

Trendkategorie: Digitalisierung und Konnektivität

# Cloud Computing

*Cloud Computing ist definiert als die Bereitstellung von speziellen Online-Diensten (meist) über das Internet (die „Cloud“). Diese Dienste umfassen den netzwerkbasieren Zugriff auf einen Pool gemeinsam nutzbarer physischer oder virtueller Ressourcen, z. B. Speichergeräte, Datenbanken, Server, Rechenkapazität, Betriebssysteme, Software, Analytics-Funktionen<sup>1</sup>. Die Spannweite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst somit das komplette Spektrum der Informationstechnik.*



Cloud Computing gilt als Basistechnologie für Industrie 4.0<sup>2</sup>. Mithilfe von Cloud Computing kann man Geräte im Internet of Things (IoT) vernetzen und verwalten und den Zugang zu Tools ermöglichen, die mit künstlicher Intelligenz (KI) oder Machine Learning arbeiten. Es lassen sich Anwendungen wie Apps entwickeln, bereitstellen und skalieren, Audio- und Videoinhalte streamen, Backup-Lösungen zur Verfügung stellen, Daten im Falle eines Verlusts schnell wiederherstellen und Tools zur Analyse großer Datenmengen (Big Data) anbieten<sup>3</sup>.

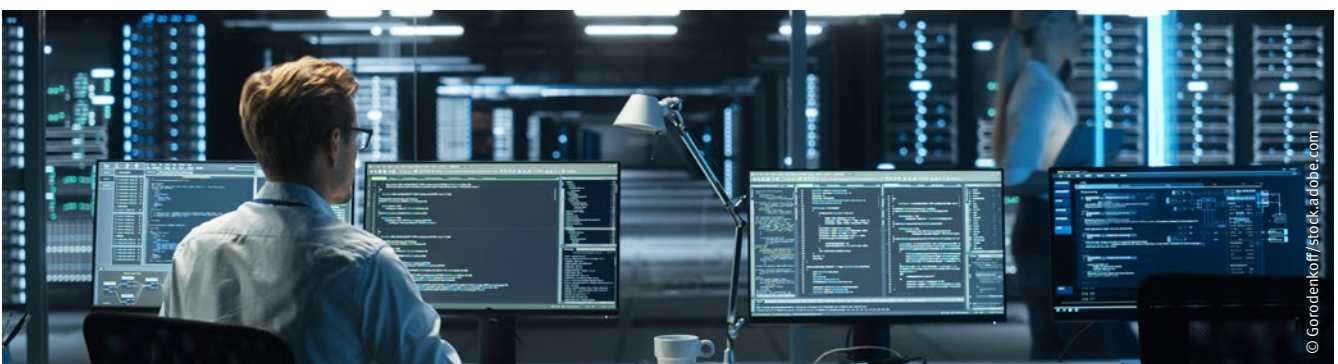
Im Jahr 2024 nutzten 81 % der Betriebe in Deutschland Cloud Computing, weitere 14 % planten dies oder diskutieren darüber, für nur 5 % war die Cloud kein Thema<sup>4</sup>. Andere Quellen gehen davon aus, dass sogar 94 % der Unternehmen<sup>5</sup> bzw. 98 % der Betriebe ab 50 Beschäftigten von Cloud-Diensten Gebrauch machen<sup>6</sup>. 58 % der befragten Unternehmen hatten im Jahr 2024 bereits eine dezidierte Cloud-Strategie, 64 % hielten ein Cloud-Projekt-Team oder ein Cloud Center of Excellence (CCoE) vor, das die Unternehmensexpertise bündelt<sup>7</sup>.

In einer Private Cloud wird die Cloud-Infrastruktur nur für eine Institution betrieben, eine Public Cloud stellt ihre Dienste der Allgemeinheit oder einer großen Gruppe, z. B. einer Industriebranche zur Verfügung. In einer Community Cloud wird die Infrastruktur von mehreren Institutionen mit ähnlichen Interessen geteilt. Werden mehrere eigenständige Cloud-Infrastrukturen über standardisierte Schnittstellen gemeinsam genutzt, spricht man von einer Hybrid Cloud<sup>1</sup>.

Man unterscheidet verschiedene Kategorien von Servicemodellen: 1) Infrastructure as a Service (IaaS): Nutzende mieten z. B. Rechenleistung, Arbeits- und Datenspeicher an und lassen darauf ein Betriebssystem mit Anwendungen ihrer Wahl laufen. 2) Platform as a Service (PaaS): Der Provider stellt eine komplette Infrastruktur (Betriebssystem, Hardware) bereit und bietet auf der Plattform standardisierte Schnittstellen an, über die Nutzende eigene Anwendungen laufen lassen können – ohne Kontrolle über das zugrundeliegende IT-System. 3) Software as a Service (SaaS): Es werden vorgefertigte

Software-Anwendungen zur Verfügung gestellt. Die komplette IT-Administration, Wartungsarbeiten und Softwareaktualisierung obliegen dem Provider<sup>1</sup>. 4) Big Data as a Service (BDaaS) ist eine spezielle Form des Cloud Computing. BDaaS stützt sich auf Cloud Storage, ein Dienstleistungsmodell, bei dem Daten übertragen und auf (entfernten) Speichersystemen abgelegt werden, wo sie gewartet, verwaltet, gesichert und den Nutzenden über das Internet zur Verfügung gestellt werden<sup>8;9</sup>. Das serverlose Computing integriert viele der Funktionen und Vorteile von IaaS, PaaS und SaaS<sup>10</sup> und konzentriert sich auf das Entwickeln von App-Funktionen. Der Cloud-Anbieter übernimmt das Setup, die Kapazitätsplanung und die Serververwaltung<sup>3</sup>.

Die Nutzung von Cloud Services bietet einige Vorteile und geht über das klassische Outsourcing hinaus. In einer Cloud teilen sich mehrere Nutzende eine gemeinsame Infrastruktur und können so ihre Investitionskosten reduzieren. Cloud Services sind flexibel und dadurch innerhalb viel kürzerer Zeiträume nach oben und unten skalierbar. Cloud-Computing-Dienste werden in der Regel in einem globalen Netzwerk aus sicheren Rechenzentren ausgeführt, die regelmäßig auf die neueste Generation Computinghardware aufgerüstet werden. Die Steuerung der in Anspruch genommenen Cloud-Dienste erfolgt in der Regel mittels einer Webschnittstelle durch die Anwendenden selbst. Diese können die gewünschten Dienste über Web-Oberflächen oder passende Schnittstellen administrieren, wobei wenig Interaktion mit dem Provider erforderlich ist. Zudem sind auch beträchtliche Mengen an Computing-Ressourcen innerhalb weniger Minuten verfügbar. Mithilfe von Cloud Computing werden Datensicherung und Notfallwiederherstellung vereinfacht und die zugehörigen Kosten gesenkt, da Daten an mehreren redundanten Standorten im Netzwerk des Cloud-Anbieters gespiegelt werden können. Durch die beim Cloud Computing genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte zu verteilen, die geographisch weit verstreut sein können (im Inland ebenso wie im Ausland)<sup>3</sup>.





Das im Jahr 2019 gegründete Projekt GAIA-X soll die nächste Generation einer leistungsfähigen und sicheren Dateninfrastruktur in Europa bilden. Daten und Dienste sollen zukünftig in einem transparenten und offenen digitalen Ökosystem zur Verfügung gestellt, technisch zusammengeführt sowie sicher geteilt werden können, um unabhängig von den USA und von China zu werden.

GAIA-X will auch die Verbreitung von Cloud-Lösungen in Deutschland und der EU maßgeblich vorantreiben<sup>11</sup>. Ob das Ziel einer souveränen europäischen Daten-Cloud über GAIA-X oder über andere Plattformen wie IPCEI-CIS (Important Project of Common European Interest – Cloud Infrastructure and Services) erreichbar ist, ist noch offen<sup>12</sup>.



## Was beschleunigt, was bremst den Trend?

Technologische Entwicklungen sind ein maßgeblicher Treiber für Cloud-Dienste. So ermöglichen beispielsweise 6G, die sechste Generation des Mobilfunks, und Glasfaserkabel höhere Internetgeschwindigkeiten und damit schnelleren und zuverlässigeren Cloud-Zugriff. Die Integration von KI und Edge Computing – die dezentrale Datenverarbeitung am Rand des Netzwerks – erlauben intelligentere und effizientere Cloud-Lösungen. Edge Computing und Cloud Computing können sich ergänzen und synergistisch in einer hybriden Vernetzung zusammenarbeiten, auch Distributing Computing („verteiltes Rechnen“) genannt. Dieser Einsatz mehrerer Computer oder Prozessoren, die über ein Netzwerk miteinander verbunden sind, um eine gemeinsame Aufgabe zu erledigen, ist besonders für einen schnellen Zugriff auf große Datenmengen oder Echtzeit-Berechnungen von Bedeutung<sup>13</sup>. Durch eine steigende Anzahl an Anbietern (Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) etc.) ist zu erwarten, dass sich Cloud-Infrastrukturen weiter etablieren und verbessern. Auch die zunehmende Verbreitung von Big Data & Analytics sorgen dafür, dass Unternehmen vermehrt Cloud-Dienste zur Speicherung und Verarbeitung großer Datenmengen nutzen.

Der schnelle technologische Fortschritt, die hohe Komplexität moderner IT-Lösungen und der zunehmende Wettbewerb zwingen Unternehmen dazu, innovative Lösungen zu implementieren und ihre IT-Infrastruktur zu modernisieren. Cloud Computing bietet Zugang zu den neuesten Technologien und Anwendungen. Besonders Startups und kleine Unternehmen sind auf flexible IT-Lösungen angewiesen. Pay-as-you-go-Modelle bei Cloud-Diensten bieten Flexibilität und geringere Anfangsinvestitionen und Open-Source-Cloud-Technologien können die Einstiegshürden für Unternehmen senken. Bei diesem Modell steht der Quellcode öffentlich zur Verfügung, sodass er für alle einzusehen, nutzbar und weiterzuentwickeln ist, meist sogar kostenfrei. Auch die wachsende Akzeptanz und

Verbreitung von mobiler Arbeit (Remote Work) – auch in globalem Zusammenhang – basiert auf cloudbasierten Tools und verstärkt deren Nutzung.

Vertrauen in die Sicherheit und Zuverlässigkeit der Cloud-Dienste ist ein wichtiger Faktor für deren Akzeptanz. Viele Cloud-Anbieter investieren stark in Sicherheitsmaßnahmen wie Verschlüsselung, Zugriffskontrollen und Zero-Trust-Modelle (diese gehen davon aus, dass es auch hinter der Firmenfirewall keine Sicherheit gibt und prüfen jede Anforderung). Cloud-Lösungen erleichtern ebenso die Einhaltung umfangreicher gesetzlicher Vorschriften (z. B. die Datenschutz-Grundverordnung, DSGVO) und können angesichts der enorm steigenden Cyberkriminalität für eine höhere Ausfallsicherheit sorgen. Bei der Cloud Disaster Recovery handelt es sich beispielsweise um eine Kombination von Strategien und Diensten zur Sicherung von Daten, Anwendungen und anderen Ressourcen in einer Public Cloud oder bei einem speziellen Dienstleister. Im Falle eines Cyberangriffs lassen sich die betroffenen Daten, Anwendungen und anderen Ressourcen bei einem Cloud-Anbieter wiederherstellen<sup>14</sup>.

Angesichts der wachsenden Bedeutung von Umweltschutz und eines nachhaltigen Handelns erkennen immer mehr Unternehmen die Notwendigkeit, ihre IT-Infrastruktur umweltfreundlicher zu gestalten. Im Vergleich zu traditionellen Infrastrukturen, bei denen IT-Ressourcen lokal in den eigenen Rechenzentren eines Unternehmens betrieben werden, können Cloud-Lösungen den Energieverbrauch signifikant reduzieren. Dies liegt unter anderem daran, dass Cloud-Anbieter in der Regel energieoptimierte Rechenzentren betreiben, die ihrer Kundschaft zu einer besseren Energieeffizienz verhelfen. Auch eine umweltfreundliche Energieversorgung geht mit Cloud Computing Hand in Hand. Viele Cloud-Provider setzen zunehmend auf erneuerbare Energien, um ihre Rechenzentren zu betreiben. Nicht



zuletzt können Unternehmen durch die Nutzung von Cloud-Diensten ihre eigene IT-Hardware reduzieren, was zu einer Verringerung von Elektronikabfällen führt, da weniger Geräte entsorgt und recycelt werden müssen<sup>15</sup>. Das Thema energieeffizientes Cloud Computing ist für die EU angesichts des hohen Energiebedarfs digitaler Technologien zu einem wichtigen Handlungsfeld geworden. Die EU-Kommission prüft derzeit Maßnahmen zur Verbesserung der Energieeffizienz und der Leistung der Kreislaufwirtschaft bei Cloud Computing und in Rechenzentren<sup>16</sup>.

Laut der Studie „Cloud Transformation 2024“ stellt Cloud Computing die Unternehmen vor allem mit Blick auf Datenschutz und Compliance (43 %) sowie hinsichtlich Datensicherheit (37 %) vor Herausforderungen. Strategische Hürden sind die Komplexität des Themas (41 %) und Budget-Probleme (30 %)<sup>7</sup>. Kleinstunternehmen haben nicht per se eine niedrigere Affinität zum Einsatz von Cloud-Diensten. Auch bei ihnen sind Datensicherung und -sicherheit das größte Hemmnis, hinzu kommen

Sorgen der Anbieterabhängigkeit (etwa Preissteigerungen oder nicht abzulehnende Anpassungen von Konditionen), Unklarheiten bezüglich der Datenschutzlage und eine unzureichende Internetgeschwindigkeit<sup>17</sup>. Besonders für international operierende Unternehmen ist die Umsetzung der IT-Sicherheit und umfassender rechtlicher Anforderungen (IT-Compliance) eine große Herausforderung. Da sich die Gesetzgebung in Bezug auf die relativ junge Technologie regional zum Teil erheblich unterscheidet und einer hohen Dynamik unterliegt, können bei Unternehmen Bedenken hinsichtlich der Sicherheit ihrer Daten in der Cloud entstehen<sup>18</sup>.

Herausforderungen bei der technischen Umsetzung können ebenfalls blockierend wirken. So ist etwa die Integration bestehender Systeme und Anwendungen in die Cloud anspruchsvoll und zeitaufwendig, da sie oft umfangreich angepasst werden müssen. Auch hegen Unternehmen Bedenken hinsichtlich der Verfügbarkeit und Zuverlässigkeit von Cloud-Diensten, insbesondere bei geschäftskritischen Anwendungen. Bei instabilen und langsamen Internetverbindungen kann es überdies bei Echtzeitanwendungen zu problematischen Verzögerungen kommen.

Auch können die langfristigen Cloud-Kosten höher sein als eigene IT-Infrastruktur – etwa bei großen Datenmengen mit hoher Aus- und Eingabelast oder bestehender, abgeschriebener Infrastruktur – und komplexe Preismodelle die Kostenkontrolle erschweren. Schließlich sind mangelndes Fachwissen und Widerstand gegen Veränderungen innerhalb der Organisation grundsätzlich hinderlich für die Etablierung von Cloud-Strukturen.



## Wer ist betroffen?

Cloud Computing findet schon fast flächendeckenden Einsatz, folgende Branchen nutzen Cloud-Technologien besonders intensiv: IT & Software-Entwicklung, Telekommunikation, Finanz- und Bankensektor, E-Commerce &

Einzelhandel, Gesundheitswesen, öffentlicher Sektor, verarbeitende Industrie, Automobilindustrie, Bildung & Forschung, Logistik & Transport, Medien & Unterhaltung.



## Beispiele

### Beispiel 1

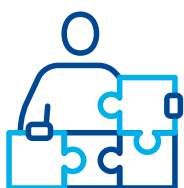
☞ [Schulungen zu Datenschutz und Compliance in der Cloud](#)

### Beispiel 2

☞ [Cloud-Computing wird zum Standard in der Finanz-IT](#)

### Beispiel 3

☞ [Vernachlässigte Cloud-Ressourcen erhöhen Gefahr von Hackerangriffen](#)



## Welche Veränderungen ergeben sich für die Sicherheit und Gesundheit

Die Veränderungen für Sicherheit und Gesundheit durch Cloud Computing sind den Aspekten sehr ähnlich, die in den Trendberichten Cyberkriminalität und Big Data beschrieben wurden. Und grundsätzlich sind sowohl die Beschäftigten bei Cloud-Betreibenden als auch die Nutzenden von Cloud Computing betroffen.

Die Arbeit von Cloud-Betreibenden stellt erhebliche Ansprüche an die Kenntnisse der Beschäftigten hinsichtlich Datenverarbeitung, Rechtssicherheit, Datensicherheit und Datenschutz. Technische Probleme, auch durch Cyberangriffe und höhere Gewalt wie Naturkatastrophen, können den Betrieb massiv beeinträchtigen und schon die Folgen kurzzeitiger Ausfälle (des Internets) gravierende Folgen für das Unternehmen und auch die Cloud-Nutzenden mit sich bringen, die dann zusätzlichen Druck ausüben. Alle diese Faktoren können zu Überforderung und Stress führen. Zudem können Schicht- und Nachtarbeit im operativen Betrieb belastend wirken. Ergänzend kommen eine sedentäre Arbeit hinzu sowie der Druck, sich ständig weiterzubilden, da Kenntnisse in diesem Sektor extrem schnell veralten. Schließlich können Ängste um den Arbeitsplatz entstehen, da Aufgaben in Rechenzentren (z. B. Wartung, Überwachung, Fehlererkennung) in steigendem Maß automatisiert werden.

Der Umgang mit technologisch anspruchsvollen Cloud-Technologien auf Nutzerseite geht mit einem beachtlichen finanziellen und personellen Aufwand einher und erfordert von allen Beschäftigten ein weitreichendes Maß an IT-Expertise und -Kenntnissen und einen hohen zeitlichen Aufwand, naturgemäß besonders bei den zuständigen Beschäftigten im IT-Sektor. Besonders bei Zeitdruck und besonderen Vorfällen kann es zu Arbeitsverdichtung und Überforderung kommen. Die oft knappen Personalressourcen können zusätzlich zu einer hohen psychischen Belastung und Stress beitragen.



Der Schutz sensibler Daten ist von grundlegender Bedeutung, denn Schwachstellen können geschäftskritische Informationen offenlegen und den Geschäftsbetrieb beeinträchtigen. Bei Datenverlusten oder Cyberangriffen können den Datenschutz und die Persönlichkeitsrechte am Arbeitsplatz verletzen können; es droht ein enormes Schadensmaß bis hin zu physischen Schäden und Unfällen (s. Trendbericht Cyberkriminalität). Zudem sind Unternehmen mit langfristigen Reputationsverluste und hohen Compliance-Bußgelder konfrontiert<sup>19</sup>. Diese Verantwortung trägt zu einer hohen mentalen Beanspruchung der Verantwortlichen bei.

Cloud-Technologien sind wesentliche Treiber für die weitere Verbreitung von digitaler Arbeit. Cloud Computing erfordert nicht nur fundierte IT-Kenntnisse und -Qualifikationen, sondern aufgrund einer stärkeren Vernetzung auch Fähigkeiten zur Koordination, Planung und Überwachung. Nicht zuletzt werden vermehrt soziale und kommunikative Kompetenzen benötigt, um den stärker kollaborativ ausgerichteten, komplexen Aufgaben gerecht zu werden<sup>2</sup>. Diese Fähigkeiten müssen sich die Beschäftigten zusätzlich zu ihrer fachlichen Expertise

aneignen. Umgekehrt können Beschäftigte ortsunabhängig mobil von überall auf der Welt auf Unternehmensressourcen zugreifen, was die Produktivität und Zusammenarbeit fördern kann. Die Ressourcennutzung kann insgesamt effizienter erfolgen und die Arbeit durch eine vereinfachte, schnellere Sammlung und Verarbeitung von Daten aller Art erleichtert werden.

Es ist zu vermuten, dass Cloud Computing laufende Entgrenzungsprozesse von Arbeit wie das klassische Outsourcing weiter vorantreiben und auch die Grundlage für neue digitale Arbeitsformen wie die plattformbasierte Ökonomie und Crowdfunding darstellen können. So werden wahrscheinlich die Grenzen von Arbeitsort

und -zeit noch stärker verwischen, um den steigenden Anforderungen an Kundennähe und Flexibilität zu begegnen. Bei einer veränderten, flexibleren Arbeitsorganisation mit Arbeitsmodellen wie Remote Work und hybrider Arbeit werden neue Kommunikations- und Führungsstrategien wichtiger, um soziale Isolation oder Überlastung zu verhindern und zu einem Austausch und einem positiven Betriebsklima beizutragen<sup>2</sup>. Inwieweit Cloud- und Crowdfunding und Outsourcing zu großflächigen Beschäftigungsverlusten führen werden, ist noch unklar<sup>2</sup>.



## Was sind Erkenntnisse und Perspektiven für den Arbeitsschutz?

- ❖ Cloud Computing wird von der überwiegenden Mehrheit der Unternehmen genutzt, ist ein maßgeblicher Treiber der digitalen Transformation und verändert grundlegend die Art und Weise, wie IT-Dienste erbracht und genutzt werden. Für den Arbeitsschutz verknüpfen sich damit allerdings wenig neue Themen. Viele davon betreffen auch die Trends Cyberkriminalität und Big Data.
- ❖ Cloud Computing geht mit hohen zeitlichen und qualitativen Anforderungen an die Leistungsfähigkeit der Beschäftigten bei Cloud-Betreibenden und von Cloud-Nutzenden einher und kann Belastungsmuster verändern. Die Gefährdungsbeurteilung

psychischer Belastung sollte dies konkret berücksichtigen, um ungünstige Arbeitsbedingungen frühzeitig zu erkennen.

- ❖ Cloud-Dienste sind einem beträchtlichen (externen) Bedrohungspotenzial auf die Cloud-Infrastruktur ausgesetzt und stellen hohe Anforderungen an die Informationssicherheit und den Datenschutz. Wichtig ist, „Cloud Security“ von Anfang an mitzudenken und frühzeitig entsprechende Sicherheitsmaßnahmen zu ergreifen, auch um Stress und Überforderung von betroffenen Beschäftigten in Notfällen vorzubeugen.

### Herausgegeben von:

Deutsche Gesetzliche Unfallversicherung e.V.  
(DGUV)  
Glinkastraße 40 · 10117 Berlin  
Telefon: 030 13001-0 (Zentrale)  
E-Mail: info@dguv.de  
Internet: www.dguv.de

Institut für Arbeitsschutz der Deutschen  
Gesetzlichen Unfallversicherung (IFA),  
Risikoobservatorium der DGUV

Verfasst von: Dr. Ruth Klüser

### Ausgabe:

August 2025

### Satz & Layout:

Atelier Hauer + Dörfler, Berlin

### Copyright:

Diese Publikation ist urheberrechtlich geschützt. Die Vervielfältigung, auch auszugsweise, ist nur mit ausdrücklicher Genehmigung gestattet.

Bezug: [www.dguv.de/publikationen](http://www.dguv.de/publikationen)

Die **Literaturliste** ist in der Online-Fassung der Trendbeschreibung verfügbar.

❖ [www.dguv.de/ifa](http://www.dguv.de/ifa)  
🔍 risikoobservatorium

