BSI C5

Warum Sie Ihre Daten in der Cloud trotzdem absichern müssen

Eine Testierung nach dem „Cloud Computing Compliance Criteria Catalogue“ (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist für Cloud-Kunden ein wichtiger Indikator. Es beweist, dass der Provider strenge Sicherheitsstandards erfüllt und geeignete Maßnahmen zum Schutz der Kundendaten implementiert hat (Typ-I). Das Typ-II-Testat bestätigt zudem, dass die Wirksamkeit der Maßnahmen über einen bestimmten Zeitraum geprüft wurde. Die BSI-C5-Auditierung bezieht sich auf verschiedene Aspekte, darunter Datenschutz, Informationssicherheit, Risikomanagement und Compliance.

Sicherheitsbewusste Unternehmen sollten auf ein C5-Testat für Cloud-Dienste bestehen. Gleichzeitig ist die Testierung jedoch kein Garant für den vollständigen Schutz der Kundendaten. Die Absicherung der Daten „in der Cloud“ liegt weiterhin in der Verantwortung des Unternehmens. Daher ist eine eigene Cloud-Security-Strategie unumgänglich.

Shared Responsibility in der Cloud verstehen

Sicherheit in der Cloud folgt dem „Shared Responsibility Model“, bei dem sowohl der Cloud-Anbieter als auch der Kunde Verantwortung übernehmen müssen. Die genaue Verteilung kann je nach Cloud-Plattform variieren. Im Allgemeinen lassen sich zwei Hauptbereiche unterscheiden:

+ Infrastrukturschicht (Hardware, Netzwerke, Virtualisierung)
+ Anwendungsschicht (Betriebssystem, Anwendungen, Daten)

Auf die Anwendungsschicht hat der Provider weder Zugriff, noch kann er diese absichern. Daher sollten Sie als Kunde dafür Sorge tragen, interne Sicherheitsrichtlinien aufzustellen, Zugangskontrollen zu verwalten, Datenverschlüsselung zu nutzen und regelmäßige Sicherheitsüberprüfungen durchzuführen.

Sie möchten mehr darüber erfahren, wie Sie Ihre Daten in der Cloud schützen können?

Sprechen Sie uns gerne an für ein kostenfreies Erstgespräch mit unseren Security-Experten.

> Mehr erfahren

> Prüfbericht zu BSI C5 downloaden

Provider-Verantwortlichkeiten	Kunden-Verantwortlichkeiten
+ Physische Sicherheit: Der Anbieter ist für die physische Sicherheit der Rechenzentren verantwortlich, einschließlich Zugangskontrollen, Überwachung und Umweltsicherheit.	**+ Identitäts- und Zugriffsmanagement:** Der Kunde ist verantwortlich für die Verwaltung von Benutzerzugriffen, Authentifizierung und Autorisierung innerhalb seiner Cloud-Ressourcen.
+ Netzwerkinfrastruktur: Der Anbieter stellt die grundlegende Netzwerkinfrastruktur bereit und sichert diese ab – einschließlich Shared-Firewalls, Router und Switches –, um den Datenverkehr zu steuern.	**+ Daten:** Der Kunde ist für die Sicherheit seiner Daten verantwortlich, einschließlich Verschlüsselung, Zugriffskontrollen und Datenmanagement.
+ Virtualisierungsschicht: Der Anbieter verwaltet die Virtualisierungsebene, auf der die Kunden ihre virtuellen Maschinen (VMs) erstellen und ausführen.	**+ Anwendungen:** Die Sicherheit von Anwendungen, die auf Cloud-Ressourcen laufen, liegt in der Verantwortung des Kunden.

plusserver
Eine souveräne, zukunftsfähige und sichere Cloud

Wir bieten deutschen Unternehmen eine datensouveräne und anbieterunabhängige Basis für ihre digitalen Geschäftsprozesse. Auf unseren sicheren, skalierbaren Cloud-Plattformen realisieren Kunden zukunftsfähige und kosteneffiziente digitale Anwendungen. Wir beraten unsere Kunden zu Cloud-Architekturen sowie zur Integration bestehender IT-Umgebungen. Dabei agieren wir schnell, dynamisch und stets persönlich.

Sie haben Fragen? Kontaktieren Sie uns.
Wir helfen gerne weiter.
Schnell und unkompliziert.

+49 2203 1045 3500
beratung@plusserver.com

gaia-x · Sovereign Cloud Stack · TÜV SÜD · TÜV SÜD · JAN-2024 · BSI C5 CLOUD SECURITY · DATENSCHUTZ IDW PH 9.860.1 · ISAE 3402