



HAUFE

Haufe Zeugnis Manager und Amazon Web Services

Einsatz von AWS

Der Haufe Zeugnis Manager ist die marktführende Lösung zur Erstellung von Arbeitszeugnissen.

Wir haben das Ziel unseren Kunden die höchsten Standards in Bezug auf rechtssichere Inhalte, Produktperformance und Datenschutz zu bieten.

Aus diesem Grund wird der Haufe Zeugnis Manager zukünftig auf die Dienste von Amazon Web Services (AWS) setzen.

AWS ist bereits für andere Produkte ein bewährter Partner der Haufe Group und hat sich als zuverlässiger und sicherer Dienstleister etabliert.

Deshalb haben wir neben den technischen Vorkehrungen auch vertragliche Maßnahmen getroffen, um die bestmögliche Sicherheit Ihrer Daten zu gewährleisten.

Dieses Dokument bietet Ihnen einen detaillierten Einblick in unsere technischen Maßnahmen zum Schutz Ihrer Daten und richtet sich an Datenschutz und Informationssicherheitsbeauftragte.



Management Summary

Der Haufe Zeugnis Manager setzt auf die Dienste von Amazon Web Services EMEA SARL (AWS) als Hosting-Provider. Die AWS-Rechenzentren sind nach den Sicherheitsstandards DIN ISO/IEC 27001, 27017, 27018 zertifiziert und C5 zertifiziert. AWS erfüllt strengste Sicherheits- und Compliance-Anforderungen und gewährleistet höchste Stabilität und Skalierbarkeit unserer Infrastruktur. Alle Kundendaten werden sicher auf Servern innerhalb Deutschlands (Frankfurt) gespeichert und sind sowohl im Ruhezustand als auch während der Übertragung verschlüsselt. Zusätzlich implementiert Haufe Zeugnis Manager umfassende technische und organisatorische Maßnahmen, um die Sicherheit der Datenverarbeitung zu gewährleisten.

01

Compliance und Rechtliches

Wir haben AWS nach einem sorgfältigen Auswahlprozess aufgrund seiner Sicherheits- und Compliance-Standards als Infrastruktur-Partner gewählt. AWS ist nach den international anerkannten Standards ISO/IEC 27001, 27017 und 27018 und PCI DSS zertifiziert und das erste Unternehmen, das die BSI-Zertifizierung nach C5 erhalten hat. Eine vollständige Übersicht über alle Compliance-Programme und Zertifizierungen von AWS sind online verfügbar.

02

Beschränkung der Server-Standorte auf Deutschland

Um den Datenschutzanforderungen gerecht zu werden, haben wir die Nutzung der Dienste technisch und vertraglich auf Deutschland beschränkt (EU-central-1 (Frankfurt)). Das umfassende Datenschutz- und IT-Sicherheitskonzept basiert auf dem „Shared Responsibility Model“. AWS sorgt für die Sicherheit der Cloud-Infrastruktur, während wir zusätzliche Sicherheitsmaßnahmen implementieren.

03

Verschlüsselung

Zur Verschlüsselung der Kundendaten setzen wir auf das Schlüsselverwaltungssystem von AWS (AWS KMS). Dieses System ist so konzipiert, dass niemand die Verschlüsselungs-Schlüssel im Klartext abrufen kann – auch nicht die Mitarbeiter von AWS oder Haufe. AWS KMS verwendet Hardware-Sicherheitsmodule (HSMs), die nach FIPS 140-2 validiert sind, um die Vertraulichkeit und Integrität Ihrer Schlüssel zu schützen. Die Klartext-CMKs verlassen nie die HSMs und werden nur temporär im Speicher verwendet. Software-Updates und Firmware-Aktualisierungen unterliegen einer strengen Mehrparteien-Zugangskontrolle und werden von einem NIST-zertifizierten Labor geprüft.



04

Monitoring

Jeder Zugriff und jede Verwendung von AWS KMS-Schlüsseln wird überwacht und aufgezeichnet, um unautorisierte Zugriffe zu entdecken. Der Zugriff auf das Schlüsselverwaltungssystem wird auditiert und bei Verdacht auf Sicherheitsvorfälle überprüft. AWS KMS-Key Rotation Events werden in CloudTrail überwacht. Darüber hinaus verwenden wir Guard Duty, AWS Config und CloudWatch welche uns eine umfassende Kontrolle aller Aktivitäten in der Infrastruktur ermöglicht und uns damit in die Lage versetzt, Bedrohungen zu erkennen und abzuwehren.

05

Datentrennung im Rahmen der Verschlüsselung

Die Daten sind zwischen verschiedenen AWS-Konten strikt getrennt. Ein KMS-Schlüssel von einem AWS-Konto kann nicht zum Ver- oder Entschlüsseln von Daten in einem anderen Konto verwendet werden.

06

Transportverschlüsselung

Die Systeme des Haufe Zeugnis Managers verwenden eine Transportverschlüsselung immer dann, wenn Daten über unsichere oder öffentliche Netzwerke übertragen werden. Das Webinterface und die API sind nur über HTTPS-Verbindungen erreichbar, und Client-Systeme müssen mindestens TLS 1.2 verwenden.

07

Administrativer Zugang

Der administrative Zugang zu den Systemen erfolgt ausschließlich über sichere und authentifizierte Verbindungen. Haufe Zeugnis Manager nutzt das Identity and Access Management (IAM) von AWS, welches eine feine Granulierung des Zugriffs auf verschiedene Services innerhalb der AWS-Cloud ermöglicht. IAM-Berechtigungen werden automatisch über SSO bereitgestellt, und das „Need-to-Know“-Prinzip wird strikt angewendet. Regelmäßige Audits überprüfen die Einhaltung dieses Prinzips.

08

Firewall und Netzwerktrennung

Zum Schutz vor gängigen Web-Exploits und Bots wird eine Web-Firewall verwendet. Unterschiedliche Netzwerke werden durch verschiedene AWS-Accounts und Virtual Private Clouds (VPCs) getrennt. Ein direkter Netzwerkzugriff zwischen VPCs in verschiedenen AWS-Accounts ist nicht möglich.

09

Verfügbarkeit

Ihre Daten werden ausschließlich in AWS-Rechenzentren in Frankfurt am Main gespeichert. Alle Systeme sind redundant ausgelegt und über mehrere Verfügbarkeitszonen verteilt, um eine hohe Verfügbarkeit sicherzustellen.

10

Intrusion Detection

Haufe Zeugnis Manager verwendet ein hochentwickeltes Intrusion Detection System (IDS), das Logdateien, Systemdateien, Login-Versuche, Rechteänderungen, Netzwerktraffic und bekannte Exploits überwacht. Sicherheitsrelevante Anomalien werden automatisch gemeldet und kritische Anomalien wie Rootkits automatisch unterbunden. Das IDS unterstützt ein Security Policy Enforcement gemäß PCI DSS 3.0.

12

Change-Management

Konfigurationen von Systemen und Software werden mittels „Infrastructure as Code“ verwaltet. Änderungen werden in einer Staging-Umgebung getestet, bevor sie in die Betriebsumgebung eingespielt werden.

14

Performance

Wir nutzen horizontale und vertikale Auto-Scaling-Funktionen von AWS, um die Leistung zu optimieren und Ressourcen automatisch anzupassen.

11

Logging und Audit-Trail

Wir nutzen umfassendes Logging für System-Ereignisse, Error Logging, Benutzer-Aktivitäten, Anmeldungen und Anfragen an Datenbank-Systeme sowie sicherheitsrelevante Ereignisse. AWS CloudTrail ermöglicht die Aufzeichnung sämtlicher Events innerhalb der Cloud-Umgebungen zur forensischen Analyse.

13

Backup

Tägliche Backups aller notwendigen Daten und Kundendaten werden erstellt, um die Infrastruktur und Kundendaten zu sichern.

15

Security Audits

Die Sicherheit der Haufe Zeugnis Manager-Applikation wird regelmäßig durch externe und interne Audits überprüft, um mögliche Schwachstellen zu identifizieren und zu beheben. Mit dem Haufe Zeugnis Manager und AWS als Partner an unserer Seite bieten wir Ihnen eine sichere, skalierbare und zuverlässige Lösung für Ihre Zeugnisse. Vertrauen Sie auf unsere umfassenden Sicherheitsmaßnahmen und profitieren Sie von der erstklassigen Performance und Verfügbarkeit unserer Systeme.

Haufe Zeugnis Manager

Wir sind davon überzeugt, dass es die Menschen sind, die nachhaltigen Erfolg möglich machen. Als Anbieter für integrierte Unternehmens- und Arbeitsplatzlösungen stellen wir daher den:die Mitarbeiter:in ins Zentrum des Denkens und Handelns. Zusammen mit Personalverantwortlichen aus der Praxis haben wir dieses Zeugnistool entwickelt, das Ihre tägliche Arbeit und die der Vorgesetzten dauerhaft erleichtert: Den Haufe Zeugnis Manager. Mit wenigen Klicks erstellen Sie ein individuelles, rechtssicheres und perfekt formuliertes Arbeitszeugnis.

haufe.de/zeugnis