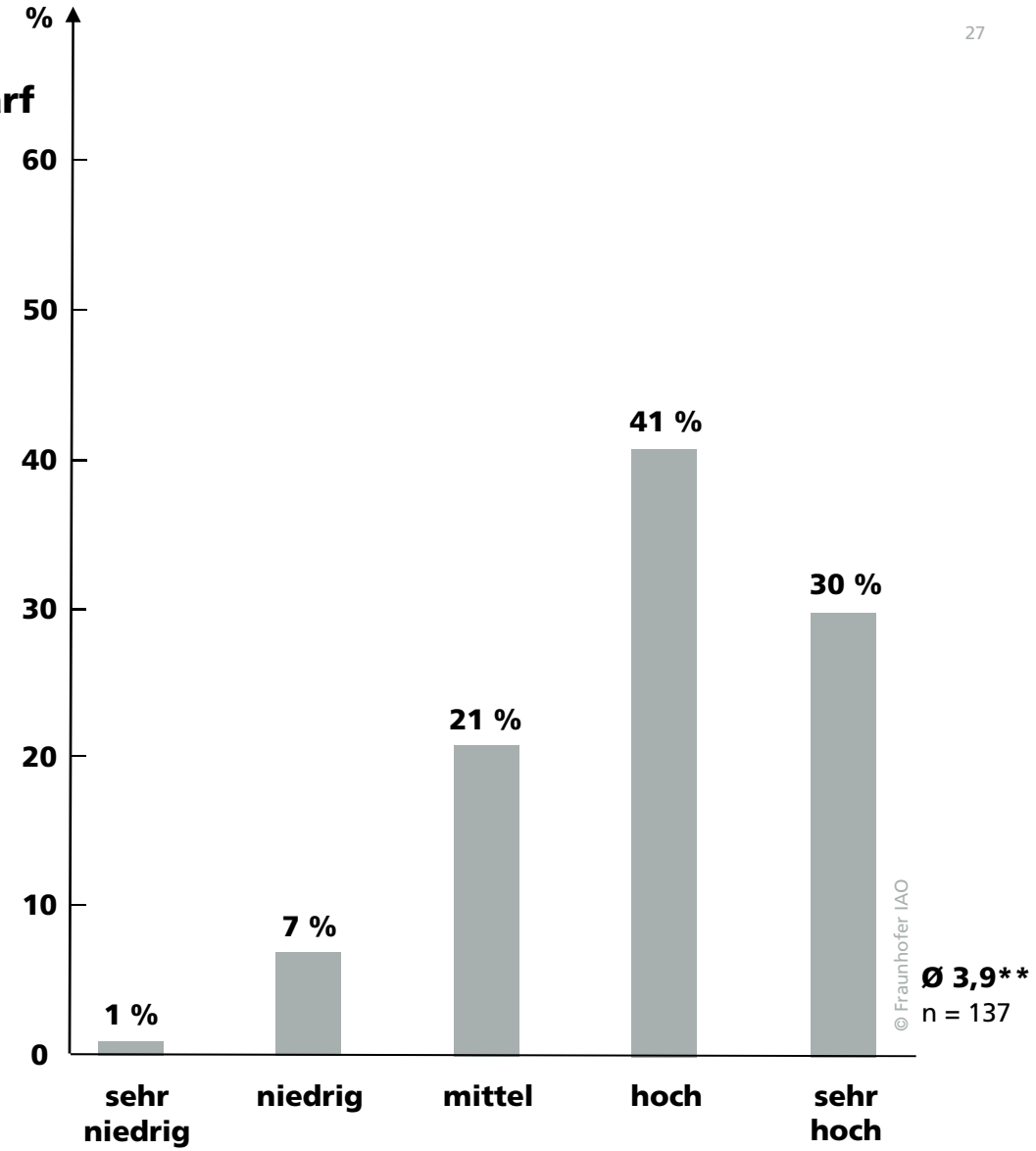


* VPN, Verschlüsselung etc.
** 1 entspricht »sehr niedrig«, 5 entspricht »sehr hoch«

Der Sicherheitsbedarf bei der **externen Kommunikation** betrifft den Austausch mit externen Partnern und eigenen Kollegen über ein Netzwerk. Informationen, die über diesen Kanal laufen, sind unter Umständen geheim und sind über Mechanismen wie Nachrichtenverschlüsselung oder Trennung eines Netzwerkes über VPN abzusichern. Auch hier gibt eine große Mehrheit der Befragten (85 Prozent) einen hohen bis sehr hohen Sicherheitsbedarf an. Absprachen, die über digitale Kommunikationswege getroffen werden, sind wichtig und müssen entsprechend gesichert werden.

Wie schätzen Sie den Sicherheitsbedarf in ihrem Unternehmen in den folgenden Punkten ein?

Authentisierung
Datensicherheit / Datenschutz
Datenverfügbarkeit
Externe Kommunikation
> Patch-Level*
Daten-Integrität

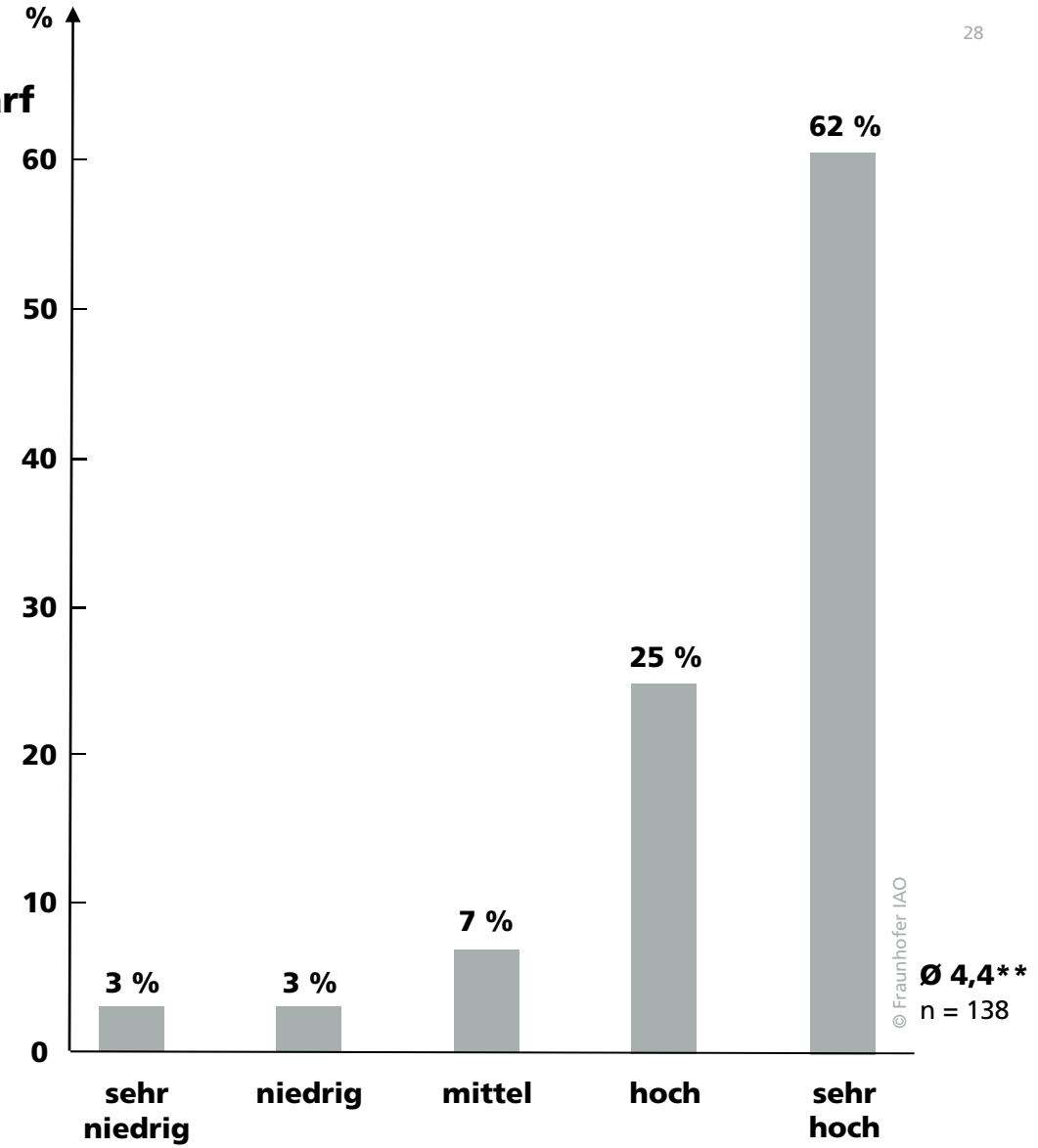


* z.B. die durchschnittliche Zeit bis zum Einspielen neuer Sicherheitspatches
** 1 entspricht »sehr niedrig«, 5 entspricht »sehr hoch«

Der Sicherheitsbedarf beim **Patch-Level** betrifft die Aktualisierung von Softwareprodukten. Dies ist nötig, da neue Versionen oftmals Sicherheitslücken beheben oder neue Funktionalitäten enthalten. Es ist nicht nur das Betriebssystem betroffen, sondern jegliche installierte Software. Die Befragten unterstützen die Wichtigkeit dieses Punktes und geben einen hohen Bedarf an. Die Dringlichkeit ist jedoch nicht so stark wie bei den vorangegangenen Punkten Datenschutz, Verfügbarkeit oder externe Kommunikation.

Wie schätzen Sie den Sicherheitsbedarf in ihrem Unternehmen in den folgenden Punkten ein?

Authentisierung
Datensicherheit / Datenschutz
Datenverfügbarkeit
Externe Kommunikation
Patch-Level
> Daten-Integrität*

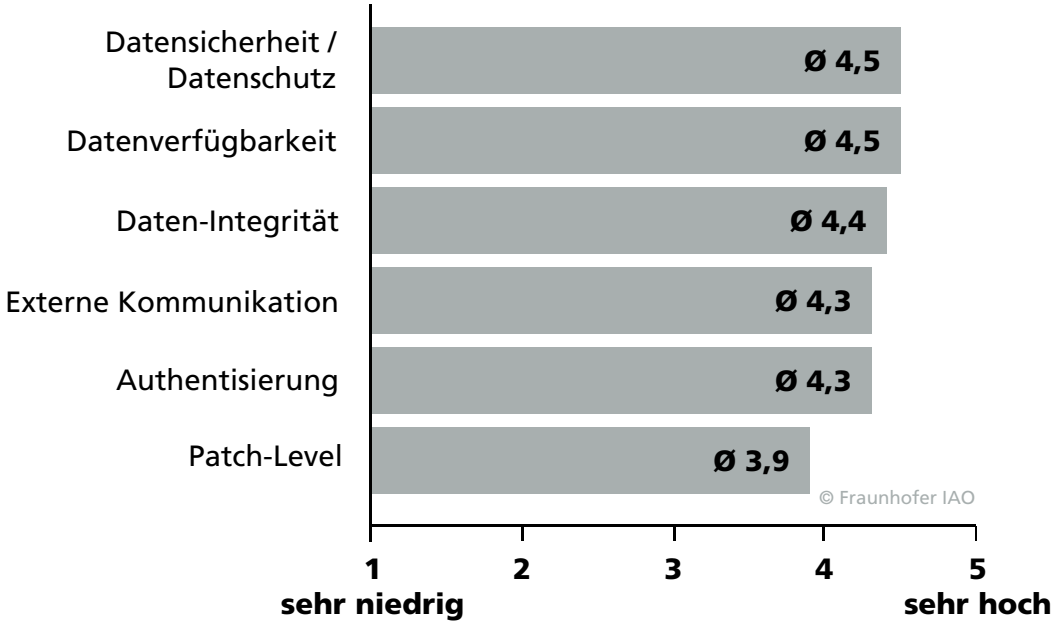


* z.B. Manipulierbarkeit von Daten – sowohl im Haus als auch bei der externen Kommunikation
** 1 entspricht »sehr niedrig«, 5 entspricht »sehr hoch«

Der Sicherheitsbedarf bei der **Daten-Integrität** betrifft hauptsächlich die nicht nachvollziehbare Veränderung von Daten, sei es auf dem Übertragungsweg oder bei der Speicherung. Die Befragten geben in der großen Mehrheit (87 Prozent) einen hohen bis sehr hohen Sicherheitsbedarf an. Daten-Integrität ist vor allem wichtig für Vertragsdaten, deren Inhalt nach Abschluss nicht mehr verändert werden darf.

Wie schätzen Sie den Sicherheitsbedarf in ihrem Unternehmen in den folgenden Punkten ein?*

Authentisierung
Datensicherheit / Datenschutz
Datenverfügbarkeit
Externe Kommunikation
Patch-Level
Daten-Integrität

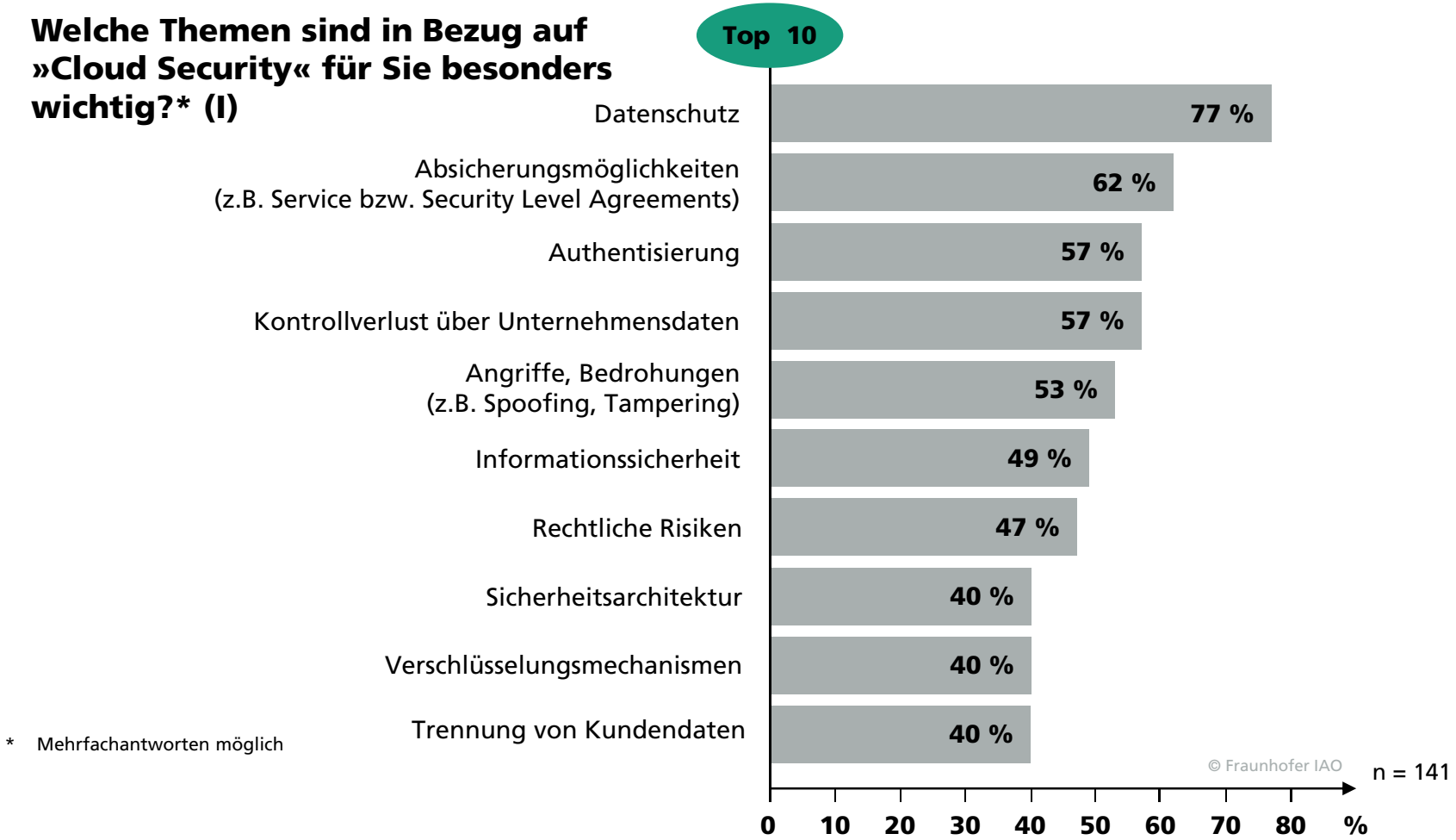


Ø (n) = 137

* Mittelwerte

Der direkte Vergleich der Mittelwerte ordnet die Sicherheitsbedarfe nach ihrer Wichtigkeit an.

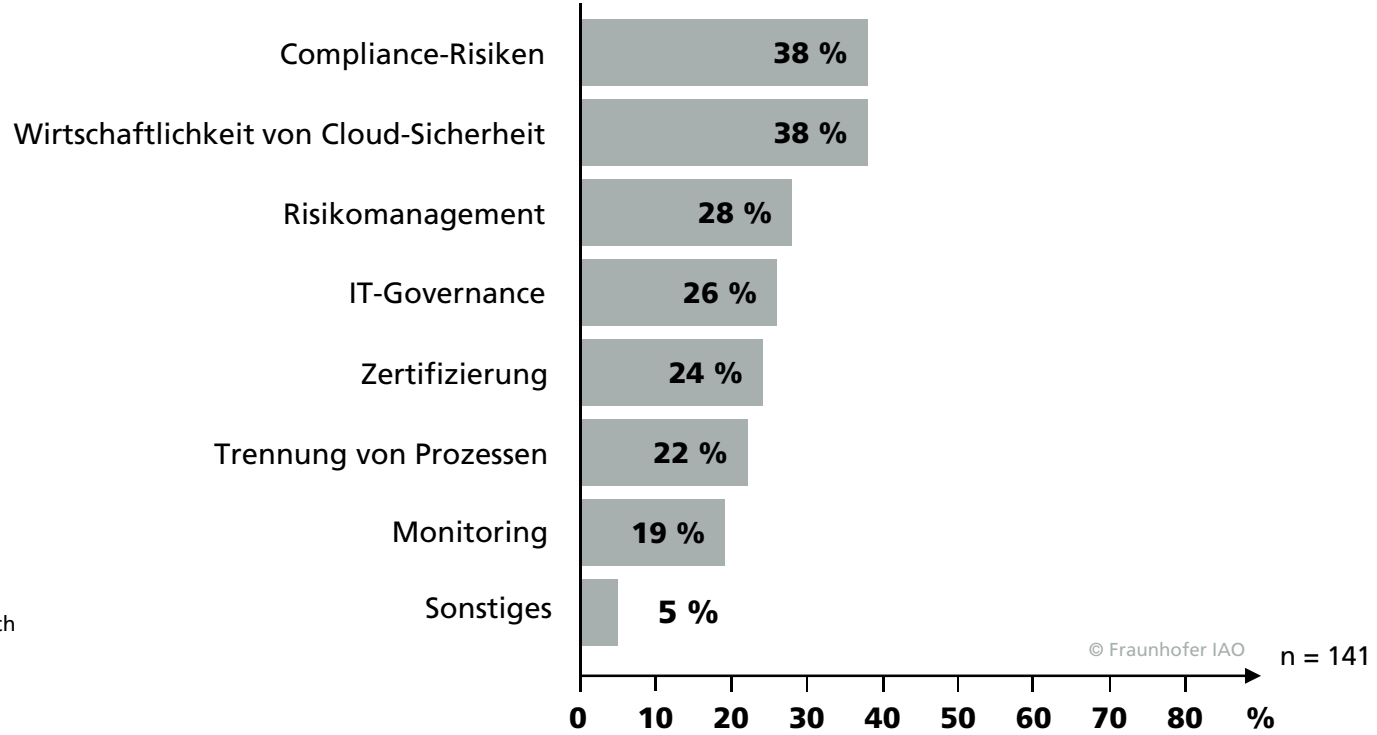
Welche Themen sind in Bezug auf »Cloud Security« für Sie besonders wichtig?* (I)



* Mehrfachantworten möglich

Die Antworten auf die Frage nach den wichtigsten Themen erlauben Aussagen darüber, welche Sicherheitseigenschaften in Cloud-Computing-Lösungen als erstes angegangen werden müssen. An erster Stelle steht der Datenschutz, was sich auch in den vorangegangenen Ergebnissen widerspiegelt. An zweiter Stelle stehen die Absicherungsmöglichkeiten, die im Schadensfall klären, wie der Anbieter reagieren muss. An vierter Stelle steht die Sorge, dass durch Cloud Computing ein Kontrollverlust über Unternehmensdaten entsteht, da diese nicht mehr im eigenen Unternehmen gespeichert sind. Zusammen mit den rechtlichen Risiken, die auf Platz sieben genannt sind, lässt sich schließen, dass vielen Unternehmen noch nicht klar ist, was sie extern speichern dürfen, können oder sollten bzw. besser nicht sollten.

Welche Themen sind in Bezug auf »Cloud Security« für Sie besonders wichtig?* (II)



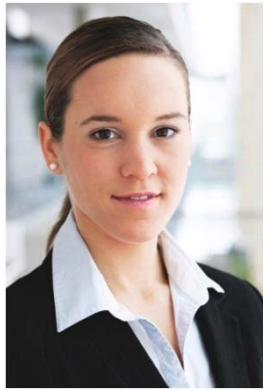
* Mehrfachantworten möglich

Zu den sonstigen Themen, die als Freitext angegeben wurden, gehören Datenverfügbarkeit, Verantwortlichkeit (Kunde versus Cloud-Betreiber), notwendige Änderungen an den IT-Anwendungen, um sie Cloud-fähig zu machen, Privacy, Wiederherstellungszeit für Daten nach einem Crash und die generelle Aussage: »In Bezug auf Sicherheit sind alle diese Themen wichtig«.

»SICHERE CLOUD«

- Untersuchungsdesign
- Ergebnisse der Studie
- **Ansprechpartner**

Ansprechpartner



Sabrina Lamberth

Fraunhofer-Institut für
Arbeitswirtschaft
und Organisation IAO
Nobelstraße 12
70569 Stuttgart

Telefon +49 711 970-5137
Telefax +49 711 970-2192
sabrina.lamberth@iao.fraunhofer.de

Erik Hebisch

Fraunhofer-Institut für
Arbeitswirtschaft
und Organisation IAO
Nobelstraße 12
70569 Stuttgart

Telefon +49 711 970-2408
Telefax +49 711 970-2192
erik.hebisch@iao.fraunhofer.de

www.swm.iao.fraunhofer.de

www.cloud.fraunhofer.de

www.dienstleistung.iao.fraunhofer.de

Fraunhofer IAO