# Datenschutz, IT Infrastruktur und der Einsatz von Cloud Technologien bei Capmo

## Einleitung

Zusammen mit verschiedener Experten (e.g. Datenschutzbeauftragte, IT-Sicherheitsberater, öffentliche Einrichtungen) definieren wir technische und organisatorische Maßnahmen um Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten, die in Capmo gespeichert werden zu garantieren.

Capmo setzt dabei auf Infrastrukturlösungen von Amazon Web Services (AWS), welche bis dato marktführend in den Bereichen Sicherheit, Stabilität und Verfügbarkeit sind. Wir sind von der Datensicherheit seitens AWS vollends überzeugt. Nachfolgend zeigen wir Ihnen anhand verschiedener technischer und organisatorischer Maßnahmen, wie wir bei Capmo die Sicherheit Ihrer Daten sicherstellen.

## Amazon Web Services

Amazon Web Services, insbesondere die Rechenzentren innerhalb der EU, verfügen über zahlreiche, international anerkannte Zertifizierung, die von renommierten Beratungsgesellschaften attestiert worden sind und somit höchste Sicherheitsanforderungen erfüllen.

Die AWS Cloud und weiterführende Dienstleistungen wurden im Bereich IT Sicherheit & Datenschutz nach DIN ISO/IEC 27001, 27017, 27018, ISO/IEC 9001, sowie CSA STAR CCM 3.0.1 zertifiziert. Weiterführende Informationen zu diesen Zertifizierungen finden Sie hier.

Des Weiteren wurde AWS nach dem international anerkannten Payment Card Industry Data Security Standard (PCI DSS) zertifiziert, welcher verbindlich von Kreditkartenorganisationen angewandt wird und als einer der strengsten Sicherheits-Regelwerke weltweit gilt. Informationen zum PCI Standard finden Sie hier.

Amazon gilt auch als Vorreiter für Cloud Sicherheit innerhalb Deutschlands. So wurde AWS als erstes Unternehmen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) die Sicherheit der Cloud Umgebung nach dem Anforderungskatalog Cloud Computing (Cloud Computing Compliance Controls Catalogue, C5) bestätigt. Eine detaillierte Übersicht zum C5 Standard, sowie weiterführende Informationen finden Sie hier.

Generell können Sie Zertifizierung, die von AWS erworben worden sind hier einsehen. Dort finden Sie beispielsweise auch globale Programme wie SOC 1/2/3.

Selbstverständlich ist AWS auch DSGVO-konform. Informationen speziell zur DSGVO finden Sie im DSGVO-Zentrum von AWS unter diesem Link.

**Beschränkung des Infrastruktur Standortes auf den EU Raum**
Trotz des globalen Fußabdrucks von AWS beschränkt Capmo die Nutzung eigener Infrastruktur und Server ausschließlich auf den EU-Raum, insbesondere auf die Region Frankfurt.

# Verschlüsselung

**Verschlüsselung at-rest**

Zur Verschlüsselung von Daten verwendet Capmo den von AWS bereitgestellten Dienst AWS Key Management Service (AWS KMS). Datenbanksysteme der Capmo Anwendung nutzen AWS KMS, um Daten beim Schreiben & Lesen zu verschlüsseln. So ist es nicht möglich, im Falle eines Hardwarezugriffs Daten ohne den zugehörigen Schlüssel zu lesen.

*Persistente Datenbanksysteme*

Datenbanksysteme mit persistentem Speicherziel (beispielsweise relationale Datenbanksysteme, RDBMS) nutzen AWS KMS mithilfe nativer Integrationen, um Daten at-rest zu verschlüsseln.

*Kurzweilige Datenspeicher / Caches*

Ebenso wie persistente Datenbanksystem wird für kurzweilige Datenspeichersysteme, wie beispielsweise Caches, eine at-rest Verschlüsselung mithilfe einer nativen Integration zu AWS KMS erzielt.

*Speicher für Binäre Daten*

In der Cloud gespeicherte binäre Daten werden verschlüsselt abgelegt. Dafür nutzt Capmo Amazon Simple Storage Service (AWS S3) - S3 ist ein hoch robustes Speichersystem mit höchsten Sicherheitsanforderungen (SOC, PCI DSS, HIPAA u.a.)

**Verschlüsselung in-transit**

Die Kommunikation zwischen den Clients der Capmo Anwendung und den Backend Services erfolgt über HTTPS (TLS). Entsprechende Zertifikate werden von AWS automatisiert generiert und erneuert. Um die Sicherheit des Netzwerkverkehrs im Internet zu gewährleisten, nutzen wir ausschließlich TLS 1.2 und höhere Protokolle.

Dies gilt sowohl für Netzwerkverkehr über das Internet, als auch für Netzwerkverkehr innerhalb des internen Netzwerks der Capmo Anwendung.

# Authentifizierung

Die Capmo Anwendung nutzt AWS Cognito zur Authentifizierung von Nutzern. AWS Cognito ist Teil des AWS Compliance Programs und wird dadurch regelmäßigen Audits unterzogen - diese erfüllen die gleichen Standards wie die restliche, physikalische Infrastruktur (bspw. PCI DSS, SOC).

# Netzwerksicherheit

Die Server und andere Infrastruktur Komponenten der Capmo Anwendungen befinden sich in sogenannten Virtual Private Clouds (VPCs). Dies bedeutet, dass sich diese Komponenten in logisch abgetrennten Netzwerken befinden. Dabei kann unterschieden werden, ob eine Infrastrukturkomponente über das Internet erreichbar sein soll (öffentliches Subnetz) oder nicht (privates Subnetz). Dies erlaubt es, insbesondere jene Komponenten, die ein hohes Schutzniveau benötigen wie beispielsweise Datenbanken, in privaten Subnetzen zu platzieren. Dadurch ist ein Zugriff bereits auf Netzwerkebene ausgeschlossen.

Zusätzlich werden Komponenten über individuelle Netzwerkregeln logisch voneinander getrennt, sodass der Netzwerkzugriff innerhalb der VPC auf einer ‘as-need’ Basis erfolgt. Nur diejenigen Server, die auch wirklich Zugriff auf eine Datenbank benötigen, können eine Verbindung herstellen. Andere Komponenten, die sich im selben logischen Netzwerk befinden, können dies nicht. Dafür verwenden wir sogenannte Security Groups (SGs), welche den Netzwerkzugriff über entsprechende Regeln steuern.

Des Weiteren verwendet Capmo eine sogenannte Multi-Account Trennung. Dies bedeutet, dass weitere Umgebungen, wie eine Entwicklungsumgebung, auf Account Ebene vom Produktivsystem getrennt sind. So ist gewährleistet, dass im Falle einer Kompromittierung / Fehlbedienung der Infrastruktur im Entwicklungsbereich keine Risiken für das Produktivsystem bestehen.

# Organisatorische Maßnahmen und Zugriffsregelung

Der Zugriff auf interne Infrastrukturkomponenten erfolgt ausschließlich über VPN. Die benötigten Komponenten werden nur bei Bedarf bereitgestellt. Genereller Zugriff auf den Account des Produktivsystems (über die technische Leitung hinaus) wird intern nur auf Anfrage ermöglicht und entsprechend erfasst.

Die Zugänge zur technischen Infrastruktur sind über eine 2-Faktor-Authentifizierung abgesichert. Die entsprechenden Schlüssel werden regelmäßig rotiert. Dazu nutzen wir Funktionen des AWS Identity and Access Management (IAM) um entsprechende Regeln zu definieren und durchzusetzen.

Neben den Schlüsseln werden auch die internen Passwörter bei Capmo hochfrequent rotiert. Zudem werden Passwörter über spezielle Software generiert und verwaltet, sodass die Kriterien gemäß dem aktuellen Stand der Technik eingehalten werden (e.g. Länge, Varianz, Zeichensatz, Passwort Monitoring).

# Verantwortliche für Datenschutz

Capmo bildet im Rahmen der DSGVO ein Informationssicherheitsteam (DST), welches aus folgenden Personen besteht:

- Datenschutzbeauftragte/-r (DSB)
- Chief Technology Officer (CTO)
- Rechtsabteilung (Legal)

Die Verantwortlichkeiten für den Datenschutz sind zwischen Capmo und AWS aufgeteilt. Die Aufteilung ergibt sich anhand des Shared Responsibility Model. Eine detaillierte Dokumentation dazu ist hier zu finden.

Neben dem DST wird jeder Mitarbeiter explizit im Bereich Datenschutz geschult. Sowohl vertraglich als auch operativ durch regelmäßige Trainings wird sichergestellt, dass alle Mitarbeiter ein hohes Maß an Achtsamkeit beim Umgang mit Daten jeglicher Natur ausüben. Im Zuge der DSGVO wurde außerdem ein Datenschutzmanagementsystem (DMS) eingerichtet, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu organisieren, zu optimieren und zu kontrollieren.

# Ausfallsicherheit & Performance

Um eine hohe Ausfallsicherheit zu gewährleisten nutzt die Capmo Anwendung für kritische Komponenten mehrere sogenannte Verfügbarkeitszonen (Availability Zones, AZs). Dies bedeutet, dass kritische Infrastrukturkomponenten redundant über physikalische Verfügbarkeitszonen verteilt sind. Im Fall einer physikalischen Störung (e.g. Stromausfall, Elementarkräfte) kann so der Betrieb sichergestellt werden. AWS stellt dabei zusätzlich sicher, dass jede Verfügbarkeitszone über redundante Strom- und Netzwerkversorgung verfügt.

Kritische Anwendungskomponenten werden standardmäßig im Cluster Modus betrieben. Das bedeutet, dass auf Anwendungsebene eine Redundanz von i.d.R. mindestens dem Faktor 2 besteht. Über Monitoring wird sichergestellt, dass zu jedem Zeitpunkt die Mindestgröße des Clusters erhalten bleibt. Im Falle einer Störung oder unter Last, werden automatisch zusätzliche Kapazitäten zur Verfügung gestellt. Jedes Cluster verfügt über einen separaten Application Load Balancer (ALB), welcher die Last gleichmäßig auf alle Instanzen verteilt.

Für Anwendungskomponenten mit besonders hoher Leistungsanforderung nutzen wir sogenannte Serverless Technologien (AWS Lambda). AWS Lambda verfügt über ein extrem hohes Skalierungspotenzial um selbst unter hohem Lastaufkommen den reibungslosen Betrieb sicherstellen zu können.

Für alle Infrastrukturkomponenten sind verschiedene Monitoringdienste im Einsatz um den Betrieb zu überwachen. Die Daten werden zudem automatisiert auf Anomalien überprüft. Im Falle einer Störung wird technisches Fachpersonal umgehend informiert, um so den reibungsfreien Betrieb der Anwendung sicherstellen zu können.

# Logging, Audit Trail & Incident Response

Zur Überwachung der Infrastruktur, sowie der Anwendungen, nutzen wir Logging. Insbesondere system- und sicherheitsrelevante Ereignisse werden über ein globales Logging System (AWS Cloudtrail) aufgezeichnet. Dieses hält unter anderem die Nutzeraktivität, System Ereignisse und Informationen zum Datenzugriff für die Auswertung und Analyse vor.

Im Rahmen des Datensicherheitskonzepts hat Capmo zudem einen Incident Response Management Prozess etabliert, um im Falle eines Cyber-Angriffs schnell, strukturiert und zielgerichtet vorgehen zu können. Dabei orientieren wir uns am aktuellen Stand der Technik und den Vorgaben nationaler Einrichtungen, wie dem BSI.

# Konfiguration und Change Management

Die Systemkomponenten und deren Konfiguration werden ausschließlich über “Infrastructure as code” verwaltet. Dies ermöglicht es, den Systemzustand nachzuvollziehen und zeitliche Zusammenhänge zu erkennen. Diese Konfiguration wird als Teil der Anwendungskomponenten in versionierbarer Form (GIT VCS) abgelegt. Desweiteren werden automatisierte Dienste von AWS eingesetzt um Konfigurationsfehler von Infrastrukturkomponenten zu identifizieren.

# Backups

Die Datenbanken verfügen über automatische, mindestens tägliche Backups. Diese sind, wie die Datenbanksysteme selbst, entsprechend mit AWS KMS verschlüsselt. Die Backupfrequenz variiert je nach Datenbanktechnologie von kontinuierlich bis hin zu täglich.

# Applikationsseitige Maßnahmen

Applikationsseitig nutzt die Capmo Anwendung unter anderem folgende weitere Maßnahmen:

**Global einzigartige Identifikatoren**
Die Entitäten im Capmo System erhalten ausschließlich global einzigartige Identifikatoren. Diese bestehen aus 32-stelligen zufallsgenerierten UUIDs und sind extrem schwer zu erraten. Dies bietet zusätzlichen Schutz im Gegensatz zu fortlaufenden oder trivialen Identifikatoren wie ganze Zahlen.

**Rollen & Rechte**
Der Zugriff auf Ressourcen wird über ein rollenbasiertes Rechtesystem abgebildet, welches vor dem Datenzugriff abgefragt wird. So wird verhindert, dass Abfragen unautorisiert stattfinden.

**Firewalling**
Die internetseitigen Komponenten sind über eine Web Application Firewall (AWS WAFv2) abgesichert. Diese bietet Schutz vor gängigen Missbrauchsversuchen (e.g. XSS, SQL Injection, DDoS) und ist mit den jeweiligen ALBs assoziiert.

**Automatisierte Aktualisierung von Programmbibliotheken**
Um etwaige Sicherheitslücken von Programmbibliotheken schnell zu identifizieren und zu schließen, benutzt Capmo ein automatisiertes System zur Überwachung der genutzten Bibliotheken. Dependabot (als Teil des VCS bei Github) überprüft einmal täglich die genutzten Programmbibliotheken und erzeugt automatisiert Meldungen im Falle sicherheitsrelevanter Updates. Diese werden vom Engineering Team ausgewertet und zeitnah angewendet.

Des Weiteren wird im Zuge jedes Deployments eine SBOM (Software Bill of Materials) Auswertung durchgeführt und regelmäßig ausgewertet. Auch hier werden kritische Schwachstellen automatisiert an das Engineering Team gemeldet.

**Application Security Management**
Die Capmo Anwendung verfügt über ein Sicherheitsmonitoring zur Laufzeit. Das System wertet geschäftsrelevante Events (wie z.B. Login/Sign up) und HTTP Anfragen auf Muster aus, welche dem Engineering Team automatisiert zur Verfügung gestellt werden. Die Auswertung erfolgt in Echtzeit mithilfe des Drittanbieters Datadog.

# Überprüfung durch Dritte

Im Abstand von 6 Monaten werden Penetrationstests durch Dritte durchgeführt. Die Tests alle Bestandteile der Cloud Anwendung (internetseitige Komponenten). Ein Bericht kann auf Anfrage zur Verfügung gestellt werden.

# Weitere Informationen

Weitere Informationen stellen wir Ihnen gerne unter www.capmo.de/datenschutz zur Verfügung. Dort finden Sie zudem Kontaktdaten zu Ihren direkten Ansprechpartnern rund um das Thema Datenschutz und Sicherheit.