Datenschutz für Ihre AWS-Umgebungen

Die Haltung von AWS zu Datenschutz und Vertrauen

AWS weiß, dass das Vertrauen der Nutzer in die Cloud-Leistungen von zentraler Bedeutung ist. Daher engagiert sich AWS kontinuierlich für Datenschutz und Privatsphäre – von der physischen Infrastruktur bis zu den darauf befindlichen Softwareanwendungen.

Aktuell bietet AWS mehr als fünfzig Datenschutzservices an, die – bei korrekter Implementierung – sicherstellen, dass Geschäftsdaten umfassend geschützt sind: vor Cyberkriminalität, betrügerischer Nutzung, Datenschutzverletzungen. Und dass Unternehmen vor kostspieligen Rechtsstreitigkeiten wegen Nichteinhaltung lokaler Datenschutzbestimmungen geschützt sind. AWS hilft Unternehmen, bei diesen wichtigen und legitimen Anliegen im digitalen Zeitalter.

Die Identifikation der relevanten Dienste aus dem AWS-Portfolio zum Schutz von Daten und deren korrekter Einsatz erfordert Fachexpertise und fundierte technische Kenntnisse der Cloud-Technologie. Außerdem ist Erfahrung im Umgang mit Datenschutz in verschiedenen Branchen und Regionen mit sehr spezifischen Vorschriften und Compliance-Anforderungen notwendig.

Es ist wichtig, dass Nutzer auf eine Vielzahl von Diensten zum Schutz Ihrer Daten zurückgreifen können. Doch viel wichtiger ist es, die richtigen Dienste auszuwählen, optimal zu konfigurieren und nahtlos zu implementieren – darin liegt der Schlüssel für Datenschutz in der Cloud.

Datenschutz und -sicherheit in AWS basieren auf dem Modell der geteilten Verantwortung: AWS sorgt für die Sicherheit der Cloud-Infrastruktur („Security of the Cloud“), Kunden erfüllen Sicherheitsanforderungen bei der Nutzung von AWS-Diensten („Security in the Cloud“). Es ist wichtig, diese Aufgabenteilung im Auge zu behalten.

Data Protection as a Managed Service von T-Systems löst Datenschutz-Herausforderungen

Möglicherweise haben Sie nicht die Zeit oder die Ressourcen, um eine umfassende Datenschutzstrategie zu entwickeln. Wir können Ihnen dabei helfen und Sie konzentrieren sich auf Ihr Business-Ziele: Umsatz, Wachstum und Verbesserung Ihrer Produkte sowie Dienstleistungen. Währenddessen konzentrieren wir uns bei T-Systems mit unserem Team von Sicherheitsexperten auf Ihre Datenschutzanforderungen.

T-Systems hilft Ihnen, Lösungen für Datenschutz optimal einzurichten, zu konfigurieren, zu implementieren, einzusetzen und deren Wirksamkeit zu testen. Wir nutzen Best Practices für die Einhaltung lokaler Vorschriften. Aber wir gehen noch einen Schritt weiter und haben vier Pfeiler für den Datenschutz definiert.

1. **Vertrauenswürdige Cloud Landing Zones**
2. **Nachweise der Datenresidenz**
3. **Vertraulichkeit der Daten**
4. **Europäischer Kunden-Support**

Die vier Pfeiler des Datenschutzes als Managed Service definiert von T-Systems im Detail:

T Systems

1 Vertrauenswürdige Cloud Landing Zones

Beginnen Sie Ihre Cloud-Reise in AWS mit einer Trusted Cloud Landing Zone, die von T-Systems konfiguriert und betrieben wird. Sie basiert auf dem Well Architected Framework, das in das Data Privacy and Data Residency Framework integriert ist.
Die Trusted Cloud Landing Zone bietet:

1. Ein **detailliertes Identitätsmanagement** inklusive Least-Privilege-Prinzipien
2. Kontinuierliche **Nachvollziehbarkeit**
3. Mehrstufige Sicherheitskontrollen
4. **Automatisierte** Best Practices*
5. **Proaktive Erkennung und Lösung** von Bedrohungen und Sicherheits-Vorfällen
6. Einschränkung des direkten oder manuellen Zugriffs*
7. **Gespeicherte und übertragene Daten** werden durch Verschlüsselung und Zugriffskontrollen geschützt

**Diese Funktionen reduzieren menschliche Fehler*

2 Nachweise der Datenresidenz

Ein AWS-Konto von T-Systems bietet Ihnen vom ersten Tag an Kontrolle für die Datenresidenz. Das Datenresidenz-Dashboard liefert folgende Funktionen:

1. Präventive und detektive Leitplanken für das Datenresidenz-Management, z. B. Regions-Whitelisting und Service-beschränkungen für Compliance (C5, SOC, PCI usw.)
2. Überwachung und Berichterstattung der Datenresidenz
3. Beratung zur Datenresidenz

Der Nachweis erfolgt über einen Data Residencies Access Report. Der Service bietet auch eine Echtzeit-Überwachung für Zugriffs- und Flag-Warnungen sowie die Lokalisierung und Anonymisierung über einen externen Identitätsanbieter.

3 Vertraulichkeit der Daten

Wir stellen Anleitungen und Lösungen bereit, welche Cloud-Verschlüsselungstools entsprechend der jeweiligen Datenklassifizierung zu verwenden sind. So können Sie sicher sein, dass zum Schutz Ihrer Daten die richtige Verschlüsselungsstufe angewendet wird.

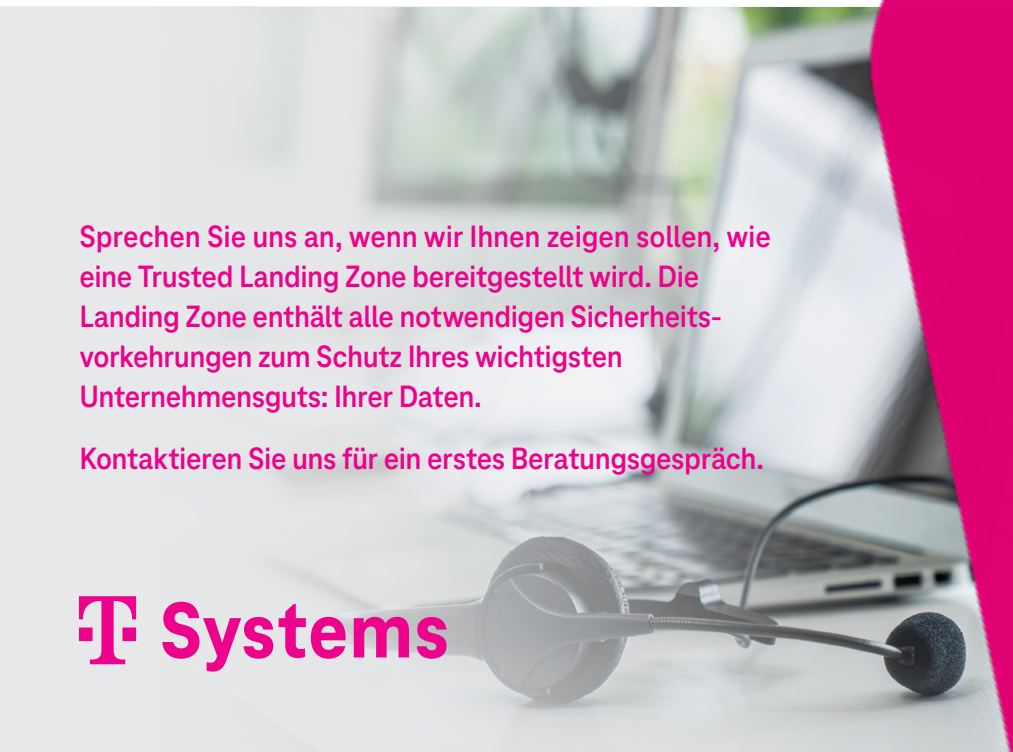
Für den Datenschutz enthält das Paket folgende Funktionen:

1. **Encryption by Default** – das stellt sicher, dass die Verschlüsselung für alle AWS-Services aktiviert ist
2. **Schlüssel, die vom Nutzer verwaltet werden**
3. **Eine gemanagte Speicherverschlüsselung**
4. **Nitro-Architektur** für hardwarebasierte Isolation
5. **Anonymisierte IAM-Daten**
6. Beschränkung auf **C5/ CISPE/ SOC**-zertifizierte AWS-Services
7. Beratung zu Datenvertraulichkeit und **Verschlüsselung**

4 Europäischer Kunden-Support

Ihr Support-Team hat seinen Sitz in Europa bei einem zertifizierten AWS-Partner. Das Support-Team bietet:

1. Support durch einen deutschen **AWS Digital Sovereignty Competency Partner** (T-Systems)
2. **24/7 Service Desk** in Europa in Ihrer Landessprache
3. AWS-**zertifizierte** Spezialisten
4. **Kundenspezifische SLAs** mit RTOs
5. Beratung, ob und wann der **3rd-Level-AWS**-Support **Datenzugriff** auf Ihr Konto benötigt



Sprechen Sie uns an, wenn wir Ihnen zeigen sollen, wie eine Trusted Landing Zone bereitgestellt wird. Die Landing Zone enthält alle notwendigen Sicherheits-vorkehrungen zum Schutz Ihres wichtigsten Unternehmensguts: Ihrer Daten.

Kontaktieren Sie uns für ein erstes Beratungsgespräch.

T Systems

NOCH FRAGEN?

Weitere Informationen erhalten Sie über:

Email: AWS-Info@t-systems.com
Internet: www.t-systems.com

HERAUSGEBER

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Deutschland

Version Stand 11/2024