# Akzeptanz von Security-as-a-Service-Lösungen

BITKOM

UR

## Impressum


| | |
|---|---|
| Herausgeber: | BITKOM<br>Bundesverband Informationswirtschaft,<br>Telekommunikation und neue Medien e. V.<br>Albrechtstraße 10 A<br>10117 Berlin-Mitte<br>Tel.: 030.27576-0<br>Fax: 030.27576-400<br>bitkom@bitkom.org<br>www.bitkom.org |
| Ansprechpartner: | Lutz Neugebauer<br>Tel.: 030.27576-242<br>l.neugebauer@bitkom.org |
| Autor: | Christian Senk (Universität Regensburg) |
| Redaktion: | Lutz Neugebauer (BITKOM), Leila Ambrosio (BITKOM) |
| Gestaltung / Layout: | Design Bureau kokliko / Astrid Scheibe (BITKOM) |
| Copyright: | BITKOM 2011 |
| Titelbild: | Fotokomposition, beide Bilder: www.punchstock.com |

# Akzeptanz von Security-as-a-Service-Lösungen

BITKOM

# Inhaltsverzeichnis

# Management Summary

## Hintergrund

Die zunehmende Flexibilisierung und Automatisierung von Geschäftsprozessen erhöht für Unternehmen das Risiko, Opfer von IT-basierten Angriffen zu werden. 35 Prozent aller Unternehmen sind häufig oder gelegentlich das Ziel solcher Schädigungsversuche. Dies setzt hohe Anforderungen an betriebliche IT-Sicherheitssysteme. Diese müssen zunehmend effektiv, transparent und flexibel sein. Security-as-a-Service wird als möglicher innovativer Lösungsansatz diskutiert. Hierbei werden Sicherheitsfunktionen gekapselt und von unabhängigen Anbietern nach dem Software-as-a-Service-Modell zu Verfügung gestellt. Kunden können derartige Dienste, z. B. für die Benutzerauthentifizierung oder die Virenbekämpfung, maßgeschneidert und kostenflexibel für den Einsatz im eigenen Unternehmen mieten.

Diese Studie dient als Bestandsaufnahme der aktuellen Verbreitung und zukünftiger Entwicklungen von Security-as-a-Service-Lösungen und analysiert derzeit wahrgenommene Nutzen- und Risikofaktoren des Einsatzes solcher Dienste.

## Kernergebnisse

- Security-as-a-Service eröffnet Unternehmen den einfachen Zugang zu Sicherheitstechnologien. Treiber sind wahrgenommene Kostenvorteile sowie die Möglichkeit, vorhandene Ressourcen auf das Kerngeschäft zu konzentrieren.

- Einsatzhemmnisse sind insbesondere strategische sowie sicherheitsbezogene Risiken. Zudem werden Probleme bei der Einführung und beim Customizing der Sicherheitslösungen erwartet.

- Mittelfristig möchte jedes vierte der befragten Unternehmen Security-as-a-Service-Dienste einsetzen. Schon heute setzen nach eigenen Angaben etwa 20 Prozent solche Lösungen ein.

- Security-as-a-Service-Lösungen spielen für Großunternehmen derzeit eine größere Rolle als für kleine oder mittelständische Betriebe.

## Ausblick

Sicherheitstechnologien aus der Cloud versprechen kostengünstige und maßgeschneiderte Lösungen, was insbesondere für Mittelständler enorme Potenziale eröffnet. Gerade diese verhalten sich diesbezüglich allerdings im Gegensatz zu Groß- und Kleinunternehmen noch erstaunlich zögerlich. Insbesondere wahrgenommene Einsatzrisiken hemmen einen Einsatz. Vorreiter beim Einsatz von Security-as-a-Service-Lösungen sind die IT- und die Finanzdienstleistungsbranche. Aber auch Industrieunternehmen werden langfristig nachziehen. Der derzeitige Fokus auf Endpoint und Content Security-Produkte wird sich auch auf andere Anwendungssegmente ausdehnen.

# 1 Security-as-a-Service

Security-as-a-Service (SECaaS) stellt einen Spezialfall von Software-as-a-Service dar und beschreibt den Bezug von IT-Sicherheitsfunktionalität gemäß dieser Prinzipien. Hierbei können wiederum je nach Anwendungsbereich verschiedene Security-as-a-Service-Klassen unterschieden werden:

- Security Information & Event Management
- Endpoint Security
- Identity & Access Management
- Vulnerability & Threat Management
- Application Security
- Content Security (und Content Safety)
- Compliance Management
- Managed Devices

Das Security-as-a-Service-Modell stellt eine besondere Form des Outsourcings von IT-Sicherheit dar. Im Vergleich mit dem organisations- oder domäneninternen Betrieb entsprechender Sicherheitsdienste, d. h. einer sogenannten „On-Premises Security“ (siehe Abbildung 1 A), müssen hierbei keine dedizierten technischen und menschlichen Ressourcen zur Verfügung gestellt werden. Da ein Dienstanbieter potenziell eine Vielzahl an Dienstnehmern versorgt, kann dieser Skaleneffekte ausnutzen und einen Dienst vergleichsweise kostengünstiger erbringen, als es bei einer On-Premises-Umsetzung möglich wäre. Das Outsourcing von IT-Security im Allgemeinen wird unter dem Begriff Managed Security zusammengefasst. Im traditionellen Sinne entspricht dies allein jedoch nicht dem Cloud-Gedanken, da pro Dienstnehmer jeweils eine eigene Systeminstanz mit einer jeweils eigenen Dienstschnittstelle aufgesetzt wird und die organisatorische Bindung zwischen Dienstnehmer und -anbieter so vergleichsweise hoch ausgeprägt ist (siehe Abbildung 1 B). Von Security-as-a-Service spricht man erst, wenn der IT-Sicherheitsdienst mandantenfähig ist, d. h. eine einzige Systeminstanz eine Vielzahl an Kunden bedient und der Aufwand für das Aufsetzen eigener Systeminstanzen entfällt (siehe Abbildung 1 C). Aus Sicht des Dienstnehmers stellt der Dienst eine vollständig virtualisierte Ressource da, welche er idealerweise ad-hoc ohne zusätzliche dedizierte Hard- und Software nutzen kann und deren Nutzung feingranular verbrauchsbezogen abgerechnet wird. Diese Form der Dienstnutzung, die eine Art Software-Miete darstellt, maximiert aus Sicht des Dienstnehmers sowohl die operationelle als auch der organisatorische Flexibilität. Das bedeutet, dass der Dienstnehmer nur für Leistungen bezahlt, welche er auch tatsächlich in Anspruch nimmt. Zudem entsteht theoretisch keine langfristige Abhängigkeit zum Dienstanbieter. Für den Dienstanbieter ergibt sich durch die Nutzung einer gemeinsamen virtualisierten Infrastruktur für alle Kunden die Möglichkeit einer optimalen Ressourcenausnutzung, was eine noch kostengünstigere Erbringung eines Dienstes ermöglicht.

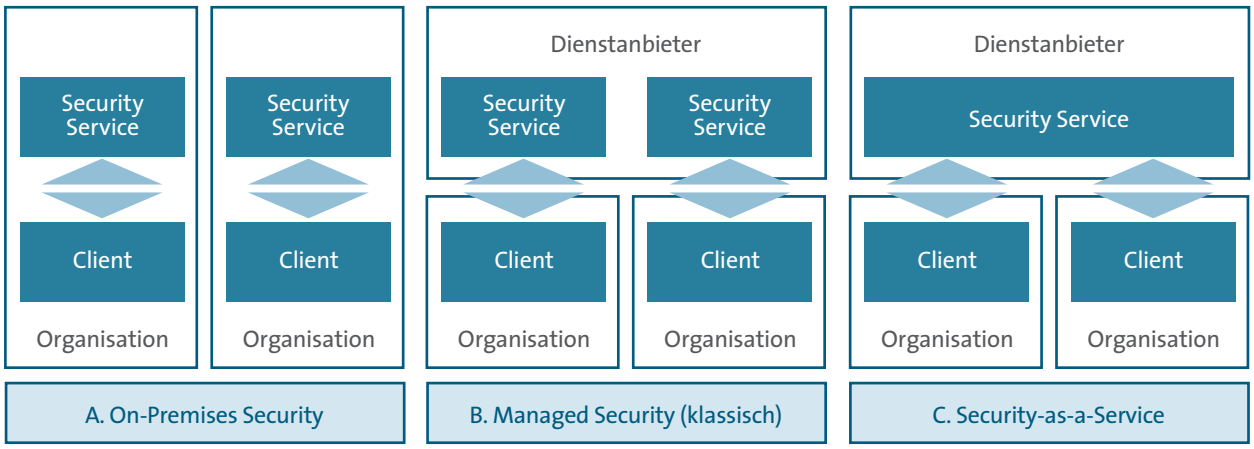


Abbildung 1: Abgrenzung von Security-as-a-Service

# 2 Studiendesign

## 2.1 Zielsetzung der Studie

Cloud-Dienste werden nach heutigen Prognosen in der Zukunft wesentlich an Bedeutung gewinnen. Gleichzeitig spielt Informationssicherheit für private und staatliche Organisationen eine zunehmend wichtige Rolle. Wenn man diese beiden Entwicklungen zusammen betrachtet, ergibt sich die Notwendigkeit, sich mit Security-as-a-Service auseinanderzusetzen. Hier sind bereits erste Angebote am Markt vorhanden. Der BITKOM Kompetenzbereich Sicherheit ist gemeinsam mit der Universität Regenburg der Fragestellung nachgegangen, wie sich diese Services in der Zukunft entwickeln werden.

Dabei sind die folgenden Fragestellungen betrachtet worden:

- Welche Faktoren spielen für die Akzeptanz von Security-as-a-Service eine Rolle?
- Wie wird sich die Nachfrage nach derartigen Lösungen entwickeln?
- Welche Unterschiede ergeben sich aus Organisationsspezifika wie beispielsweise Unternehmensgröße und Branche?

## 2.2 Konzept und Herangehensweise

Grundlage für die vorliegende Untersuchung bildet ein wissenschaftliches Akzeptanzmodell. Hierbei wird zugrunde gelegt, dass sich die Akzeptanz von Cloud-Diensten statistisch über vier Faktoren erklären lässt. Diese sind der wahrgenommene Nutzen des möglichen Einsatzes, das wahrgenommene Einsatzrisiko, die wahrgenommene Barrierefreiheit sowie eine bestehende Technologiegrundhaltung. Zudem sollte analysiert werden, inwiefern Faktoren wie Organisationsgröße, Branche, die Relevanz oder Kritikalität der IT-Sicherheit für das Geschäft des Unternehmens sowie die Tatsache, ob sich ein Unternehmen primär als Abnehmer- oder Anbieter von Cloud-Lösungen sieht, die Einstellung gegenüber Security-as-a-Service-Lösungen beeinflussen. Aus der resultierenden Modellstruktur, welche in Abbildung 2 dargestellt ist, wurde ein spezifischer Fragebogen abgeleitet und auf einer Online-Plattform implementiert. Die Beantwortung inhaltlicher Fragen erfolgte anhand einer mehrstufigen Bewertungsskala, um differenzierte statistische Auswertungen durchführen zu können.

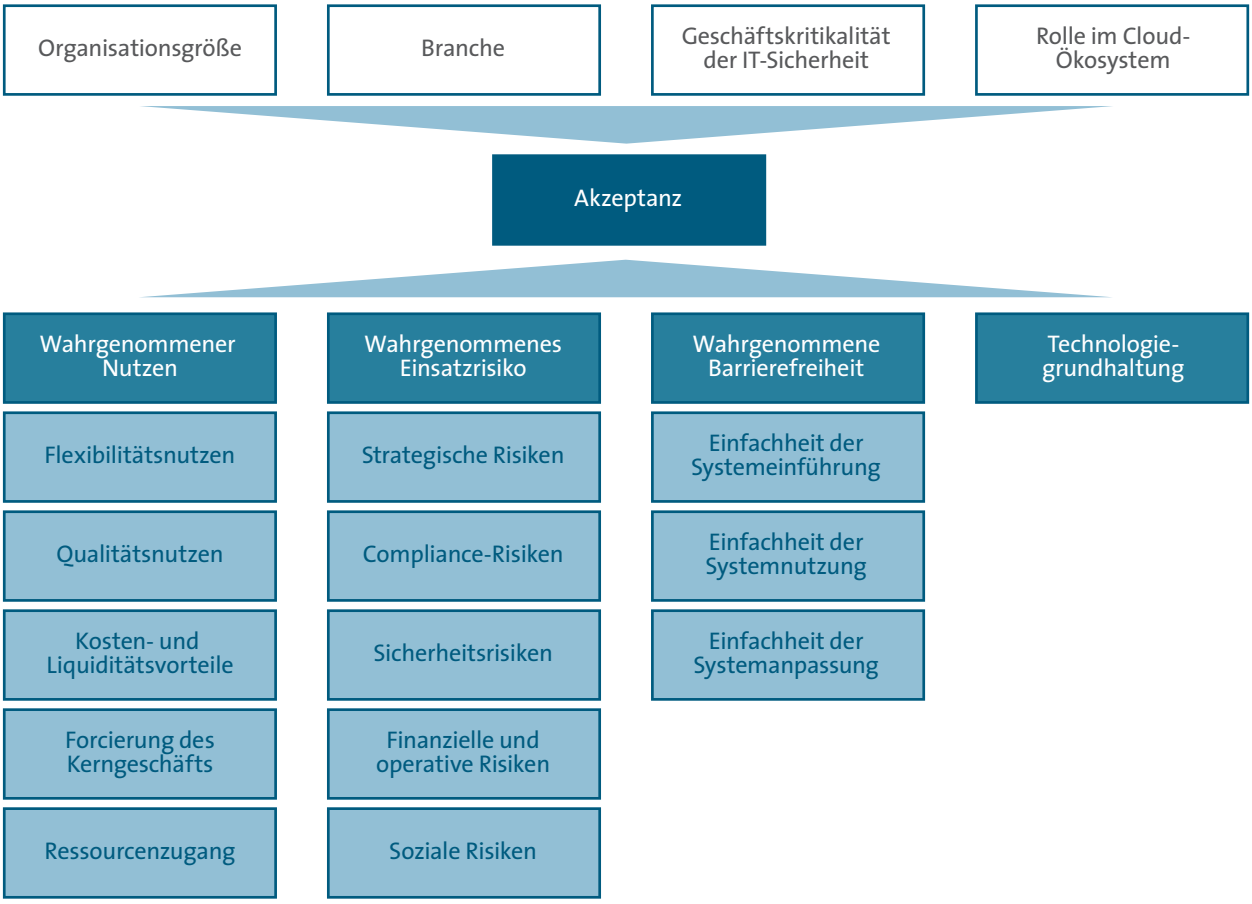


Abbildung 2: Akzeptanzerklärungsmodell

## 2.3 Datenerhebung

Im Zeitraum von 15. Februar bis 16. April 2011 wurde eine Onlinebefragung durchgeführt. Die Umfrage richtete sich explizit an mögliche Firmenkunden von Security-as-a-Service-Lösungen bzw. an personelle Vertreter, welche an einer möglichen Investitionsentscheidung direkt oder indirekt beteiligt wären. Die Befragung lieferte 202 Rückläufer. Hiervon waren 25 unvollständig und wurden entfernt. Unter Anwendung eines statistischen Verfahrens wurden zudem drei Ausreißer ermittelt, welche ebenfalls entfernt wurden. Die folgenden Analysen basieren auf den resultierenden 174 Datensätzen.

Die Mehrheit der Teilnehmer ist hierbei mit über 40 Prozent der IT-Branche zuzuordnen; Zweitstärkste Gruppe bildet die Industrie mit 15 Prozent (siehe Abbildung 1). Während etwa die Hälfte aller Teilnehmer Großunternehmen repräsentiert, machen mittelgroße und Klein- bzw. Kleinstunternehmen jeweils etwa ein Viertel aus (siehe Abbildung 4).

Frage: In welcher Branche ist Ihre Organisation tätig?

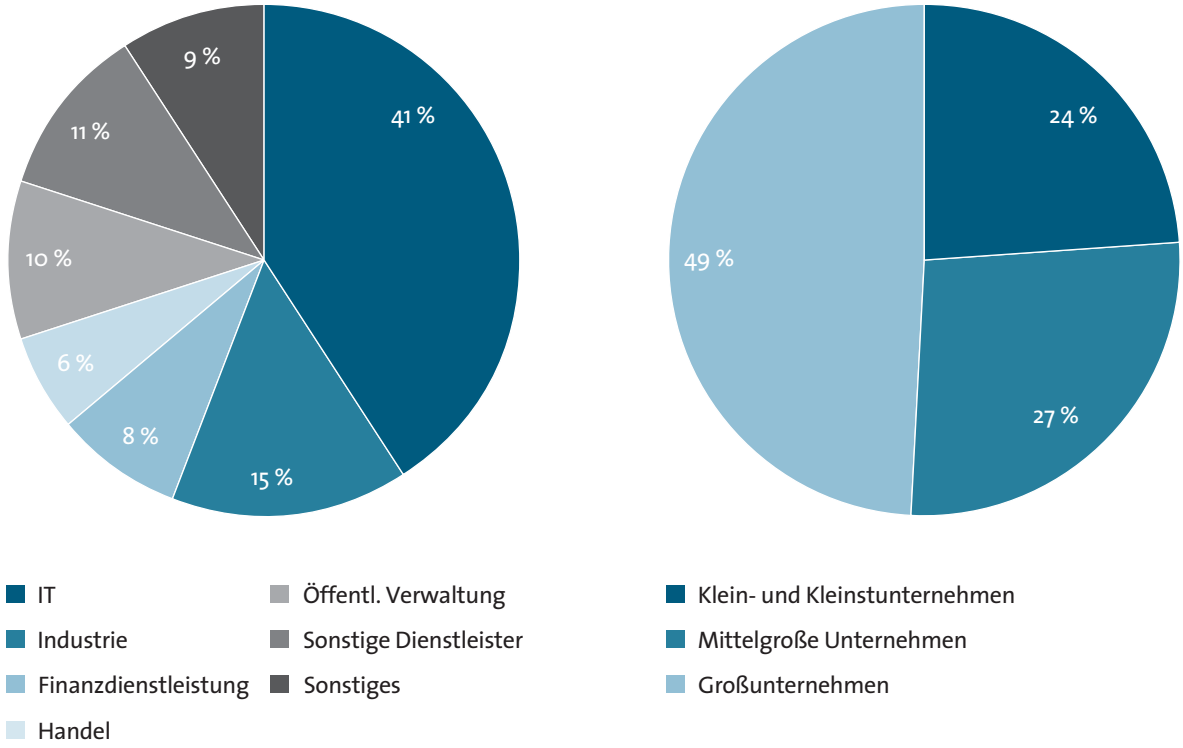


Abbildung 3: Verteilung der Teilnehmer nach Branche (n=174)




Abbildung 4: Verteilung der Teilnehmer nach Organisationsgröße (n=174)[1]

1 Klassenzuordnung erfolgte gemäß der Definition der Europäischen Kommission anhand des Jahresumsatzes und der Mitarbeiterzahl der Teilnehmerorganisationen.

# 3 Ergebnisse der Studie

## 3.1 Allgemeine Ergebnisse

Frage: Inwieweit setzt Ihre Organisation Security-as-a-Service-Lösungen bereits ein oder plant dies zu tun...

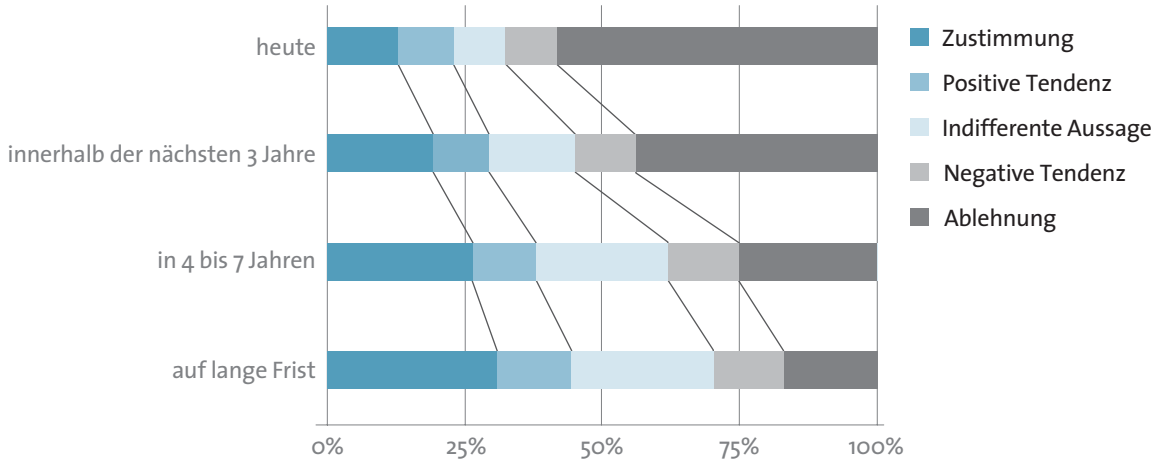


Abbildung 5: Einsatz und Einsatzplanung (n=174)

Trotz einer weltweit stark wachsenden Nachfrage nach Cloud-Diensten, zeigen sich deutsche Unternehmen aktuellen Erkenntnissen zu Folge diesbezüglich noch zurückhaltend. Umso bemerkenswerter ist eine bereits verhältnismäßig hohe Akzeptanz bei den Security-as-a-Service-Lösungen. Bereits 17 Prozent der befragten Organisationen setzen solche Dienste heute bereits ein oder planen den Einsatz zeitnah. Für rund 60 Prozent ist der Einsatz heute noch kein Thema. Die übrigen 22 Prozent trafen hierzu keine klare Aussage. Analog erfolgte eine Einschätzung des kurz-, mittel- und langfristigen Einsatzes. Hierbei zeigte sich jedoch ein deutlich positiver Trend. Mittel- bis langfristig äußern sich deutlich über 25 Prozent positiv zum Bezug von IT-Sicherheitsdiensten aus der Cloud. Gleichzeitig reduziert sich die Anzahl derer, die einen Einsatz ausschließen. Langfristig sind dies weniger als 20 Prozent.

Frage: Inwieweit stimmen Sie folgender Aussage zu:
**In folgenden Kategorien setzen wir Security-as-a-Service-Lösungen bereits ein oder planen dies...**

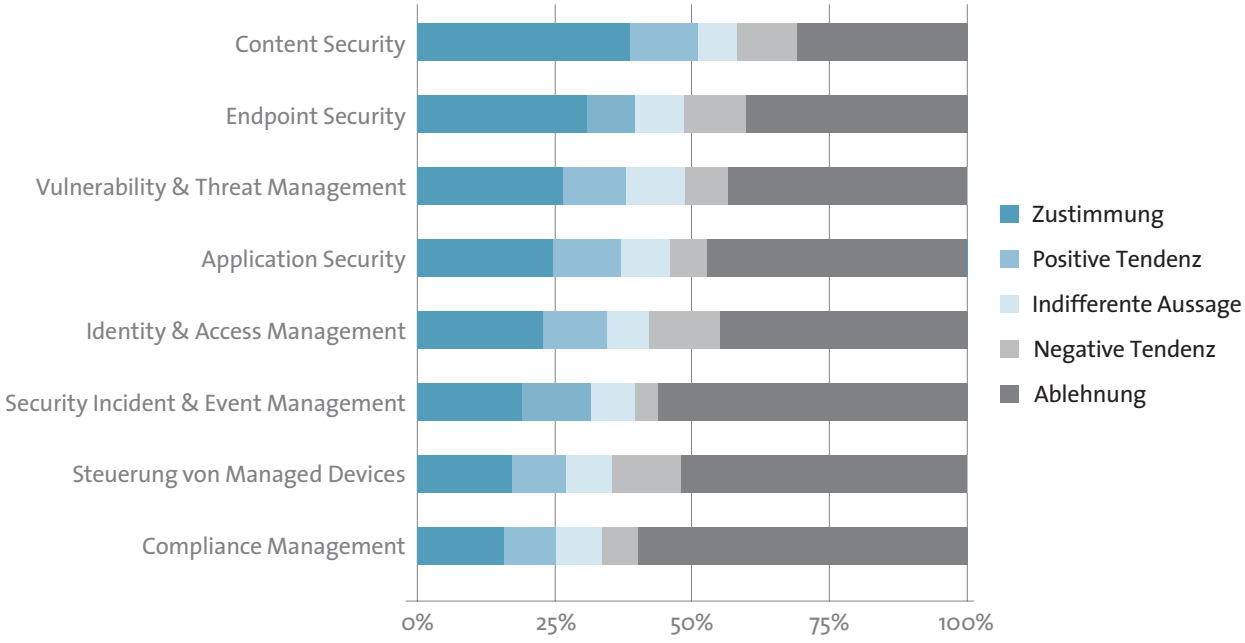


Abbildung 6: Einsatz- und Einsatzplanung nach Anwendungstyp (n=174)

Bezogen auf konkrete Anwendungsfelder innerhalb der IT-Sicherheit weisen insbesondere Lösungen für E-Mail-Sicherheit sowie die Überwachung und Filterung von Inhalten (Content Security) eine hohe Akzeptanz auf. So setzen über 40 Prozent der Befragten derartige Lösungen entweder bereits ein oder planen einen Einsatz. Weiterhin sind Produkte für Anwender attraktiv, welche unmittelbar die Sicherheit von Serversystemen oder Desktop PCs betreffen (35 Prozent). Dies umfasst die Abwehr von Schadsoftware, Intrusion Detection, Datenverschlüsselung und Datenverfügbarkeit sowie das Konfigurationsmanagement eines Systems. Die Akzeptanz von Applikationen für Vulnerability & Threat Management, Application Security und Identity & Access Management kann ebenfalls positiv bewertet werden. In jeweils etwa einem Viertel der befragten Organisationen werden solche Systeme entweder bereits eingesetzt oder ein Einsatz ist explizit geplant. Eine vergleichsweise untergeordnete Rolle spielen hingegen Produkte für die Steuerung sogenannter Managed Devices sowie für das Compliance Management. Abbildung 6 stellt eine Zusammenfassung der applikationsspezifischen Ergebnisse dar.

Der Nutzen von Security-as-a-Service-Lösungen wird generell positiv bewertet. Diese wird primär durch Kostenvorteile, die Konzentration auf das eigentliche Kerngeschäfts und den besseren Zugriff auf sicherheitsbezogene Ressourcen bestimmt. Mögliche Qualitäts- und Flexibilitätsvorteile werden deutlich niedriger bewertet.

Frage: Inwieweit stimmen Sie folgender Aussage zu:
**Security-as-a-Service-Lösungen begünstigen folgende Nutzenfaktoren...**

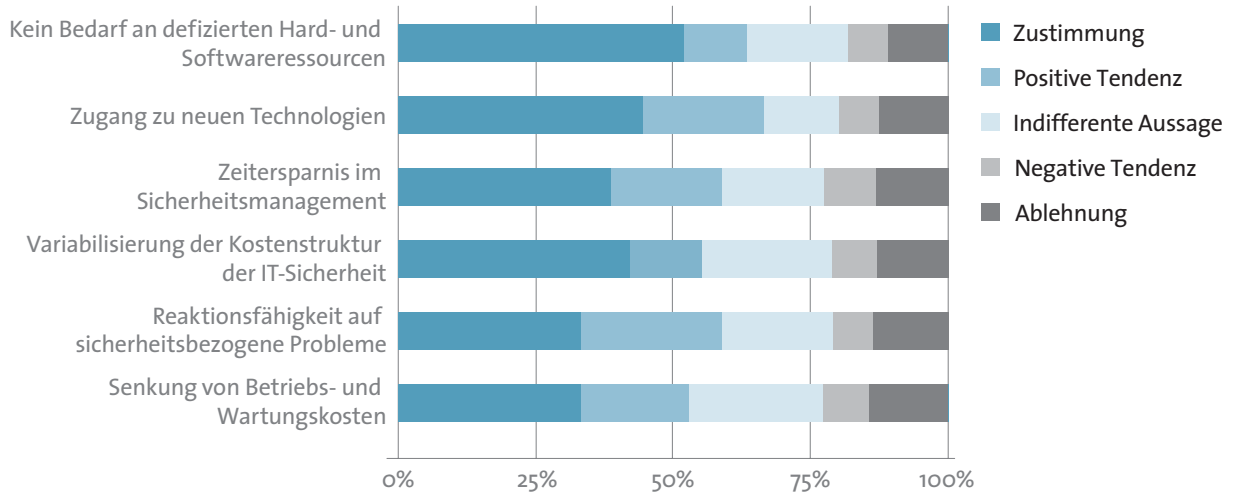


Abbildung 7: Wahrnehmung der sechs relevantesten Nutzenfaktoren (n=174)

Als besonders vorteilhaft wird gesehen, dass Informationssicherheit in der Organisation ohne zusätzliche dedizierte Hard- oder Softwareressourcen möglich wird. Etwa 64 Prozent der Befragten unterstützen diese Aussage (Abbildung 7). Weiterhin ermöglicht ein Security-as-a-Service-Bezugsmodell den einfachen Zugang zu neuen Sicherheitstechnologien und fördert somit das Ziel, IT-Sicherheitsinfrastrukturen jederzeit auf einem aktuellen Stand zu halten. Gleichzeitig erwarten die Befragten eine Zeitersparnis bezogen auf das Sicherheitsmanagement, wodurch sich die IT-Organisation auf ihr Kerngeschäft konzentrieren kann. Zudem erwarten sich Unternehmen eine verbesserte Reaktionsfähigkeit, sollten sicherheitsbezogene Probleme auftreten. Als Vorteile aus kaufmännischer Sicht wird die Variabilisierung der Kostenstruktur aufgrund einer verbrauchsbezogenen Abrechnung der Dienstnutzung sowie die nachhaltige Senkung von Betriebs- und Wartungskosten wahrgenommen. Die Möglichkeit eines Know-How-Gewinns für die eigene Organisation sowie die mögliche Abwälzbarkeit von Haftungsrisiken werden ebenso wie qualitätsbezogene Auswirkungen nur bedingt als Vorteile gesehen.

Obwohl das Software-as-a-Service-Modell sehr geringe Einsatzbarrieren verspricht, sind diese nach Bewertung der Befragten für sicherheitsbezogene Anwendungen dennoch nicht zu unterschätzen. Während die Bedienbarkeit der Sicherheitsanwendungen sowie allgemein der Komfort durch einen umfassenden Support des Anbieters moderat positiv bewertet werden, wird insbesondere deren Einführung und Anpassung an individuelle Bedürfnisse kritisch gesehen. 40 Prozent bezweifeln, dass die Einführung von Security-as-a-Service-Lösungen in ihrem Unternehmen ohne weiteres möglich sei, 48 Prozent sehen Probleme beim Customizing der extern betriebenen Systeme. Lediglich 10 Prozent der Befragten schätzen dies positiv ein.

Frage: Inwieweit stimmen Sie folgender Aussage zu:
**Beim Einsatz von Security-as-a-Service-Lösungen fürchtet unsere Organisation...**

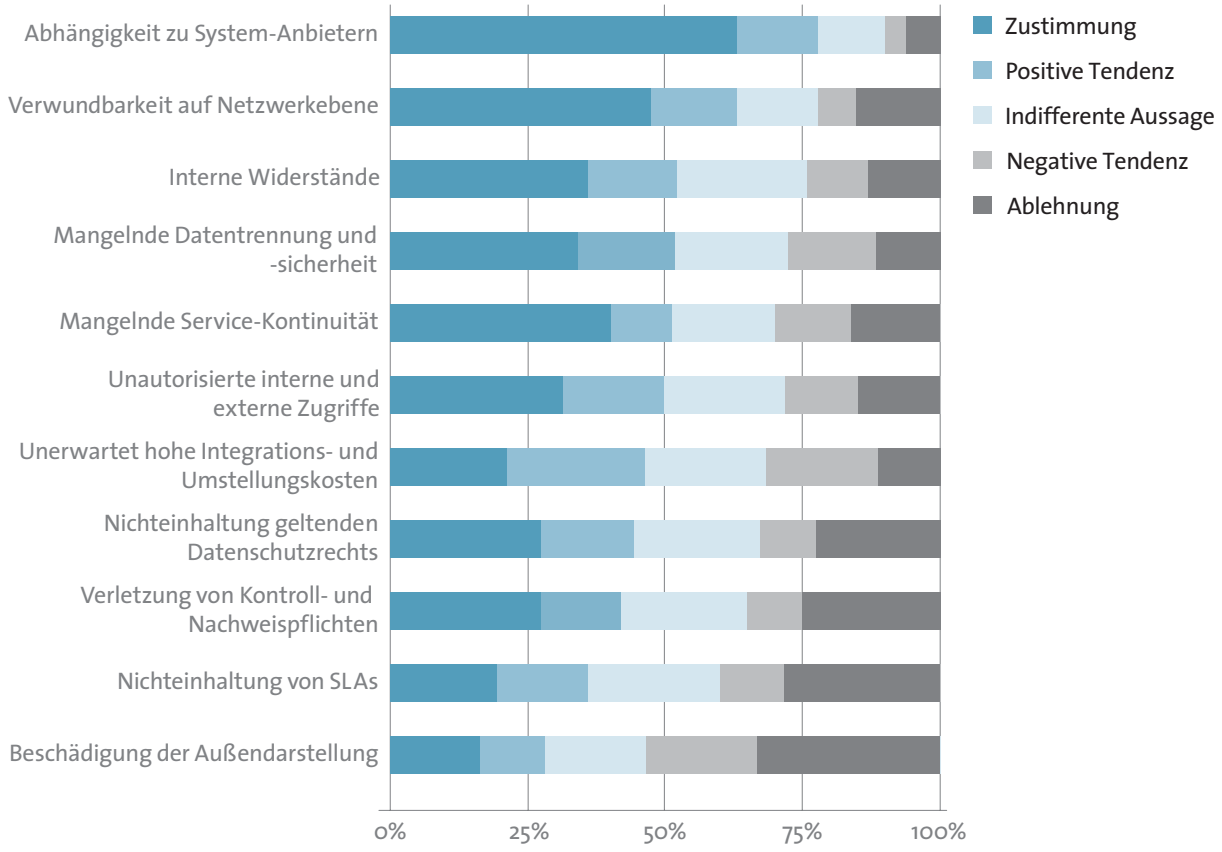


Abbildung 8: Wahrnehmung einzelner Risikofaktoren (n=174)

Das deutlich am stärksten wahrgenommene Einsatzrisiko ist eine mögliche Abhängigkeit zum Anbieter entsprechender Sicherheitsdienste, obwohl dies dem unterstellten Software-as-a-Service-Gedanken grundlegend widerspricht. Mögliche Ursachen für diese Einschätzung könnte eine bisher mangelnde Standardisierung von Service- und Datenschnittstellen oder als starr wahrgenommene Lizenzmodelle sein. Weiterhin wird die Verwundbarkeit des Services gegen Angreifer aus dem Netzwerk bzw. Internet gefürchtet. Zudem erwarten die Teilnehmer interne Widerstände und weitere sicherheitsbezogene Risiken. Führungskräfte schätzen die Gefahr interner Widerstände hierbei vergleichsweise geringer ein, als operative Mitarbeiter, die an einer möglichen Investitionsentscheidung beteiligt wären. Wahrgenommene Sicherheitsrisiken umfassen mangelnde Datentrennung und -sicherheit, die Nichtverfügbarkeit des Dienstes im Katastrophenfall sowie eine ineffektive Zugriffskontrolle. Die Nichteinhaltung von Service Level Agreements, eine negative Außenwirkung oder mögliche Auswirkungen auf die Einhaltung rechtlicher und regulatorischer Anforderungen stellen keine wesentlichen allgemeinen Einsatzrisiken dar. Eine Zusammenfassung der Risikofaktoren ist in Abbildung 8 dargestellt.

Statistische Analysen haben gezeigt, dass die allgemeine Akzeptanz von Security-as-a-Service-Lösungen primär durch das wahrgenommene Einsatzrisiko bestimmt wird. Die Teilnehmer der Studie sehen zwar einen klaren Nutzen von IT-Sicherheitsdiensten aus der Cloud, jedoch hat dieser lediglich einen schwachen Einfluss darauf, ob eine Organisation solche Lösungen einsetzt oder nicht. Die darüber hinaus untersuchten möglichen Einflussfaktoren haben ebenfalls keinen nennenswerten verallgemeinerbaren Einfluss auf die Marktakzeptanz von Security-as-a-Service-Lösungen.

Frage: **Unsere Organisation setzt Security-as-a-Service-Lösungen ein oder plant dies zu tun...**

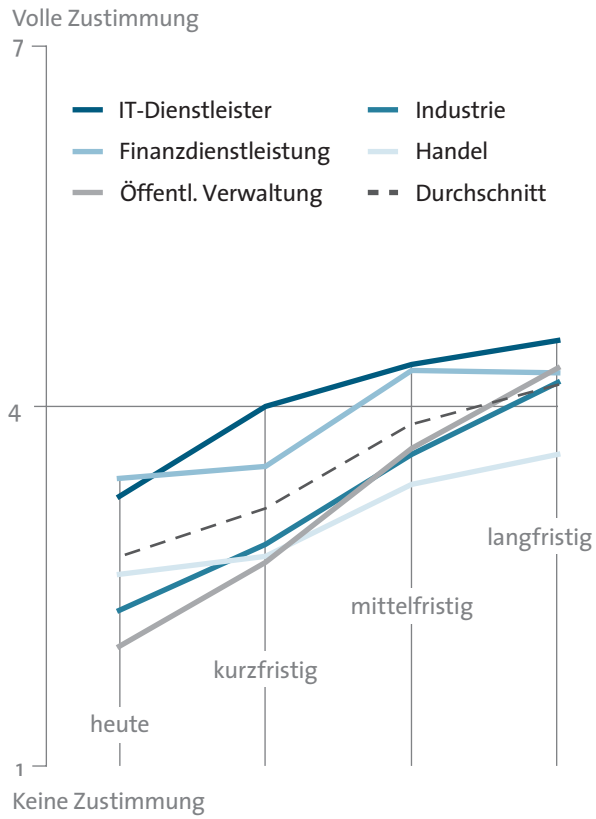


Abbildung 9: Entwicklung der Akzeptanz nach Branchenzugehörigkeit

## 3.2 Branchenspezifische Ergebnisse

IT- und Finanzdienstleister zeigen schon jetzt ein hohes Interesse an Security-as-a-Service-Lösungen und liegen hierbei auch zukünftig deutlich über dem Branchenschnitt (Abbildung 9). Industrieunternehmen und Organisationen der Öffentlichen Verwaltung planen erst mittel- bis langfristig mit dem Einsatz von IT-Sicherheitsprodukten aus der Cloud. Für den Handel spielen diese hingegen auch langfristig nur eine untergeordnete Rolle.

Exemplarisch werden im Folgenden drei Branchen für eine gesonderte Betrachtung herausgegriffen. Diese sind IT-Dienstleistung, Finanzdienstleistung und Industrie.

IT-Dienstleister zeigen eine vergleichsweise schon sehr hohe und weiterhin steigende Bereitschaft, Security-as-a-Service-Lösungen einzusetzen. Während mittelfristig im Durchschnitt etwa ein Viertel der befragten Unternehmen einen Einsatz planen, sind dies im IT-Sektor etwa ein Drittel, bei IT-Großunternehmen sogar über 40 Prozent. Neben Content Security- und Endpoint Security-Produkten sind auch Lösungen für Vulnerability & Threat Management und Identity & Access Management von Relevanz. Im Branchenvergleich bewerten IT-Unternehmen die Nützlichkeit solcher Dienste am positivsten. Insbesondere werden hier Kostenvorteile gesehen. Auf der Risikoseite stehen dem vor allem das strategische Risiko einer Abhängigkeit zum Dienstanbieter sowie mögliche Sicherheitsrisiken entgegen.

Ebenso wie IT-Dienstleister setzen auch viele Finanzdienstleister schon Security-as-a-Service-Lösungen ein oder wollen dies in naher Zukunft tun. Heute schon sind dies bereits über 30 Prozent der befragten Institute. Allerdings ist der vorhandene Positivtrend etwas schwächer ausgeprägt als bei IT-Unternehmen. Treiber eines Einsatzes sind erwartete Kostenvorteile, insbesondere solche durch Senkung von Betriebs- und Wartungskosten. Weitere Nutzenaspekte werden, wie in Abbildung 10 zu sehen ist, nachrangig wahrgenommen. Negativen Einfluss haben neben dem strategischen Risiko einer organisatorischen Abhängigkeit zum Dienstanbieter wahrgenommene Sicherheits- und Compliance-Risiken. Auch das

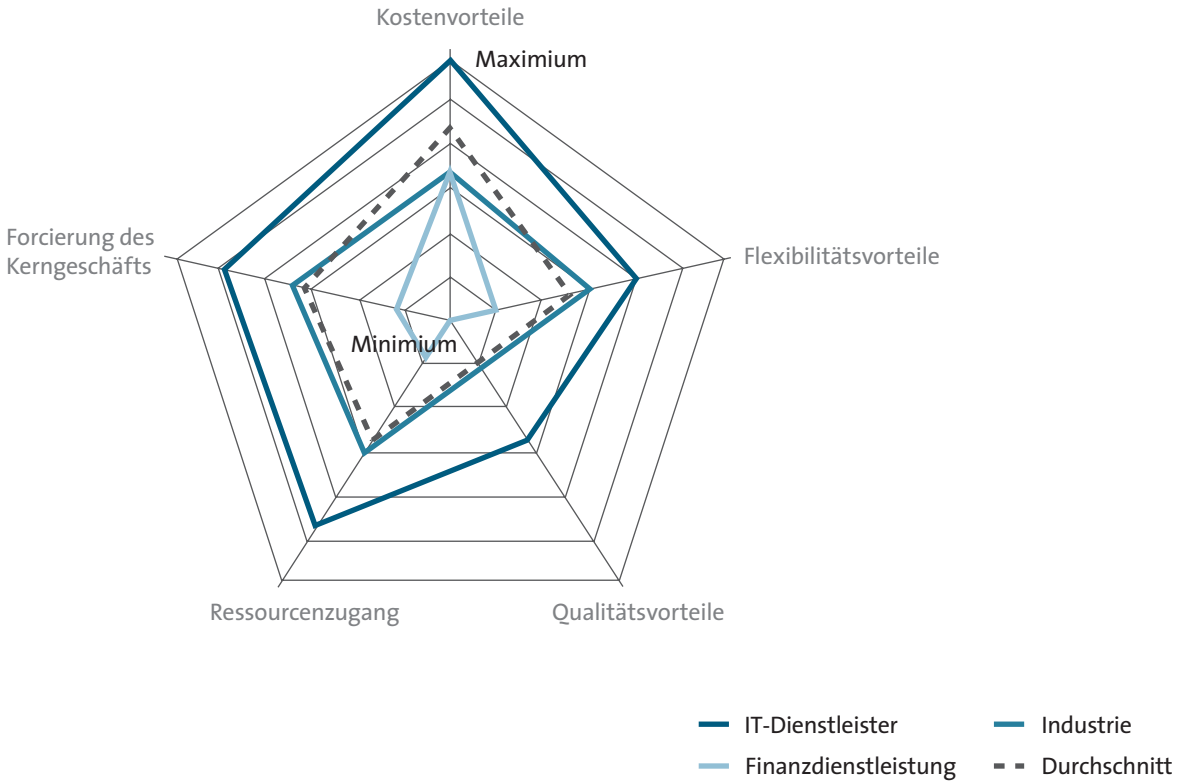


Abbildung 10: Wahrgenommener Nutzen nach Branche

finanzielle Risiko unerwartet hoher Integrations- oder Umstellungskosten wird vergleichsweise hoch eingeschätzt. Der Fokus von Finanzdienstleistern beschränkt sich im Wesentlichen auf Produkte der Bereiche Endpoint Security und Content Security und ist somit enger als der von IT- oder Industrieunternehmen.

Industrieunternehmen weisen eine bisher eher schwache Adoption von Security-as-a-Service-Lösungen auf, was sich erst mittel- bis langfristig ändern wird. So planen mittelfristig knapp über 20 Prozent einen Einsatz. Ein möglicher Grund für diese verhaltenen Prognosen sind die wahrgenommenen hohen Einsatzbarrieren insbesondere bzgl. der Anpassung des Sicherheitsdienstes an eigene Anforderungen sowie die Gefahr einer Abhängigkeitsbeziehung zum Dienstanbieter. Weitere Einsatzrisiken werden vergleichsweise gering eingeschätzt. Compliance-Risiken finden, anders als bei z. B. Finanzdienstleistern, keine wesentliche Beachtung. Nutzenaspekte werden moderat bewertet und haben keinen direkten Einfluss auf die Einsatzbereitschaft von Security-as-a-Service-Lösungen. Ein statistischer Zusammenhang konnte zwischen Organisationsgröße und Akzeptanz festgestellt werden: Je größer das Unternehmen, desto niedriger die Adoption. Anders als im IT- und im Finanzdienstleistungssektor zeigen hier kleine und mittelständische Unternehmen ein größeres Interesse an Security-as-a-Service-Lösungen als Großunternehmen. Dies umfasst primär Anwendungen der Bereiche Content Security- und Endpoint Security, aber auch Lösungen für Vulnerability & Threat Management sowie Application Security sind für Industrieunternehmen von Relevanz.

## 3.3 Einfluss der Organisationsgröße

Hingegen der weitläufigen Argumentation, dass Security-as-a-Service-Lösungen insbesondere für kleine und mittelständische Unternehmen (KMU) relevant seien, zeigt sich branchenneutral eine derzeit höhere Akzeptanz bei Großunternehmen (Abbildung 11). Lediglich Industrieunternehmen bilden hier eine Ausnahme. Neben Kostenvorteilen bewerten Großunternehmen die Möglichkeit der Forcierung des Kerngeschäfts vergleichsweise positiver. Gerade mittelständische Unternehmen sehen die Gefahr einer Abhängigkeitsbeziehung zum Dienstanbieter sowie das finanzielle Risiko unerwartet hoher Integrations- und Umstellungskosten besonders kritisch. Kleine und Kleinstunternehmen stehen einem Einsatz positiver gegenüber und weisen mittelfristig eine höhere Akzeptanz auf als mittelständische. Hierbei fokussieren diese jedoch vor allem Produkte der Bereiche Content Security und Endpoint Security, während größere Unternehmen ein breiter gefächertes Interesse an Security-as-a-Service-Lösungen haben.

Frage: **Unsere Organisation setzt Security-as-a-Service-Lösungen ein oder plant dies zu tun...**

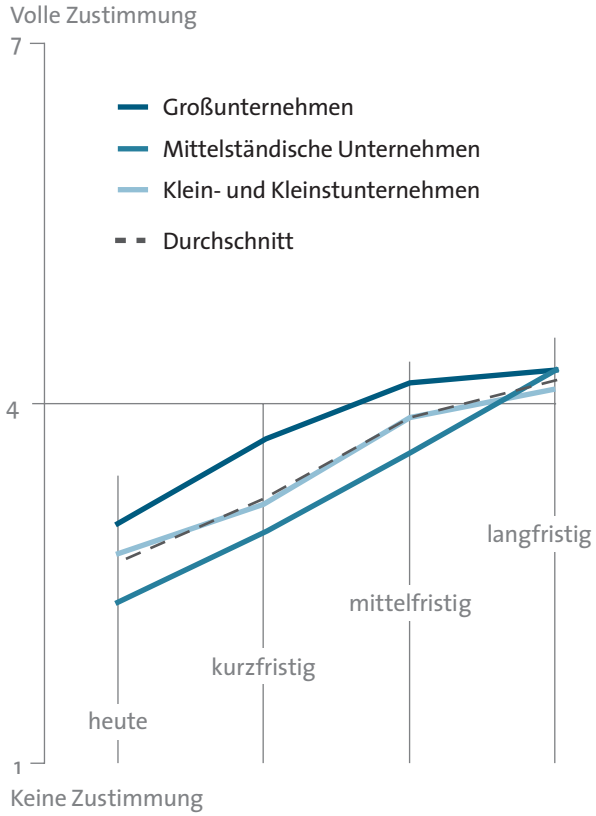


Abbildung 11: Entwicklung der Akzeptanz nach Organisationsgröße

# Fazit

Das Feedback auf die durchgeführte Untersuchung bestätigt die hohe Relevanz von Sicherheitstechnologien aus der Cloud. Viele der befragten Unternehmen beabsichtigen Security-as-a-Service-Lösungen einzusetzen oder tun dies bereits. Vorreiter sind hierbei IT- und Finanzdienstleister, welche traditionellerweise eine hohe Affinität zu IT-Innovationen besitzen. Mittel- bis langfristig werden auch andere Branchen nachziehen – vom Handel abgesehen. Vorteile werden von den Unternehmen insbesondere auf Kostenseite erwartet. Aber auch der einfache Zugang zu aktuellen IT-Sicherheitslösungen sowie die Möglichkeit, bestehende Ressourcen auf das Kerngeschäft zu konzentrieren, werden positiv bewertet. Qualität- und flexibilitätsbezogene Nutzenaspekte spielen in der Einschätzung eine untergeordnete Rolle. Negativ werden vor allem bestehende strategische und sicherheitsbezogene Risiken eingeschätzt. Insbesondere die Gefahr einer Abhängigkeit zum Dienstanbieter sticht hierbei heraus und wird in allen Branchen gleich hoch bewertet. Bemerkenswert ist, dass das derzeit wahrgenommene Risiko des Einsatzes von Security-as-a-Service-Lösungen bei einer möglichen Investitionsentscheidung eine deutlich größere Rolle spielt als der erwartete Nutzen.

Zudem zeigen die Ergebnisse, dass branchenübergreifend mittelständische Unternehmen gegenüber Klein- und Kleinst- sowie Großunternehmen eine deutliche geringere Akzeptanz von Security-as-a-Service-Lösungen an den Tag legen und auch bestehende Einsatzrisiken vergleichsweise deutlich höher einschätzen. Eine Ausnahme bildet der Industriesektor. So zeigen mittelständische Industriebetriebe eine höhere Einsatzabsicht als Großunternehmen.

Der Fokus der befragten Organisationen liegt derzeit auf IT-Sicherheitslösungen der Bereiche Content Security und Endpoint Security, was im Wesentlichen die Ergebnisse einer aktuellen Marktanalyse widerspiegelt. Dies legt den Schluss nahe, dass sich gerade derzeitig marktreife Produkte im Bewusstsein der Nachfrager befinden und mittel- bis langfristig auch Potenziale für innovative Entwicklungen anderer Applikationsgruppen zu erwarten ist.

Eine tiefergehende Analyse der Ergebnisse in einem wissenschaftlichen Format befindet sich derzeit in Planung.

# Danksagung

Dank gilt insbesondere dem Projektteam des BITKOM-Kompetenzbereichs Sicherheit für die konstruktive Diskussion der Fragestellungen der Studie sowie die Bewerbung der Online-Umfrage insbesondere im eigenen Kundenkreis und bei Partnerunternehmen.

Besonderer Dank geht an:

- Florian Dotzler (Psylock GmbH)
- Dietmar Hilke (Thales Deutschlang GmbH)
- Martin Klimke (Infineon Technologies AG)
- Xiaofeng Lou (admeritia GmbH)
- Ulrich Müller (IBM Deutschland GmbH)
- Peter Nowak (Secudomo)
- Christoph Puppe (HiSolutions AG)
- Markus Schmall (Deutsche Telekom AG)
- Beate Teller (Bosch Sicherheitssysteme GmbH)
- Stephan Wappler (IBM Deutschland GmbH)
- Holger Wöhle (Vodafone D2 GmbH)

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu gehören fast alle Global Player sowie 800 leistungsstarke Mittelständler und zahlreiche gründergeführte, kreative Unternehmen. Mitglieder sind Anbieter von Software und IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft. Der BITKOM setzt sich insbesondere für eine Modernisierung des Bildungssystems, eine innovative Wirtschaftspolitik und eine zukunftsorientierte Netzpolitik ein.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org