

# CLOUD & VIRTUALISIERUNG

---

CHANNEL  
GUIDE







Fujitsu empfiehlt Windows 11 Pro für Unternehmen

# Fujitsu Erstkauf- Konditionen

Bis zu 200€ vom  
01.09. bis 30.11. 😊

## Jetzt bis zu 200 € Erstkaufrabatt sichern!

Sichern Sie sich jetzt einen einmaligen Erstkauf-Rabatt von bis zu 200€ auf eine exklusive Auswahl LIFEBOOKs der 12. Generation. Die vielen unterschiedlichen Ausstattungsvarianten von VFY-Modellen der Fujitsu LIFEBOOK-Serien E5 und U7 finden Sie hier:

[https://extranet.ts.fujitsu.com/s/\\_CPP/ce/support/conditions/Pages/erstkauf.aspx](https://extranet.ts.fujitsu.com/s/_CPP/ce/support/conditions/Pages/erstkauf.aspx)

Aktionszeitraum: 01.09.22 – 30.11.2022



Jetzt verfügbar bei unseren Distributionspartnern:



# Entwicklung vollzieht sich in meist Wellen – auch bei der Cloud



**Dr. Stefan Riedl,**  
Leitender Redakteur IT-BUSINESS

Die **Mainframe-Architektur** war auf die Verarbeitung von Massendaten ausgelegt. Über Computer-Terminals wurde auf diese zentrale Verarbeitungsinstanz zugegriffen. Dann kam die Zeit der Personalcomputer, bei der die Verarbeitung dezentralisiert auf die Rechner der Anwender verlagert wurde. Mit Cloud Computing findet – wenn man so will – eine Wiederbelebung des Konzeptes der zentralen Recheninstanzen statt – mit weniger Cobol („dem Aramäisch der Computersprachen“) und mehr browserbasierte Applikationen.

**Doch Software-Konzepte** werden nicht nach dem Kippschalterprinzip eingeführt, denn in den seltensten Fällen entsteht IT in Unternehmen auf der grünen Wiese, die am Reißbrett völlig neu gestaltet werden kann. So beschäftigen sich Cloud-Projekte in der Regel im Lichte von Migrationsprojekten mit dem (nicht mehr wirklich) neuen Software-Paradigma. Die Arbeit mit Legacy-Software steht im Vordergrund, deren monolithische Struktur aufgebrochen und in Microservices zerlegt wird. Doch die Reise ist hier nicht zu Ende.

**Wer hat schon** eine funktionierende Kristallkugel, beherrscht die Kunst des Hühnerknochenwerfens oder klassische Kaffeesatzleserei? Vieles deutet darauf hin, dass bei der Weiterentwicklung von IT eine Wellenbewegung ist, auf die nach einer Dezentralisierung eine Zentralisierung folgt, und dann auf diese wieder eine Dezentralisierung. Mit dem Edge Computing bei der Verarbeitung von Daten auf den Geräten an Netzwerkknotenpunkten, klopft diese bereits an die Tür.

**Weitere Wellen** branden an: Beispielsweise folgt auf Hyperscaler-Dominanz das Erstarken regionaler Player (Seite 6) und rechtliche Unsicherheit weicht neuen Datentransfer-Abkommen (Seite 26).

Ich wünsche Ihnen  
eine aufschlussreiche Lektüre

stefan.riedl@vogel.de

# IT-BUSINESS

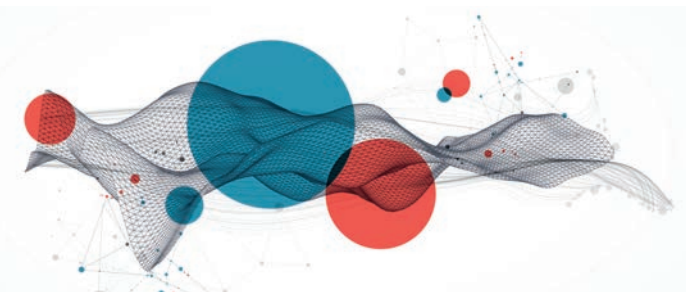
CHANNEL GUIDE Cloud & Virtualisierung



## Licht und Schatten im Cloud-Markt

Zumindest was den IaaS-Markt angeht, dominieren wenige Player das Marktgeschehen, allein schon wegen ihrer „Fancy Tools“. Die Kehrseite der immer noch hohen Wachstumsdynamik sind darüber hinaus Vendor Lock-ins.

6 - 10



## Gaia-X: europäischer Daten(t)raum

Wie steht es um den europäischen Datenraum und welche Geschäftsideen entstehen daraus? **14**



## IT-Security von AWS und Co.

AWS und IBM zählen nicht nur zu den größten Cloud-Anbietern, sie führen auch bei IT-Security. **20**



## Cloud-Storage vom Gerätehersteller

Mit Seagate und Synology bieten zwei Hardware-Hersteller eigene Public-Cloud-Lösungen an. **24**

## Die Hyperscaler dominieren **6**

Der Cloud-Markt: sonnige Dynamik und schattige Lock-in-Effekte

## Marktbarometer **12**

Die Wachstumsraten der Cloud sind ungebrochen.

## Gaia X **14**

Wie man mit Datenräumen Geschäftsmodelle der Zukunft gestalten kann

## Lotsen im Cloud-Universum **16**

Die Distribution unterstützt den Channel mit Trainings, Beratung und White Label Services.

## Windows aus der Cloud **18**

Microsoft bietet selbst zwei verschiedene Lösungen für Windows aus der Cloud an.

## Hyperscaler als Security-Provider **20**

Was bedeutet es für den Security-Channel, wenn Cloud-Provider zum Security-Anbieter werden?

## Kommunikationswege aus der Cloud **22**

Die Kommunikation in Unternehmen hat sich verändert und kommt nun meist aus der Cloud.

## Storage **24**

Inzwischen springen immer mehr Gerätehersteller mit eigenen Lösungen auf den Cloud-Zug auf.

## Der Data Act und was nun? **26**

Recht: Welchen Handlungsbedarf haben Cloud-Anbieter?

## MSPs entdecken neue As-a-Service-Welten **28**

BaaS, RaaS, DRaaS und BCaaS: MSPs befinden sich in einem Begriffs- und Abkürzungs-Wirrwarr.

## Besonderheiten von Cloud Threats **32**

Viele Sicherheitskonzepte von Cloud-Diensten greifen zu kurz. Was sind also die wichtigsten Cloud Threats?

## Impressum **34**



# Modernes Arbeiten braucht Visibilität: Mit ThousandEyes gelingt Digital Experience

Das klassische Büro ist zu einem Auslaufmodell geworden. Nur noch in den seltensten Fällen – und in sehr traditionellen Branchen – sind Mitarbeitende von Montag bis Freitag tagtäglich im Büro und arbeiten stets am gleichen Platz. Die vergangenen Jahre haben deutlich aufgezeigt, dass die Definition von Büroarbeit, wie wir sie über Jahrzehnte gepflegt haben, nicht mehr dem Zeitgeist entspricht.



BILD: THOUSANDEYES

ThousandEyes Outage Map Monitoring

An die Stelle des klassischen Büros sind neue Konzepte getreten: Hybrid Work, Homeoffice, Flexwork oder auch New Normal. Was all diesen Konzepten gemein ist? Ohne das Internet als Rückgrat der Kommunikation steht die Arbeit still. Für Unternehmen und Verantwortliche rückt daher ein zentraler Begriff in den Fokus, um auch in der modernen Arbeitswelt die Produktivität aufrecht zu erhalten und zugleich den eigenen Mitarbeitenden die Möglichkeit zu bieten, im Austausch zu bleiben: Digital Experience.

## Digital Experience – Der Schlüssel zur Produktivität

Aus den Frühzeiten des Internets sind vermutlich noch den meisten die bange Minuten bekannt, in denen man warten musste, bis eine Bilddatei auf einer Website Pixel für Pixel geladen wurde – und natürlich auch der Schockmoment, wenn gegen Ende der Ladezeiten ein Fehler auftrat oder das Modem aus einem unbekanntem Grund den Ladevorgang abbrach. Heutzutage ist man selbstverständlich weit von entsprechenden ersten digitalen Schritten entfernt. Das digitale Wohlbefinden leidet aber mittlerweile auch schneller. Ist eine Website nicht nach einem Sekundenbruchteil geladen, wird aus Frust schnell nach

Alternativen gesucht. Was im Privatleben ärgerlich ist, kann in der modernen Arbeitswelt schnell zu Problemen führen. SaaS-Anwendungen, digitale Meeting-Tools und gemeinsam genutzte Online-Dokumente müssen verfügbar sein – oder es kann nicht gearbeitet werden.

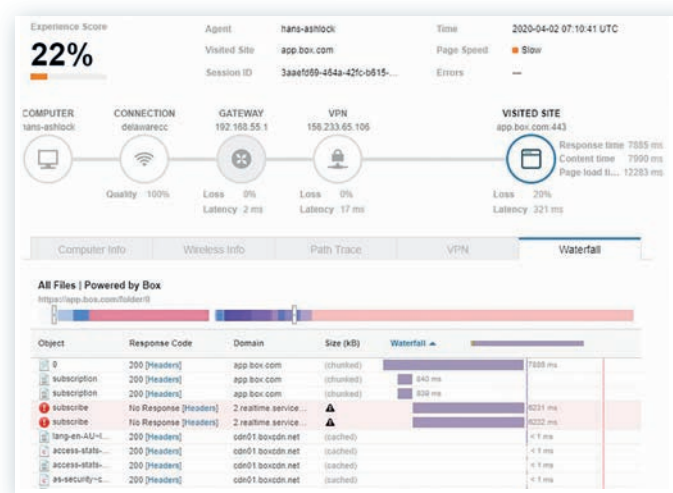
Die Digital Experience von Mitarbeitenden in der neuen Arbeitsrealität hängt dementsprechend eng mit einer funktionierenden und verlässlichen Internetverbindung zusammen. Im Gegensatz zum klassischen Unternehmensnetzwerk, in dem auf eigene On-Premises-Strukturen und Netzwerke des Unternehmens zurückgegriffen wurde, liegt das Internet nicht mehr in der Verantwortung der eigenen IT. Probleme zu erkennen und schnell zu beheben erfordert dementsprechend Visibilität weit über die Grenzen des eigenen Netzwerks hinaus.

Und genau hier kann ein Unternehmen wie ThousandEyes Abhilfe schaffen.

## Visibilität als Grundlage optimaler Digital Experience

Ist beispielsweise die von den Mitarbeitenden genutzte SaaS-Anwendung zur digitalen Zusammenarbeit nicht mehr abrufbar, kann dies eine Vielzahl von Gründen haben. Durch das Digital Experience Monitoring von ThousandEyes kann die Ursache in Echtzeit ermittelt und damit auch eine wesentlich schnellere Lösung für das Problem gefunden werden. Statt für einige Tage auf eine essenzielle Anwendung verzichten zu müssen, können entsprechende Ausfälle durch ThousandEyes in kürzester Zeit behoben werden – und aus digitaler Unzufriedenheit wird für Mitarbeitende schnell wieder digitales Wohlbefinden.

In Zeiten, in denen Mitarbeitende jederzeit und von überall auf der Welt aus auf zentrale Anwendungen zugreifen müssen, ist es entscheidend, dass Unternehmen die Kontrolle über ihre online-basierten Geschäftsanwendungen haben. Die Grundlage hierfür ist Visibilität, wie sie etwa das Digital Experience Monitoring von ThousandEyes ermöglicht. Denn wenn das Internet das Fundament der modernen Arbeitswelt darstellt, ist Visibilität die Basis des Geschäftserfolges in dieser neuen Welt!



End User Monitoring Solution Brief

BILD: THOUSANDEYES



Ist SaaS wirklich so flexibel oder geprägt vom Vendor-Lock-in-Effekten? Wohin führt die Dominanz der Hyperscaler? Auch die Cloud kennt Schattenseiten.

BILD: ARNAUD LAQUEYRIE - STOCK.ADOBE.COM

# Sonnige Dynamik und schattige Lock-in-Effekte

Zumindest was den IaaS-Markt angeht, dominieren wenige Player das Marktgeschehen, allein schon wegen ihrer „Fancy Tools“. Die Kehrseite der immer noch hohen Wachstumsdynamik sind darüber hinaus Vendor Lock-ins.





Die Dominanz der Hyperscaler konnte nicht gebrochen werden.

Kein Gaia-X, keine Mittelstandsinitiativen, keine Nischenpolitik hat geholfen: Infrastructure as a Service (IaaS) ist von Jahr zu Jahr immer fester in der Hand der Big Player zu verorten. Die Anteile von Microsoft Azure und Google Cloud am weltweiten IaaS-Markt sind in den vergangenen beiden Jahren deutlich gestiegen. Zwischen 2019 und 2021 legte Microsoft Azure von 16,5 Prozent auf 20,8 Prozent zu. Im gleichen Zeitraum stieg der Marktanteil von Google Cloud von 7,4 Prozent auf 9,5 Prozent. Amazon Web Services (AWS) verteidigte seine Marktführerschaft und blieb nahezu unverändert bei knapp 35 Prozent. Die Information Services Group (ISG) stützt diese Auswertung auf die Umsatzzahlen, die die weltweit führenden IaaS-Anbieter in ihren Geschäftsberichten ausgewiesen haben.

**Der Hyperscaler** Microsoft profitiert davon, dass eine umfangreiche Installationsbasis für Produkte aus dem Nicht-Azure-Umfeld vorhanden sei, sagt Heiko Henkes, Director & Principal Analyst bei ISG: „So etwa im Falle der Bürosoftware Office 365 respektive des neuen Bundles Microsoft 365 oder der ERP-Suite Dynamics“. Bei Google Cloud gehe das jüngste Wachstum hingegen auf eine Reihe von Faktoren zurück, vor allem auf die Expertise im Analytics- beziehungsweise Machine-Learning-Segment. Unternehmenskunden wird dabei geholfen, Erkenntnisse aus ihren Daten zu gewinnen. Hinzu komme auf technologischer Ebene ein Vorstoß in den B2B-Bereich mit Security- und Compliance-Angeboten und Open Source, beispielsweise Kubernetes. Gemein haben die großen Player, dass sie von ihrer Marktmacht,

Skaleneffekten und dem so genannten Burggraben-Effekt profitieren. Letzterer bezeichnet in der Betriebswirtschaft das Phänomen, dass große Unternehmen bestrebt sind, den Abstand zu kleineren Wettbewerbern stets groß zu halten. Beispielsweise kurzfristig durch Preisaktionen oder langfristig durch neue Produkte und Lösungen auf Basis teurer Grundlagenforschung.

**Cloud-Anbieter** aus der Riege der Hyperscaler zeichnen sich laut dem Analysten durch eine hohe Frequenz von neuen Services aus, deren Vielzahl für Laien kaum noch zu überblicken ist. „Managed Service Provider erfahren deshalb derzeit einen enormen Wachstumsschub, falls sie sich auf die jeweiligen Angebote spezialisiert haben und somit plattformspezifische Lösungen für Kunden realisieren können“, so Henkes. Die Herausforderung dabei sei, die zigfachen Kombinationsmöglichkeiten einer oder mehrerer Cloud-Plattformen zu überschauen und auf die jeweilige Branche und deren Eigenheiten zu übertragen – zum Beispiel im Einklang mit regulatorischen Anforderungen bei Finanzdienstleistern. Dafür seien meistens keine großen Teams notwendig. Angesprochen auf die „Fancy Tools“ der Hyperscaler findet Henkes eher warnende Worte in Bezug auf mögliche Lock-in-Effekte. Denn derartige Werkzeuge seien eben nur beim jeweiligen Anbieter zu finden und dann schwer zu wechseln.

**Auch der Cloud-Monitor 2022** von KPMG, der zusammen mit Bitkom Research erstellt wur-



## Zugang zu neuen Computing-Welten

### KI UND MEHR AUS DER CLOUD

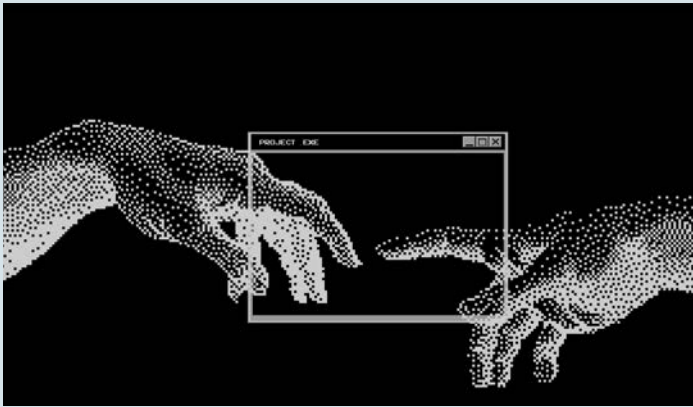


BILD: LOCAL\_DOCTOR - STOCK.ADOBE.COM

Dank Cloud Computing können kleinere Unternehmen auch an Megaprojekten wie Künstlicher Intelligenz partizipieren.

Grundlagenforschung in Sachen Künstliche Intelligenz oder Quantencomputing ist teuer, aber zu leisten, wenn Claims in diesen aufkommenden Märkten abgesteckt werden sollen. Das Budget hierfür haben vor allem Big-Tech-Companys, also die Hyperscaler, die hierbei häufig mit Hochschulen kooperieren. So wird der Abstand zu kleineren Playern im Markt tendenziell immer größer, denn KMU und Mittelständler können nicht leisten, was Hyperscaler hier zu leisten im Stande sind. Das geistige Eigentum wird durch Patente gesichert und der Burggraben zu kleineren Marktakteuren vertieft.

de, beschäftigt sich mit dem Status quo der Cloud und zeigt auf, dass die Wachstumsdynamik rund um Cloud Computing trotz immenser Steigerungen in den Vorjahren, also hohen Basiswerten, nach wie vor gegeben ist. Von den 552 in der Studie befragten Unternehmen mit mindestens 20 Beschäftigten, setzen in diesem Jahr bereits 84 Prozent auf Cloud Computing.

**Auf der einen Seite** wird die Flexibilität von Cloud-Abo-Modellen hervorgehoben, auf der anderen Seite entstehen neue Abhängigkeiten, in die sich jene begeben, die nicht auf interne Ressourcen, sondern auf As-s-Service-Dienste von Cloud-Anbietern setzen. Zur Problematik des sogenannten Vendor-Lock-ins Cloud-Kontext, also dass man sich als Unternehmen von einem Cloud-Anbieter abhängig macht, weil ein Wechsel durch

enge Verzahnung in die Unternehmens-IT doch nicht so einfach vonstatten geht, wie oft propagiert, weiß der Experte aus dem Hause KPMG folgendes zu berichten: „Grundsätzlich kann man sagen, dass der Lock-in natürlich von den unterschiedlichen Services abhängt, das heißt eine Datenbank ist sicherlich leichter austauschbar als ein trainiertes und optimiertes KI-Modell, das von einem Cloud Provider zur Verfügung gestellt wird.“

**Ein Blick ins Silicon Valley** und zu den Firmen aus dem Bereich Software as a Service (SaaS) zeige, dass einige Unternehmen bereits gezwungen waren, einen Teil ihrer Workloads zurückzuführen, so der KPMG-Manager und nennt als Beispiel die Firma Dropbox. In anderen Fällen wird ein Multi-Sourcing-Ansatz gewählt, „wie etwa bei CrowdStrike und Zscaler“. „Kosteneinsparungen beziehungsweise die Optimierung der Infrastruktur sind die Folge gewesen und so konnte Dropbox in den zwei Jahren vor seinem Börsengang insgesamt 75 Millionen US-Dollar einsparen.“

**Bei der konkreten Auswahl** einer Cloud-Lösung geht es Firmen vor allem um Leistungsfähigkeit, Stabilität und Ausfallsicherheit. Auch Vertrauen in die Sicherheit und Compliance des Cloud Providers ist für fast alle unverzichtbar. „Für 70 Prozent der Unternehmen heißt das, dass das Cloud-Rechenzentrum im EU-Raum stehen muss. Hier gibt es ganz klar Nachholbedarf“, sagt der KPMG-Partner. Europäische Anbieter würden viele regulatorische Anforderungen aus der Datenschutzgrundverordnung leichter erfüllen können als amerikanische Anbieter. Europa hat die Technologieführerschaft bei Cloud-Technologien aus der Hand gegeben. Ennemann ernüchterndes Fazit zu diesem Thema lautet: Es bleibe vor diesem Hintergrund abzuwarten, ob sich Initiativen etablieren werden, die die digitale Souveränität in Europa fördern und sich durchsetzen können.

**Es ist ja nicht so**, dass es keine mehr oder weniger erfolgreichen Bestrebungen gibt, im Zuge von Gaia-X oder schlichtweg im Sinne von Alternativenangeboten aus Deutschland beziehungsweise Europa, im Wettbewerb zu punkten. Compliance-Richtlinien und rechtliche Unsicherheiten helfen hierbei Wettbewerbsnachteile aufgrund der Größe auszugleichen. Hervorgehoben wird auch, dass „Partnerschaften auf Augenhöhe“ mit Systemhäusern und -integratoren, Fachhändlern oder IT-Dienstleistern eingegangen werden, nach dem Motto: KMU beziehungsweise Mittelständler hal-



Data Protection Solutions

# Wenn es um **Multi-Cloud-Datenschutz** geht, hat Dell Technologies die passende Lösung für Sie.



[www.tim-vad.com](http://www.tim-vad.com)

**Komplexität auflösen.**

Erfolg mit dem richtigen Partner an Ihrer Seite.

Die TIM AG ist der Channel Development Partner in der Value-Added-Distribution. Wir unterstützen Systemhäuser bei der Geschäftsentwicklung.



## SINGEN DIE EAGLES VON DER CLOUD?

Im Song „Hotel California“ heißt es „You can check-out any time you like... But you can never leave!“ Man könnte meinen, die Eagles singen von der Cloud und dem hier auftretenden Lock-in-Effekt, der in den Wirtschaftswissenschaften Wechselbarrieren und -kosten umfasst.

Der Rückweg aus der Cloud stellt sich als nicht ganz so schwierig dar, wie aus einer Sekte oder der Psychiatrie – je nach Interpretation des Songs. Wer jedoch gewisse „fancy Tools“ aus Hyperscaler-Kreisen nutzt, kann und will sie nicht mehr missen.

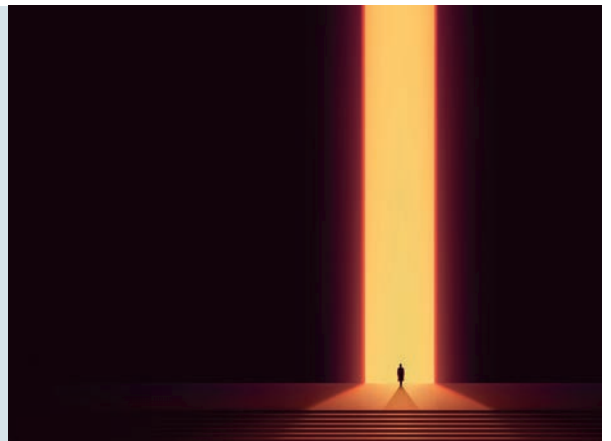


BILD: MAX\_776 - STOCK.ADOBE.COM



ten zusammen. Basisangebote bilden häufig Cloud-Speicherdienste, auf die erweiterte As-a-Service-Optionen aufsatteln.

**Die Bandbreite** an Anbietern, Partnerprogrammen und Möglichkeiten der Zusammenarbeit ist mannigfaltig. So bietet HornetDrive von Hornetsecurity einen verschlüsselten Cloud-Speicher aus deutschen Rechenzentren, der unter anderem Collaboration-Funktionen bereithält. DriveOnTheWeb ist ein weiterer, deutscher Speicherdienst, der mit einer Möglichkeit einer SAP-Integration daher kommt. Hier können



große Datenmengen in Ordnerstrukturen abgelegt werden, die automatisiert mit SAP verbunden sind. Neben dem Upload von SAP können auch Daten von DriveOnTheWeb zu SAP-Anwendungen übermittelt werden. Tresorit ist ein Cloud-Anbieter aus der Schweiz, der auf Ende-zu-Ende-Verschlüsselung setzt. LeitzCloud ist ein deutscher Cloud-Dienst, der sich vor allem an Unternehmen und Vereine richtet.

**Zu den bekanntesten** Cloud-Computing-Diensten aus Deutschland zählt HiDrive von Strato. Als Ionos HiDrive kommt dieser Dienst mit erweitertem Support, der telefonisch und per Mails auch an 24 Stunden zur Verfügung steht, daher. Mit „S3 Storage“ und „Managed Nextcloud“ sind zwei weitere Angebote aus dem Hause Ionos im Rennen. Der deutsche Anbieter Teamplace hat vor allem Teams im Fokus, die einen gemeinsamen Speicherplatz benötigen. Fabasoft betreibt die Business Process Cloud in österreichischen Rechenzentren. Fabasoft Business Process Cloud ist auf Dokumente ausgelegt, die im Rahmen der Prozes-

automatisierung verwendet werden. OVHcloud ist ein französisches Unternehmen, das zu den größten Cloud-Anbietern in Europa gehört. Als Systemhausgruppe bietet Bechtle mit „Bechtle Clouds“ nicht nur Angebote, die auf jenen der Hyperscaler aufsetzen. Als „Multi Cloud Service Provider“ bietet das Unternehmen auch eigenproduzierte Cloud-Dienste. Plusserver aus Köln ist seit 2020 mit der hauseigenen Multi-Cloud-Plattform Plus.io am Start. Neben der Pluscloud aus dem eigenen Rechenzentrum umfassen die Angebote auch das Management von Diensten der Hyperscaler.

**Auch im Channel** stark verwurzelte Anbieter, wie Wortmann, bieten IT-Dienstleistern und Systemhäusern viele Möglichkeiten, im Rahmen eines Partnerprogrammes Cloud-Dienste zu offerieren. Verbundgruppen wie die Wortmann sind auch längst Hand in Hand mit dem Fachhandel den Weg in die Cloud gegangen. Deren IaaS-Angebot besteht aus virtualisierten Ressourcen, die auf die Verlagerung von Workflows ausgelegt sind.

**Summa summarum** wird das Cloud-Business zwar aus Gründen wie dem Burggraben-Effekt von den Hyperscalern dominiert und deren Wachstum scheint nicht abzubrechen. Aber gerade im mittelständischen Umfeld können kleinere Marktakteure ihre Stärken ausspielen, insbesondere wenn sie mit Partnerprogrammen, Provisionsmodellen oder White-Label-Angeboten den Channel an sich binden, als Brücke zum Endkunden. So können sich auch „einheimische Dienste“ etablieren.



Ende der 1990er Jahre war die Zeit mit der Multitenant-Architektur reif für die Cloud, die manchmal auch als Rechnerwolke, Datenwolke oder Internetwolke bezeichnet wird.

**Autor:** Dr. Stefan Riedl



# Das ESET MSP Programm

**Einfach. Sicher. Automatisiert.**



Werden auch Sie ESET MSP Partner.  
Automatisieren Sie Ihr Business mit dem  
größten Security Endpoint Hersteller aus  
der EU.

- ✓ Ohne Risiko
- ✓ Mehr Gewinne
- ✓ Plattformunabhängig
- ✓ Volle Kontrolle
- ✓ Automatisierte Prozesse

Jetzt anmelden: [ESET.DE/MSP](https://www.eset.de/msp)



Digital Security  
**Progress. Protected.**

[ESET.DE](https://www.eset.de) | [ESET.AT](https://www.eset.at) | [ESET.CH](https://www.eset.ch)

# Steigende Ausgaben für Cloud Computing

Dem Flexera Cloud Report 2022 zufolge geben 57 Prozent der Unternehmen pro Jahr mehr als 2,4 Millionen US-Dollar für die Public Cloud aus. Bei 8 Prozent sind es sogar mehr als 60 Millionen. Die Ausgaben sind stark von der Größe der Unternehmen abhängig. So übersteigen bei 37 Prozent der großen Unternehmen die jährlichen Cloud-Kosten die Marke von 12 Millionen US-Dollar.

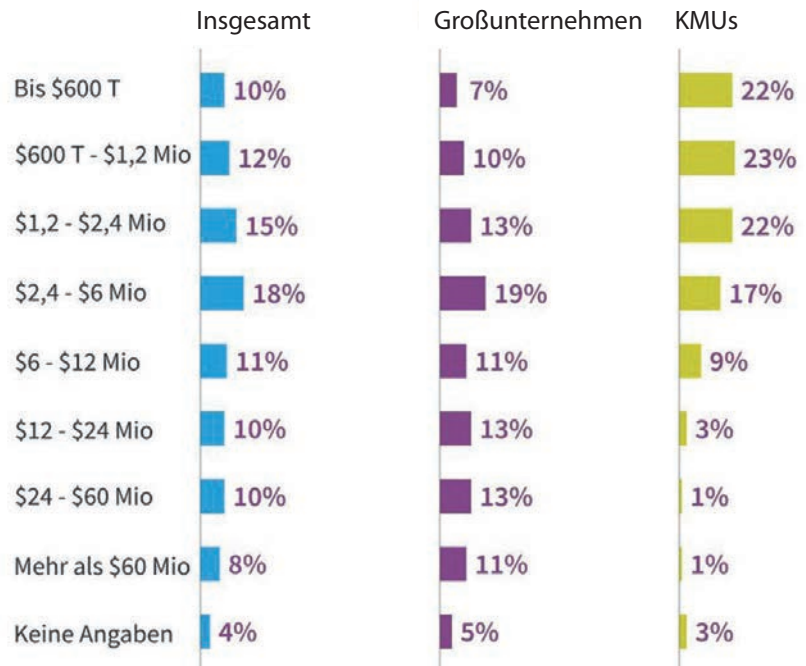


BILD: FLEXERA

## Ready for Cloud

Laut IDC sind mehr als ein Viertel der Unternehmen cloudfähig. Hierbei handelt es sich primär um klassische Anwendungen, die für die Cloud angepasst wurden.

Wie hoch sind in etwa die Anteile der Anwendungen in Ihrem Unternehmen, die Non-Cloud, cloudfähig oder cloudnative sind?

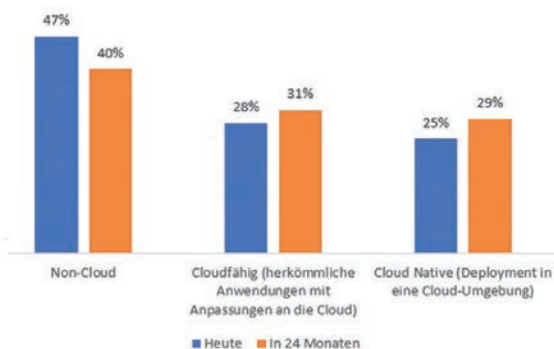


BILD: IDC

## Nach wie vor Sicherheitsbedenken

Die größten Herausforderungen für Unternehmen sind mit 85 Prozent die Sicherheit, dicht gefolgt von mangelnden Fachkräften (83%) und dem Cloud-Ausgabenmanagement (81%).



BILD: FLEXERA



## AWS macht das Rennen

Den größten Marktanteil bei Cloud Computing hat Canalsys zufolge AWS mit 33 Prozent. Die Top 3 vervollständigen Microsoft (21%) und Google (8%).

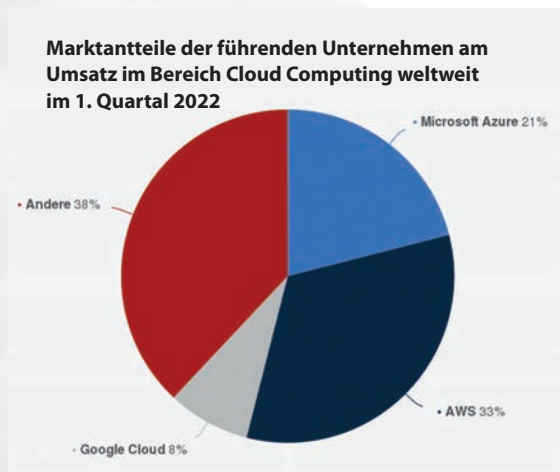


BILD: CANALYS / STATISTA

## Der Nutzen von Cloud-Technologien

Die von Ionos und Techconsult befragten Unternehmen sehen als größten Vorteil der Cloud die erhöhte Flexibilität. Gerade während der Pandemie war dieser Nutzen nicht zu verachten.



BILD: TECHCONSULT GMBH 2021

BILD: BITKOM



**„Die europäische Wirtschaft und insbesondere die Industrie brauchen hochperformante, sichere und vertrauenswürdige Technologien und Angebote für Cloud, Edge und Daten.“**

Achim Berg,  
Präsident des Bitkom

**Gaia-X stößt auf breites Interesse. In einer Bitkom-Umfrage geben 46 Prozent der Unternehmen ab 20 Mitarbeiter an, dass sie an Diensten der europäischen Cloud- und Dateninfrastruktur interessiert sind.**

## Der Wachstumskurs bleibt bestehen

Seit Jahren wächst der weltweite Cloud-Computing-Umsatz kontinuierlich. Für das Jahr 2021 zeigen die Gartner-Zahlen einen deutlichen Anstieg durch die Corona-Pandemie auf knapp 411 Milliarden US-Dollar von rund 270 Milliarden US-Dollar im Jahr 2020. Für 2023 rechnen die Marktforscher mit fast 600 Milliarden Dollar Umsatz.

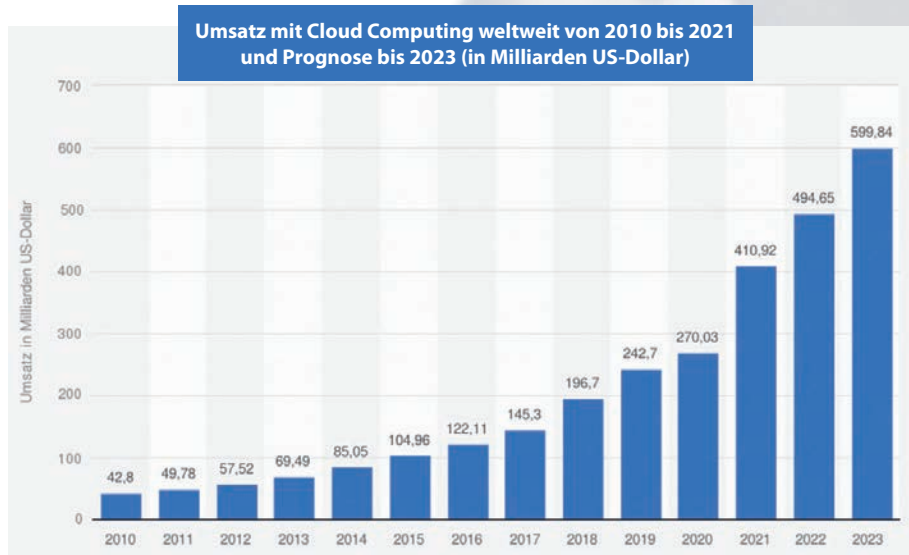
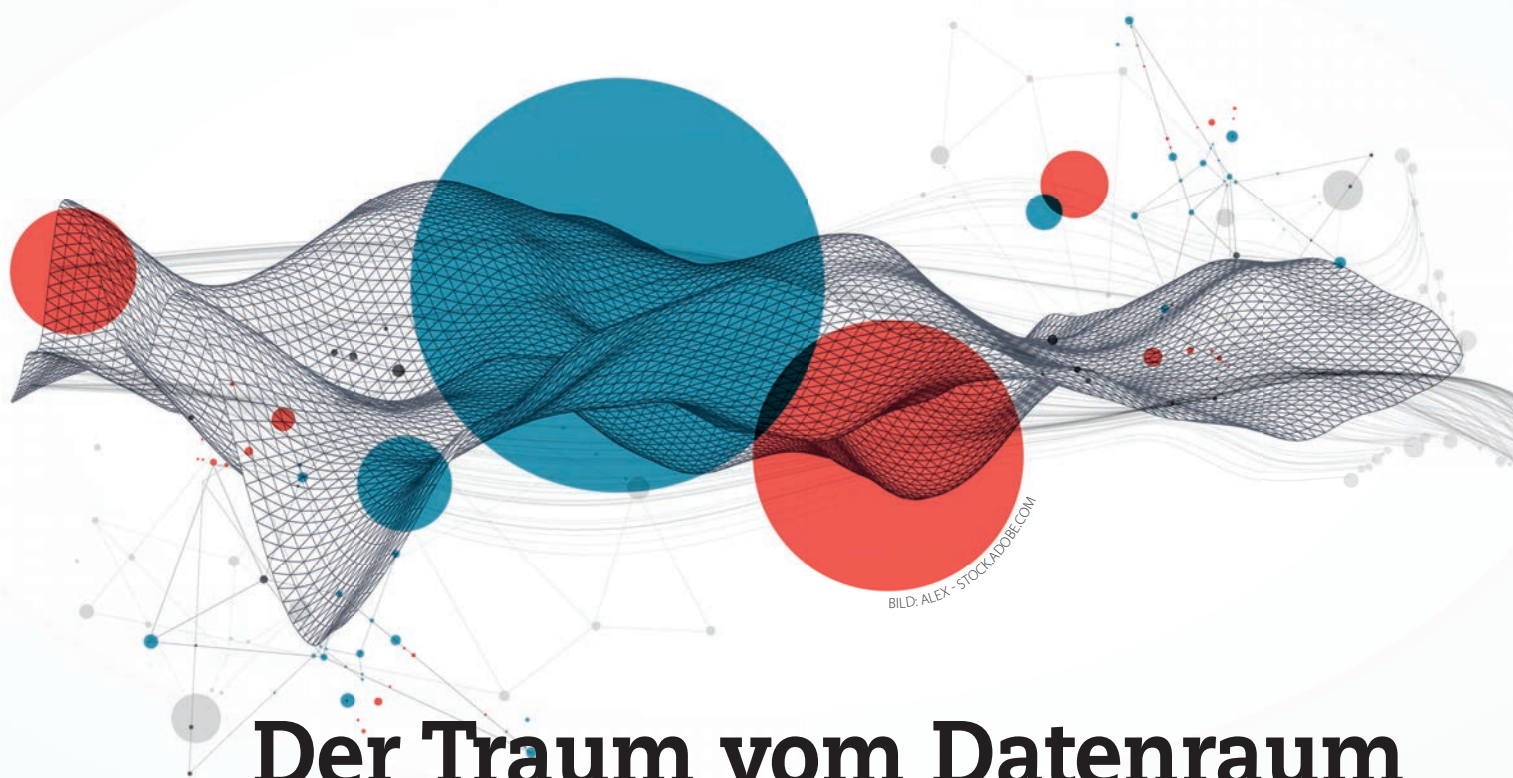


BILD: GARTNER / STATISTA



# Der Traum vom Datenraum

Neue Datenräume, neue Geschäftschancen. Hinter dieser scheinbar einfachen Formel verbirgt sich ein höchst komplexes Unterfangen. Denn es müssen die Konditionen geklärt sein, unter denen Daten Dritten zur Verfügung gestellt werden. Und genau das will, stark verkürzt, Gaia-X leisten.

„**Gaia-X entstand** aus der Fragestellung, wie datensouverän Europa geopolitisch agieren kann. Neben Deutschland, haben auch andere europäische Länder Forschungsprojekte an den Start gebracht, um dies künftig zu ermöglichen“, erläutert Steven Handgrätinger, Bereichsvorstand Public Sector bei Bechtle. Der Dienstleister ist beim Gaia-X-Forschungsprojekt Possible an Bord und hat, unabhängig von Gaia-X, gerade erst mit dem Projekt Kolibri einen ersten Datenraum-Prototypen für den Bildungssektor an den Start gebracht. In eine ähnliche Kerbe schlägt Iris Plöger, Mitglied der Hauptgeschäftsführung des Bundesverbands der deutschen Industrie, auf der GFXSConnect22, einer Veranstaltung des Eco Verbandes: „Ziel muss es sein, die digitale Souveränität zu stärken, ohne Protektionismus und Autarkie Vorschub zu leisten. Dafür ist eine enge Kooperation zwischen verschiedenen Akteuren unabdingbar.“ Wichtig sei, digitale Souveränität nicht in nationalen Grenzen zu denken, sondern einen europäischen und international ausgerichteten Ansatz zu verfolgen. In den vergangenen Jahren wurden die Grundlagen geschaffen, um dann konkrete Projekte umzusetzen. Wichtig sei, betont Plöger, „dass Gaia-X jetzt schnell in die Umsetzung kommt.“

„**Datenschutz haben** Amerikaner, Russen und Chinesen auch“, ordnet Rainer Sträter vom deutschen Cloud-Provider Ionos ein. „Aber wir hier in Europa haben eine andere Interpretation, ein anderes Verständnis dieser Werte. Wenn wir in Europa unseren Kunden Datenökosysteme zur Verfügung stellen wollen, möchten wir diese nach unserem Werteverständnis den Kunden anbieten. Das ist die Grundidee.“ Um das zu können, braucht man zunächst einen Konsens und eine Art „Container“ in dem man so etwas dann entwickeln und umsetzen kann. Zunächst wurden nun dafür die so genannten Gaia-X Federation Services (GXFS) entwickelt. Das Projektmanagement dafür liegt beim Eco Verband, wie Andreas Weiss, dort Leiter digitale Geschäftsmodelle, beschreibt: „Wir koordinieren die Ausarbeitung von Servicespezifikationen und haben fünf Kernservices erarbeitet.“ Dazu gehört das Identitäts- und Vertrauensmanagement, genauso wie ein Katalog aller verfügbarer Services, Compliance-Regeln und ein Datenaustausch-Konzept. „Hier geht es vor allem darum, die weitere Entwicklung zu unterstützen und die Interoperabilität aller Gewerke zu gewährleisten“, erläutert Weiss die Wichtigkeit der Federation Services.





**Auf dieser Basis** wird in einzelnen Projekten weitergearbeitet. Hier sind inzwischen zahlreiche Unternehmen vertreten, so auch Ionos und Bechtle. „Keines der Industrieunternehmen, das im Konsortium dabei ist, macht das wegen der Förderung, räume ich gleich mal mit einem Vorurteil auf“, schmunzelt Sträter. Die Intention ist eine andere. „Hier können wir in Konsortien arbeiten, die sich sonst so nicht finden würden. Wir können Herausforderungen gemeinsam mit Mitbewerbern lösen, die wir allein wirtschaftlich nicht stemmen könnten. Und das, ohne dass das kartellrechtlich bedenklich wäre. Denn alles ist ja öffentlich und jeder kann Mitglied werden.“

**Aktuell sind dies** 350 Unternehmen, auch die Hyperscaler sind an Bord. Ein Kritikpunkt, der immer wieder genannt wird, den Sträter aber deutlich relativiert. Denn mit dabei sein dürfen alle, abstimmen nur Unternehmen, deren Muttergesellschaft den Sitz in Europa hat. Auch wenn die Hyperscaler damit bei der Abstimmung über Regeln und Standards außen vor sind, betont Sträter „Wir sind da mit einem soliden Wertesystem unterwegs und das heißt auch Inklusion. Wir sind als Land stark im Export unterwegs, über Europa hinaus. Da ist es doch viel cleverer, wenn wir ein Wertesystem liefern, das die Hyperscaler adaptieren können. Wir wollen keinen wirtschaftlichen Protektionismus, sondern wir wollen unseren Kunden die Möglichkeit geben, nach unseren Werten zu leben, Daten zu verarbeiten und hosten.“ Und vor allem eine Cloud-Alternative bieten, die es bislang in dieser Form eben nicht gab. „Wenn wir es schaffen, Interoperabilität und Portabilität zu schaffen, das sind ja die Kernziele von Gaia-X, dann reißen wir das Vendor Lock-in ein und spielen den Vorteil föderierter Ökosysteme aus“, begeistert sich Sträter.

**Und auch wenn die Kritik** an Gaia-X von Anfang an war, dass die Umsetzung dieses europäischen Datenraumes lange dauern könnte, nimmt das Ganze langsam Formen an. Mit den GXFS stehen die Grundlagen fest, Projekte laufen und inzwischen gibt es auch schon funktionierende Datenräume wie den Marispace-X und Catena-X.

Letzteres ist ein Projekt für den Automobil-Sektor, das aber das Potenzial habe, auch für andere Branchen adaptiert werden zu können, wie Dr. Franziska Brantner, Parlamentarische Staatssekretärin im Bundesministerium für Wirtschaft und Klimaschutz, auf der GXFSConnect 2022 des Eco Verbandes verdeutlichte. Das macht auch Handgrätinger klar, wenn er über die Bechtle-Beteiligung an „Possible“ mit seinen Elementen Bildung, Verwaltung und KMU spricht. Denn natürlich muss sich das irgendwann auch einmal auszahlen. Aber da steht für Handgrätinger fest: „Dadurch, dass man über diese Projekte redet, kommen auch Industrieunternehmen auf uns zu und informieren sich.“ Hier lauert also großes Geschäftspotenzial. Auch deshalb „werden wir alles daransetzen, dass wir ein attraktives Produkt entwickeln. Zwar in erster Linie für die beiden so genannten „Domänen“ Bildung und Verwaltung. Aber eben auch mit Potenzial für die Industrie, genauer KMUs. Das demonstrieren wir mit einem Use Case für KMU innerhalb des Förderprojektes.“

**Bei diesen Projekten** wird deutlich: es geht um einen Markt, dessen Schmerz nicht die Cloud-Infrastruktur ist, sondern der Datenaustausch mit mehreren Akteuren. Sträter: „Heute tauschen wir Daten meist bilateral aus. Verträge werden einzeln ausgehandelt. Das ist teuer und macht die Sache wirtschaftlich unattraktiv.“ Das andere Extrem wäre, alle Daten in einen Pool zu werfen auf den jeder zugreifen darf. Aber das macht keiner. Denn wenn Daten das neue Gold sind, warum sollten Unternehmen diese kostenfrei zur Verfügung stellen. „Das wird nicht passieren“, ist sich Sträter sicher. „Das Konzept des Data Lake ist tot. Wir reden heute über Data Meshes oder Data Spaces. Das sind verteilte Datenquellen, die Eigentum der jeweiligen Unternehmen bleiben. Dann regle ich nur noch wer, wann, wie lange auf welcher meine Daten zugreifen darf, und kann diese entsprechend monetarisieren.“

„Wenn wir in Europa unseren Kunden Daten-ökosysteme zur Verfügung stellen wollen, möchten wir diese nach unserem Werteverständnis den Kunden anbieten.“

Rainer Sträter,  
Senior Vice President  
Cloud Services and  
Global Platform Hosting  
bei Ionos

„Dadurch, dass man über diese Projekte redet, kommen auch Industrieunternehmen auf uns zu und informieren sich.“

Steven Handgrätinger,  
Bereichsvorstand  
Public Sector bei Bechtle



Mehr zu Gaia-X  
beim BMWK:  
[www.it-business.de/gaia/](http://www.it-business.de/gaia/)  
Autor:  
Sylvia Lösel





BILD: IPOBBA - STOCK.ADOBE.COM

# Hilfsbereite Lotsen im Cloud-Universum

In der Cloud ist die Distribution als Mittler zwischen Anbietern und Channel besonders gefordert. Ausbildung, Beratung und White Label Services sind Leistungen, auf die viele Systemhäuser in diesem Geschäft angewiesen sind.

**Um die Cloud** ranken sich Mythen und Irrtümer. Wer etwa meint, man müsse eine lokale Anwendung nur einfach zu einem Hyperscaler shiften und könne dann in der neuen Umgebung alles wie gehabt betreiben, der täuscht sich. Diese Vorstellung scheint im Channel aber noch verbreitet zu sein. So erlebt es das Cloud-Team von Ingram Micro nicht selten, dass „ein Partner wegen einer Konfiguration anfragt, die eine Eins-zu-eins-Replikation der bestehenden On-Premises-Infrastruktur ist“, berichtet Igor Guss, Business Group Manager IaaS bei dem Dornacher Distributor.

„Sicherlich ein denkbares Vorgehen“, sagt der Experte. Das Angebot würde dann allerdings „für den Kunden sehr teuer werden“. Denn in einer On-Premises-Umgebung werden den virtuellen Maschinen üblicherweise mehr Ressourcen zugewiesen, als sie im Normalbetrieb brauchen. Eine Überprovisionierung ist in der Cloud aber nicht nötig, da sich die Ressourcen beliebig skalieren und daher flexibel der Last anpassen lassen. „In solchen Fällen greifen wir dann sofort zum Hörer und zeigen dem Partner die Möglichkeiten auf, wie das Projekt zweckmäßig angepackt werden kann.“ Allein schon durch das richtige Sizing der

Instanzen lasse sich der Preis für das Angebot um etwa ein Drittel reduzieren, erläutert Guss. Wenn die Umgebung dann steht, könne der Partner durch automatisiertes An- und Abschalten von Maschinen oder den Einsatz reservierter Instanzen zu festen Laufzeiten die Kosten für seinen Kunden weiter optimieren.

**Zu den Leistungen** von Distributoren gehört neben Einkauf, Vertrieb und Logistik seit jeher auch die Wissensvermittlung. Sie bringen Fachhändlern neue Technologien und deren spezifische Eigenheiten nahe, sei es durch Trainings, sei es durch individuelle Beratung im Tagesgeschäft, so wie in dem geschilderten Beispiel. Letzten Endes schaffen die ITK-Großhändler so die Voraussetzungen für ihre künftigen Umsätze. Das ist in der Cloud nicht anders. Allerdings handelt es sich hier um mehr als eine neue Technologie oder einen neuen Ansatz. Die Cloud verändert von Grund auf die Art und Weise, wie IT bereitgestellt und genutzt, wie Infrastrukturen aufgebaut und betrieben, wie Anwendungen designt und entwickelt werden. Spätestens als Microsoft im Herbst 2015 das Programm für Cloud Solution Provider (CSP) einführte, war absehbar, dass der Paradig-



menwechsel nun auch die Masse der Partner erreichen und ihr Geschäft langfristig transformieren würde.

**Auch Cloud Provider** sind somit auf Distributoren angewiesen, weil sie den Channel in der Breite zu diesem Geschäft befähigen. Kleine und mittelgroße Systemhäuser sind häufig nicht in der Lage, die dafür notwendige Kompetenz eigenständig aufzubauen. Darüber hinaus wickeln Distributoren das Transaktionsgeschäft ab, die unzählig vielen Bestell- und Abrechnungsprozesse. Oft betreiben sie dafür elektronische Marktplätze. So hat Microsoft im Rahmen des CSP-Programms in Deutschland inzwischen 24 sogenannte Indirect Provider gezeichnet, die Angebote wie Azure oder Microsoft 365 an Reseller vertreiben dürfen. Zu diesem Kreis zählen neben den Distributoren ADN, Also, Arrow, Bluechip, Ingram Micro, Komsa, Tarox, Tech Data, Westcon und Wortmann auch größere Lizenzhändler und Service Provider.

**AWS konzentriert** sich dagegen in Deutschland auf Partnerschaften mit Arrow, Ingram Micro und Tech Data. Google Cloud hat bislang noch keinen Distributor, wird aber voraussichtlich noch in diesem Herbst die Zusammenarbeit mit Tech Data aufnehmen. Über IT-Großhändler vertreiben auch Cloud-Anbieter wie IBM (Arrow, Ingram Micro, Tech Data), Oracle (Arrow, Tech Data), Exoscale powered by Lenovo (Also, Bytec, Tech Data, TIM), Ionos Cloud (ADN, Brainworks, Infinigate) und Plussserver (TIM). Nicht zuletzt bietet Wortmann dem Channel die eigene Terra Cloud an.

**Die Dienstleistungen**, die die Distributoren neben der Vermarktung der Cloud-Services anbieten, unterscheiden sich in Art und Umfang. Besonders breit ist das Portfolio bei Ingram Micro und Tech Data. Generell tun sich Broadliner in dieser Hinsicht wegen ihrer Größe und internationalen Reichweite leichter. Sie unterhalten Competence Center, auf deren Expertise die Cloud-Teams in den einzelnen Ländern zugreifen können. Dabei bieten die Distributoren als White Label auch Leistungen an, die Partner idealerweise selbst erbringen sollten. Dazu zählen Professional Ser-

vices auf Gebieten wie Assessment, Architekturdesign und Migration sowie Managed Services, also Betriebsleistungen.

„**Wir bauen unser Service-Portfolio immer weiter aus**“, betont Stefan Bichler, Director Security, Cloud & Software bei Tech Data Deutschland. Dafür gibt es offenbar einen Bedarf. Auch wenn die Cloud den Channel bereits seit einigen Jahren beschäftigt, hat längst noch nicht jeder ein solides Grundwissen erworben. „Wir sehen bei den Partnern die ganze Bandbreite, vom Absolute Beginner bis zum Cloud-Profi“, berichtet Bichler. „Beim Wissen öffnet sich die Schere sogar noch weiter.“ Allerdings gehen Systemhäuser, die zu wenig Cloud-Expertise erwerben, nach Überzeugung des Managers ein Risiko ein. Denn die Anfragen von Endkunden, die Workloads in die Cloud migrieren wollen, nehmen zu. Und viele Projekte werden derzeit von Cloud-Native-Partnern gewonnen. „Ein Systemhaus, das solche Anfragen seiner Kunden nicht bedienen kann, wird sie über kurz oder lang verlieren.“

**Bei den Hyperscalern** helfen Distributoren dem Fachhandel nicht zuletzt dabei, die Komplexität ihrer Ökosysteme handhabbar zu machen. So bieten AWS und Microsoft den Partnern in ihren Programmen viele Möglichkeiten der Zertifizierung und Spezialisierung, die auf den Status einzahlen und die zugleich für Rabatte und Fördergelder relevant sind. Wer sich damit nicht auskennt, tut sich nicht nur schwer, sein Potenzial sinnvoll zu entwickeln. Er läuft auch Gefahr, Geld liegenzulassen. Umso hilfreicher ist es, wenn Distributoren die Partner durch die umfangreichen Programme navigieren. 2022 ist diese Leistung besonders wertvoll. Zu Beginn des Jahres hat das AWS Partner Network (APN) eine neue Struktur erhalten. Und der Rivale reformiert gerade das Microsoft Partner Network (MPN) und baut es mit vielen Neuerungen zum Microsoft Cloud Partner Program (MCP) um.



**Mehr unter:**  
<https://voge.ly/vgll7a5/>

**Autor:**  
Michael Hase



BILD: INGRAM MICRO



**Igor Guss, Business Group Manager IaaS bei Ingram Micro Deutschland**

Systemhäuser stehen unter Zugzwang: Wenn sie Kunden nicht in die Cloud bringen, weil ihnen dazu noch Knowhow und Skills fehlen, besteht das Risiko, dass ihnen Born-in-the-Cloud-Dienstleister die Projekte streitig machen.

BILD: TECH DATA



**Stefan Bichler, Director Security, Cloud & Software bei Tech Data Deutschland**

Mein Appell an Systemhäuser lautet, dass sie vor der Cloud nicht die Augen verschließen. Ansonsten können sie noch drei, vier Jahre lang Hardware und Service-Verträge verkaufen. Aber danach wird es für sie eng.



# Zwei mal Windows aus der Microsoft-Cloud

Microsoft bietet mit Windows 365 und mit Azure Virtual Desktop gleich zwei Desktop-as-a-Service-Lösungen an. Sie sind jeweils für unterschiedliche Zielgruppen geeignet. Hier gilt es, die richtige Wahl zu treffen.

**Anfang August 2021** hat Microsoft die Bereitstellung von Windows 365 gestartet, einen Service der Anwendern einen nutzerbasierten virtuellen Rechner mit Windows 10 oder Windows 11 aus der Cloud zur Verfügung stellt. Mit der Lösung, die auf Microsoft Azure läuft, erhalten Firmen oder Einzelanwender konfigurierbare Cloud-PCs unterschiedlicher Leistungsklassen, die von verschiedenen Geräten aus zugänglich sind. Dabei favorisiert Microsoft natürlich Windows-Rechner als Einstiegspunkt und belohnt Nutzer auch mit einem Rabatt.

**Bei Windows 365 gibt es zwei Varianten:** Business und Enterprise. Erstere ist für kleinere Unternehmen ohne eigene IT-Abteilung bestimmt, die einen schnell einsetzbaren Cloud-PC ohne großen Verwaltungsaufwand benötigen. Das Limit liegt bei 30 Cloud-PC-Arbeitsplätzen. Es gibt verschiedene Basispakete mit zwei, vier oder acht virtuellen CPUs, die individuell angepasst werden können, etwa durch zusätzliche vCPUs, mehr RAM und einen größeren Massenspeicher. Abhängig von der Konfiguration gibt es feste Monatspreise, die im Abo bezahlt werden. Die ausgehende Netzwerknutzung ist im Preis enthalten, aber abhän-

gig von der Zahl der vCPUs auf 20 bis 70 GB pro Monat limitiert. Eine Veränderung der Leistung und Speichergröße eines Cloud-PC ist bei Windows 365 Business nicht möglich. Diese Option, und auch nur eine Skalierung nach oben, ist derzeit Windows 365 Enterprise vorbehalten. Diese Cloud-PC-Version ist für größere Unternehmen bestimmt. Hier müssen die Benutzer über eine Windows-Enterprise-Lizenz verfügen und für den Microsoft Endpoint Manager sowie Azure AD P1 lizenziert sein. Der Netzwerk-Traffic läuft über das Azure VNet und wird separat abgerechnet.

**Die Basis von Windows 365** ist der Azure Virtual Desktop, den Microsoft als eigenständigen Service weiter anbietet. Bei bereits vorhandenen Microsoft-365-Lizenzen der passenden Stufen oder Windows 10 VDA fallen Kosten lediglich für die Nutzung von Compute-, Storage- und Netzwerk-Ressourcen für die virtuellen Maschinen in Azure an. Dabei müssen die Administratoren die Kosten im Auge behalten, etwa indem sie die passenden Storage-Optionen wählen und gegebenenfalls verändern. Ein Beispiel ist das Verlagern nicht genutzter VMs von SSD- auf günstigeren HDD-Speicher. Die Kosten für Azure Virtual Desktop sind



also stark von der Nutzung abhängig und können so höher oder niedriger sein, wie bei Windows 365 Enterprise. Für potenzielle Nutzer von Windows 365 Business ist Azure Virtual Desktop dagegen kaum eine Alternative.

**Einige Neuerungen** in Windows 365 sollen den Umgang mit dem Cloud-PC vor allem für hybride Arbeitskonzepte vereinfachen. So hat Microsoft eine Windows-365-App angekündigt, die auf Windows-Rechnern den schnellen Start eines virtuellen PCs in der Cloud vom Startmenü oder der Taskleiste aus ermöglicht, ohne erst einen Umweg über den Webbrowser oder den Microsoft-Remotedesktop zu nehmen. Mit der Funktion Windows 365 Switch wird ein Windows 365 Cloud PC in den Task Switcher von Windows 11 eingebunden. Das ermöglicht einen schnellen Wechsel zwischen lokalem und virtuellem Rechner. Für Rechner, die primär als Basis für den Cloud-PC dienen, kommt mit Windows 365 Boot die Option, ihn in das Bootmenü von Windows aufzunehmen und sogar als Standardauswahl zu setzen. In Windows 365

Enterprise gibt es zudem die Option der Nutzung virtualisierungsbasierter Workloads mittels Hyper-V, dem Windows Subsystem für Windows oder der Sandbox.

**Die Liste der Technologiepartner** für Windows 365 hat Microsoft in den vergangenen Monaten ebenfalls erweitert. Zu ihnen zählen beispielsweise Igel mit einer angepassten Igel-OS-Version sowie Nerdio, Netapp mit Spot und Citrix mit Angeboten für die effiziente Verwaltung der Cloud-PCs. Zudem soll Citrix HDX künftig das Streaming von grafisch oder multimedial anspruchsvoller Anwendungen verbessern. Systemhäuser können Windows 365 durch zusätzliche Dienste für ihre Kunden anreichern und etwa Datensicherungen anbieten. MSPs haben die Möglichkeit, Windows-365-PCs für Kunden in Lighthouse zu verwalten.



**Mehr unter:**  
[www.it-business.de/-a-1110434/](http://www.it-business.de/-a-1110434/)

**Autor:**  
Klaus Länger



## UNSERE PARTNER SIND SMARTER!

### Verpassen Sie nicht, mit NFON voll durchzustarten!

Partner waren, sind und bleiben unsere Basis für Erfolg! Deshalb bedeutet eine starke Partnerschaft für uns, gemeinsam zu wachsen und Ziele zu erreichen. Unser Fokus dabei: Ihre Unternehmensentwicklung. Wir belohnen Ihr Engagement und bieten Ihnen das beste Partnererlebnis.

Um unseren Partnern den besten Start für Ihre NFON Reise zu ermöglichen, haben wir exklusive Incentives definiert.



#### Exklusive Q&A Session zum Start Ihrer NFON Reise.

Eine exklusive Session, in der ein NFON Partner Manager und ein NFON Technical Consultant Ihnen Frage und Antwort stehen.



#### Exklusive Unterstützung für Ihr Pilot Projekt mit NFON.

Erhalten Sie echten VIP-Support für Ihr allererstes Projekt mit NFON. Profitieren Sie von dem Wissen unserer Vertriebs- und Technik-Experten.



#### Education for Free!

Absolvieren Sie innerhalb von sechs Monaten erfolgreich unsere Pflichtschulungen und NFON erstatten Ihnen die Kosten.

**JETZT PARTNER WERDEN!**





BILD: ALEX - STOCK.ADOBE.COM

# Hyperscaler als Security-Provider

Marktforscher sehen AWS inzwischen als führenden Anbieter auf dem Cybersicherheitsmarkt. Sind also Cloud-Provider die Security-Anbieter der Zukunft? Was bedeutet die Entwicklung für den Security-Channel?

**Eine Studie von Juniper Research** besagt, dass die weltweiten Unternehmensausgaben für Cybersicherheit im Jahr 2027 mehr als 226 Milliarden US-Dollar betragen werden, gegenüber 179 Milliarden US-Dollar im Jahr 2022. Dieses Wachstum von 26 Prozent in den nächsten fünf Jahren spiegelt die zunehmende Reife des Cybersicherheitsmarktes wider, der sich mit dem Aufkommen neuer Bedrohungen weiterentwickelt, so die Marktforscher.

**Diese Umsatzprognose** für Cybersicherheit ist weniger eine Überraschung als das „Competitor Leaderboard“ von Juniper Research für den Cybersicherheitsmarkt. Dort nennen die Marktanalysten als die fünf führenden Security-Anbieter AWS, IBM, Cisco, Oracle und Sophos. Dazu erklärte die Co-Autorin der Studie Damla Sat: „Cloud Computing hat Unternehmen transformativ verändert, daher ist es nicht verwunderlich, dass zwei der größten Cloud-Computing-Anbieter, AWS und IBM, auch im Bereich der Cybersicherheit führend sind.“ Damla Sat sieht die starke Position von Cloud-Anbietern im Security-Markt als logische Folge der erforderlichen Cloud-Sicherheit: „Für Cloud-Anbieter ist effektive Cybersicherheit eine

Grundvoraussetzung – durch das Angebot interner Cybersicherheitslösungen profitieren AWS und IBM von ihrer bestehenden großen Nutzerbasis.“

**Tatsächlich ist Security** im Cloud Computing für die Anwender gleich mehrfach ein Thema: So spielen die Themen Datensicherheit und Datenschutz eine entscheidende Rolle bei der Wahl der Cloud-Lösung, daher gelten Vertrauen in Sicherheit und Compliance des Cloud-Providers für 95 Prozent als Must-have, so der Cloud-Monitor 2022 von Bitkom und KPMG. Aber nicht nur das: Viele Cloud-Nutzer erhoffen sich durch die Verwendung von Cloud-Services auch eine Verbesserung ihrer eigenen Security. Der Cloud-Monitor gibt auch hierfür ein Beispiel: Knapp 40 Prozent der befragten Unternehmen berichten, dass sie in den vergangenen zwölf Monaten Attacken durch Ransomware ausgesetzt waren. Aber hier hilft die Cloud, denn 72 Prozent konnten die Angriffe mit Cloud-Security-Maßnahmen abwehren. Aus Anwendersicht ist es also durchaus ein logischer Schluss, dass Cloud-Provider zunehmend auch als Security-Anbieter gesehen werden. Doch sehen dies die Partner des Hyperscalers AWS genauso?



Von der Positionierung von AWS als führendem Security-Anbieter ist Benjamin Hermann, Geschäftsführer des IT-Beratungsunternehmens Zoi TechCon, nicht überrascht: „Die Größe und auch die Anzahl der Services, verbunden mit echtem Kundenmehrwert, sind da.“ Das sieht auch Sven Ramuschkat, Geschäftsführer der Tecracer Group so: „Durch die hohen Investitionen in eigenes Knowhow, eigene Software sowie Hardware bleibt

len-Management ist bereits aber da.“ Gleichzeitig profitiert die ganze Security von der Cloud: „Der Gang in die Cloud zwingt dazu, aufzuräumen. Es ist eben kein pures Lift & Shift, sondern es zwingt zur Dokumentation und Analyse der eigenen IT-Infrastruktur. Die Cloud lädt ein, Dinge richtig zu bauen. Alleine dieser kulturelle Mehrwert zur ‚Selbstreinigung‘ zahlt auf die IT-Security ein“, so Hermann.

## >> Die Cloud lädt ein, Dinge richtig zu bauen. Allein dieser Mehrwert zur ‚Selbstreinigung‘ zahlt auf die IT-Security ein.

Benjamin Hermann, Geschäftsführer bei Zoi TechCon



BILD:ZOI

AWS vorne. Die AWS-eigene Hardware, zum Beispiel Graviton 3, besitzt Features wie ‚always-on memory encryption‘, was auf wenigen Technologieplattformen zu finden ist.“ Hermann sieht eine Vielzahl von leistungsstarken Security-Funktionen bei AWS und betont: „Die Funktionen kommen meist recht grün und unscheinbar, wachsen dann aber, wie immer bei AWS, so wie die Kunden sie brauchen.“ Als Beispiel nennt Hermann die AWS WAF. „Sie war zu Beginn uninteressant für viele Fälle, da man viele Regeln selber bauen musste. Nun aber gibt es ein wachsendes Ecosystem an Managed Rules.“ Die Vorteile macht er deutlich an einem Beispiel: „Mit Log4J war direkt eine Managed-Regel da, die schneller und hochwertiger gepflegt wurde, als bei so manchem Managed Security Provider.“ Ramuschkat betont weitere Vorteile: „Die AWS-Security-Lösungen sind integriert in AWS. Daher kann zum Beispiel ein Container Image, welches in AWS gespeichert wird, direkt und kontinuierlich mit AWS Inspector 2 auf Schwachstellen gescannt werden. Dabei gibt es keine der üblichen Kompatibilitätsprobleme, wie sie zwischen verschiedenen Anbietern auftreten.“

**Doch lohnt sich** eine AWS-Partnerschaft alleine schon wegen der Security-Funktionen? Hermann weist auf den Cloud-Fokus der Security-Funktionen hin: „AWS bietet ein exzellentes Security-Ökosystem für sichere Cloud-Lösungen. On-Prem ist dabei nicht oder kaum im Fokus.“ Doch es kommt Bewegung in die Security von AWS, wie Hermann erläutert: „Basierend auf dem Shared-Responsibility Model geht AWS erst langsam in die Kunden-Felder. Endpoint Protection oder XDR fehlen zum Beispiel bisher, ein Schwachstel-

Ramuschkat macht seine Sicht einer AWS-Partnerschaft deutlich: „AWS-Partner sollte man werden, wenn man wesentliche Teile der AWS-Plattform für seine Kunden nutzen möchte. Die Anwendungen der Kunden müssen bestmöglich geschützt werden, sowohl gegen Konfigurationsfehler als auch gegen Angriffsvektoren. Hier bietet AWS, bis auf das Malware-Scanning, hervorragend unterstützende Security Services.“ Entsprechend besteht Bedarf für weitere Security-Lösungen Dritter, denn zum Beispiel Malware-Scanning für hochgeladene Inhalte auf S3 oder EC2 werden von AWS aktuell nicht angeboten, so Ramuschkat.

**Keine Frage: Die Cloud-Provider** werden sich nicht zu alleinigen Security-Anbietern entwickeln. Doch die Cloud transformiert Security. So wie es die Entwicklung zu Hybrid Cloud Computing gibt, findet eine Verschiebung hin zu einer hybriden Security statt, wobei der Cloud-Anteil durchaus zunehmend von den Hyperscalern kommen kann. Aber es wird nicht den einen Cloud-Security-Anbieter geben. Vielmehr entsteht wie bei dem Multi-Cloud-Ansatz ein Multi-Security-Ansatz, an dem Cloud-Anbieter wie AWS einen wichtigen Anteil haben werden. Der Security-Channel sollte sich deshalb vermehrt mit den Security-Portfolios der Cloud-Anbieter befassen, ebenso sollte der Cloud-Channel die Chancen des Security-Marktes nicht ungenutzt lassen.



**Interview mit**  
**Michael Hanisch, AWS:**  
[www.it-business.de/Hanisch/](http://www.it-business.de/Hanisch/)  
**Autor:**  
Oliver Schonscheck



# Kommunikation zwischen alt und modern

Mit dem modernen Arbeitsplatz hat sich die Kommunikation in Unternehmen geändert und die kommt jetzt meistens aus der Cloud.



BILD: KIMSONGSAK - DANIEL BERKMANN / SKELLEN / NATALYA YUDINA - STOCKADOB.COM / [M] J RATH

**Der feste Arbeitsplatz** hat ausgedient. Heutzutage wird mit Laptop oder Tablet von überall aus gearbeitet. Mobiles und insbesondere hybrides Arbeiten sind zum festen Bestandteil geworden. Grundlage dafür sind geeignete Lösungen für Kommunikation und Zusammenarbeit. Dabei planen Unternehmen vor allem Investitionen in Kommunikationsplattformen aus der Cloud, wie aus dem „Recruit, Retain and Grow“-Report von Poly hervorgeht. 92 Prozent der dort befragten Entscheider investieren in Software für die Zusammenarbeit sowie Cloud-Anwendungen.

**Die Vorteile** von Cloud-basierte Telekommunikationslösungen sind vielfältig, wie Sebastian Tietz, CMO & Head of Strategic Partnership bei Atos Unify erklärt: „Dabei sind Flexibilität, Skalierbarkeit, überschaubare Kosten ohne Anfangsinvestment und Unterstützung von hybriden Arbeitsmodellen ausschlaggebend für die Entscheidung.“ Ferner hat der Einsatz von UCC-Tools mehr Vorteile, als nur standortunabhängiges Arbeiten zu ermöglichen. Kunden versprechen sich effizientere Teamarbeit, höhere Flexibilität sowie neue Service-Möglichkeiten.

**Doch die Kommunikationslösungen** wurden in den vergangenen beiden Pandemie-Jahren oft schnell und zur Überbrückung eingeführt. Jetzt treten in Firmen die Schwachstellen zu Tage: „Ein wahrer Flickenteppich verschiedenster Anwendungen, Dienste und Applikationen“, beschreibt Erik Thiele, Director Competence Center UCC bei dem Münchner Dienstleister Cancom die Lage. „Das stellt nicht nur die IT, sondern auch die Anwender vor Herausforderungen.“ Nun geht es laut Thiele verstärkt um die Integration der Lösungen im Sinne ganzheitlicher UCC-Konzepte und um die nahtlose Anbindung an Besprechungsräume.

**Die immer komplexer** werdenden Anforderungen an die IT sowie der Mangel an Fachkräften lassen den Bedarf an Managed Services wachsen. Hinzu kommt, dass Unified Communication & Collaboration oft sowieso als Unified Communications as a Service (UCaaS) aus der Cloud bezogen wird. „Für die Bereitstellung und den Betrieb von UCC-Lösungen kommen mittelfristig eigentlich nur noch Managed-Service-Konzepte infrage“, ist sich Markus Etzel, Teamleiter Unified Communications bei HanseVision, ein Unternehmen der Bechtle Gruppe sicher. „Nur so lassen sich moderne Kommunikations-Infrastrukturen kostenoptimiert skalieren, ausbauen und können technologisch immer auf dem neuesten Stand gehalten werden. Auch Collaboration-Angebote, die infrastrukturell aus der Cloud kommen, müssen, unter Berücksichtigung lokaler Gegebenheiten und Anforderungen, an bestehende Security-Richtlinien angepasst und entsprechend konfiguriert werden.“ Demnach wird die Nachfrage nach wiederkehrende Kommunikationsleistungen aus der Cloud weiter zunehmen.



**Mehr unter:**  
<https://voge.ly/vglfG73/>

**Autor:**  
Ann-Marie Struck



Daten-Management und Cloud-Computing:

# Das sollten KMUs beachten

Gastbeitrag von Wasabi Technologies CEO David Friend

Kleine und mittelständische Unternehmen greifen bei der Wahl einer Datenmanagement-Strategie in den letzten Jahren verstärkt auf Cloud-Services zurück, äußern aber immer noch Bedenken in Bezug auf Datensicherheit und technische Umsetzung.

## Eine Frage der Strategie

Entscheiden sich Unternehmen für eine Datenmanagement-Strategie, haben sie die Wahl: Verwalten sie Daten über ein lokales Rechenzentrum (On-Premises) oder verlagern sie das Datenmanagement an einen spezialisierten Service-Provider (Cloud-Computing)?

Jede Entscheidung birgt ihr Für und Wider: Inhouse-Lösungen sind auf Hard- und Softwareausstattung der Organisation zugeschnitten. Eine eigene Datenverwaltung bietet außerdem ein hohes Maß an Sicherheit und Compliance, da die Organisation ihre eigenen (hohen) Standards setzt, ist aber immer nur so gut wie das Personal, das sich um die Wartung der Infrastruktur kümmert.

In Zeiten von Homeoffice sind Flexibilität und schneller Zugriff gefragt. Der Vorteil Cloud-basierter Speicher: sie können mit Risiken wie menschlichem Versagen, Ransomware und anderen Gefahren umgehen. Eine dezentralisierte Cloud-Infrastruktur ist auch besser vor Katastrophen wie Überschwemmungen oder Bränden gesichert als ein lokales Rechenzentrum.

## Worauf kommt es bei der Wahl eines Cloud-Service-Providers an?

Die Anzahl an Cloud-Anbietern ist riesig: Im letzten Jahrzehnt stieg das globale Marktvolumen beim Umsatz von Cloud-Dienstleistungen konstant.

### Folgende Kriterien können helfen:

**1. Systemkompatibilität:** Unternehmen sollten wissen, wie gut sich das Anbieter-System in Ihre Infrastruktur integrieren lässt und einschätzen können, inwieweit sich die Firma in den nächsten Jahren entwickelt. Die Cloud-Strategie sollte mit dem Unternehmenserfolg skalieren – oder zumindest die Möglichkeit haben, sich anzupassen.

**2. Compliance:** Unternehmen müssen die Europäische Datenschutzgrundverordnung (DSGVO) beachten. Beim Umstieg in die Cloud braucht es daher einen Anbieter, der es Firmen erlaubt, die Speicherbedingungen und Compliance ihrer Daten zu berücksichtigen und verschiedene Serverstandorte abzudecken.

**3. Preis-Leistungs-Verhältnis:** Das richtige Angebot zu finden gilt vor allem beim Leistungsumfang: von der Hardware-Ausstattung über die Datensicherungsstrategien bis hin zur Wiederherstellungsgeschwindigkeit verlorener Daten. Firmen sollten sich stets umfassend über die Preis- und Leistungsmodelle am Markt informieren – auch wenn das manchmal heißt, Geschäftsbeziehungen zum aktuellen Lösungsanbieter zu beenden und sich einen neuen Partner zu suchen.

## Über Wasabi Technologies

Wasabi Technologies ist ein amerikanisches Hot-Cloud-Storage-Unternehmen mit Sitz in Boston, welches seinen Kunden eine schnelle, zuverlässige und kostengünstige On-Demand-Lösung zur Cloud-Speicherung anbietet. Das Unternehmen ermöglicht es, Daten zu speichern und bietet sofortigen, unkomplizierten Zugriff auf eine unbegrenzte Menge an Daten – konkurrenzfähig, kostengünstig und ohne versteckte Gebühren. Wasabi genießt bereits das Vertrauen von über Zehntausend Kunden weltweit und gilt als eines der am schnellsten wachsenden, visionärsten Technologieunternehmen. Das Unternehmen wurde von den Carbonite-Mitbegründern und Cloud-Storage-Pionieren David Friend und Jeff Flowers gegründet und hat bis heute fast 275 Millionen US-Dollar an Finanzmitteln erhalten. Wasabi Technologies ist stolzer Partner der Boston Red Sox und offizieller Cloud-Storage-Partner des Liverpool Football Club und der Boston Bruins.



BILD: WASABI TECHNOLOGIES

Für weitere Informationen zu Wasabi, besuchen Sie unsere Webseite [wasabi.com/de](https://wasabi.com/de) und testen Sie Wasabi 30 Tage kostenlos! [wasabi.com/sign-up](https://wasabi.com/sign-up)

### Folgen Sie uns auf Social Media:

**Twitter:** [https://twitter.com/wasabi\\_cloud](https://twitter.com/wasabi_cloud)  
**Facebook:** <https://www.facebook.com/WasabiCloud/>  
**Instagram:** [https://www.instagram.com/wasabi\\_cloud/](https://www.instagram.com/wasabi_cloud/)  
**The Bucket:** <https://wasabi.com/blog/>



# Aus der Quelle: Clouds von Storage-Herstellern

Einige Storage-Hersteller beginnen mit Public-Cloud-Angeboten auf der Basis ihrer eigenen Hardware. Zwei Beispiele dafür sind Seagate und Synology.

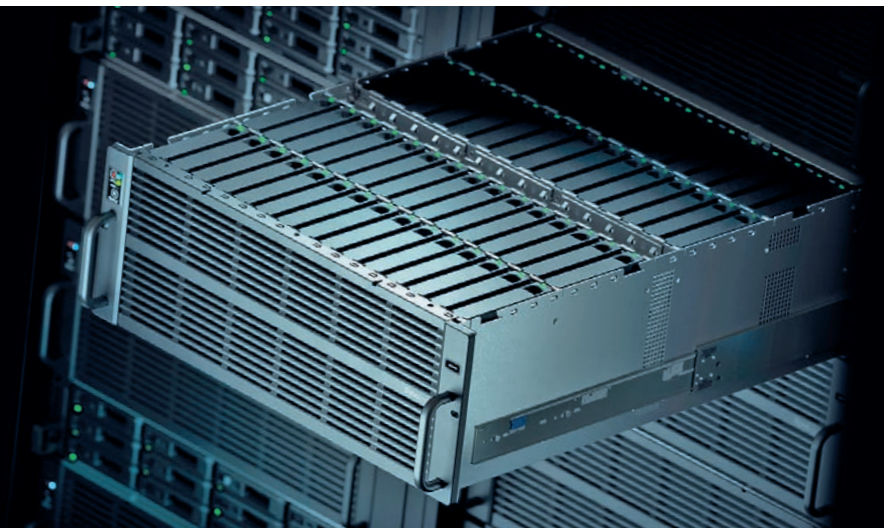


BILD: SYNOLOGY

**Seagate** ist einer der drei verbliebenen Hersteller von HDDs und ist auch im Geschäft mit Enterprise-SSDs vertreten. Die Firma gibt sich nicht mehr mit der Rolle als Zulieferer der Hyperscaler und anderer Public-Cloud-Anbieter zufrieden, sondern steigt mit der Lyve Cloud selbst in das Business ein. Sie ist ein HDD-basierter und bei Equinix gehosteter S3-kompatibler Objektspeicher für Einsatzszenarien mit großen Datenmengen. Seagate nennt hier Big Data mit großen Datensätzen, Media-Streaming sowie das Speichern von Videodaten für die Analyse. Eine weitere Verwendung ist die Konsolidierung älterer Backups auf Bändern. Die Migration der Daten von Tapes oder veralteten Speichermedien sowie die Digitalisierung analoger Medien bietet der Hersteller als zusätzlichen Service an. Ein weiterer Service ist Lyve Cloud Archive als reiner Archivierungs-Cloud-Speicher für große Mengen an Video- und Bilddaten, sekundäre Datensätze, Sicherungskopien und weitere Daten, auf die nicht häufig für Analysen oder Transaktionen zugegriffen wird. Im Gegensatz zu AWS Glacier bleiben die Daten unbegrenzt auf den HDDs und werden nicht auf Tape ausgelagert. Seagate betont, dass die Lyve

Cloud Host-agnostisch ist und dass außer der genutzten Kapazität keine Kosten anfallen, etwa für den Transport oder API-Calls. Schnittstellen gibt es zu AWS, Azure und der Google Cloud. Über den Lyve Cloud Marketplace können Kunden durch Seagate validierte Partnerlösungen von zum Beispiel Commvault, Veritas, Rubrik, Cohesity, Veeam oder Zadora ordern und abrechnen. Insgesamt sind zehn Regionen mit 16 Verfügbarkeitszonen geplant. Kunden und Partner haben zudem die Option, bei Equinix eigene Server für einen schnellen Zugriff auf die Daten in der Lyve Cloud aufzustellen.

**Synology** war bisher vor allem mit NAS-Geräten für Consumer und Storage-Lösungen für KMU aktiv. Nun nimmt die Firma mit einem High-Density-Storage-Server und der eigenen C2 Cloud Kurs auf das Enterprise-Segment. Mit dem HD6500, einem High-Density-Storage-System im Formfaktor 4U, macht Synology einen weiteren großen Schritt in das Enterprise-Segment. Ein erster Kunde für die Systeme ist die eigene Cloud-Business-Unit, die auf Basis der Systeme den neuen S3-kompatiblen Dienst C2 ObjectStorage anbietet, der sich im DACH-Markt ebenfalls primär an Enterprise-Kunden richtet. Bisher waren die C2-Cloud-Services als Ergänzung zu den NAS-Systemen und auf die Anforderungen von Heimanwendern sowie kleinen und mittleren Unternehmen ausgerichtet. Synology betreibt für den Service Rechenzentren in Europa, den USA und Asien. Synology wirbt für die eigene Cloud-Lösung vor allem mit deutlich günstigeren Preisen im Vergleich zu den Hyperscalern. Der Synology-Deutschlandchef Jeffrey (Ting-Wen) Huang betont dabei die transparente Preisgestaltung ohne Gebühren für API-Anforderungen und Datenlöschung.



**Mehr unter:**  
[www.it-business.de/-a-1115885/](http://www.it-business.de/-a-1115885/)

**Autor:**  
Klaus Länger



# TERRA CLOUD

## IT-LÖSUNGEN - AUS EINER HAND

### DIE CHANNEL CLOUD

Das Thema Sicherheit wird bei uns großgeschrieben, deshalb setzen wir auf unsere **Always-private-Strategie**. Jede Infrastruktur beinhaltet eine Firewall, so dass ein privates Kundenetzwerk inklusive VLAN und IP zugrunde liegt.

H

Housing

#### HOUSING

Die hochverfügbare Infrastruktur der TERRA CLOUD bietet Ihren Servern einen sicheren Standort.

Ho

Hosting

#### HOSTING

Erhalten Sie Ihre individuellen dedizierten Hardware Server mit gewünschter Konfiguration für maximale Flexibilität.

I

IaaS

#### IAAS

Mit unseren hochverfügbaren Cloud-Servern erhalten Sie skalierbare Rechenleistung in Form virtueller Maschinen. Flexibel, schnell, leistungsfähig.



Managed IaaS

#### MANAGED IAAS

Sie erhalten von uns Ihre dedizierte Umgebung inklusive des gesamten Managements und des automatisierten Deployments auf Virtualisierungsebene.

B

Backup

#### BACKUP

Wissen, wo Ihre Daten liegen. Professionelles und automatisiertes Backup aus der TERRA CLOUD.



Sicheres Netzwerk

#### FWAAS

Ihre Firewall ist als monatliche Leistung virtuell oder als Hardware Appliance erhältlich.

Erfahren Sie mehr zur **TERRA CLOUD**

Telefon: +49 5744.944 188 | E-Mail: [cloud@wortmann.de](mailto:cloud@wortmann.de)  
[www.wortmann.de](http://www.wortmann.de) | [www.terracloud.de](http://www.terracloud.de)

**WORTMANN AG**  
IT. MADE IN GERMANY.



Der Data Act der EU ist ein ambitionierter Antritt, denn es handelt sich um nichts weniger als eine grundlegende Neuregelung des Zugangs zu, beziehungsweise der Nutzung von Daten und der verbindlichen Schaffung einer neuen Cloud-Generation in Europa.



BILD: TEAMDAF - STOCK.ADOBE.COM

# Der rechtliche Rahmen für die Datenwirtschaft

**Der Data Act** ist ein konkreter Schritt zu dem im komplexen Grundsatzpapier „Eine europäischen Datenstrategie“ der EU-Kommission dargestellten Ziel der Sicherung der technologischen Zukunft Europas. Die darin zur Erreichung dieses Ziels entwickelten Strategien sind die Durchsetzung europäischer Grundwerte und europäischen Rechts bei der Entwicklung einer internationalen Datenwirtschaft sowie die Herstellung von Datensouveränität.

**Welche Maßnahmen** zieht dies in Bezug auf die beiden Kernelemente Datenwirtschaft und Datensouveränität nach sich?

**Die Datenwirtschaft** soll insbesondere durch folgende Maßnahmen umgesetzt werden:

- Ausbau sicherer, energieeffizienter, erschwinglicher und hochwertiger Datenverarbeitungskapazitäten und -infrastrukturen zu fairen vertraglichen Konditionen (Ausbau von Kapazitäten)

kapazitäten und -infrastrukturen zu fairen vertraglichen Konditionen (Ausbau von Kapazitäten)

- Entwicklung und Anwendung verpflichtender Interoperabilitätsstandards für Daten, Schnittstellen und Protokolle (Interoperabilität von Kapazitäten)
- Aufbau zusammenschlossener Cloud-Infrastrukturen (Zusammenschluss von Kapazitäten)
- Entwicklung gemeinsamer Daten- und Cloud-Infrastrukturen

**Der Umsetzung** von Datensouveränität dienen folgende Maßnahmen:

- Entwicklung von Interoperabilitätsstandards für Daten
- die Schaffung europäischer Datenräume und Daten-Pools



- die Einführung von Schutzvorkehrungen gegen die unrechtmäßige Übermittlung nicht personenbezogener Daten an staatliche Institutionen von Drittländern durch Cloud-Diensteanbieter

Die EU-Kommission sieht die Fähigkeit von Cloud-Kunden, einfach und kostengünstig von einem Anbieter zu einem anderen zu wechseln, als wesentliche Voraussetzung für einen vom Wettbewerb geprägten Markt mit geringen Marktzutrittsschranken für neue Diensteanbieter. Die Portabilität der Cloud-Anwendung trägt Studien zufolge zum Ausbau der Kapazitäten bei. Nachdem der Selbstregulierungsansatz der „Free flow of Data Verordnung“ aus dem Jahr 2018 zur Beseitigung von Hindernissen für einen Wechsel zwischen Cloud-Anbietern gescheitert ist, legt der neue Verordnungsentwurf nun rechtliche Mindestanforderungen gewerblicher, technischer, vertraglicher und organisatorischer Art für Cloud-Anbieter verbindlich fest. Es gilt, wie schon bei der DSGVO, das Marktortprinzip mit der Folge, dass die Vorschriften der Verordnung auch Anbieter mit Sitz außerhalb der EU betreffen, soweit sie Cloud-Lösungen für Kunden in der EU anbieten. Reine Infrastrukturanbieter sind zum Erhalt der so genannten Funktionsäquivalenz nach dem Anbieterwechsel verpflichtet. Funktionsäquivalenz bedeutet nach Art. 2 Nr. 14 Data Act (E), „die Aufrechterhaltung eines Mindestfunktionsumfangs in der Umgebung eines neuen Datenverarbeitungsdienstes nach dem Wechselvorgang, sodass der Nutzer bei einer Eingabe zu Kernelementen des Dienstes vom übernehmenden Dienst das gleiche Ergebnis mit der gleichen Leistung und dem gleichen Niveau der Sicherheit, Betriebsstabilität und Dienstqualität erhält wie vom vorherigen Dienst zum Zeitpunkt der Vertragskündigung“.

Diejenigen, die Zugang zu Betriebsdiensten, zu Software und zu Anwendungen gewähren, müssen offene Schnittstellen kostenlos bereitstellen und die Kompatibilität ihrer Systeme mit bestimmten bestehenden, offenen Interoperabilitätsspezifikationen und europäischen Normen oder noch zu erlassenden, detaillierten europäischen Interoperabilitätsnormen gewährleisten. Wenn und solange, solche Vorgaben nicht bestehen, sind alle erzeugten Daten auf Wunsch des Kunden, einschließlich relevanter Datenformate und Datenstrukturen, in einem strukturierten, gängigen und maschinenlesbaren Format an den

Kunden oder an einen von ihm bestimmten Dritten zu exportieren. Und: Ab dem vierten Jahr nach Inkrafttreten des Data Act darf der Anbieter für den Wechsel keine Entgelte mehr verlangen.

Von den übrigen Vorschriften ist Art. 33 von besonderer praktischer Bedeutung. Er verpflichtet die Mitgliedstaaten zur Festlegung von wirksamen, verhältnismäßigen und abschreckenden Sanktionen, die bei Verstößen gegen Vorschriften des Data Act zu verhängen sind. Bezieht sich der Verstoß auf eine Regelung des Data Act zum Schutz personenbezogener Daten, kann die Geldbuße bis zu 20 Millionen Euro oder 4 Prozent des gesamten weltweit erzielten Jahresumsatzes erreichen. Dass eine solche Festlegung für andere Verstöße nicht erfolgte, muss kein Indiz dafür sein, dass die zu erwartenden Sanktionen geringer sein werden.

Der sich ergebende Handlungsbedarf kann für Cloud-Anbieter eine erhebliche Belastung sein. Neben der Anpassung der Produkte sind auch Allgemeine Geschäftsbedingungen und Vertragsmuster grundlegend zu überarbeiten. Für Anwender erwartet die EU-Kommission auf Basis einer rechtlichen und regulierungstechnischen Beratung und einer problemlosen Übertragbarkeit von Daten und anderen digitalen Vermögenswerten zwischen konkurrierenden Anbietern von Cloud-Diensten, zahlreiche neue, datengestützte Geschäftsmodelle. Übersehen wird dabei jedoch, dass es nicht allein die Cloud-Anbieter sind, die eine Portierung erschweren. Für die Qualität der Daten in der Cloud-Anwendung ist der Nutzer selbst verantwortlich. Migrationsprojekte ohne Datenbereinigung sind mit operativen und rechtlichen Risiken verbunden, die im Vorfeld zu klären und vertraglich zuzuordnen sind.



Marion Schultz ist seit 1999 als Rechtsanwältin tätig und berät Kunden und Anbieter in allen IT- und datenrechtlichen Fragestellungen, die sich in produzierenden Unternehmen ergeben. Mit ihrer langjährigen Erfahrung in international agierenden Unternehmen machte sie sich nun mit ihrer Trenchant Rechtsanwaltskanzlei mbH selbstständig.

**Kontakt:**

Marion Schultz – Rechtsanwältin  
IT-Compliance-Manager (ISACA)  
IT-Risk-Practitioner (ISACA)  
Datenschutzbeauftragte DSB TÜV  
Trenchant Rechtsanwaltskanzlei mbH i. Gr.  
Marion.schultz@trenchant-legal.de

[www.schultz-ra.com](http://www.schultz-ra.com)



**DRaaS**  
**RaaS**  
**BaaS** **BCaaS**

## MSPs entdecken neue As-a-Service-Welten

Klassisches Backup aus der Cloud heißt Backup as a Service (BaaS). Managed Service Provider bieten jedoch inzwischen RaaS, DRaaS und BCaaS und befinden sich in einem Begriffs- und Abkürzungs-Wirrwarr.

„**Better** have a Backup!“ lautet ein geflügeltes Sprichwort in der IT. Jedoch greift das Thema „Backup“ als Prinzip der Datensicherung eher im privaten Umfeld oder bei sehr kleinen Unternehmen. Bei steigender Größe geht es zunehmend um Anforderungen, bei denen die reine Sicherungskopie im Sinne eines Backups nur Mittel zum Zweck sein kann. Oder lediglich ein Teilaspekt eines komplexen Systems wird, das der schnellen Wiederherstellung des Geschäftsbetriebs zu vorgegebenen RTOs (Recovery Time Objectives) und RPOs (Recovery Point Objective) dient (siehe Kasten). Auch an MSPs gehen diese Kundenanforderungen nicht vorbei. Wird

Disaster Recovery aus der Cloud angeboten und nachgefragt, generiert der MSP Umsätze mit Disaster Recovery as a Service (DRaaS). Disaster Recovery wird eher selten im Deutschen auch „Katastrophenwiederherstellung“ genannt. Es beschreibt im Vorfeld definierte Prozesse, die nach beliebigen Katastrophen den Wiederaufbau der IT-Dienste ermöglichen, also die Lösung von Problemen im Bereich nicht mehr benutzbarer Hardware und Infrastruktur. Darunter fällt als Maß-

nahme die Datenwiederherstellung, und das gängige Mittel zum Zweck hierzu sind besagte Backup-Technologien.

**Auch der Begriff** Recovery as a Service (RaaS) ist inzwischen im Business rund um Managed Services genauso gang und gebe wie Business Continuity as a Service (BCaaS). RaaS fasst Dienste rund um Datenwiederherstellung (auch Datenrettung) zusammen und meint die Wiederherstellung von Originaldaten nach einem Datenverlust auf Datenträgern, aber auch das Erkennen fehlerhaft übertragener Dateneinheiten und deren Reparatur. Mit BCaaS ist der Business-Continuity-Ansatz in der As-a-Service-Welt angekommen. Bei sehr niedrigen RTO-Werten (siehe Kasten) geht es im Prinzip nicht mehr um Wiederherstellung, sondern darum, unterbrechungsfreie Geschäftsabläufe als Maßstab anzusetzen. Dann ist von „Business Continuity Management“ (BCM) in der On-Premises-Welt, beziehungsweise in der As-a-Service-Ausprägung von BCaaS die Rede. Hier geht es aber nicht nur um Maßnahmen, die die IT betreffen. Vielmehr kommt der Begriff ursprünglich aus der Betriebswirtschaftslehre, in der Vor-



# Cloudbasierte Infrastrukturen kalkulieren

Einfach. Schnell. Transparent.



Mit dem Kalkulator der Infinigate direkt erfahren, welche Kalkulation zielführend ist - **kostenlos**.



Remote-Arbeit und Dienste aus zentralen Server-Landschaften prägen das Cloud-Zeitalter.



BILD: ANDSUS - STOCK.ADOBE.COM

bereitungen auf „Betriebsstörungen“ ein Thema sind, sodass auch von „Betriebskontinuitätsmanagement“ (BKM) gesprochen wird.

**Hand in Hand** gehen die beiden Trends Cloud Computing und As-a-Service im Channel. Diese „Digitale Transformation“ führt tendenziell zu einem Einsatz von immer mehr Virtuellen Maschinen (VMs). Die IT wird immer komplexer und stellt neue Anforderungen, wie etwa an die Herangehensweisen bei Backup und Disaster-Recovery, die als Cloud-Dienste angeboten werden. Soll ein Produktivsystem schnell wieder hochgefahren werden, spielt beispielsweise die Boot-Reihenfolge der einzelnen Virtuellen Maschinen und Datenbanken, Delay-Zeiten und sich ändernde IP-Adressen und Pfade, eine Rolle. BCaaS muss berücksichtigen, dass ein virtualisiertes IT-System im Zusammenspiel der Komponenten wieder hochgefahren wird. Vor diesem Hintergrund werden in zunehmendem Maße „schlafende Rechenzentren in der Cloud“ angestrebt, die im Notfall die wiederherzustellende IT

räumlich getrennt vorhalten. Zum bewährten Snapshot-basierten Ansatz für Backups im Rahmen von IT-Resilienz oder Disaster-Recovery-Strategien gesellt sich mehr und mehr das so genannte Journaling. So basiert die Snapshot-Technologie darauf, virtuelle Abbilder eines Speichermediums vorzunehmen, das zu bestimmten Zeitpunkten als Backup ausgeführt wird. Snapshots dienen der Sicherung eines Zustandes einer Virtuellen Maschine. Auf diese Weise kann eine Virtuelle Maschine jederzeit auf einen bestimmten Snapshot zurückgesetzt werden – je größer die Abstände der Snapshots, desto größer der RTO-Wert. Beim Journaling hingegen werden virtualisierte Applikationen konsistent im Sekundenbereich zurück bis zu 30 Tage gesichert. So kann man bei der Wiederherstellung per Mausklick in einer virtuellen Zeitleiste zurückgehen.



Der aktuelle durchschnittliche Stundenpreis (auch remote) für IT-Serviceleistungen liegt bei rund 90 Euro.

**Autor:** Dr. Stefan Riedl

## DIESE ABKÜRZUNGEN MUSS MAN KENNEN: RPO, CDP, RTO, BCM, BKM

Eine wichtige Kenngröße, die im BCaaS-Geschäft bemüht wird, ist der „Recovery Point Objective“ (RPO), der die Frage widerspiegelt, wie viel Datenverlust in Kauf genommen werden kann. Es liegt in der Natur der Backup-Technologie, dass das RPO letztlich der Zeitraum ist, der zwischen zwei Datensicherungen liegen darf, da diese Zeit bestimmt, wie viele Daten oder Transaktionen verloren gehen, wenn der vielzitierte Komet in das Datacenter einschlägt. Wenn für den Betrieb kein Datenverlust hinnehmbar ist, beträgt die RPO null Sekunden, wie beim elektronischen Geldverkehr. Hier ist von so genannter „Continuous Data Protection“ (CDP) die Rede, beziehungsweise in anderem Kontext von „Realtime Backup“. Die Kennzahl „Recovery Time Objective“ (RTO) ist artverwandt und beschäftigt sich mit der Frage,

wie viel Zeit ab dem katastrophengebunden Ausfall der Systeme bis zu ihrer Wiederinbetriebnahme vergehen darf. Die Bandbreite reicht hier von (mehr oder weniger fiktiven) null Minuten, bei denen der Geschäftsbetrieb, egal was kommt, nicht abbrechen darf, bis hin zu mehreren Wochen. Bei sehr niedrigen RTO-Werten geht es im Prinzip nicht mehr um die Wiederherstellung, sondern darum, unterbrechungsfreie Geschäftsabläufe als Maßstab anzusetzen. Dann ist von „Business Continuity Management“ (BCM) oder BCaaS die Rede. Hier geht es aber nicht nur um Maßnahmen, die die IT betreffen. Inzwischen bietet fast jeder Software-Hersteller aus diesem Segment seine Produkte auch als As-a-Service-Varianten für MSPs an. Die räumliche Trennung der Datacenter, kommt dem Sicherheitsaspekt zugute.

# Reine Backups sind Geschichte: Acronis Cyber Protect bietet verbesserte Backup Protection

Verhindern Sie Datenverlust, Datenlecks und Ausfallzeiten  
mit integrierter Cyber Protection.

## Gründe für Cyber Protection

Cyberkriminelle führen immer raffiniertere Angriffe aus, wodurch es Unternehmen schwerer fällt, sie abzuwehren. Schon ein ungepatchtes System, eine böswillige URL oder eine schädliche Datei reichen den Cyberkriminellen aus, um sich Zugriff auf Ihr Netzwerk und verschlüsselte Dateien zu verschaffen und Ransomware einzusetzen.

Backups sind für die Wiederherstellung Ihrer Daten weiterhin unerlässlich – aber sie allein genügen nicht, um Ihre Daten zu schützen. Daher benötigen Sie einen umfassenden Ansatz für Cyber Protection, der Ihnen hilft, die mit den neuen Bedrohungen verbundenen Risiken zu minimieren.

## Profitieren Sie von Acronis Cyber Protect

Ein proaktiver Cyber Security-Ansatz bietet diese Vorteile:

- Maximale Sicherheit mit nur einem Tool, das Ihre Daten vor allen Bedrohungen schützt
- Vereinfachte Verwaltung mit Automatisierungen und Integrationen, die Zeit und Ressourcen sparen
- Verhinderung von Datenverlust, Datenlecks und Ausfallzeiten – mühelos

## Vertrauen Sie Ihrem Security-Anbieter? Falls nicht, wechseln Sie JETZT!

Acronis bietet einen **100%igen Rabatt** auf die Nutzung von Acronis **bis zum Ende des verbleibenden Vertrages** mit dem aktuellen Anbieter des Service Providers. Wenn die Anzahl der von einem Partner **migrierten Workloads** im Rahmen dieses Angebots **100 übersteigt**, stellt Acronis **Professional Services-Unterstützung für bis zu 3 Manntage zur Verfügung**, um die Migration zu unterstützen, die in diesem Angebot enthalten ist.

Die vollen Aktionsbedingungen (auf englisch) finden Sie unter folgendem QR-Code:

Sehr gerne stehen Ihnen unsere Acronis Lizenz-Spezialisten auch für weitere Fragen zur Verfügung.



Weitere Infos zu Acronis bei Siewert & Kau:



# Acronis

Alle in dieser Anzeige enthaltenen Angebote sind, sofern nicht anders angegeben, rein netto und freibleibend. Nur solange der Vorrat reicht. Angegebene Konfigurationen können abweichen.

Weitere Informationen zur Siewert & Kau Computertechnik GmbH finden Sie auf der Website <http://www.siewert-kau.de>.

Informationen zu Produkten werden im Online-Shopsystem unter <http://shop.siewert-kau.de> zur Verfügung gestellt. Es gelten unsere AGBs.

Geschäftsführer: B. Siewert, O. Kau, H. Kau  
Amtsgericht Köln HRB Nr. 40720 | Ust.-ID-Nr. DE812098823

**Siewert & Kau**  
Distribution – live

[www.siewert-kau.de](http://www.siewert-kau.de)

# Die Besonderheiten der Cloud Threats

Viele Sicherheitskonzepte für Cloud-Dienste greifen zu kurz, weil sie die Eigenheiten der Bedrohungen nicht berücksichtigen. Was sind die wichtigsten Cloud Threats und wo liegen die besonderen Herausforderungen für die Sicherheit?

**97 Prozent der Unternehmen** nutzen bereits heute Cloud-Lösungen oder erwägen derzeit ihren Einsatz, wie der Cloud-Monitor 2022 von KPMG und Bitkom Research ergab. Ebenfalls 97 Prozent der Unternehmen betrachten Leistungsfähigkeit und Stabilität der Cloud als Must-have. Auch die Themen Datensicherheit und Datenschutz spielen eine entscheidende Rolle bei der Wahl der Cloud-Lösung, daher gelten Vertrauen in Sicherheit und Compliance des Cloud-Providers für 95 Prozent als entscheidend. Nun ist Sicherheit und Datenschutz generell ein zentrales Thema für die meisten Unternehmen, denn Security gilt als Fundament der erfolgreichen Digitalisierung. Trotzdem ist die Sicherheit im Fall von Cloud-Diensten von besonderer Bedeutung, denn die Cloud-Risiken und -Bedrohungen unterscheiden sich von den allgemeinen Cyberisiken.

**So hat die Cloud Security Alliance (CSA)** die „Top Threats to Cloud Computing: The Pandemic II“ für das Jahr 2022 veröffentlicht. Der Bericht ist bereits der sechste in der Reihe „Threats to Cloud Computing“, aber er unterscheidet sich spürbar von den Vorgängern. So beschreibt der Bericht eine deutliche Veränderung in Bezug auf die Sicher-

heitsprobleme von Cloud-Anbietern, die als besorgniserregend angesehen werden.

**Zu den Sicherheitsproblemen** werden nun stärker die Konfiguration, die Authentifizierung sowie die Schwächen der Steuerungsebene gezählt, eine deutliche Abkehr von allgemeineren Bedrohungen, Risiken und Schwachstellen wie Datenverlust und Denial-of-Service, die in früheren Top-Threats-Berichten stärker vertreten waren, erklärt die CSA. „Insgesamt sind diese Sicherheitsprobleme ein Aufruf zum Handeln für die Entwicklung und Verbesserung des Cloud-Sicherheitsbewusstseins, der Konfiguration und des Identitätsmanagements“, sagt Jon-Michael Brook, Co-Vorsitzender der CSA Top Threats Working Group und einer der Hauptautoren der Studie. „Da sich Cloud-Geschäftsmodelle und Sicherheitstaktiken weiterentwickeln, besteht ein noch größerer Bedarf, Sicherheitsprobleme anzugehen, die sich weiter oben im Technologie-Stack befinden.“

**Betrachtet man die dominierenden** Cyberattacken wie die Ransomware-Angriffe, dann bedrohen diese jede Form der Datennutzung, die unzureichend vor dem Missbrauch von Identitäten und

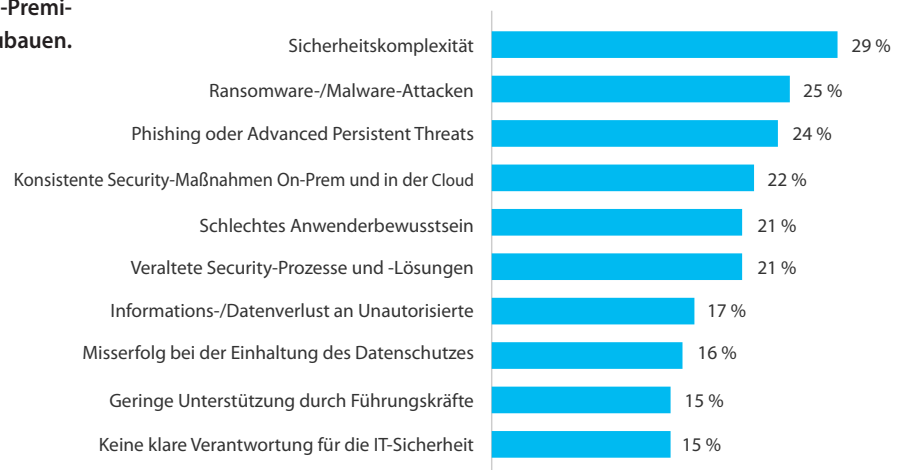


Die IDC-Studie „Cybersecurity in Deutschland 2021“ besagt: 22 Prozent der Unternehmen haben Schwierigkeiten, für die Cloud und für die On-Premises-IT eine konsistente Sicherheit aufzubauen.

Berechtigungen und lückenhaft gegen böartige Applikationen geschützt sind. Doch die Daten in Cloud-Diensten sind besonders gefährdet, ein Umstand, der in den Sicherheitskonzepten nicht übersehen werden sollte. So ist es die eingeschränkte Sichtbarkeit sowie die schwierigere Kontrolle, die Bedrohungen, Risiken und Schwachstellen in der Cloud noch mehr zur Herausforderung werden lassen als in der On-Premises-IT. Gleichzeitig fordern Compliance-Vorschriften wie der Datenschutz aber die Übernahme von Verantwortung und Monitoring durch die Cloud-Nutzenden. Zudem herrscht im Cloud Computing das Prinzip der geteilten Verantwortung, wonach sich das Anwenderunternehmen „aus der Ferne“ um die Sicherheit der Daten kümmern muss, die sich in den Cloud-Rechenzentren befinden.

**Cloud Computing bedeutet** also die volle Verantwortung für die Daten bei gleichzeitiger Abgabe der direkten Kontrolle. Das hat Folgen für die Bedrohungslage durch Ransomware & Co. und muss sich in den Sicherheitskonzepten stärker als bisher niederschlagen. Wenn man sich die größten Cyberbedrohungen und damit die gefährlichsten Attacken ansieht, sollte man immer den speziellen Cloud-Blick darauf werfen. Die eingeschränkte Sicht und die schwierige Kontrolle bei Nutzung von Cloud-Diensten machen viele der Angriffsformen noch riskanter. Zudem können Angriffe dadurch besonders interessant werden, dass sich mehrere Unternehmen in der Cloud Ressourcen und damit auch Schwachstellen teilen. Attacken

### Die 10 größten Sicherheitsherausforderungen in den befragten Unternehmen



N = 200; MEHRFACHNENNUNGEN MÖGLICH; MAXIMAL DREI NENNUNGEN; QUELLE: IDC

auf ein anderes Unternehmen können zu „Streufire“ auf das eigene Unternehmen führen.

**Berücksichtigt man** die von der CSA genannten Top 3 Cloud Threats, ergibt sich eine neue Sicht auf die Gefahren durch die dominierenden Cyberattacken. Erhöht man die Sichtbarkeit und Kontrolle in der Cloud, hat man erst einmal nur das Bedrohungspotenzial auf das Niveau gesenkt, das bei einer anderen IT-Nutzung herrscht. Dann müssen genau wie bei der restlichen IT weitere Security-Maßnahmen zum Schutz, zur Erkennung und Abwehr der Attacken folgen. Cloud-Sicherheit ist also wirklich anders und bedarf zusätzlicher Maßnahmen für Transparenz und Kontrolle.



**Zum CSA-Bericht:**  
[www.it-business.de/Pandemic-11/](http://www.it-business.de/Pandemic-11/)

**Autor:**  
Oliver Schonscheck



## TOP THREATS TO CLOUD COMPUTING: THE PANDEMIC 11

Die Cloud Security Alliance (CSA) hat eine Liste mit den häufigsten Bedrohungen im Bezug auf Cloud Computing erstellt:

1. Unzureichende Identitäts-, Berechtigungs-, Zugriffs- und Schlüsselverwaltung
2. Unsichere Schnittstellen und APIs
3. Fehlkonfiguration und unzureichende Änderungskontrolle
4. Fehlende Cloud-Sicherheitsarchitektur und -strategie
5. Unsichere Softwareentwicklung
6. Unsichere Ressourcen von Drittanbietern
7. Systemschwachstellen
8. Versehentliche Offenlegung/Offenlegung von Cloud-Daten
9. Fehlkonfiguration und Ausnutzung von serverlosen und Container-Workloads
10. Organisierte Kriminalität/Hacker/APT
11. Exfiltration von Cloud-Speicherdaten

Vogel IT-Medien GmbH  
 Max-Josef-Metzger-Straße 21, 86157 Augsburg  
 Tel. 0821/2177-0, Fax 0821/2177-150  
 eMail: it-business@vogel.de  
 www.it-business.de

**Geschäftsführer:**

Werner Nieberle, Günter Schürger

**Co-Publisher:** Lilli Kos (-300)

(verantwortlich für den Anzeigenteil)

**Chefredaktion:** Sylvia Lösel (sl)

**Chef vom Dienst:** Heidi Schuster (hs)

**Chefreporter:** Michael Hase (mh)

**Leitender Redakteur:** Dr. Stefan Riedl (sr)

**Redaktion:** Klaus Länger (kl),  
Ann-Marie Struck (amy)

**Weitere Mitarbeiter dieser Ausgabe:**

Oliver Schonschek, Marion Schultz

**Account Management:**

Besa Agaj, Hannah Lamotte, Stephanie Steen  
 eMail: media@vogel.de

**Anzeigendisposition:**

Alexandra Breuer, Denise Falloni (-202)

**Grafik & Layout:** Carin Boehm, Udo Scherlin,  
Johannes Rath

**Titelbild:** Daniel Berkmann / Skellen / Natalya  
Yudina - stock.adobe.com / [M] Udo Scherlin

**EBV:** Carin Boehm

**Anzeigen-Layout:**

Carin Boehm, Udo Scherlin, Johannes Rath

**Leserservice / Mitgliederbetreuung:**

Sabine Assum (-194), Fax (-228)  
 eMail: vertrieb@vogel.de

**Fragen zur Abonnement-Rechnung:**

DataM-Services GmbH  
 97103 Würzburg  
 Tel.: 0931/4170-462 (Fax -494)  
 eMail: vogel-it@datam-services.de

**Druck:**

Vogel Druck- und Medienservice GmbH  
 Leibnizstr. 5  
 97204 Höchberg

**Haftung:** Für den Fall, dass Beiträge oder Informationen unzutreffend oder fehlerhaft sind, haftet der Verlag nur beim Nachweis grober Fahrlässigkeit. Für Beiträge, die namentlich gekennzeichnet sind, ist der jeweilige Autor verantwortlich.

**Copyright:** Vogel IT-Medien GmbH. Alle Rechte vorbehalten. Nachdruck, digitale Verwendung jeder Art, Vervielfältigung nur mit schriftlicher Genehmigung der Redaktion.

**Manuskripte:** Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Sie werden nur zurückgesandt, wenn Rückporto beiliegt.



Vogel IT-Medien, Augsburg, ist eine 100prozentige Tochtergesellschaft der Vogel Communications Group, Würzburg, einem der führenden deutschen Fachinformationsanbieter mit 100+ Fachzeitschriften, 100+ Webportalen, 100+ Business-Events sowie zahlreichen mobilen Angeboten und internationalen Aktivitäten. Seit 1991 gibt Vogel IT-Medien Fachmedien für Entscheider heraus, die mit der Produktion, der Beschaffung oder dem Einsatz von Informationstechnologie beruflich befasst sind. Dabei bietet er neben Print- und Online-Medien auch ein breites Veranstaltungsportfolio an.

Die wichtigsten Angebote des Verlages sind IT-BUSINESS, eGovernment Computing, Healthcare Computing, BigData-Insider, Blockchain-Insider, CloudComputing-Insider, DataCenter-Insider, Dev-Insider, IP-Insider, Security-Insider und Storage-Insider.

## IT-Wissen zum Nachlesen: Hier geht es zu den CHANNEL GUIDES 2022



In unseren Channel Guides finden Sie umfassende Informationen zu ausgesuchten Themenkomplexen. Dank unserer Online-Bibliothek haben Sie jederzeit Zugriff auf Grundlagen, Trends und Highlights.



[www.it-business.de/CG-2022/](http://www.it-business.de/CG-2022/)

### Redaktionell erwähnte Unternehmen

Firma	Seite	Firma	Seite	Firma	Seite
ADN	16	Equinix	24	OVHcloud	6
Also	16	Fabasoft	6	Plusserver	6, 16
Arrow	16	Flexera	12	Poly	22
Atos Unify	22	Gaia-X	6	Rubrik	24
AWS	12, 16, 20, 24	Gartner	12	Seagate	24
Bechtle	14	Google	6, 12, 16, 24	Sophos	20
Bechtle Gruppe	22	HanseVision	22	Strato	6
Bitkom	12, 20	HornetDrive	6	Synaxon	6
Bitkom Research	6, 32	IBM	16, 02	Synology	24
Bluechip	16	IDC	12, 32	Tarox	16
Brainworks	16	Igel	18	Teamplace	6
Bytec	16	Infinigate	16	Tech Data	16
Canalys	12	Information Services Group	6	Techconsult	12
Cancom	22	Ingram Micro	16	Tecracer Group	20
Cisco	20	Ionos	12, 14, 16	TIM	16
Citrix	18	Juniper Research	20	Tresorit	6
Cloud Security Alliance	32	Komsa	16	Veeam	24
Cohesity	24	KPMG	6, 20, 32	Veritas	24
Commvault	24	LeitzCloud	6	Westcon	16
CrowdStrike	6	Lenovo	16	Wortmann	6, 16
DriveOnTheWeb	6	Micosoft	6, 12, 16, 18, 24	Zadora	24
Dropbox	6	Netapp	18	Zoi TechCon	20
Eco	14	Oracle	16, 20	Zscaler	6

### Inserenten

Firma	Seite	Firma	Seite
Cisco ThousandEyes	5	Siewert & Kau Computertechnik GmbH	31
Eset Deutschland GmbH	11	TIM AG	9
Fujitsu Technology Solutions GmbH	2	Wasabi Technologies LLC	23
Infinigate Deutschland GmbH	29	Western Digital Deutschland GmbH	36
NFON AG	19	WORTMANN AG	25
RSA Security Germany GmbH	35		

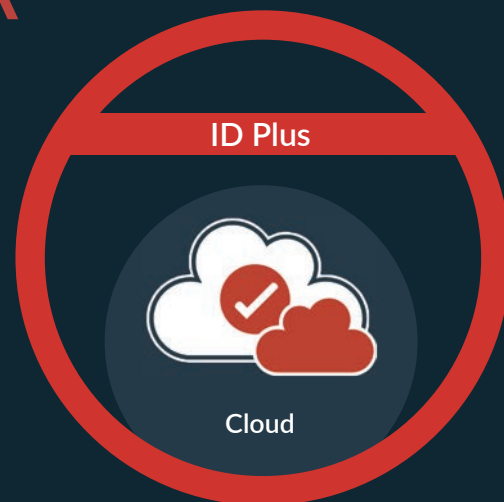
Durch die Rückkehr von RSA zu ihren Wurzeln, dem Identity Bereich als dem wichtigsten Bedrohungsvektor im Bereich der Cybersicherheit, hat RSA sein IAM-Angebot auf nur zwei Marken vereinfacht:

## ID Plus und SecurID.

RSA



On-premise-Produkte, die ein Gleichgewicht zwischen strenger Sicherheit und bequemem Zugang für sicherheitsbewusste Unternehmen herstellen.



Eine Cloud- und Hybrid-IAM-Plattform der nächsten Generation, die Sicherheit, Flexibilität und Komfort vereint.

Mit der Verfügbarkeit der innovativen neuen SaaS-Lösungssuite namens ID Plus handelt es sich um eine vollständige und flexible IAM-Plattform, die Kunden die Wahl zwischen **Cloud-, On-Premise- und Hybrid-**Implementierungen bietet.

Die leistungsstarke und flexible Cloud Lösung, die auf alle Anforderungen des Identitäts- und Zugangsmanagements zugeschnitten ist, bietet Kunden eine umfassende Lösung in einer einzigen Lizenz, die MFA, SSO, adaptive Zugriffskontrollen, RSA Authentication Manager, On-Premises-Authentifizierungs-Failover u.a. je nach Bedarf umfasst.

Innerhalb von ID Plus bietet RSA dazu **drei neue, subscription-basierte Modelle an (E1, E2 und E3).**

Zur ID Plus-Familie gehört auch der brandneue **DS100-Authentifikator** - die erste und einzige passwortlose, multifunktionale Sicherheitslösung, die die kryptografischen Vorteile von FIDO-Protokollen mit den Sicherheitsvorteilen von Einmal-Passwort-Lösungen verbindet.



**Sie möchten sich näher informieren oder RSA Partner werden?**

Sprechen Sie mit uns – sprechen Sie mit den RSA Experten bei Arrow.  
+49 89 93099-0



# UNLOCK THE POWER OF AI

Enterprise Speicherlösungen –  
Ihr Schlüssel zu endlosem Potenzial



## Speicher erweckt KI-Daten zum Leben

Künstliche Intelligenz (KI) ist der Schlüssel zur Erschließung des Datenpotenzials in einer Vielzahl von Unternehmen – vom Gesundheitswesen über Finanztechnologie bis hin zur wissenschaftlichen Forschung. Trotz der scheinbar „unsichtbaren“ Technologie, die dahinter steckt, erfordert KI eine Menge Speicherplatz, Rechenleistung und Hardware, um Daten zum Leben zu erwecken. Tatsächlich handelt es sich um eine der anspruchsvollsten Anwendungen, die von Verbrauchern, Unternehmen und ihren Technologieanbietern eingesetzt werden, um eine hocheffiziente Entscheidungsfindung für transformative Veränderungen zu ermöglichen.

Ganz gleich, ob Sie Ihr eigenes Speichersystem aufbauen oder eine sofort einsatzbereite Lösung suchen, Western Digital bietet ein umfassendes Portfolio an Ultrastar SSDs und HDDs auf Unternehmensniveau sowie JBOD- oder JBOF-Plattformen mit hoher Kapazität.



### HDD

Massive Kapazität  
für Big Data



### JBOD

Konzipiert für hohe  
Datendichte und Flexibilität



### SSD

Hochleistung für  
Big Data Workloads  
in Unternehmen



### JBOF

Die nächste Generation  
leistungsstarker, vernetzter  
Speicher