Whitepaper

Cloud Security

Cloud Security für den Mittelstand

Leitfaden für Entscheider:innen

vodafone business

Together we can

Vorwort

Cloud-Lösungen bieten Unternehmen aller Größen und Branchen enorme Vorteile im Hinblick auf Flexibilität, Kosten und Effizienz. Schon viele Unternehmen haben mehr oder weniger große Teile ihrer IT-Infrastruktur in die Cloud ausgelagert. Dadurch rücken Cloud-Sicherheitskonzepte und deren Umsetzung auf der Agenda der IT-Verantwortlichen nach ganz oben.

Leider steigt die Zahl an Cyber-Angriffen stark – und damit in vielen Firmen die Frage, wie sie ein Cloud-Sicherheitskonzept erstellen und etablieren können. Denn in der IT-Sicherheit ist Cloud Security eine neue Disziplin. Und sie reicht von der Auswahl des Providers über gezielte technische Maßnahmen bis zur Aufklärung der Mitarbeitenden und der Erhöhung ihres Sicherheitsbewusstseins.

Sie bekommen mit diesem Whitepaper einen Überblick über alle wesentlichen Aspekte der Cloud Security: von den Veränderungen in der Sicherheitsarchitektur über die Neuordnung der Zuständigkeiten bei Cloud-basierten Infrastrukturen bis zu wichtigen Technologien wie Zero Trust. An Beispielen aus der Praxis sehen Sie, wie entscheidend Partner bei der Orchestrierung einer effektiven Cloud-Sicherheit sind.

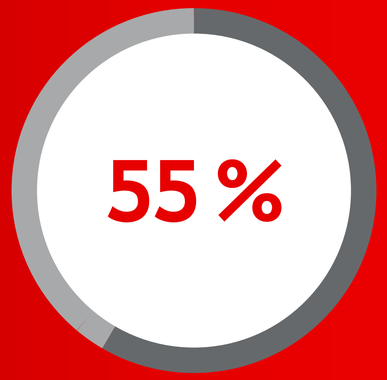
Inhaltsverzeichnis

Unternehmensprioritäten bei Cloud Security

Insights aus Studienergebenissen von IDG Research und Vodafone

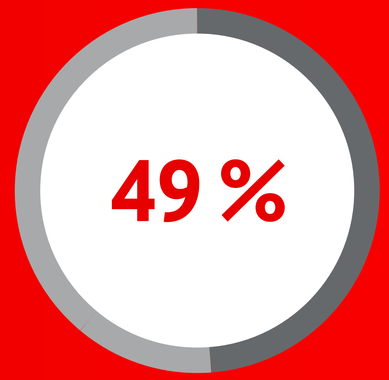
der mittelständischen Unternehmen wollen ihre Cloud Security stärken.

Seite 4



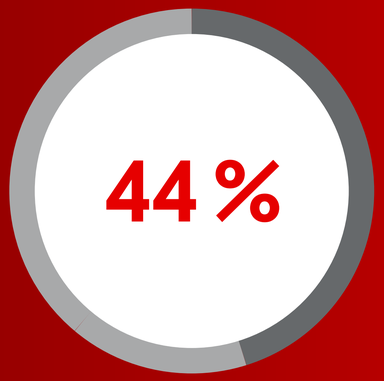
nennen die integrierten Sicherheitsfeatures der Cloud-Provider als wichtigsten Faktor für bessere Cloud-Sicherheit.

Seite 14



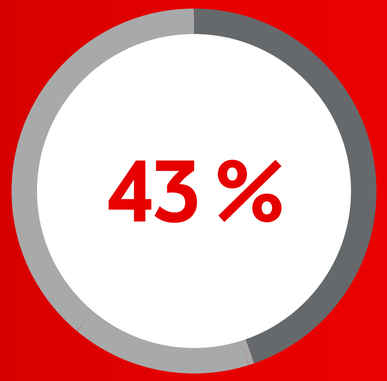
wollen übergeordnete Security-Konzepte wie Zero Trust einsetzen, um für mehr Sicherheit in Cloud-Projekten zu sorgen.

Seite 14



haben schon verschlüsselte Kommunikationsleitungen zu Cloud-Instanzen eingeführt.

Seite 15



sehen in der Zusammenarbeit mit qualifizierten Partnern einen wichtigen Faktor zur Stärkung der Cloud Security.

Seite 14

haben im Unternehmen schon die Zuständigkeiten im Cloud-Umfeld definiert oder neu definiert.

Seite 6

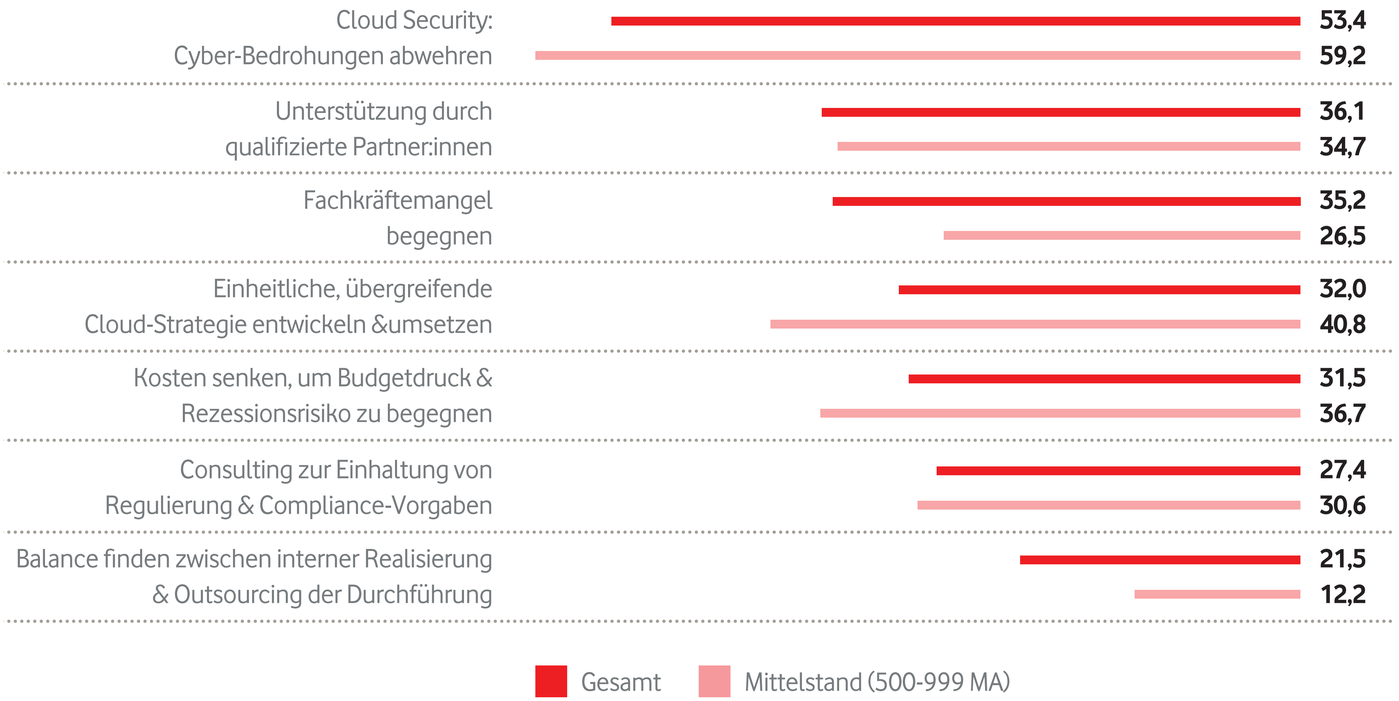
Sicherheit als Top-Priorität bei Cloud-Vorhaben – Partner spielen eine wichtige Rolle

IT-Security ist eine hochkomplexe Wissenschaft geworden, die die IT-Teams mittelständischer Unternehmen schnell überfordern kann. Gleichzeitig setzen Unternehmen immer mehr auf Cloud Computing und Cloud-Anwendungen, um sich Wettbewerbsvorteile zu sichern.

Da ist es sinnvoll auf die Ressourcen etablierter Cloud-Provider und die Unterstützung erfahrener Partner zurückzugreifen, um auch die IT-Sicherheit auf eine neue, solide und zukunftssichere Basis zu setzen. Das Bereitstellen von IT-Ressourcen wird immer mehr zu einer Dienstleistung – IT-Security inbegriffen. Und bei der Security in der Cloud ist die Unterstützung durch externe Partner noch wichtiger, 43 % siehe **Seite 14**, als bei Cloud-Projekten im Allgemeinen, 36 % siehe Abbildung rechts.

Ziele und Maßnahmen zur erfolgreichen Cloud-Transformation

Angaben in Prozent. Mehrfachnennungen möglich. Basis: n = 219



Besonders mittelständische Unternehmen stellen bei Cloud-Vorhaben die Sicherheit in den Fokus. 59 % von ihnen versprechen sich durch die Migration in die Cloud ein höheres Sicherheitsniveau, jedes 3. setzt dabei auf die Hilfe qualifizierte Partner. Bei Unternehmen aus dem unteren Mittelstand mit bis zu 500 Mitarbeitenden ist der Wunsch nach qualifizierter Hilfe besonders ausgeprägt: 42 % zählen auf ihre Implementierungspartner. Bei Unternehmen mit 500 bis 999 Mitarbeitenden steht außerdem die Entwicklung einer einheitlichen, übergreifenden Cloud-Strategie im Vordergrund.

Quelle: Exklusive Umfrage von Vodafone und IDG über die Prioritäten der Unternehmen bei der Umsetzung künftiger Cloud-Vorhaben.

Die Cloud braucht eine neue Art von Security-Architektur

Cloud Computing braucht IT-Ressourcen außerhalb des eigenen Rechenzentrums. Sei es durch das Auslagern eigener Anwendungen zu einem Cloud-Provider oder die Nutzung von Cloud-Anwendungen verschiedener Drittanbieter. Das verändert die komplette IT-Architektur. Die IT-Ressourcen sind zum Teil über mehrere Cloud-Instanzen verteilt und die Nutzenden greifen auch über den Internet-Anschluss im Homeoffice und von unterwegs darauf zu, nicht nur übers Netzwerk im Firmengebäude. Damit wird das Firmennetzwerk immer dezentraler und ist schwer einzugrenzen. Es hat keinen festen Perimeter mehr.

Cloud Security wird unterteilt in:

Datensicherheit

Sichern von Daten vor unbefugtem Zugriff sowie vor unbefugter Änderung und Löschung, und zwar im Ruhezustand und während der Übertragung. Zur Sicherung der Übertragungswege gehören das Verschlüsseln der Daten und das Verfolgen des Datenflusses.

Identitäts- und Zugriffsmanagement

Das sogenannte Identity & Access Management, IAM, regelt den Zugriff berechtigter Nutzender auf Daten, Anwendungen und Systeme über entsprechende Technologien, Verfahren und Richtlinien. Ziel ist, dass nur autorisierte Personen auf bestimmte Informationen und Ressourcen zugreifen können.

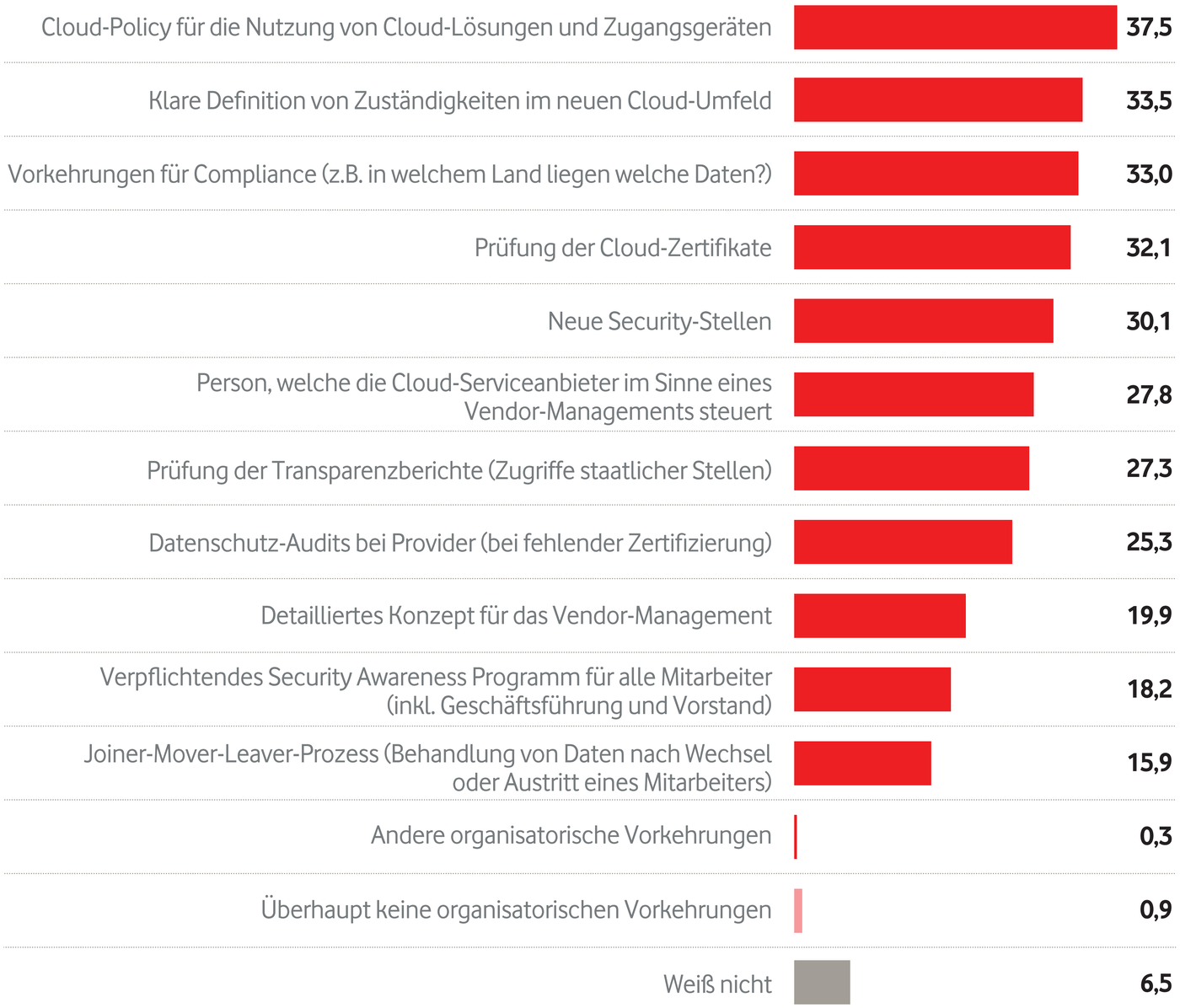
Compliance, also Rechtskonformität

Einhalten aller einschlägigen Regeln, Vorschriften und Gesetze, die für die jeweiligen Daten gelten, z.B. die DSGVO-Richtlinie zum Schutz persönlicher Daten von EU-Bürgern.

Die IT-Sicherheit organisiert sich neu

Welche organisatorischen Vorkehrungen sind in Ihrem Unternehmen in Bezug auf Cloud Security getroffen worden?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 352



Die Migration in die Cloud erfordert eine **Neuordnung der Arbeitsprozesse** und der **Zuständigkeiten** innerhalb der IT-Abteilung – auch im Bereich Security.

Jedes 3. Unternehmen hat schon eine **klare Definition der Zuständigkeiten** im neuen Cloud-Umfeld vorgenommen, 30 % haben **neue Security-Stellen geschaffen** und jedes 4. Unternehmen führt **Datenschutz-Audits** beim Provider durch.

Quelle: Studie Cloud Security 2021 von IDG und Vodafone

Security-Verantwortlichkeiten je nach Cloud-Service-Modell

Die Verantwortlichkeiten für die einzelnen Komponenten einer Cloud können sehr verschieden sein. Je nach Cloud Service und Cloud-Umgebung. Entsprechend verschieden ist der Umfang, in dem Anwender-Unternehmen selbst für Sicherheit verantwortlich sind. Um einen optimalen Schutz zu schaffen, ist wichtig zu verstehen, wie die verschiedenen Services und Umgebungen aufgebaut sind.

Cloud Services werden eingeteilt in diese Modelle:

Infrastructure-as-a-Service (IaaS)

Der Provider stellt die **Infrastruktur** bereit, auf deren Basis das Anwender-Unternehmen Software installieren und nutzen kann, z.B. ein Betriebssystem oder eine Anwendung. Der Provider kontrolliert die Infrastruktur. Das Unternehmen schützt die Software.

Platform-as-a-Service (PaaS)

Der Provider stellt die **Hardware und die Software-Plattform** bereit und verwaltet sie. Das Anwender-Unternehmen organisiert die Anwendungen auf der Plattform und schützt die Apps und die Daten.

Software-as-a-Service (SaaS)

Der Provider bietet **ganze Anwendungen als Cloud Services** an. Das Anwender-Unternehmen kann nicht auf die Infrastruktur und die Plattform zugreifen und hat höchstens eingeschränkt individuelle Sicherungsoptionen.

In jedem Fall ist der **Cloud Service Provider** verantwortlich für den **Schutz der Hosting-Infrastruktur und des Netzwerks vor physischen Schäden**.

Je nach Modell, also IaaS, PaaS oder SaaS, **teilen sich Provider und Unternehmen die Verantwortung** für das **sichere Funktionieren einzelner Anwendungen** und den **Schutz von Anwendungen**.

Hauptsächlich in der **Verantwortung der Unternehmen** liegt das **Identity & Access Management**, also die Festlegung, wer was wie nutzen oder ausführen darf. Das gilt auch für die **Sicherung des Zugangs für Geräte**, über den sich Mitarbeitende mit der Cloud verbinden: Das Unternehmen stellt das Monitoring und die Verwaltung aller Geräte sicher.

Mitarbeitende laden oft Daten aus der Cloud auf ihre Smartphones und Laptops, um mit ihnen zu arbeiten. Auch die schützt das Unternehmen. Genauso wie die Cloud-Instanz selbst.

Security-Verantwortlichkeiten in Abhängigkeit vom Cloud-Service-Modell

Sicherheitsaspekte bei IaaS

Bei diesem Cloud-Service-Modell trägt das Anwender-Unternehmen deutlich **mehr Sicherheitsverantwortung** als bei den anderen Modellen. Achten Sie auf Folgendes:

- Gründliche Evaluierung des **Sicherheitsmodells des Providers**. Wichtig: Provider nutzen teilweise verschiedene Begriffe für ähnliche Konzepte.
- **Verschlüsselung von Daten im Ruhezustand** und Überprüfung, wie sich die Verschlüsselung auf Dienste wie Backup und Wiederherstellung auswirkt.
- **Konsequentes Einspielen von Sicherheitsupdates**
- Definition des **Identitäts- und Zugriffsmanagements**

Sicherheitsaspekte bei PaaS

Hier hostet der **Provider die Hard- und Software** auf seiner Infrastruktur. Auch dabei sind die Verträge mit den Providern wichtig sowie die **Überprüfung und Validierung der Provider-Umgebungen und -Prozesse**. Das gilt auch für die Identifizierung der Sicherheitsmodelle und der sicherheitsrelevanten Tools, die dem Anwender-Unternehmen zur Verfügung gestellt werden.

Achten Sie außerdem auf die **Verschlüsselung der Daten bei der Übertragung** und der **Speicherung**.

Und denken Sie an die **Portabilität**. **APIs, Security-Dienste** und teilweise sogar die Programmiersprache hängen vom Provider ab. Wählen Sie eine Sprache, die von verschiedenen Providern unterstützt wird. Das verbessert die Portabilität und verringert die Abhängigkeit von einem bestimmten Provider.

Sicherheitsaspekte bei SaaS

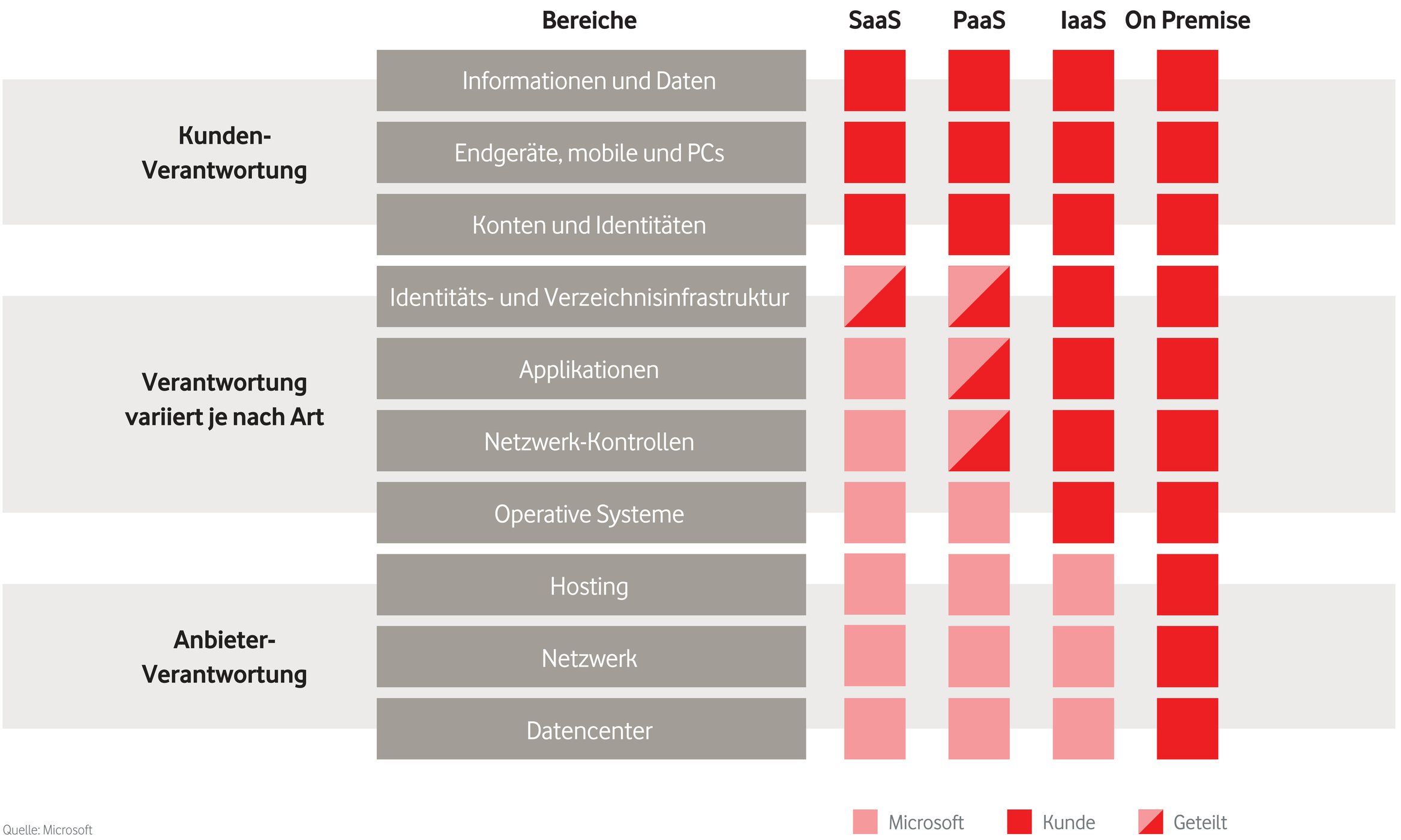
SaaS-Anwendungen müssen **genauso geschützt werden wie andere Anwendungen** im Unternehmen. Dabei gibt es keine Security-Checkliste, die für alle Anwendungen gleichermaßen funktioniert. Welche Maßnahmen zur Absicherung nötig sind, hängt von der Organisation, den Geschäftsprozessen sowie den Arbeitsweisen und Anforderungen ab.

Hier steht der **Zugriff aufs Internet** im Mittelpunkt. Überprüfen Sie wie die Nutzenden auf die SaaS-Ressourcen zugreifen, also wie die Authentifizierung erfolgt.

Prüfen Sie **Cloud-Verträge und SLAs** gründlich. Die Bedingungen, Anhänge und Anlagen enthalten viel, was sich auf die Sicherheit auswirken kann. Ein Vertrag kann den Unterschied ausmachen zwischen der Verantwortung Ihres Cloud Service Providers für Ihre Daten und dem Besitz der Daten.

Achten Sie darauf wem die **Daten gehören** und und was mit ihnen geschieht, wenn die Dienste beendet werden. Und ob der Provider verpflichtet ist, Einsicht in sicherheitsrelevante Vorfälle zu gewähren.

So sieht das Shared-Responsibility-Modell für die 3 Cloud-Bereitstellungsarten bei Microsoft Azure aus:



Quelle: Microsoft

Cloud-Sicherheit basiert auf dem Zero-Trust-Prinzip

Hardware, Software und Anwendungen werden zunehmend in die Cloud verlagert. Das bringt traditionelle Sicherheitsarchitekturen an ihre Grenzen. Modernere Sicherheitsarchitekturen zum Schutz dezentral aufgestellter IT-Ressourcen basieren auf dem Zero-Trust-Prinzip. Das Firmennetzwerk wird dabei als dynamischer, sich ständig wandelnder Organismus betrachtet. Nicht mehr als monolithisches Konstrukt mit festen Grenzen.

Das Zero-Trust-Modell beruht auf 3 Prinzipien:

1

Die **gesamte IT-Umgebung wird als nicht vertrauenswürdig eingestuft**. Bei klassischen Sicherheitsarchitekturen werden – im Gegensatz zu Zero-Trust-Modellen – Nutzende im Netzwerk grundsätzlich als vertrauenswürdig eingestuft. Das ist problematisch, da sich so Eindringlinge frei im Netzwerk bewegen und sich sensiblen Bereichern nähern können. Gefahren sind auch netzwerkfähige Geräte wie Drucker und Scanner. Lange galten sie als vertrauenswürdig, doch ihre meist wenig bekannten Sicherheitslücken werden von Kriminellen als Einfallstore genutzt. Diese Gefahren klassischer IT-Sicherheitsarchtekturen mindert das Zero-Trust-Modell, indem es alle Transkaktionen zunächst als nicht vertrauenswürdig einstuft.

2

Das **Verhalten der Nutzenden soll besser verstanden werden**, um zu prüfen, welche Nutzenden und welche Anwendungen im Netzwerk als vertrauenswürdig und legitim eingestuft werden können und welche nicht.

3

Auf Vertrauen basierende Beziehungen zwischen Systemen in allen Teilen der IT-Umgebung sollen identifiziert werden. Dann brauchen die **Security-Teams** sich nur mit den Verbindungen zu befassen, die **für die zentralen Unternehmenssysteme oder -Anwendungen relevant** sind.

Das Zero-Trust-Konzept gibt es schon seit einigen Jahren. Früher wurde es oft nur zum Segmentieren und Sichern von Netzwerken über verschiedene Standorte und Hosting-Varianten eingesetzt. Und es wurde ständig weiterentwickelt. Heute eignet es sich auch zum Schutz individueller Server und Workloads. Dabei lassen sich auch einzelne Komponenten von Anwendungen, ausführbare Dateien und das Verhalten von kommunizierenden Systemen prüfen.

Im Mittelpunkt des Zero-Trust-Konzepts stehen in der Praxis **die Identitäts- und die Kontextprüfung**. Relevant sind dabei die Zugangsdaten eines Nutzers und der Kontext, in dem der Zugriff stattfindet:

- Welche Art Gerät wird verwendet?
- Von wo aus wird zugegriffen?
- Zu welcher Uhrzeit?
- Welche Daten sollen aufgerufen werden?
- Welche Policies gelten für diese Daten?

Fällt etwas auf, z.B. wenn ein Zugriff aus Südamerika zu später Stunde erfolgt, während der:die Nutzende einige Stunden vorher von Deutschland aus zugegriffen hatte, verschärft das System selbstständig die Sicherheitsprüfung oder alarmiert die Administrator:innen.

Mit der Weiterentwicklung von Zero Trust sind zwei weitere Prinzipien dazugekommen:

4

Die **gesamte Kommunikation wird standortunabhängig abgesichert**. Verbindungen werden getrennt und Zugriffsanforderungen überprüft. Dabei werden alle verfügbaren Kontextdaten zu den Nutzenden und zur Anforderung berücksichtigt.

5

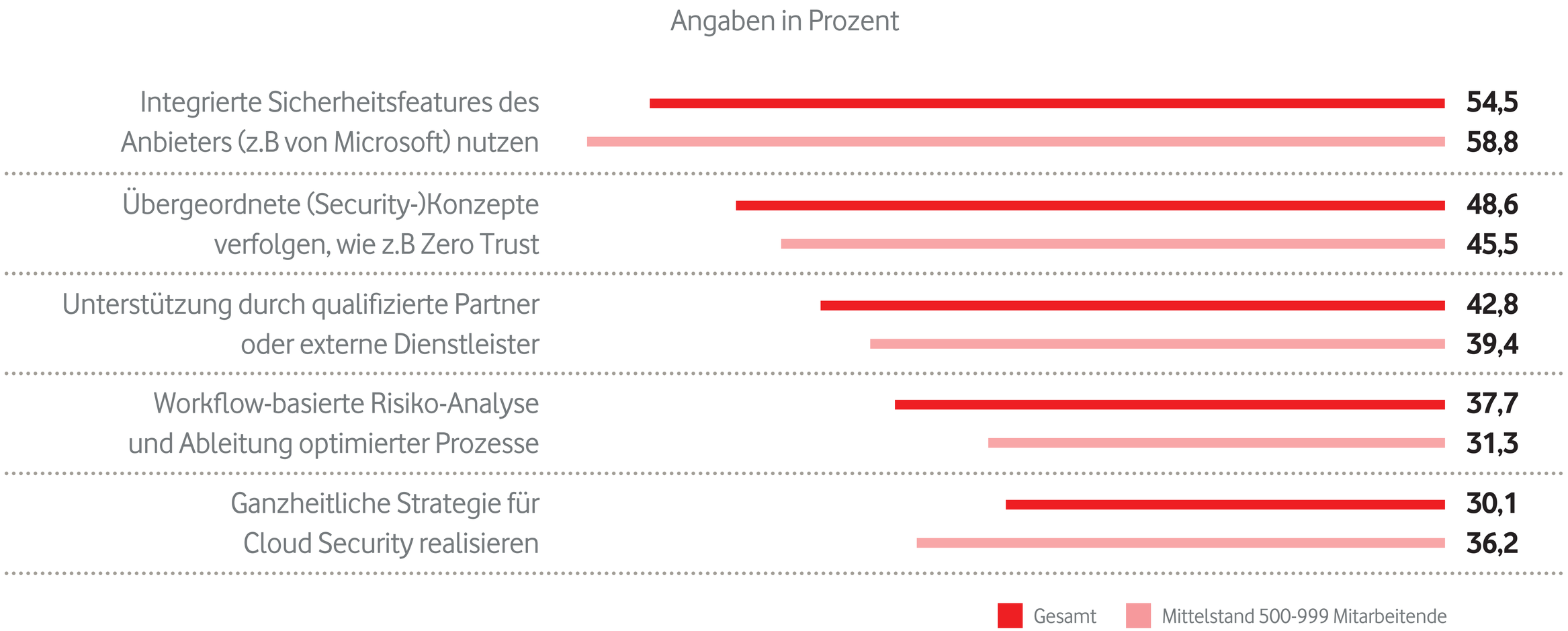
Alle Ressourcen werden **dynamisch authentifiziert und autorisiert**. **Ein Zugriff erfolgt erst nach strikter Prüfung**.

Zero Trust wurde als Methode zum Schutz von Firmennetzwerken entworfen. Und die Grundsätze des Zero-Trust-Konzepts haben sich für viele weitere Anwendungsfälle bewährt. Das gilt besonders für den **Schutz von SaaS-Anwendungen**, von **ein- und ausgehendem Traffic in öffentlichen Clouds** sowie von **Nutzenden, die aufs Internet zugreifen**.

Zero Trust ist inzwischen die **tragende Säule für den Aufbau ganzheitlicher Sicherheitsarchitekturen in der Cloud-Ära**. Auch in unserer Umfrage steht die Schlüsseltechnologie weit oben auf der Agenda der IT-Verantwortlichen. Zero Trust schützt Nutzende, Anwendungen, Prozesse und vernetzte Geräte. Und sorgt für eine gute und sichere Erfahrung der Nutzenden.

Cloud Security setzt Zusammenarbeit voraus

Was sind für Ihr Unternehmen die wichtigsten Faktoren für mehr Security in Cloud-Projekten?



Rund 55 % der Unternehmen sehen die integrierten Sicherheitsfeatures der Cloud Provider als wichtigste Komponente für bessere Cloud Security. Jedes 2. Unternehmen will übergeordnete Security-Konzepte wie Zero Trust einsetzen, um für mehr Sicherheit in Cloud-Projekten zu sorgen. Und 43 % arbeiten mit ihrem Cloud Provider in Sicherheitsfragen zusammen und wollen für die Stärkung ihrer Cloud-Sicherheit qualifizierte Partner oder externe Dienstleister einsetzen.

Quelle: Exklusive Umfrage von Vodafone und IDG über die Prioritäten der Unternehmen bei der Umsetzung künftiger Cloud-Vorhaben

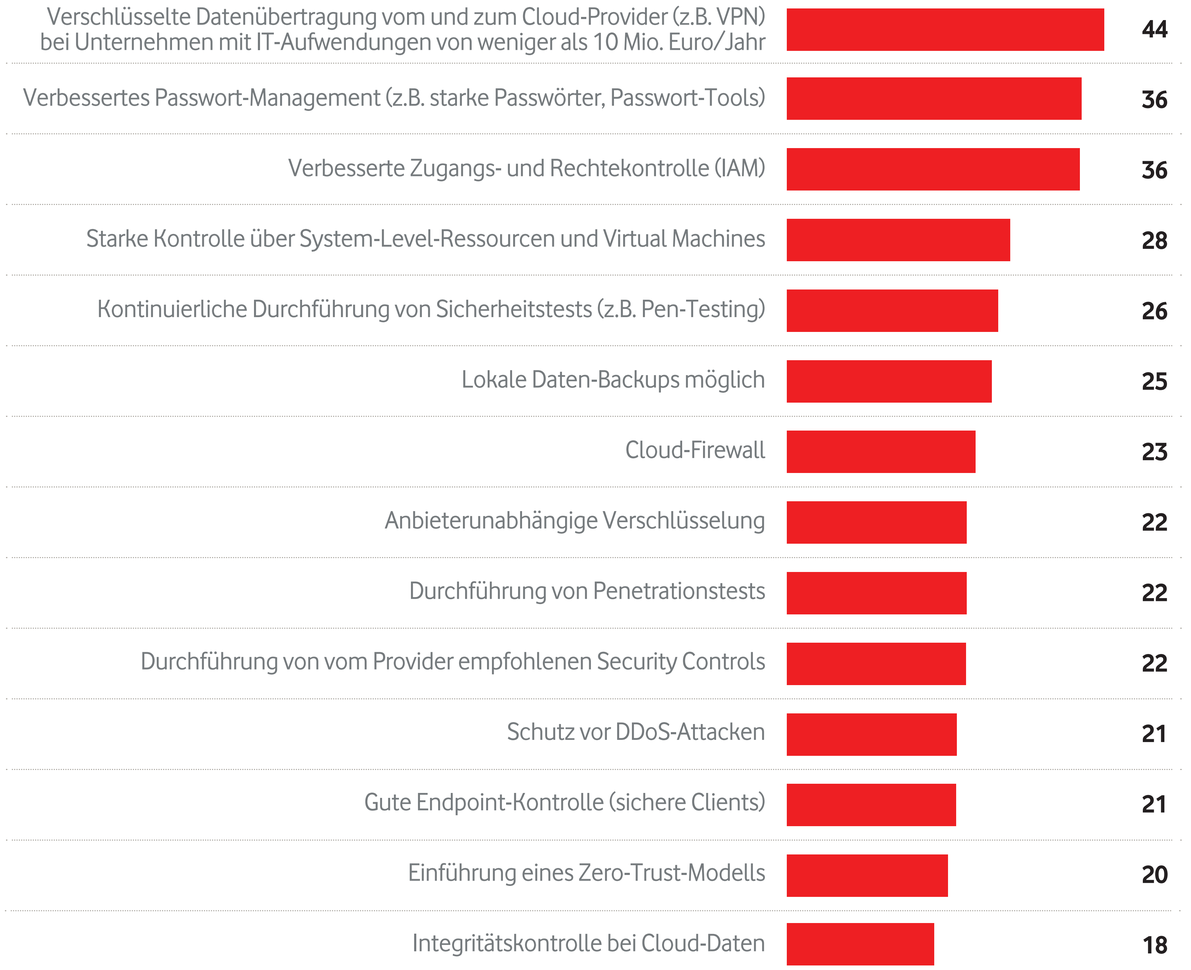
Sichere Kommunikation geht über alles

Dezentrale und Cloud-basierte Infrastrukturen bringen eine **höhere Datenmobilität** mit sich. Cloud-Anwendungen greifen oft auf Daten zu, die im Rechenzentrum lagern. Und lokale Apps verarbeiten Daten aus der Cloud.

Dieser intensive Datenaustausch zwischen den verschiedenen Verarbeitungs- und Speicherorten setzt eine rundum **abgesicherte Datenkommunikation** voraus. Die wird in der Regel durch **Ende-zu-Ende-verschlüsselte Datenleitungen** realisiert. Deshalb gehört die **Absicherung der Datenleitungen vom und zum Cloud-Provider** zu den allerersten Maßnahmen, die in Bezug auf Cloud-Sicherheit implementiert werden.

Welche technischen Vorkehrungen sind in Ihrem Unternehmen in Bezug auf Cloud Security getroffen worden?

Angaben in Prozent. Mehrfachantworten möglich. Basis: n = 352



Die verschlüsselte Datenübertragung vom und zum Cloud-Provider ist eine grundlegende technische Sicherheitsmaßnahme, die als eine der ersten von Unternehmen eingeführt wird. Bei den Unternehmen mit IT-Aufwendungen von weniger als 10 Millionen Euro sind es 44 %. Neben der verschlüsselten Datenübertragung spielt der abgesicherte Zugang zu Daten und Anwendungen über fortschrittliche Tools für das Passwort- und das Identitätsmanagement für Unternehmen eine wichtige Rolle. Erfreulich: Jedes 5. Unternehmen hat schon Zero-Trust-Verfahren eingeführt.

Quelle: Studie Cloud Security 2021 von IDG und Vodafone

Cloud Security in der Praxis

Die Anwendung des Zero-Trust-Prinzips in der Praxis bedeutet, dass grundsätzlich alle **aktiven Instanzen** innerhalb eines Netzwerks – Nutzende, Geräte und Anwendungen – **kontinuierlich und auf mehrfache Weise geprüft** werden. Dazu kann gehören:

- Identität und Standort der Nutzenden
- Integrität der Geräte
- Kontext der Zugriffe auf IT-Ressourcen
- Klassifizierung der Daten, auf die sie zugreifen
- Eventuelle Anomalien in Zusammenhang mit den Zugriffen

Außerdem werden bei jedem Zugriff die Zugriffsrechte auf das Minimum beschränkt, das für die Erledigung der jeweiligen Aufgabe nötig ist. Alle Netzwerk-Ressourcen, Nutzenden, Geräte und Anwendungen sind bestimmten Segmenten zugewiesen. So kann eingeschleppte Schadsoftware sich nicht ungehindert im Netzwerk verbreiten. Der **Schaden durch einen böswilligen Zugriff wird minimiert**. Abgesichert sind auch alle Datenverbindungen zwischen Nutzenden, Standorten und Cloud-Anwendungen.

Tipps zur Einführung von Zero Trust

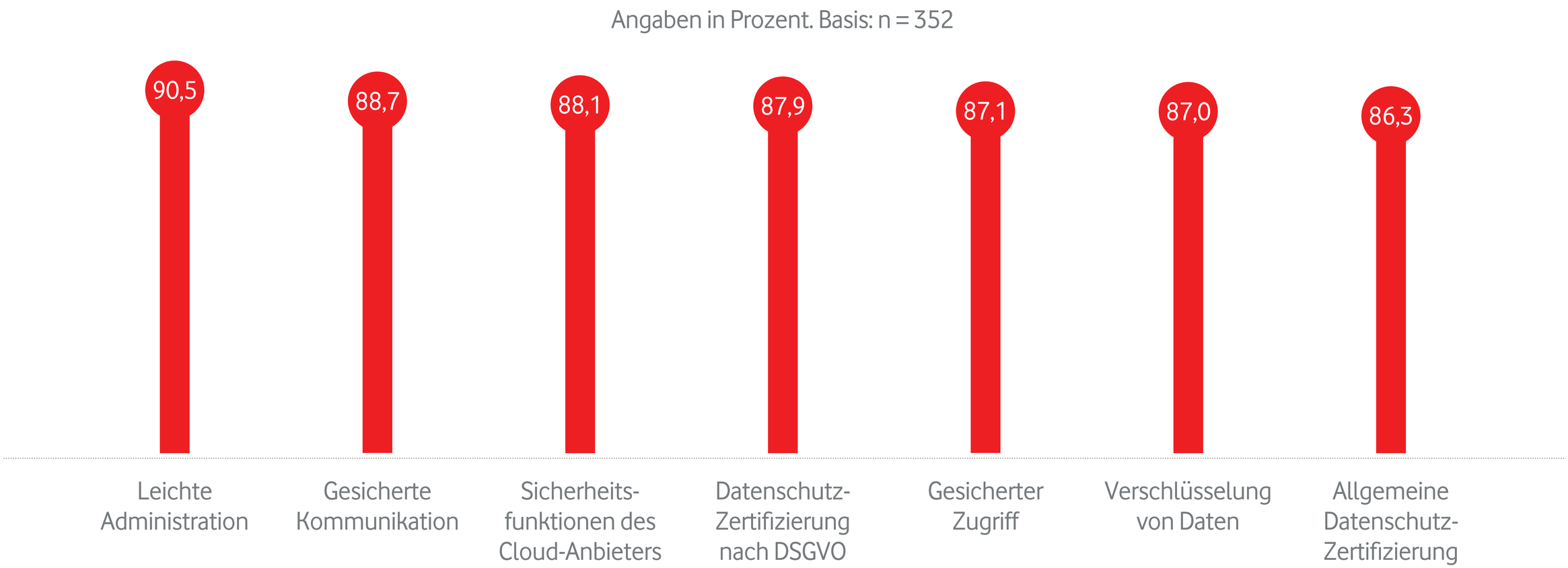
1. Schritt:
Bestandsaufnahme der Anwendungen durch Monitoring des Netzwerk-Verkehrs
Registrieren Sie alle genutzten Verbindungen und fordern Sie die Nutzenden auf zu beschreiben, wie normale Nutzungsmuster und Kommunikationen zwischen den verwendeten Systemen aussehen sollen.

2. Schritt:
Netzwerk auf Basis der Ergebnisse der durchgeführten Bestandsaufnahme segmentieren
Definieren Sie außerdem die nötigen Schutz- und Zugangskontrollen in der IT-Umgebung. An den Grenzen der verschiedenen Netzwerksegmente können Sie rein virtuelle Mechanismen oder physische Geräte einsetzen.

3. Schritt:
Asset-Identitäten nutzen, die mit Ihrer Anwendungsarchitektur zusammenhängen
Kategorisieren Sie Ihre Anwendungen und Systeme sorgfältig. So können Sie erwünschte Verbindungen und Verhaltensweisen leichter erfassen und zuordnen. Das können Sie auch mit Cloud-basierten Tools wie Microsoft Azure Active Directory Conditional Access, Microsoft Intune und Microsoft Cloud App Security. Auch von anderen Anbietern gibt es inzwischen Produkte und Dienste, mit denen Sie Workloads und Cloud-Anwendungen voneinander isolieren können.

Prioritäten bei der Cloud-Migration

Wie wichtig sind Ihnen in Bezug auf Cloud Services die folgenden Kriterien?



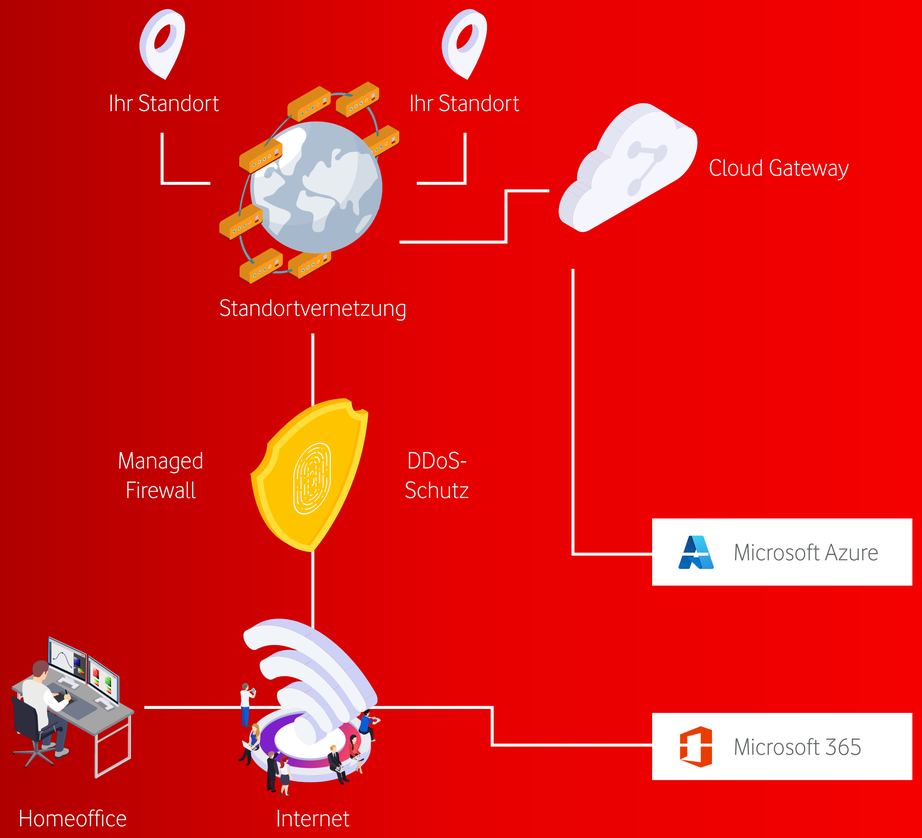
Neben der einfachen Administration beziehen sich alle anderen Kriterien, die Unternehmen bei ihrer künftigen Cloud-Plattform wichtig sind, auf die Sicherheit. Die gesicherte Kommunikation mit der Cloud-Plattform des Anbieters steht dabei an erster Stelle, gefolgt von den Sicherheitsfunktionen des Cloud-Anbieters, der DSGVO-Konformität und dem gesicherten Zugriff auf Daten und Anwendungen.

Quelle: Studie Cloud Security 2021 von IDG und Vodafone

Security als Komplett-Service bei Vodafone

Je nach Struktur der IT-Landschaft eines Unternehmens erfordert Cloud Security verschiedene Tools, Verfahren und Policies, um Nutzende und Infrastruktur zu sichern. Sie als mittelständisches Unternehmen bekommen bei uns Cloud Security als Komplett-Service aus einer Hand. Das heißt für Sie: größtmögliche Sicherheit bei geringstmöglichem eigenem Aufwand.

Wir kombinieren die Produkte und Lösungen so, dass die Cloud Services sicher in Ihre IT-Infrastruktur integriert sind. Auch ergänzen wir die Cloud-Ressourcen mit Services wie Cloud-Gateway für die sichere und performante Einbindung in die Standort-Vernetzung und Security-Diensten wie Managed Firewall und DDoS-Schutz. Bei Bedarf übernehmen zertifizierte Partner auch die Migration und den Betrieb vor Ort.



Mehr Infos im Web: vodafone.de/cloud

Infos zu den verwendeten Studien

Für die Studie Cloud Security wurden 383 IT-Entscheidende in der DACH-Region interviewt, darunter strategische (IT-)Entscheidende im C-Level-Bereich und den Fachbereichen sowie Entscheidende und Spezialist:innen aus dem Bereich IT.

Die Stichprobe stammt aus der IT-Entscheider-Datenbank von IDG Business Media und, um Quotenvorgaben zu erfüllen, aus externen Online-Access-Panels. Sie umfasst alle Branchen.

Verteilung der Stichprobe nach Unternehmensgröße

Weniger als 100 Beschäftigte:	6,0 %
100 bis 499 Beschäftigte:	28,7 %
500 bis 999 Beschäftigte:	25,3 %
1.000 bis 9.999 Beschäftigte:	27,4 %
10.000 Beschäftigte und mehr:	12,5 %

Erhebung: Die Umfrage wurde über 383 abgeschlossene und qualifizierte Interviews zwischen 1. und 15. März 2021 durchgeführt. Die persönlichen Einladungen zur Umfrage erfolgten per E-Mail.
Fragebogen-Entwicklung: IDG Research Services in Abstimmung mit den Studienpartnern.

Exklusive Umfrage von Vodafone und IDG
Im September 2022 wurde die Erhebung der wichtigsten Maßnahmen für die erfolgreiche Cloud-Migration mit einem analogen Studien-Setup durch IDG Research Services durchgeführt. Hierbei wurden insgesamt 323 Firmen befragt.