

Cloud never felt more solid.

In die Cloud? Aber souverän!



Sieben Kernfragen, um die Kontrolle über die eigenen Daten zu behalten

Vertrauen ist gut, Kontrolle ist besser – insbesondere, wenn es um die Cloud-Nutzung und die Kontrolle über die eigenen Daten geht. Um sicherzustellen, dass Sie auch in Zukunft frei und selbstbestimmt über Ihre Daten verfügen und Ihre IT-Landschaft schnell und agil an neue Anforderungen anpassen können, sollten Sie sich mit folgenden Kernfragen mit Blick auf Datensouveränität beschäftigen:

1. Wie schützenswert sind Ihre Daten und Prozesse?

Nicht alle Daten und Prozesse sind gleich: Je nach Sensibilität der Daten und ihrer Bedeutung für die Prozessabläufe gelten unterschiedliche Schutzbedarfe. Diese wiederum bilden die Grundlage für die Auswahl der notwendigen technischen und organisatorischen Schutzmaßnahmen. Hierzu zählen beispielsweise Zugriffsrechte und Verschlüsselungstechniken. Die Klassifikation und Bewertung Ihrer Daten und Geschäftsprozesse ist somit der Ausgangspunkt jeglicher Informationssicherheits-Maßnahmen.

2. Haben Sie eine Cloud-Strategie definiert?

Im Rahmen einer Cloud-Strategie sollten Sie festlegen, welche Prozesse und Daten für eine Migration in die Cloud in Frage kommen und welche Rahmenbedingungen einzuhalten sind. Neben der Analyse der Wirtschaftlichkeit sind weitere Themen wie Sicherheit, Datenschutz, Exit-Möglichkeiten und der Ort der Datenhaltung wichtige, zu analysierende Punkte. Diskutieren Sie die Vor- und Nachteile. Finden Sie passgenaue und nachhaltige Lösungen, die auf Ihren Bedarf bzw. Ihr Unternehmen ausgerichtet sind.

3. Haben Sie einzuhaltende Soll-Maßnahmen definiert?

Durch die vorherigen Fragen haben Sie beleuchtet, welche Daten und Prozesse grundsätzlich in die Cloud migriert

werden sollen. Zudem kennen Sie den Schutzbedarf dieser Daten und Prozesse. Nun gilt es, festzulegen, welche technischen und organisatorischen Maßnahmen einzuhalten sind, um Ihre Daten ausreichend zu schützen. Hierbei ist darauf zu achten, welche regulatorischen und ggf. vertraglichen Anforderungen zwingend einzuhalten sind. Den Rahmen bilden die sogenannten Soll-Maßnahmen. Der Soll-Maßnahmen-Katalog kann sich an gängigen Marktstandards orientieren und definiert die Mindestanforderungen, die je nach Schutzbedarf einzuhalten sind. Basierend auf diesen Anforderungen kann auch die Passgenauigkeit von Cloud-Lösungen und Cloud-Dienstleistern bewertet werden. Wichtige Aspekte sind:

• Sicherheitsanforderungen /-settings

z.B. Verschlüsselung, Intrusion Detection / Prevention, DDoS-Schutz, Kontrollmöglichkeiten über die Daten und Metadaten wie etwa Rollen und Berechtigungen, Festlegung von Regionen und Zonen, die Verwaltung von Zugriffsrechten und das Löschen von Daten

• Anforderungen an das Notfallmanagement

z.B. Datensicherungs- und -Wiederherstellungsprozesse sowie -Zeiten, Notfallpläne und Tests der Disaster-Recovery-Szenarien

• Datenschutzerfordernisse

z.B. Erfassung der Verarbeitungsprozesse im Verzeichnis der Verarbeitungstätigkeiten (VVT), Durchführung von Schwellwertanalysen / Datenschutzfolgeabschätzungen, Prüfung des Verarbeitungsortes (Inland / Ausland), wenn Daten im Ausland verarbeitet werden: Durchführung und Dokumentation besonderer datenschutzrechtlicher Überprüfungen gemäß DSGVO

• Anforderungen an das Auslagerungsmanagement

z.B. Überprüfung der regulatorischen und institutsindividuellen Anforderungen, Überprüfung des Dienstleisters und der ggf. eingesetzten Subdienstleister, Überprüfung der Dienstleistungsgüte

Cloud never felt more solid.

In die Cloud? Aber souverän!



4. Kennen Sie die möglichen Cloud-Lösungen und Cloud-Dienstleister und können diese bewerten?

Schaffen Sie Transparenz durch eine strukturierte Bewertung der Cloud-Dienstleister und Cloud-Dienstleistungen, die für Ihr Vorhaben in Frage kommen – unter anderem von Infrastructure-as-a-Service- bis hin zu Software-as-a-Service-Angeboten. Nutzen Sie die definierten Soll-Maßnahmen, um die passgenaueste Marktlösung für Ihre Bedürfnisse und Daten zu finden. Bewerten Sie diese Lösung anschließend innerhalb des Auslagerungsprozesses und überführen Sie bestehende Risiken in den Risikomanagementprozess.

5. Enthalten die Verträge / Service Level Agreements alle relevanten Anforderungen?

Die vertraglichen Anforderungen ergeben sich aus Ihren individuellen Anforderungen (vgl. Punkt 1 bis 4) sowie gegebenenfalls aus gesetzlichen und regulatorischen Vorschriften und Standards. So definiert beispielsweise der Digital Operational Resilience Act (DORA) vertragliche Mindestanforderungen, die von Unternehmen im Finanzsektor einzuhalten sind. Es empfiehlt sich, die wesentlichen vertraglichen Vereinbarungen in einer Vertragsdatenbank zu hinterlegen und die Anforderungen im Zuge des Outsourcing-Prozesses zu managen und zu überwachen.

6. Welche Konfigurationen haben Sie vorgenommen?

Cloud-Dienstleistungen bieten eine Vielzahl an Konfigurationen, die Nutzer beim Aufsetzen vornehmen können. Sie sollten die Konfigurationsmöglichkeiten kennen und eine Standardkonfiguration festlegen. Mit technischen Compliance Scans können Sie die vorgenommenen Konfigurationseinstellungen vor der Produktivnahme oder auch während des Betriebs überprüfen und bei Bedarf anpassen. Orientierung bieten hierbei unter anderem Frameworks.

Außerdem gibt es Möglichkeiten, Cloud-Konfigurationen automatisiert zu bewerten. Solche Scans können als Bestandteil des Vulnerability-Managements prozessual etabliert und langfristig umgesetzt werden.

7. Haben Sie einen Überblick über die Performance der Dienstleistung und des Dienstleisters?

Über die Verträge und Service Level Agreements wurden Mindestanforderungen an die Dienstleistungsgüte definiert. Hierzu sind während des Auslagerungsprozesses sowie der laufenden Steuerung des Dienstleisters Nachweise wie beispielsweise Zertifikate und SLA-Berichte einzuholen und die Performance regelmäßig anhand von Key Performance Indikatoren zu bewerten. Dies betrifft sowohl die Dienstleistung als auch den Dienstleister. Auch Audits und Review-Meetings sind Bestandteil des turnusmäßigen Bewertungsprozesses.

Fazit: Eine Cloud-Strategie ist unerlässlich und bildet den Rahmen, um die Kontrolle über die eigene Daten- und IT-Landschaft zu behalten. msg unterstützt Sie bei der Planung, Umsetzung und Überwachung Ihrer Cloud-Transformation. Mit unserem interdisziplinären Team und unserer Expertise in verschiedenen Branchen, berücksichtigen wir alle relevanten Faktoren und mögliche Risiken, damit Sie Ihr Business sicher und souverän in der Cloud betreiben können.

Kontaktieren Sie uns gerne unter:
sales.security-advisors@msg.group

Erfahren Sie mehr zum Thema auf unserer Trendseite:
Datensouveränität in der Cloud

msg systems ag

Robert-Bürkle-Str. 1 | 85737 Ismaning/ München | Telefon: +49 89 96101-0
www.msg.group | info@msg.group

msg