T Systems

Externes Schlüsselmanagement für AWS

Wie steuere ich meine Daten unabhängig von einem Cloud-Dienstleister?

Regulatorische Anforderungen an die Datenresidenz (Data Residency) unterliegen weltweit ständigen Änderungen, und es wird für Entscheidungsträger immer schwieriger, erforderliche Maßnahmen zu treffen, um diesen Änderungen zu entsprechen. Sicherheit- und Risikomanagementverantwortliche müssen dringend Maßnahmen ergreifen, um die Risiken in Bezug auf Sicherheit, Datenschutz und Datenresidenz zu minimieren.

Das Thema der Datenresidenz in der Cloud erfordert komplexe Entscheidungen. Geschäftsanforderungen müssen gegenüber wachsenden Risiken abgewogen werden, um angemessene Datensicherheit und Compliance zu gewährleisten.

Bei der sicheren Nutzung der Cloud geht es zentral um die Speicherung und der Verwendung der Verschlüsselungsschlüssel. Die Verschlüsselung selbst ist ein wesentlicher Bestandteil der Sicherheitsstrategie in der Cloud. Die Verschlüsselungsschlüssel werden jedoch in einem speziellen Schlüsselverwaltungsdienst auf der Hyperscaler-Plattform gespeichert.

Dies hindert die Möglichkeit der Nutzung der AWS-Cloud in regulierten Branchen oder für bestimmte datenempfindliche Workloads. Unternehmen tendieren daher dazu, ihre jeweiligen Anwendungen in einer Umgebung laufen zu lassen, die sie besser steuern können. Damit vermeiden sie zwar Diskussionen mit den Regierungsbehörden, können aber die Vorteile der Cloud für diese Workloads nicht nutzen.

Die Schlüssel verbleiben in der EU und werden von der Telekom, dem in Deutschland führenden Sicherheitsdienstleister, verwaltet.

T-Systems ist der Marktführer für Sicherheit in Deutschland. Die Telekom verfügt über jahrelange Erfahrung bei der Bereitstellung von Lösungen für Kunden mit einem ganzheitlichen, konvergenten und integrierten Sicherheitsmanagement, das die gesamte Wertschöpfungskette, einschließlich Menschen und Prozesse, Infrastruktur und Technik, Produkte und Dienste sowie Daten und Informationen umfasst. T-Systems bietet Verschlüsselungsschlüssel aus den Rechenzentren der Telekom, die sich in Deutschland und an anderen EU-Standorten befinden. Das externe Schlüsselmanagement wird außerhalb der AWS-Plattform betrieben und AWS hat keinen Zugriff auf die Schlüssel der Kunden. T-Systems fungiert als Verwahrer für die auf AWS verwendeten Schlüssel.

Unser Verschlüsselungsansatz auf AWS
T-Systems bietet den Kunden eine hochverfügbare, skalierbare und sichere Infrastruktur für die Nutzung von AWS. Die Schlüssel werden in einem hochverfügbaren Rechenzentrum der Telekom in Hardware-Sicherheitsmodulen (FIPS 140–2 Level 3-zertifizierten Hardware Security Modulen) gehostet, die je nach Kundenwunsch und Kundenanforderung entweder einem Kunden vorbehalten oder gemeinsam genutzt werden. Als Basis wird eine Sicherheitssoftware (CipherTrust Manager, CTM) von Thales eingesetzt. Diese Software hält die höchsten Sicherheitsstandards ein. Auf der AWS-Seite sind KMS-Dienste (Key Management Services) mit diesen Backend-Systemen verbunden. So wird ein externer Schlüsselspreicher (External Key Store - XKS) im AWS-Account des Kunden eingerichtet. Auf diese Weise kann der Kunde die Schlüssel weitgehend regulär wie die von AWS verwalteten KMS-Schlüssel verwenden, d.h. die Schlüssel lassen sich problemlos in alle AWS-Dienste integrieren, die KMS unterstützen.

T-Systems bietet den Kunden eine Self-Service-Schnittstelle für die Erstellung, Änderung und Löschung der Schlüssel. T-Systems übernimmt die Verwaltung der Schlüsselinfrastruktur einschließlich der Einrichtung einer hochverfügbaren Infrastruktur.

Der EKM-Service unterstützt die Einhaltung gesetzlicher Vorschriften und Auditing-Anforderungen durch Protokollierung und Monitoring der Schlüsselverwendung.

Das externe Schlüsselmanagement: Umsetzung der Verschlüsselung in der AWS-Cloud

01 **Schlüsselinfrastruktur:** Die Schlüssel werden in Rechenzentren der Deutschen Telekom, die sich in Deutschland und an anderen EU-Standorten befinden, gehostet. Deutsche Telekom/T-Systems ist führender Sicherheitsdienstleister in Deutschland.

02 **Verwaltung der Verschlüsselungsschlüssel außerhalb der Cloud:** Die Schlüsselverschlüsselung wird außerhalb der AWS verwaltet, was den Kunden Dienstleister-unabhängige Kontrolle bietet.

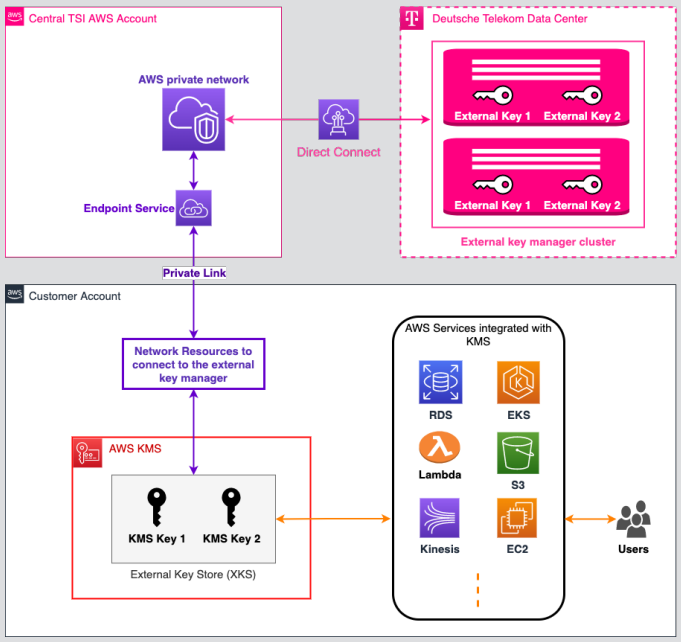
03 **Speicherung der Verschlüsselungsschlüssel auf sicherer Hardware:** Die Verschlüsselungsschlüssel werden in FIPS 140–2 Level 3-zertifizierten Hardware Security Modulen (HSM) gespeichert.

04 **Unterstützung bei der Einhaltung gesetzlicher Vorschriften:** Ermöglicht den Kunden sichere und vertrauliche Verschlüsselung von Daten und Anwendungen, die sensible Inhalte verwalten, und unterstützt bei der Einhaltung der Regierungs- und Branchenvorschriften.

05 **Nahtlose Integration in AWS-Dienste:** Integration in die meisten AWS-Dienste, die KMS unterstützen.

06 **Auditing der Schlüsselverwendung:** Protokollierung und Monitoring der Schlüsselverwendung.

07 **Hochverfügbare und skalierbare Infrastruktur:** Die Schlüssel werden in einer hochverfügbaren Infrastruktur in Rechenzentren der Deutschen Telekom gehostet. AWS-Dienste sind über redundante IPSec Site-to-Site VPN-Verbindungen mit den Rechenzentren verbunden.



Quelle: Amazon Web Services

Unsere AWS-Sicherheitsexperten stehen gern für Ihre Fragen zur Verfügung und bieten die Durchführung eines POCs für die Lösung an. Nehmen Sie noch heute Kontakt auf und machen Sie den Schritt in eine sichere und erfolgreiche Zukunft mit AWS.

„Wir nehmen die Einhaltung der DSVGO bei ITONICS sehr ernst. Als wir daher recherchierten, wie wir die Schrems-II-Vorschriften einhalten können, begannen wir nach Möglichkeiten zu suchen, unsere Daten mit Schlüsseln zu verschlüsseln, die innerhalb der EU verwaltet werden. Wir waren erfreut, dass wir zum Beta-Programm des Schlüsselmanagement-Dienstes der Deutschen Telekom eingeladen wurden, um die Integration mit einer Reihe von AWS-Diensten zu testen. Die Ergebnisse dieser Tests waren positiv, und wir gehen nun in die Umsetzungsphase des Projekts über.“ **Martin Hignett, CTO ITONICS GmbH**

T Systems

Kontakt

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Tel: 00800 33 090300
E-Mail: info@t-systems.com
Internet: www.t-systems.com

Herausgeber

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