Cloud Compliance is King

Wie Unternehmen Sicherheit und Vertrauen bei Cloud-Anwendungen gewährleisten

distributed by

BORGWARE
IT-SOLUTIONS & SERVICES

IONOS

Inhalt

1 Einleitung

Cloud Computing entwickelt sich zunehmend zum favorisierten IT-Ansatz für effektive Zusammenarbeit und moderne Geschäftsmodelle für Unternehmen – auf digitaler Grundlage. Software-Anbieter, Unternehmen und Behörden sehen zurecht immenses Potenzial in der Verlagerung von IT-Services in die Cloud. Laut einer bitkom-Studie[1] bleibt Cloud Computing daher auch auf Wachstumskurs: Immerhin drei von vier Unternehmen – und damit 76 Prozent der Befragten – haben im Jahr 2019 bereits Rechenleistungen aus der Cloud bezogen. Im Vergleich zum Jahr 2017 ist das eine Steigerung um 10 Prozent. Weitere 19 Prozent planen bereits, Cloud Computing einzusetzen, oder diskutieren zumindest darüber. Das ist auch nicht verwunderlich, denn die Vorteile liegen auf der Hand: Die Cloud bietet mehr Flexibilität und Agilität, eine höhere Wirtschaftlichkeit sowie eine sehr gute Skalierbarkeit. Zudem bindet Cloud Computing weniger Kapital und reduziert den IT-Beschaffungsaufwand. Unternehmen profitieren von einer nutzungs- bzw. aufwandsbezogenen Kostenberechnung.

Ob Public Cloud, Private Cloud, Hybrid Cloud oder Multi Cloud, ob Infrastructure (IaaS), Platform (PaaS) oder Software as a Service (SaaS) – egal, für welches Cloud- und Service-Modell sich Unternehmen entscheiden: Jede Auslagerung von IT-Ressourcen bedeutet, dass sie sukzessive die physische Verfügbarkeit über ihre IT-Infrastruktur, ihre Software und die zumindest mittelbare Kontrolle über ihre Daten (darunter auch personenbezogene Daten sowie Geschäftsgeheimnisse) an den Cloud-Anbieter übermitteln. IT-Sicherheit und IT-Compliance nehmen daher eine bedeutende Rolle ein – insbesondere im Hinblick auf den Datenschutz. Genau aus diesem Grund sind einige Unternehmen bis dato auch noch zögerlich, vor allem gegenüber Public-Cloud-Angeboten. 70 Prozent der Nichtnutzer befürchten einen unberechtigten Zugriff auf kritische Unternehmensdaten.[2] 60 Prozent empfinden die Rechtslage als unklar und 59 Prozent sind nicht davon überzeugt, dass sich eine Cloud problemlos in die bestehende Infrastruktur integrieren lässt.

Digitalisierung und Cloudisierung bieten mit ihrer zunehmenden Durchdringung zudem attraktive Ziele für Kriminelle. Nicht überraschend, dass die Zahl der Cyberangriffe in den letzten Jahren zugenommen hat. Zu dem Schluss kommt auch der eco – Verband der Internetwirtschaft.[3] Die Kriminalität reicht von der Veröffentlichung sensibler Datensätze über Industriespionage bis hin zu Erpressung und Schutzgeldforderungen. Umso dringender ist eine Cloud Compliance gefragt, die für Transparenz und Vertrauen in die Cloud-Anwendungen sorgt. Denn ohne Vertrauen gibt es kein Business.

Dieses White Paper zeigt daher auf, wie Unternehmen die Sicherheit von Cloud-Anwendungen und das Vertrauen in sie gewährleisten und wie sich Cloud Compliance realisieren lässt.

---

[1] bitkom (2020): Drei von vier Unternehmen nutzen Cloud-Computing, online verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Drei-von-vier-Unternehmen-nutzen-Cloud-Computing.

[2] Ebd.

[3] eco (2020): eco Studie zeigt Anstieg von Cyberangriffen: Unternehmen sollten stärker auf Sicherheitsexperten setzen, online verfügbar unter: https://www.eco.de/presse/eco-studie-zeigt-anstieg-von-cyberangriffen-unternehmen-sollten-staerker-auf-sicherheitsexperten-setzen/.

Die Unternehmen erfahren in diesem White Paper,

... wie sie gegenüber ihren Stakeholdern Vertrauen aufbauen und erhalten,

... wie sie ihre IT-Infrastruktur revisions-/prüfungstauglich aufstellen,

... wie Cloud Compliance aussehen sollte und

... wie sie den passenden Cloud-Anbieter auswählen.

2 Warum braucht es Cloud Compliance?

2.1 Definition von Compliance

Im engeren Sinn meint Compliance, dass ein Unternehmen und seine Mitarbeiter geltende Gesetze einhalten. Beim Compliance Management handelt es sich um den strukturierten Aufbau von internen Regeln und Richtlinien, die von allen einzuhalten sind. Setzen Unternehmen und öffentliche Organisationen ein funktionierendes Compliance Management um, reduzieren sie damit erheblich das Risiko straf- und zivilrechtlich belangt zu werden. Zudem kann Compliance auch einen Wettbewerbsvorteil verschaffen: Nicht selten erteilen Kunden Aufträge nur, wenn Unternehmen ein solides Compliance Management vorweisen können.

2.2 Was gehört zu Cloud Compliance?

Deshalb sind auch Compliance-Anforderungen im Cloud Computing nicht neu. In weiten Teilen gibt es sogar Überschneidungen zum klassischen IT-Outsourcing. Je nach Branche variieren die spezifischen Vorgaben durch Gesetze und andere Regularien. Allerdings betreffen sie alle dieselben Kategorien: Datenschutz, Governance, Business, Service Continuity und IT-Security. Potenzielle Bedrohungen, etwa Datenverlust oder Missbrauch, gibt es überall – innerhalb und außerhalb der Cloud.

- **Cloud Governance**
  Von Governance oder Corporate Governance ist die Rede, wenn ein Unternehmen einem rechtlichen, aber auch einem faktischen Ordnungsrahmen unterworfen ist. Führungskräfte und letztlich die Geschäftsleitung sind für deren Einhaltung verantwortlich. Mit der Cloud Governance erweitert sich diese Aufgabe auf die Cloud. Etablieren Unternehmen diese nicht, dann können schnell viele unbeantwortete Fragen entstehen, die das Vertrauen unternehmensfremder Stakeholder wie Investoren, Aufsichtsstellen oder Wirtschaftsprüfer in den Betrieb und dessen IT-Basis schwächen. Ohne klar definiertes Zielbild der Governance sind Betrieb und Sicherheit von Cloud-Lösungen schwierig. Deshalb sollten Unternehmen und öffentliche Verwaltungen vor der Cloud-Migration genau überlegen, wie diese aussehen soll. Dabei sollten sie sich immer an Vorschriften, Gesetzen und Verträgen orientieren und diese einhalten. Auch abseits der juristischen Regelungen leitet Cloud Governance die Mitarbeiter an und bewirkt dadurch, dass Unternehmen ihre Ziele erreichen.

- **IT-Sicherheit**
  Wie eingangs erwähnt, wächst der Umfang von Cyber-Kriminalität rasant. Oftmals sind veraltete IT-Landschaften und mangelhaft durchgeführte Software Updates ein Einfallstor für Hacker. Es hat für Unternehmen aber die oberste Priorität, eigene Informationen und kritische (Kunden-)Daten zu schützen. Wurde die IT-Sicherheit noch bis vor einigen Jahren als reine IT-Aufgabe verstanden, ist heute klar, dass die Sicherung von Daten eine unternehmerische, strategische Aufgabe ist. Gleichzeitig nehmen Unternehmen daher auch regulatorische Richtlinien ernst. Cloud-Sicherheit sollte deshalb Hand in Hand mit dem Thema IT-Sicherheit gehen.

- **Schutz sensibler Daten**
  Viele Unternehmen steigen gleich in die Public Cloud ein. Dieser Einstieg gilt als besonders unkompliziert, denn die Dienste sind – nach dem Selbstbedienungsprinzip – jederzeit verfügbar und je nach Cloud Provider leicht aufzusetzen. Zudem ist kein überbordender Anpassungsaufwand nötig, was Unternehmen mit geringen IT-Ressourcen zugutekommt. Allerdings weiß man als Nutzer auch nicht, wo mancher Anbieter für Public Cloud die Daten tatsächlich hostet. US-amerikanische Unternehmen mit Rechtssitz innerhalb der USA unterliegen dem US CLOUD Act, müssen also auf Verlangen der US-Behörden – auch ohne richterlichen Beschluss – sämtliche (Kunden-)Daten offenlegen. Dies gilt selbst dann, wenn das US-Unternehmen Rechenzentren in Europa unterhält. Public Clouds von europäischen Cloud-Anbietern bieten hier deutlich mehr Sicherheit. Mit einer Private Cloud von einem europäischen Anbieter mit Rechenzentrum in Europa sind Unternehmen auf jeden Fall auf der sicheren Seite, denn hier stellt der Provider die Cloud-Ressourcen ausschließlich einem Unternehmen zur Verfügung. Über weitere Vorteile informiert das White Paper „Private Cloud“, das unter folgendem Link kostenfrei abrufbar ist: https://cloud.ionos.de/white-paper/private-cloud.

- Natürlich muss es nicht zwingend (Public) Cloud Computing sein. Auch On-Premise-Lösungen sind denkbar, jedoch liegt hierbei deutlich mehr Verantwortung hinsichtlich der Umsetzung von Compliance komplett in den Händen des nutzenden Unternehmens. Von der veränderten, nachteiligen Kostensituation und eingeschränkter Skalierung ganz zu schweigen. Ein Vergleich der Vor- und Nachteile:

Vorteile	Nachteile
Betrieb On-Premises	
Daten sind auch ohne Internet abrufbar	*Die Eigenverantwortung über die Daten liegt beim Unternehmen*
Uneingeschränkte Kontrolle über die Infrastruktur	*Mangelnde Flexibilität, etwa wenn es um die Skalierung der Ressourcen geht*
Hohe Personalisierungsmöglichkeiten	*Kosten für Personal*
	Kosten für Wartung, Updates und Support
Betrieb in der Cloud	
Daten sind auch ohne Internet abrufbar	*Teilweise geringerer Funktionsumfang als On-Premises*
Uneingeschränkte Kontrolle über die Infrastruktur	*Oftmals eingeschränkte Personalisierungsmöglichkeiten (insbesondere bei Public Cloud)*
Hohe Personalisierungsmöglichkeiten	*Monatliche bzw. jährliche Kosten*
	Keine uneingeschränkte Kontrolle über die Daten

- **Systemresilienz**
  Wie die Sicherheitslücken namhafter Prozessoren-Hersteller (Stichworte: Meltdown und Spectre) gezeigt haben, kann die Hardware einer Cloud zu einem echten Problem werden. Und vor technischen Pannen ist niemand gefeit. Deshalb ist es empfehlenswert – insbesondere hinsichtlich der Cloud Compliance – Anbieter auszuwählen, die in beide Richtungen sehr gut aufgestellt sind. Diese haben bspw. ihre Cloud-Virtualisierungsarchitektur von Grund auf selbst aufgebaut und können sie Schicht für Schicht bestens überblicken. Gespiegelte Anwendungen und geografisch mehrfach redundante Backups von Daten – gerne auch auf unterschiedlichen physischen Speichermedien – sind sehr empfehlenswert. Nur so ist der Schutz sensibler und geschäftskritischer Daten sichergestellt. Darüber hinaus benötigt es Lösungen, die neben Systemressourcen auch Log-Dateien überwachen, um die Cloud zu kontrollieren. Ein gut durchdachtes Rechtemanagement ist gleichfalls notwendig. Softwareseitig sollte diese Risiken wie Cyberangriffe, versehentliche Offenlegung von Daten oder übermäßige Freigaben rechtzeitig erkennen und bedarfsgerecht entgegensteuern.

Exkurs Object Storage:

Hinsichtlich des Object Storages gibt es immer wieder technische Sicherheitslücken oder schlicht Unbedachtheit, die die Sicherheit von Daten in Unternehmen gefährden. Diese Schwachstellen nutzen Cyber-Kriminelle bewusst aus – sie entwenden Daten oder sabotieren das Unternehmen. Welche Vorteile S3 Object Storage hat und welche Rolle die Auswahl des passenden Cloud-Dienstleisters hier spielt, erfahren Sie im kostenlosen White Paper „Cloud Storage Security“: https://cloud.ionos.de/white-paper/cloud-storage-security.

- **Faktor Mensch**
  Oftmals stellen auch die Mitarbeiter ein hohes Sicherheitsrisiko dar. So berichtet bspw. der Human Factor 2019 Report[4], dass Cyberangriffe zu 99 Prozent auf die Mitwirkung der Geschädigten basieren. Mitarbeiter aktivieren bspw. unbeabsichtigt Makros, öffnen unbedacht Dateien oder Dokumente, deren Herkunft sie nicht kennen oder klicken auf Links, hinter denen sich Viren verbergen. Damit machen sie es Hackern sehr einfach, Zugriff auf Daten zu erlangen. Deshalb sollten Unternehmen ihre Mitarbeiter unbedingt hinsichtlich Themen wie Datengeheimnis und Datenschutz regelmäßig schulen, um diesem Einfallstor keine Chance zu bieten.

Wieso Unternehmen einen europäischen bzw. deutschen Cloud-Dienstleister auswählen sollten

Mit dem Kippen des Privacy-Shield-Abkommens im Juli 2020 hat der Europäischen Gerichtshof (EuGH) noch einmal klargestellt, dass die USA aufgrund dortiger Gesetze wie CLOUD Act und FISA kein angemessenes Datenschutzniveau bieten. Damit ist ein Transfer personenbezogener Daten in die USA nicht mehr ohne Weiteres zulässig. Doch dieser Datentransfer ist selbst gar nicht notwendig. Selbst ein US-Unternehmen oder dessen Tochtergesellschaft, die ihre Server innerhalb der EU betreiben, können sich dem Wirkungsbereich des CLOUD Acts nicht entziehen. Denn sie haben auch innerhalb der EU Kontrolle über Daten, die dann in die USA abfließen können. Auch Standardvertragsklauseln der EU-Kommission ändern an dieser Problematik nichts. Deshalb ist es empfehlenswert, wenn sich Unternehmen bei der Auswahl auf europäische Anbieter konzentrieren. Weitere Informationen dazu gibt es im kostenlosen White Paper „Streitfrage CLOUD Act“ unter: https://cloud.ionos.de/white-paper/cloud-act.

[4] proofpoint (2019): HUMAN FACTOR REPORT, online verfügbar unter: https://derschenner.at/files/dokumente/studien/gtd-pfpt-us-tr-human-factor-2019.pdf.

3 Was Cloud Compliance bewirkt

Viele Unternehmen haben die verschiedenen Risikoszenarien hinsichtlich Cloud Computing bereits erkannt. Doch welche Auswirkungen hat die Cloud Compliance auf interne Entscheidungsverantwortliche aus Geschäftsleitung, IT-Betrieb und Controlling oder externe Stakeholder eines Unternehmens – also Kunden, Partner, Lieferanten etc. – und welche auf das Business? Cloud Compliance sorgt innerhalb des Unternehmens für die Sicherheit des Geschäfts und eigener Innovationen. Doch die Cloud Compliance muss auch Vertrauenswürdigkeit gegenüber allen Stakeholdern gewährleisten, die sich auf den Schutz ihrer sensiblen Daten wie auch ihres finanziellen Investments verlassen müssen. Dies umfasst rechtliche Erfordernisse, bilanzprüfungsrelevante Ergebnisse, technische Performance, effiziente Usability sowie unbedingte Ausfallsicherheit. Die Cloud-Lösung muss den strengen Vorgaben der EU-Datenschutzgrundverordnung (DSGVO) sowie den unterschiedlichsten Anforderungen an Datenschutz entsprechen. Hierfür gibt es bspw. eine Fülle von nationalen und internationalen Gütesiegeln, Standards und Zertifikate für Datenschutz und -sicherheit in Cloud-Umgebungen. Doch als Unternehmen oder öffentliche Organisation hier den Überblick zu behalten, ist alles andere als leicht.

Um Cloud Compliance im Unternehmen rechtssicher zu gestalten, gibt es zahlreiche Möglichkeiten:

- **Interne Revision**
  Die interne Revision ist zuständig für interne Arbeitsprozesse und prüft diese auf deren Richtigkeit, Wirtschaftlichkeit sowie Ordnungs- und Zweckmäßigkeit. Neben der Effizienzsteigerung verfolgt sie das Ziel, Risiken im Unternehmen zu mindern. Gegenüber der Geschäftsleitung stellen Mitarbeiter der internen Revision daher auch Handlungsalternativen vor. Neben dem

- **Financial Auditing,**

- **dem Operational Auditing und dem**

- **Management Auditing gehört ebenso der**

- **Compliance Audit**
  zu den Aufgaben eines internen Revisors. Hinsichtlich Cloud Compliance kann die interne Revision sowohl hinsichtlich anzulegender Kriterien für eine Evaluierung von Anbietern als auch in Rolle des Prüfers nach Abschluss eines Vertrages tätig werden. Die Entscheidungen eines Revisors haben somit hohen Einfluss auf die Wirtschaftlichkeit, Sicherheit und Compliance eines Unternehmens.

- **Prüfschemata, bspw. ISO-Normen**
  Die Digitalisierung bringt Unternehmen viele Vorteile – sie muss aber auch sicher sein. Um erfolgreich und rechtskonform arbeiten zu können, müssen Unternehmen hohe Standards hinsichtlich der Informationssicherheit einhalten. Deshalb gibt es die Internationale Organisation für Standardisierung (ISO), die hierfür Normen entwickelt hat:

- **ISO 27001**
  Die Norm ISO 27001 zeigt, dass ein Unternehmen oder eine Organisation Standards für die Informationssicherheit geschaffen hat. Dabei hat die Unternehmensgröße oder die Branche keinerlei Einfluss auf die Umsetzung. Wer die Vorgaben umsetzt, kann sich dafür durch unabhängige Prüfstellen – etwa durch den TÜV – zertifizieren lassen. Gegenüber Kunden und Geschäftspartnern – und allen weiteren Stakeholdern – ist somit nachgewiesen, dass es sich dabei um eine vertrauenswürdige Organisation handelt, die sich dem Thema Informationssicherheit verschrieben hat. Viele Cloud-Anbieter sind nach ISO 27001 zertifiziert. Bei der Auswahl des Cloud Providers ist es empfehlenswert, auf diese – oder weitere Normen – zu achten. Weitere Informationen, etwa, welchen Inhalt und Bestandteil die ISO 27001-Norm hat und welche Voraussetzungen für die Zertifizierung notwendig sind, finden Sie unter folgendem Link: https://www.ionos.de/digitalguide/server/sicherheit/
- **ISO 27017/27018**
  Cloud Services gehören für viele Menschen und Unternehmen zum Alltag, bergen neben Chancen aber mitunter auch Risiken, bspw. der unbefugte Zugriff auf personenbezogene Daten, den Verlust oder die Integrität der Daten. Unternehmen stellen deshalb hohe Anforderungen an die Sicherheit von Cloud-Dienstleistern. Die Zertifizierungen nach ISO 27017 bzw. ISO 27018 zeigen, dass ein Cloud-Anbieter umfassende Maßnahmen hinsichtlich der Cloud-Sicherheit unternommen hat. Der ISO-Standard 27017 baut auf dem ISO 27001 auf und ergänzt diese Norm um wichtige Leitlinien zum Cloud Computing. Das bedeutet aber nicht zwangsläufig, dass Cloud Provider nicht sicher sind, wenn sie ISO 27017/27018 nicht explizit ausweisen.

BSI-Vorgaben

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine nationale Cyber-Sicherheitsbehörde, die Mindeststandards für die Sicherheit der Informationstechnik des Bundes auf Grundlage des §8 Abs. 1 BISG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) erarbeitet. Es definiert Mindeststandards für ein konkretes Mindestniveau an Informationssicherheit. Dies richtet sich vor allem an IT-Verantwortliche, IT-Sicherheitsbeauftragte und IT-Betriebspersonal. Durch die wachsende Komplexität von IT-Systemen ergeben sich in der Regel höhere Anforderungen an die Informationssicherheit. Deshalb gibt es auch für Cloud Computing entsprechende Leitlinien seitens des BSI:

- **Anforderungskatalog Cloud Computing (C5)**
  Cloud Computing basiert generell auf einem hohen Maß an Standardisierung hinsichtlich Hard- und Software. Ein hohes Maß an Vertrauen in den Cloud-Anbieter ist deshalb zwingend erforderlich. Das BSI verfolgt mit seinem Anforderungskatalog, eine hohe Standardisierung in der Informationssicherheit zu erreichen, obgleich es durch ISO-Normen nicht an Standards mangelt. Mit dem Anforderungskatalog Cloud Computing (C5) legt das BSI seine Sichtweise zu einem informellen Konsens dar. Damit möchte es eine vertiefte fachliche Diskussion ermöglichen – etwa zwischen Cloud Providern und ihren Kunden. Dafür hat das BSI sich bekannter Sicherheitsstandards bedient und diese – wo nötig – konkretisiert oder ergänzt. Die Herkunft der Anforderungen hat das

BSI transparent dokumentiert, sodass Cloud-Anbieter auch einen Vergleich mit dem eigenen Sicherheitsniveau anstreben können. Der stets aktuelle Anforderungskatalog ist hier abrufbar.

Internationale IAASB Audits
Der International Auditing and Assurance Standards Boards (IAASB) fungiert als unabhängiges Standardsetzungsgremium unter dem internationalen Wirtschaftsprüferverband, der International Federation of Accountants (IFAC). Der ISSAB erarbeitet qualitativ hochwertige Standards zu Themen wie Prüfung, Beratung, Qualitätskontrolle und den damit verbundenen Dienstleistungen. Weitere Informationen finden Sie hier.

Darüber hinaus gibt es natürlich weitere branchenspezifische gesetzliche oder regulatorische Vorgaben, die Unternehmen einhalten müssen. Im Finanzbereich hat bspw. die BaFin eine Orientierungshilfe zur Auslagerung von Daten an Cloud-Anbieter entwickelt, derer sich Finanzinstitute bedienen können. Weitere Informationen stehen für Sie hier bereit.

4 Checkliste: Wie finden Unternehmen einen rechtssicheren Cloud-Anbieter?

Nach immer mehr Datenskandalen und wachsenden Cyber-Kriminalitätsstatistiken ist es nicht verwunderlich, dass deutsche Unternehmen und öffentliche Organisationen hinsichtlich der Themen Datenschutz und -sicherheit sensibel sind. Für die große Mehrheit der IT-Entscheider in Deutschland (85 Prozent) ist es laut einer Studie von Censuswide im Auftrag von IONOS sehr wichtig, dass der Cloud Provider seinen Sitz und seine Rechenzentren innerhalb der EU hat. Fast neun von zehn Befragten (88 Prozent) wünschen sich sogar, dass die Cloud innerhalb von Deutschland gehostet wird. 44 Prozent lehnen US-Anbieter als Provider sogar gänzlich ab – insbesondere wegen der Unsicherheit, was dort mit den Daten geschieht.

Eine Basis für eine vertrauensvolle und Compliance-konforme Zusammenarbeit ist daher eine gemeinsame Rechtsordnung – deutsche Cloud-Anwender sollten ihre sensiblen Daten daher bestenfalls auch bei einem deutschen Cloud Provider hosten. Doch welche Aspekte gibt es noch zu berücksichtigen? Folgende Checkliste gibt nützliche Tipps für die Anbieterauswahl:

1. **Es handelt sich um einen Anbieter aus der EU oder des Europäischen Wirtschaftsraums, der Daten auch ausschließlich dort hostet.**
   Wie schon erwähnt, sind Unternehmen rechtlich auf der sicheren Seite, wenn sie sich für einen europäischen Anbieter entscheiden, der seine Rechenzentren auch dort betreibt. Nur so ist es möglich, die strengen Vorgaben seitens der DSGVO einzuhalten und damit nicht den Gesetzen wie dem US CLOUD Act zu unterliegen.

2. **Beide Partner schließen eine Auftragsverarbeitungsvereinbarung ab.**
   Die DSGVO regelt, wie personenbezogene Daten zu verarbeiten sind – dafür gibt es die sogenannte Auftragsverarbeitung. Diese verpflichtet Unternehmen, mit

ihrem Cloud Provider einen Auftragsverarbeitungsvertrag abzuschließen. Darauf zu verzichten – in Form einer bilateralen Vereinbarung – ist rechtlich unzulässig. Deshalb sollten Unternehmen oder öffentliche Organisationen zwingend hellhörig werden, wenn der Cloud-Dienstleister diese nicht anbietet oder nicht abschließen möchte.

3. **Performantes Rechtemanagement in der Cloud-Lösung sichert die Cloud Compliance.**
   Die Cloud-Lösung sollte in der Lage sein, zwischen Lese-, Schreib-, Änderungs- und Ausführrechten zu unterschieden und zudem Zugriffsberechtigungen sehr detailliert vergeben zu können. Unternehmen sollten dabei sehr sorgsam vorgehen und wirklich nur im Bedarfsfall und im erforderlichen Umfang Rechte gewähren. Viele gehen hierbei zu großzügig vor – und das nicht nur innerhalb des Unternehmens selbst, sondern auch was die Weitergabe an weitere Stakeholder (Kunden, Geschäftspartner etc.) angeht. Seriöse Cloud Provider bieten hierfür ein ausgefeiltes Identity Access Management (IAM) an.

4. **Der Cloud-Dienstleister ist zertifiziert.**
   Zuvor wurde bereits beschrieben, welche Zertifizierungen und Normen es gibt. Den Cloud-Nutzern sollte es aber auch möglich sein, diese einzusehen. Auf der Website des Cloud-Anbieters sollte zudem der Datenschutzhinweis leicht erreichbar und verständlich formuliert sein.

5. **Der Cloud Provider unterstützt seine Kunden beim Datenschutz.**
   Der Dienstleister bietet bspw. Webinare, Tutorials oder Workshops zu diesem Thema. Zudem sollten Unternehmen einen ständigen persönlichen Ansprechpartner beim Cloud-Anbieter haben, um diesen jederzeit bei Rückfragen kontaktieren zu können.

5 Auf der sicheren Seite mit IONOS Cloud

Rechtssicher und Compliance-konform agieren Unternehmen, wenn sie mit einem europäischen Cloud-Anbieter zusammenarbeiten. Provider wie IONOS Cloud sind sich ihrer hohen Verantwortung bewusst: Sie nehmen ihre Aufgabe ernst, sicherzustellen, dass die Produkte und Dienste mit wichtigen Standards und Compliance-Kontrollen übereinstimmen:

- Es wird eine Hierarchie der in der Cloud verwendeten Ressourcen definiert.
- Für die Authentifizierung und Zugriffsverwaltung in der Cloud gibt es eigene Konten. Zwei- und Multi-Factor-Authentifizierung sind als Standard gesetzt.
- Ein Multi-User-Management gestattet die Erteilung von Berechtigungen zur Nutzung der Cloud-Ressourcen in unterschiedlichen Berechtigungs-Levels.
- Es ist möglich, Rollen in der Cloud zu vergeben und Nutzer zu Gruppen hinzuzufügen, anstelle Nutzern einzelne Rollen zuzuweisen.
- Um Ressourcen abzuschirmen und Anwendungen diskreter zu betreiben, kommt (S)NAT zum Einsatz.
- Firewall-Regeln helfen dabei, Ressourcen zu isolieren.
- Flow und Activity Logs erlauben das planmäßige Verfolgen und Auswerten von Vorgängen im Netzwerkverkehr wie auch im operativen Umgang mit der Cloud.
- Activity Logs stellen einen Prüfpfad für die gesamte Nutzung der Cloud-Ressourcen durch Entwickler und IT-Teams sicher.
- Managed Services von IONOS Cloud helfen dabei, sicherheits- und Performance-relevante Updates und Patches zeitnah zu installieren, um Gesamtbetriebskosten und Management-Aufwände zu reduzieren.
- Die in der Cloud ausgeführten Anwendungen lassen sich als High-Availability-Installation einrichten, um das Risiko von Ausfällen zu minimieren und funktions- sowie reaktionsfähig zu bleiben.
- 3-2-1 heißt die Devise: Strategien für Backup und Notfallwiederherstellung helfen dabei, im Bedarfsfall darauf zurückgreifen zu können.

IONOS Cloud bekennt sich zu einem besonders hohen Standard der Cloud Compliance. Denn das Unternehmen ist die europäische Cloud-Alternative – und der einzige Anbieter mit eigenem Code Stack „Made in Germany“. Der Provider bietet Unternehmen all das, was sie brauchen, um mit und in der Cloud erfolgreich zu sein – selbstverständlich gemäß den Datenschutzrichtlinien der EU-Datenschutzgrundverordnung. Die Vorteile von IONOS Cloud auf einen Blick:

Performant

- *Garantierte Compute Performance*
- *Hochgeschwindigkeits-netzwerk dank SDN & InfiniBand*
- *Unterbrechungsfreies Live Vertical Scaling*
- *Vielfältige Storage Volumes mit hoher IOPS*

Sicher

- *Maximale Sicherheit vor US CLOUD Act*
- *Neueste SIEM- und IPS/IDS-Technologien*
- *ISO-zertifizierte Rechenzentren mit hohem Tier*
- *Private Cross Connect für Anwendungen*
- *Identification Access Management*

Einfach

- *Flexible Konfiguration virtueller Rechenzentren*
- *Data Center Designer*
- *In wenigen Minuten startklar*
- *Automatisierung über API und Microservices*
- *Software Container Orchestration mit Managed Kubernetes*

Fair

- *Keine Vertragsbindung*
- *Pay-per-Minute-Abrechnung*
- *Einfache Migration ohne Vendor Lock-in*
- *Kein Lizenzdickicht*
- *Umfangreiche Testressourcen ohne Berechnung*

Kundenorientiert

- *Persönliches Account Management*
- *Professionelle Beratung durch Cloud Consultants*
- *Unterstützung bei Spezifikationen im laufenden Betrieb*
- *Kostenloser 24/7 Support aus Deutschland*
- *Managed Services durch breites Partnernetzwerk*

6 Fazit

In vielen Unternehmen nimmt das Thema Compliance immer mehr an Bedeutung zu. Das ist nicht verwunderlich – wer sich nicht regelkonform verhält, geht ein immenses Risiko ein, gegen Gesetze zu verstoßen. Hohe Bußgelder sind die harmlosesten Folgen – viel schlimmer ist der Imageschaden, der einem Unternehmen drohen kann. Deshalb ist es essentiell, dieses Thema auch hinsichtlich der Cloud anzugehen. Denn nur wer Cloud Compliance geeignet umsetzt, schafft gegenüber Kunden, Partnern und Mitarbeitern das notwendige Vertrauen. Schließlich gibt es immer noch Vorbehalte gegenüber Cloud-Angeboten, insbesondere hinsichtlich des Datenschutzes. Außerdem lässt sich nur so das Risiko von Cyberangriffen reduzieren. Wer weiß, was im Ernstfall zu tun ist, kann den Schaden für sein Unternehmen geringhalten – sowohl in finanzieller Hinsicht als auch im Hinblick auf die Reputation. Die Einhaltung von Recht und Gesetz ist daher auch im Cloud Computing oberstes Gebot – und sollte daher die Basis des unternehmerischen Handelns bilden.

distributed by

BORGWARE
IT-SOLUTIONS & SERVICES

IONOS

Über IONOS

IONOS ist mit mehr als acht Millionen Kundenverträgen der führende europäische Anbieter von Cloud-Infrastruktur, Cloud-Services und Hosting-Dienstleistungen. Das Produktportfolio bietet alles, was Unternehmen benötigen, um in der Cloud erfolgreich zu sein: von Domains über klassische Websites und Do-It-Yourself-Lösungen, Online-Marketing-Tools bis hin zu vollwertigen Servern und einer IaaS-Lösung. Das Angebot richtet sich an Freiberufler, Gewerbetreibende und Konsumenten sowie an Unternehmenskunden mit komplexen IT-Anforderungen.

IONOS Cloud ist die europäische Cloud-Alternative und Teil von IONOS. Unser Produktportfolio umfasst mit der Cloud Compute Engine eine IaaS Compute Engine mit eigenem Code Stack für Virtualisierung, Managed Kubernetes für Container-Anwendungen, eine Private Cloud powered by VMware sowie S3 Object Storage. Mit unserem Angebot bieten wir etablierten mittelständischen und großen Unternehmen, regulierten Industrien, der Digitalwirtschaft und dem öffentlichen Sektor alle notwendigen Dienste und Services um in und mit der Cloud erfolgreich zu sein.

IONOS entstand 2018 aus dem Zusammenschluss von 1&1 Internet und dem Berliner IaaS-Anbieter ProfitBricks. IONOS SE ist Teil der börsennotierten United Internet AG (ISIN DE0005089031). Zur IONOS SE Markenfamilie gehören STRATO, Arsys, Fasthosts, home.pl, InterNetX, SEDO, United Domains und World4You.
Weitere Informationen unter cloud.ionos.de

Rufen Sie uns jetzt an!

Ihr Ansprechpartner:
Jochen Schmid

Telefon: +49 7474 698 52

E-Mail: jochen.schmid@borgware.de

Impressum

IONOS SE
Elgendorfer Str. 57
56410 Montabaur, Germany

IONOS Cloud Kontakt

Telefon +49 30 57700 850
Telefax +49 30 57700 8598
E-Mail info@cloud.ionos.de
Website https://cloud.ionos.de

Vorstand

Hüseyin Dogan, Dr. Martin Endreß, Claudia Frese, Henning Kettler,
Arthur Mai, Britta Schmidt, Achim Weiß

Aufsichtsratsvorsitzender

Markus Kadelke

Handelsregister

IONOS SE: Amtsgericht Montabaur / HRB 24498

Umsatzsteuer-IdentNummer

IONOS SE: DE815563

Copyright

IONOS