Implementierung von Datensouveränitätsstrategien mit starkem kryptografischem Schutz

Höchste Souveränitätsstufen durch die Trennung von verschlüsselten Daten und Schlüsselmaterial erreichen

Die entscheidende Frage, die jedes Unternehmen beantworten können muss

Datensouveränität ist entscheidend für die Sicherheit und Offenlegung digitaler Daten sowie aus rechtlichen und Compliance-Gründen.

Unternehmen sind gezwungen, die richtigen Schutzmaßnahmen zu implementieren, um folgende Frage mit Zuversicht beantworten zu können:

Wer kann auf unsere Daten zugreifen?

Wenn ein Unternehmen es versäumt, die richtige digitale Schutzstrategie zu implementieren, riskiert es, dass seine Daten Dritten zugänglich werden und interne sowie externe Anforderungen nicht erfüllt werden.

Datensouveränität durch starken kryptografischen Schutz erschließen

Die Implementierung vollständiger Datensouveränität erfordert die richtige Kombination aus starker Verschlüsselung und zuverlässigen Schlüsselmanagementfähigkeiten.

Das bedeutet, Folgendes sicherzustellen:

- Strikte Trennung von verschlüsselten Daten und kryptografischen Schlüsseln
- Sichere Schlüsselspeicherung außerhalb von CSP-Umgebungen
- Zentrale Schlüsselkontrolle und zuverlässiges Zugriffsmanagement
- Vollständige Audit-Trails
- Einhaltung von Sicherheitsrichtlinien und regulatorischen Anforderungen



Die Herausforderung: Die Kontrolle über digitale Informationen in verteilten Umgebungen behalten

Datensouveränität in digitalen Umgebungen ist entscheidend für die Sicherheit und Offenlegung von Daten sowie aus rechtlichen und Compliance-Gründen.

Die Unternehmen von heute werden zu Endpunkten eines globalen Netzwerks digitaler Umgebungen und müssen sich der Herausforderung stellen, ihre sensiblen digitalen Informationen an jedem Zugangspunkt wirksam vor externem Zugriff zu schützen und gleichzeitig für autorisierte Nutzer zugänglich zu halten.

Daten, die innerhalb der Grenzen eines Staates entstehen, unterliegen den Gesetzen und regulatorischen Rahmenbedingungen dieses Staates. Das bedeutet auch, dass dieses Land die Hoheit darüber hat, wie auf die Daten zugegriffen wird, wie sie gespeichert und genutzt werden. Wenn Unternehmen sowohl öffentliche als auch private Cloud-Infrastrukturen nutzen, entsteht dadurch Komplexität, da sich Daten auf Servern außerhalb des Herkunftslands der Daten oder des Unternehmensstandorts befinden können.

Um von den Vorteilen der Cloud zu profitieren und dabei die lokalen Gesetze und Compliance-Anforderungen vollständig einzuhalten, müssen Unternehmen die richtigen Datenschutzmaßnahmen implementieren.

Datensouveränität: Wie sicherer und konformer Datenschutz gestaltet werden muss

Wenn Unternehmen ihre Daten bei globalen Cloud-Service-Providern (CSPs) wie AWS, Azure oder Google hosten, stehen sie häufig vor einem „Souveränitätsparadoxon“, das mit ausländischen Gesetzen zusammenhängt. Im Fall des U.S. CLOUD Act kann ein CSP mit Sitz in den USA rechtlich dazu verpflichtet werden, diese Daten herauszugeben, selbst wenn sie in einer bestimmten geografischen Region außerhalb des US-Territoriums gespeichert sind.

Indem Sie die Schlüssel, die zur Verschlüsselung Ihrer in der Cloud gespeicherten Daten verwendet werden, außerhalb der Cloud speichern, entweder in einem On-Premises-Schlüsselmanager oder bei einem verwalteten Drittanbieterdienst, sind Ihre Daten und Schlüssel vollständig geschützt. Mit diesem vollständigen Schlüsselschutz heben Sie automatisch das Schutzniveau Ihrer digitalen Daten an, bis hin zur vollständigen Datensouveränität, je nach eingesetztem Modell, einschließlich Sicherheit, Compliance und Verhinderung der Offenlegung. Ohne Ihre Schlüssel haben Cloud-Anbieter keinen Zugriff auf Ihre Daten und können diese selbst bei rechtmäßigen Anfragen nicht offenlegen.

Schlüsselmanagementlösungen von Utimaco zur Unterstützung Ihrer Datensouveränitätsstrategie

Starke Verschlüsselung ◆ Cloud-agnostisches Schlüsselmanagement ◆ Zuverlässige Trennung von verschlüsselten Daten und Schlüsseln ◆ Flexibilität über alle Cloud-Umgebungen hinweg

Datensouveränität hat durch Cloud Computing und globale Datenflüsse, bei denen Daten in mehreren Ländern gespeichert und verarbeitet werden können, zunehmend an Bedeutung gewonnen.

Indem Unternehmen starken kryptografischen Schutz mit den logischen Verwaltungsfunktionen eines geeigneten Schlüsselmanagementsystems kombinieren, können sie vollständige Datensouveränität in ihrer gesamten Umgebung einfach herstellen, das Risiko eines Drittzugriffs im Rahmen des U.S. CLOUD Act verhindern und die Einhaltung von Datenschutzbestimmungen weltweit sicherstellen, beispielsweise DSGVO & Schrems II, PIPEDA, PDPL, PIPL, PDPA und APPI.

Als führender Anbieter von Cybersicherheitslösungen unterstützt Utimaco Sie mit den richtigen Werkzeugen zur Umsetzung Ihrer Datensouveränitätsstrategie.

Hardware Root of Trust mit General Purpose HSM für sichere Datenverschlüsselung

Die General Purpose Hardware-Sicherheitsmodule (GP HSMs) von Utimaco bilden das Fundament für den starken Schutz digitaler Daten und Kommunikation. Das HSM generiert und schützt kryptografische Schlüssel innerhalb manipulationssicherer Hardware, aus der sie nicht extrahiert werden können.

Zukunftsfähige Sicherheit mit Krypto-Agilität

Digitale Infrastrukturen, die heute eingesetzt werden, müssen auch angesichts aufkommender Bedrohungen, einschließlich der Fortschritte im Quantencomputing, sicher bleiben.

Die GP HSMs von Utimaco sind krypto-agil konzipiert und ermöglichen es Unternehmen, mit fortschreitendem Standardwandel zu Post-Quanten-Algorithmen überzugehen. Die GP HSMs von Utimaco sind krypto-agil konzipiert und ermöglichen es Unternehmen, mit fortschreitendem Standardwandel zu Post-Quanten-Algorithmen überzugehen.

Indem Unternehmen das Anwendungspaket Quantum Protect in ihre GP-HSMs einbinden, aktivieren sie heute ihre krypto-agile Infrastruktur und stellen sicher, dass die Vertrauensfundamente ihrer KI-Systeme auch im Post-Quanten-Zeitalter sicher bleiben.

Ermöglichen Sie mit Quantum-Protect zukunftsfähige Sicherheit

Zentralisiertes Schlüsselmanagementsystem für zuverlässiges Schlüsselzugriffsmanagement

Während HSMs kryptografische Schlüssel innerhalb manipulationssicherer Hardware generieren und schützen, ist die Verwaltung der Verteilung, Speicherung, Nutzung und Rotation dieser Schlüssel über die Endpunkte ihrer digitalen Umgebungen hinweg für die Datensouveränitätsstrategien von Unternehmen unerlässlich.

Die zentralisierten Schlüsselmanagementsysteme (KMS) von Utimaco ermöglichen es Unternehmen,

- **Vollständige Schlüsselsouveränität bewahren:** Vollständige Eigentümerschaft und Kontrolle über Verschlüsselungsschlüssel auf Basis eines strikten Zugriffsmechanismus behalten. Kontrolle unabhängig von der Infrastruktur des Cloud-Anbieters behalten, um digitale Souveränität zu ermöglichen.
- **Datensouveränitäts-Compliance stärken:** Organisatorische regulatorische Strategien durch klare, unabhängige Kontrolle über kritische Sicherheits-Assets unterstützen.
- **DSGVO- und U.S.-CLOUD-Act-Risiken begegnen:** Die DSGVO-Risikoexposition bei der Datensouveränität sowie das Risiko eines Drittzugriffs im Rahmen des U.S. CLOUD Act verringern.
- **Flexibel in jeder Cloud bleiben:** Bring Your Own Key (BYOK) und Hold Your Own Key (HYOK) über öffentliche, private, hybride und Multi-Cloud-Umgebungen hinweg nutzen.
- **Sich von Vendor Lock-in befreien:** Die Datensouveränität in der Cloud bewahren und die Kontrolle behalten, unabhängig davon, wo sich die Daten befinden.

Utimaco u.trust General Purpose HSM Se-Series/CSe-Series	vor-Ort	**Utimaco** Enterprise Secure Key Manager	vor-Ort
Utimaco u.trust General Purpose HSM as a Service	aaS	**Utimaco** Enterprise Key Manager as a Service	aaS

Datensouveränität ist kein Feature, das man einfach aktiviert, sondern das Ergebnis von Datenverschlüsselung, Schlüsselkontrolle, lückenloser Überwachung jeder Operation und der zuverlässigen Erfüllung von Compliance-Anforderungen.

Kontaktieren Sie unser Vertriebsteam, um zu besprechen, wie Sie mit Ihrer digitalen Souveränitätsstrategie beginnen können.

Weitere Informationen zu Produkten von Utimaco finden Sie unter utimaco.com oder senden Sie eine E-Mail an hsm@utimaco.com

© Utimaco IS GmbH 10/26 – Version 1.0
Utimaco® ist ein Warenzeichen der Utimaco GmbH. Alle anderen genannten Marken sind Marken des jeweiligen Rechteinhabers. Alle Rechte vorbehalten. Die Spezifikationen können ohne vorherige Ankündigung geändert werden.