PRESSEMITTEILUNG

Diese vier Maßnahmen schützen Business-kritische Daten in der Public Cloud

München, 19. September 2019 – Unternehmen gehen immer öfter in die Public Cloud, sorgen sich gleichzeitig aber auch immer stärker um die Sicherheit ihrer Unternehmensdaten. Consol gibt vier Empfehlungen, die die Sicherheit in der Public Cloud gewährleisten. Diese und weitere Tipps stehen auch im Leitfaden „Cloud Security“ von Consol kostenlos zum Download bereit.

Was viele Unternehmen, die Angebote aus der Public Cloud nutzen, nicht wissen: Zwar ist der Cloud-Provider für die Sicherheit verantwortlich – aber lediglich für die Service-Schichten, die er seinen Kunden anbietet. Bei Infrastructure-as-a-Service (IaaS) zum Beispiel sind dies Netzwerk, Speicher, Server und Virtualisierung. Für die restlichen IaaS-Schichten Betriebssysteme, Middleware, Runtime, Daten und Applikationen trägt der Kunde die Verantwortung und muss sich selbst um die Sicherheit kümmern. Mit den folgenden vier Empfehlungen von Consol stehen Unternehmen auch in der Public Cloud auf der sicheren Seite.

Empfehlung 1: Basis-Schutz durch Zwei-Faktor-Identifikation erhöhen. Unternehmen sollten als Basis-Schutzmaßnahme für alle Cloud-Modelle eine Zwei-Faktor-Identifikation benutzen, die aus einem starken Passwort und zum Beispiel einem mobilen Gerät besteht, über das eine zweite Identifikation erfolgt. Eine Zwei-Faktor-Identifikation erhöht die Sicherheit beträchtlich. Noch höheren Schutz für besonders kritische Unternehmensdaten bieten Multi-Faktor-Authentifikationsmethoden, also die Einführung zusätzlicher Faktoren wie biometrische Fingerabdruck-Scanner, Iris-Scanner, eine Stimm-Erkennung oder ein Sicherheits-Token.

Empfehlung 2: Nur Zugriffsrechte vergeben, die tatsächlich gebraucht werden. Administratoren sollten nur die Zugriffsrechte vergeben, die ein Unternehmensmitarbeiter tatsächlich benötigt. Wird ein Account trotz aller Vorsichtsmaßnahmen kompromittiert, erhält der Cyberkriminelle dadurch nur Zugriff auf einen kleinen, klar umgrenzten Bereich der Unternehmens-IT.

Empfehlung 3: Cloud-Speicherorte im PaaS-Modell mit Bedacht auswählen. Bei Infrastructure-as-a-Service und Platform-as-a-Service sind die Unternehmen für die Sicherheit einiger Layer des Cloud-Stacks selbst verantwortlich. Wer zum Beispiel Platform-as-a-Service-Angebote nutzen und gleichzeitig DSGVO-konform sein will, muss sich selbst um die Speicherorte und Speicherdauer seiner Daten kümmern. Physische Speicherorte innerhalb der deutschen Landesgrenze oder innerhalb Europas sind dabei die sicherste Option.

Empfehlung 4: Sicherheit durch dedizierte Cloud-Ressourcen erhöhen. In der Cloud teilen sich Unternehmen mit anderen Kunden des Cloud-Providers Ressourcen wie Server, Netzwerke, Betriebssysteme und Applikationen. Der Cloud-Provider erzielt durch diese Shared Ressources Synergie-Effekte, die es ihm ermöglichen, seine Dienstleistungen kostengünstiger anzubieten. Die von den Kunden gemeinsam in Anspruch genommenen Services werden durch unterschiedliche Instanzen voneinander getrennt (multi-tenancy). Unternehmen, die ein Höchstmaß an Sicherheit anstreben und „Übersprung-Effekte“ zwischen den Instanzen mit absoluter Sicherheit vermeiden wollen, sollten sich für dedizierte Hardware-Ressourcen entscheiden, die ausschließlich ihnen zugeordnet sind.

„In der Public Cloud gilt das Prinzip der Shared Responsibility. Je nach Cloud-Modell tragen Kunden für einige Layer des Cloud-Stacks selbst die Verantwortung für die Sicherheit“, sagt Lukas Höfer, Senior IT-Consultant bei Consol. „Es hält sich hartnäckig das Gerücht, dass zum Beispiel AGB-Klauseln existieren, mit denen Unternehmen die Kontrolle über ihre Daten an den Cloud-Anbieter überschreiben. Fakt ist: Die Daten, die Unternehmen in angemieteten Cloud-Services ablegen, gehören immer den Kunden.“

Leitfaden zum Download

Der Leitfaden „Cloud-Security: Mit klaren Standards sind Ihre Daten sicher“ steht kostenlos zum Download unter https://www.consol.de/download/leitfaden-cloud-security/ zur Verfügung.

Diese Presseinformation und Bildmaterial sind im Internet abrufbar unter www.pr-com.de/consol

Über Consol

Die Consol Consulting & Solutions Software GmbH betreut seit mehr als 30 Jahren Kunden aller Branchen bei nationalen und internationalen IT-Projekten. „Wir unternehmen IT“ ist dabei das Credo, auf dessen Basis die Spezialisten, Umsetzer und Innovationstreiber bei Consol passgenaue IT-Lösungen für den gesamten Software-Lifecycle erarbeiten: High-End IT-Beratung, Software Engineering, IT Operations und DevOps sind die Kernkompetenzen des 1984 gegründeten Unternehmens mit Hauptsitz in München.

Die technologischen Schwerpunkte liegen unter anderem auf Software-Architektur, Cloud-native, CI/CD, Testautomatisierung und Monitoring. Consol verfolgt hierbei einen agilen Arbeitsansatz und nutzt unter anderem Open-Source-Lösungen. Darüber hinaus entwickelt und vertreibt das Unternehmen die Software Consol CM, eine Plattform zur Digitalisierung von Geschäftsprozessen.

Consol ist Red Hat Premier Partner und unterhält strategische Partnerschaften zu AWS oder Microsoft Azure. Zu den Kunden zählen Großunternehmen wie Haribo, Daimler oder Telefónica.

Die Faszination der Consol-Mitarbeiter für technologische Herausforderungen bildet die Basis des Unternehmenserfolgs. Aktuell beschäftigt Consol rund 260 Mitarbeiter an seinen Standorten München, Düsseldorf, Wien, Krakau, Dubai sowie San Francisco.

Weitere Informationen unter https://www.consol.de und https://cm.consol.de sowie auf Twitter unter https://twitter.com/consol_de.

Pressekontakt

ConSol Consulting & Solutions Software GmbH
Isabel Baum
St.-Cajetan-Straße 43
D-81669 München
Fon: +49-89-45841-101
Fax: +49-89 45841-111
E-Mail: Isabel.Baum@consol.de
Web: https://www.consol.de und https://cm.consol.de

PR-COM GmbH
Nicole Oehl
Sendlinger-Tor-Platz 6
D-80336 München
Fon: +49-89-59997-758
Fax: +49-89-59997-999
E-Mail: nicole.oehl@pr-com.de
Web: www.pr-com.de