IT-Infrastruktur und Einsatz von **AWS bei Personio**

Datum: 24/02/2022

Inhaltsverzeichnis

1. Zusammenfassung S.03
2. Einführung S.04
3. Compliance und Rechtliches S.05
3.1 Zertifizierungen zum Nachweis von Informationssicherheit und Datenschutz S.05
3.2. Beschränkung der Server-Standorte auf den EU-Raum S.06
4. Technische und organisatorische Maßnahmen S.08
4.1 Datenbank-Verschlüsselung (Encryption at rest) S.08
Der Einsatz AWS KMS bei Personio S.09
Monitoring S.09
Datentrennung im Rahmen der Verschlüsselung S.10
4.2 Transportverschlüsselung (Encryption in transit) S.10
HTTPS S.10
Administrativer Zugang S.10
4.3 Verantwortlichkeiten im Bereich des Datenschutzes S.11
4.4 Zugriffskontrolle S.12
4.5 Firewalling und Security Groups S.13
4.6 Netzwerktrennung/Verfügbarkeitszonen/ Geolocation S.13
4.7 Intrusion Detection/Malware Detection/Logging von sicherheitsrelevanten Ereignissen S.14
4.8 Logging/Audit Trail S.15
4.9 Change Management S.16
4.10 Backups S.16
4.11 Performance und Auto Scaling S.16
4.12 Monitoring S.16
4.13 Security audits und Penetrationstests S.17

Zusammenfassung

Personio setzt Amazon Web Services Europe (AWS) als **Hosting-Provider** ein.

Die Rechenzentren von AWS sind unter anderem **DIN ISO/IEC 27001** und **DIN ISO/IEC 27018** zertifiziert und gewährleisten höchste datenschutzrechtliche Sicherheit.

AWS erfüllt nicht nur strenge **Sicherheits- und Compliance-Anforderungen**, sondern ermöglicht die Steigerung der **Stabilität** und Skalierbarkeit unserer Infrastruktur.

Alle Kundendaten werden auf **Servern innerhalb der europäischen Union** gespeichert.

Um die Sicherheit zu gewährleisten, werden alle Daten im Ruhezustand **(Encryption at rest)** und bei der Übertragung über öffentliche Netzwerke verschlüsselt **(Encryption in Transit).**

Personio ergreift **zusätzliche technische und organisatorische Maßnahmen**, um die Sicherheit der Verarbeitung zu gewährleisten.

Einleitung

Bereits im Rahmen der Vorbereitung auf die DSGVO haben wir alle unsere Prozesse, technischen Maßnahmen und Gegebenheiten hinterfragt. Auch unser Hosting-Konzept haben wir im Hinblick auf Datensicherheit, Verfügbarkeit und Skalierbarkeit überprüft. Unter Einbeziehung verschiedener Experten (u. A. Datenschutzbeauftragte und IT-Sicherheits-Consultants) haben wir eine Reihe von Maßnahmen definiert, um langfristig eine optimale Lösung für unsere Kunden zu erreichen.

Die wichtigste Änderung, die wir in diesem Zusammenhang vorgenommen haben, war der Wechsel des Hosting-Anbieters zu Amazon Web Services (AWS). Diese Entscheidung wurde auf Basis einer detaillierten Analyse getroffen, in der wir verschiedene Anbieter und Modelle verglichen haben.

Neben der Erfüllung von strengen Sicherheits- und Compliance-Anforderungen war die damit verbundene Erhöhung der Stabilität und Skalierbarkeit unserer Infrastruktur ausschlaggebend für die Entscheidung zugunsten von AWS.

AWS hat sich seitdem als zuverlässiger und sicherer Partner für unser Unternehmen erwiesen, der unsere hohen Anforderungen an die Datensicherheit bestmöglich erfüllen kann. Neben den technischen Vorkehrungen haben wir mit AWS auch auf rechtlicher / vertraglicher Ebene alle notwendigen Vorkehrungen getroffen, um die bestmögliche Sicherheit aller Ihrer Daten zu gewährleisten. Dieses Dokument soll sowohl Transparenz über unseren Entscheidungsprozess schaffen, als auch einen Einblick in unsere rechtlichen und technischen Maßnahmen geben, mit denen wir unsere Kundendaten schützen. Es ist in erster Linie für den Datenschutz- und Informationssicherheitsbeauftragten und die Rechtsabteilung Ihres Unternehmens geschrieben.

Compliance
und Rechtliches

Wir haben AWS auf der Grundlage eines sorgfältigen Auswahlprozesses unter Berücksichtigung von rechtlichen, organisatorischen und technischen Kriterien, ausgewählt. Nach intensiver Due-Diligence-Prüfung und entsprechenden Verhandlungen haben wir uns für AWS als Infrastruktur-Partner entschieden, weil AWS neben erstklassigen Produkten und Services auch ein äußerst professionelles Compliance- und Sicherheits-Setup aufweist.

Zertifizierungen zum Nachweis von Informationssicherheit und Datenschutz

Die in der AWS-Region Frankfurt und in den anderen europäischen Regionen angebotenen und von uns genutzten Dienste wie RDS (Datenbank), S3 (Dokumentenspeicher) oder KMS (Schlüsselverwaltung) verfügen über zahlreiche international anerkannte Zertifizierungen, die von unabhängigen und renommierten Beratungsunternehmen attestiert wurden und die Einhaltung höchster Sicherheitsanforderungen nachweisen.

Die AWS-Region Frankfurt, weitere Regionen und entsprechende Dienstleistungen sind sowohl zur IT-Sicherheit nach der DIN ISO/IEC 27001 als auch zum Schutz personenbezogener Daten in der Cloud nach der DIN ISO/IEC 27018 zertifiziert. Darüber hinaus ist AWS nach dem international anerkannten Payment Card Industry Data Security Standard (PCI DSS) zertifiziert. Dieser Standard wird verbindlich von Kreditkartenorganisationen angewendet und gilt als eines der strengsten Sicherheits-Regelwerke weltweit. Darüber hinaus ist AWS das erste Unternehmen, das sich die Sicherheit ihrer Cloud-Umgebung vom Bundesamt für Sicherheit in der Informationstechnik (BSI) auf Basis des Anforderungskatalogs Cloud Computing (Cloud Computing Compliance Controls Catalogue, C5) hat bescheinigen lassen. Damit gilt AWS als Vorreiter für Cloud-Sicherheit in Deutschland. Eine Übersicht über alle Compliance Programme und Zertifizierungen von AWS finden Sie hier.

Im Rahmen des Auswahlprozesses unseres neuen Hosting-Providers haben wir intensiv mit unserem Datenschutzbeauftragten der Bitkom Servicegesellschaft mbH zusammengearbeitet.

Wir sind daher überzeugt davon, dass AWS der datenschutzrechtlich bestmögliche Partner für unser Unternehmen ist. Gerne können Sie sich auch selbst von der DSGVO-Konformität von AWS überzeugen. Nähere Informationen finden Sie hier.

Beschränkung der Server-Standorte auf den EU-Raum

Um bestmöglich sicherzustellen, dass die Daten nicht unbefugt genutzt oder weitergegeben werden können, haben wir die Nutzung der Dienste technisch und vertraglich auf den EU/EWR-Raum beschränkt und die Zugriffsmöglichkeiten entsprechend geregelt.

Die Bedenken einiger Datenschutzexperten hinsichtlich einer möglichen Weitergabe von Daten auf Basis von Anfragen der US-Regierung sind uns bekannt. Wir beobachten die entsprechenden Entwicklungen in der US-Gesetzgebung, wie z. B. den Cloud Act, sowie die Bestrebungen der EU zum Austausch elektronischer Beweismittel in Strafsachen und begrüßen grundsätzlich die Absicht, Rechtssicherheit zu schaffen. Festzuhalten ist, dass weder wir noch AWS Daten ohne Anlass herausgeben werden, da dies weder im geschäftlichen Interesse der beiden Unternehmen noch unserer Kunden liegt.

Um die Daten unserer Kunden auch im unwahrscheinlichen Fall eines staatlichen Herausgabeanspruchs sowie vor “Angriffen von außen” zu schützen, haben wir gemeinsam mit AWS ein umfassendes Datenschutz- und IT-Sicherheitskonzept entwickelt. Nach dem “Shared Responsibility Model” setzen wir zum einen auf die umfangreichen Sicherheitsmechanismen von AWS (“Sicherheit der Cloud”) und werden zusätzlich eigene Sicherheitsmaßnahmen anwenden. Weitere Informationen zum “Shared Responsibility Model” von AWS finden Sie hier, weitere Informationen zu den technischen und organisatorischen Maßnahmen von AWS sind hier aufgeführt.

Ein wesentliches Kernelement unserer Sicherheitsmaßnahmen ist dabei die auch in der DSGVO geforderte Verschlüsselung. Dabei setzen wir auf Verschlüsselungsalgorithmen nach dem Stand der Technik (siehe Abschnitt „Verschlüsselung“), nach Möglichkeit auf AES-256, welches selbst in den USA für Dokumente der höchsten Geheimhaltungsstufe zugelassen ist und als nicht entschlüsselbar gilt. Wir verwenden modernste Verschlüsselungsalgorithmen (siehe Abschnitt “**Verschlüsselung**”), nach Möglichkeit AES-256, der auch in den USA für Dokumente mit höchster Vertraulichkeit zugelassen ist und als nicht entschlüsselbar gilt. Diese Verschlüsselung stellt sicher, dass selbst im sehr unwahrscheinlichen Fall eines Datendiebstahls die Daten bestmöglich vor unberechtigtem Zugriff geschützt sind.

Technische und organisatorische Maßnahmen

Im Folgenden möchten wir näher auf unser Datenschutz- und IT-Sicherheitskonzept im Zusammenhang mit dem Einsatz von AWS eingehen. Sofern Sie Fragen hierzu haben, wenden Sie sich bitte direkt an **security@personio.de** Unser Security-Engineering-Team steht Ihnen gerne zur Verfügung.

Datenbank-Verschlüsselung (Encryption at rest)

Zur Verschlüsselung der Kundendaten wird das Schlüsselverwaltungssystem von Amazon Web Services (AWS KMS) verwendet. Das Verschlüsselungssystem ist so konzipiert, dass niemand, einschließlich der Mitarbeiter von Personio und der Mitarbeiter von AWS, die Klartext-Encryption-Schlüssel abrufen kann.

Weitere Details hierzu, können Sie auch den FAQ von AWS entnehmen: AWS KMS ist so aufgebaut, dass niemand, auch keine Angestellten von AWS, Ihre CMKs im Klartext aus dem Service abrufen kann. AWS KMS verwendet Hardware-Sicherheitsmodule (HSMs), die gemäß FIPS 140-2 validiert wurden oder derzeit validiert werden, um die Vertraulichkeit und Integrität Ihrer Schlüssel zu schützen.

Ihre Schlüssel werden in diesen HSMs gespeichert, unabhängig davon, ob Sie AWS KMS oder AWS CloudHSM zum Erstellen Ihrer Schlüssel verwenden oder Schlüsselmaterial in einen CMK importieren. Ihre Klartext-CMKs verlassen nie die HSMs, werden zu keiner Zeit auf die Festplatte geschrieben, sondern lediglich für die Dauer der von Ihnen angeforderten kryptografischen Vorgänge im temporären Speicher der HSMs verwendet. Aktualisierungen der Software auf den Service-Hosts und der AWS KMS HSM-Firmware werden durch eine Mehrparteien-Zugangskontrolle gesteuert, die von einer unabhängigen Gruppe innerhalb von Amazon sowie einem NIST-zertifizierten Labor gemäß FIPS 140-2 geprüft und überprüft wird.

Alle von Personio gespeicherten Kundendaten verwenden eine Verschlüsselung at rest. Dies wird mithilfe des AWS KMS durchgeführt und gilt für alle AWS-Services, die Daten speichern, wie RDS, S3 oder EBS. Dieses Verfahren stellt sicher, dass unbefugte Dritte keinen Zugriff auf unverschlüsselte Daten

erhalten können. Alle kryptografischen Schlüssel werden einmal jährlich automatisch rotiert.

Der Einsatz von AWS KMS bei Personio

AWS KMS ist ein Managed Service, der die Erstellung und Kontrolle der Verschlüsselungsschlüssel für die Datenverschlüsselung vereinfacht. Die Hauptschlüssel (Customer Master Key - CMK) in AWS KMS werden durch FIPS 140-2-validierte kryptografische Module geschützt.

Die folgenden Funktionen werden grundsätzlich von AWS KMS unterstützt:

- Anlegen, Beschreiben und Auflisten des Master Keys.
- Aktivieren und Deaktivieren von Master Keys
- Erstellen und Anzeigen von Berechtigungen und Zugriffskontrollrichtlinien für den Master Key
- Aktivieren und Deaktivieren der automatischen Rotation des kryptographischen Materials in einem Master Key
- Importieren von kryptographischem Material in einen AWS KMS Master Key
- Markieren von Master Keys für eine leichte Identifizierung, Kategorisierung und für Tracking
- Löschen von Master Keys zum Abschließen des Lebenszyklusses von Schlüsseln

Die folgenden kryptographischen Funktionen werden von AWS KMS unterstützt:

- Verschlüsseln, Entschlüsseln und Neu-Verschlüsseln von Daten
- Generieren von Schlüsseln zur Verschlüsselung von Daten (Data Encryption Keys)
- Generieren von Zufallszahlen für kryptographische Applikationen

Monitoring

Jeder Zugriff und jede Verwendung von AWS KMS-Schlüsseln wird überwacht und aufgezeichnet. Dadurch kann die Personio GmbH sicherstellen, dass es keine unautorisierten Zugriffe auf die zur Verschlüsselung der Daten verwendeten Schlüssel gibt. Der Zugriff auf das Schlüsselverwaltungssystem wird auditiert und bei Verdacht auf einen Sicherheitsvorfall manuell durch das Security

Engineering Team von Personio überprüft. Außerdem werden AWS KMS-Key Rotation Events in CloudTrail überwacht.

Datentrennung im Rahmen der Verschlüsselung

So wie Personio dafür sorgt, dass die Daten zwischen verschiedenen AWS-Konten strikt getrennt sind (Development, Staging, Testing und Production), sind auch die für die verschiedenen AWS-Konten verwendeten Encryption-Schlüssel strikt getrennt. Ein Schlüssel wird nur in demjenigen AWS-Konto verwendet, für das er erstellt wurde. Ein KMS-Schlüssel von einem AWS-Konto kann nicht zum Ver- oder Entschlüsseln von Daten in einem anderen Konto verwendet werden.

Transport-verschlüsselung (Encryption in transit)

Die Systeme der Personio GmbH verwenden eine Transportverschlüsselung immer dann, wenn Daten über ein unsicheres oder öffentliches Netzwerk (bspw. außerhalb der Virtual Private Cloud) übertragen werden müssen.

Welche Transportverschlüsselung verwendet wird, hängt u. a. von der vom Client-System angeforderten Verschlüsselung ab. Innerhalb des Unternehmens wird nur eine sichere Transportverschlüsselung verwendet. Der Kunde ist dafür verantwortlich, sicherzustellen, dass sein Client-System die entsprechende Transportverschlüsselung nach dem Stand der Technik unterstützt und entsprechend präferiert.

HTTPS

Das Webinterface und die API der Personio-Anwendung sind nur über HTTPS-Verbindungen erreichbar. Client-Systeme müssen mindestens **TLS 1.2** verwenden, um auf das Personio-System zugreifen zu können.

Administrativer Zugang

Der Zugriff auf die Systeme von Personio zu administrativen Zwecken erfolgt ausschließlich über sichere und authentifizierte Verbindungen.

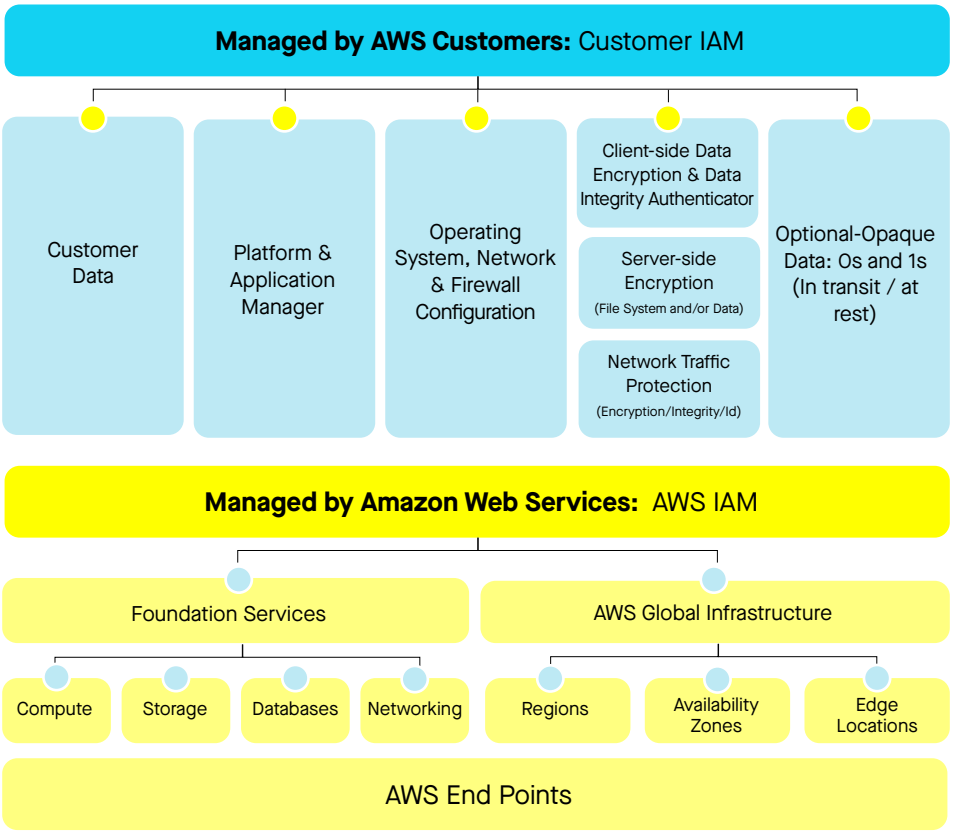
Verantwortlichkeiten im Bereich des Datenschutzes

Personio teilt sich seine Verantwortlichkeiten im Bereich Datenschutz mit AWS. Dabei fallen AWS folgende Assets zu:

- Anlagen (Rechenzentren, Klimatisierung u. ä.)
- Physische Sicherheit der Hardware
- Netzwerk-Infrastruktur (Router, Switches, Kabel etc.)
- Virtualisierungsinfrastruktur
- Betriebssysteme und Software im Fall von SaaS-Diensten

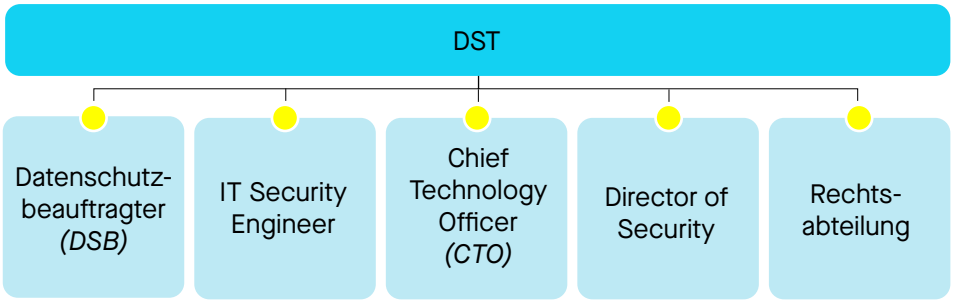
Folgende Assets fallen in die Verantwortlichkeit von Personio, wenn sie im Rahmen von IaaS genutzt werden:

- Amazon Machine Images (AMI)
- Betriebssysteme
- Applikationen und Programmbibliotheken
- Data in Transit
- Data in Rest
- Anmeldeinformationen
- Policies und Konfigurationen



Personio hat für Themen, die den Datenschutz sowie die Datensicherheit betreffen, ein Datenschutz- und Informationssicherheits-Team (DST) gebildet. Abhängig vom konkreten Sachverhalt können verschiedene Personen dieses Teams tätig werden.

Folgende Personen sind Teil des DST:



Zugriffskontrolle

Personio nutzt verschiedene Level der Zugriffskontrolle für seine Systeme und Services bei AWS. Diese werden durch das Identity and Access Management (IAM) von AWS verwaltet, das eine feine Granulierung des Zugriffs auf verschiedene Services innerhalb der AWS-Cloud ermöglicht und den Zugriff auf die Dienste aufzeichnet. IAM-Berechtigungen werden automatisch über SSO bereitgestellt.

Oberstes Prinzip bei der Rechtevergabe ist für Personio „Need-to-Know“. In der Praxis bedeutet dies, dass Mitarbeiter nur auf diejenigen Funktionen Zugriff erhalten, die sie zur Ausübung ihrer Tätigkeiten benötigen. Das Security Engineering Team überprüft in regelmäßigen Audits, ob die vergebenen Zugriffsrechte dem Need-to-know-Prinzip entsprechen.

Der Zugriff auf Backend-Systeme ist nur über sichere und authentifizierte Verbindungen möglich. Eine öffentliche Freigabe von Backend-Systemen ist untersagt.

Dem Need-to-know-Prinzip entsprechend, hat nur eine streng begrenzte Anzahl von Mitarbeitern von Personio Zugriff auf das System, das Kundendaten speichert. Dieser direkte Zugriff dient ausschließlich der Fehleranalyse und wird überwacht.

Firewalling und Security Groups

Zum Schutz vor gängigen Web-Exploits und Bots, welche die Verfügbarkeit beeinträchtigen oder die Sicherheit gefährden können, wird eine Web-Firewall verwendet. Personio verwendet Sicherheitsgruppen, um sicherzustellen, dass AWS-Services nur auf den erwarteten Ports und vom erwarteten Netzwerk aus erreicht werden können.

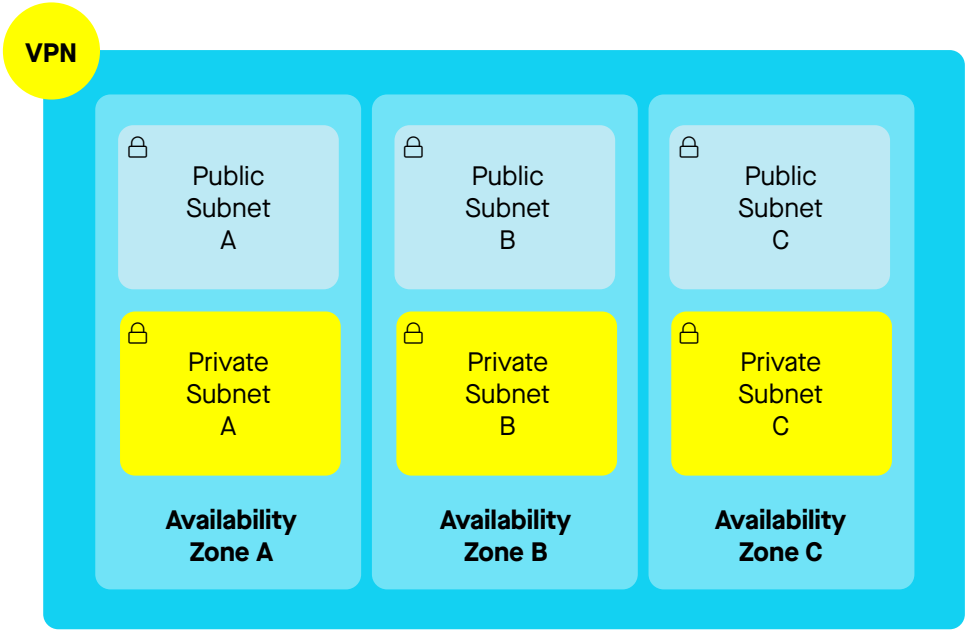
Netzwerktrennung / Verfügbarkeitszonen **/ Geolocation**

Personio stellt eine Trennung von Netzwerken, die für unterschiedliche Zwecke in der AWS-Umgebung genutzt werden, dadurch sicher, dass unterschiedliche AWS-Accounts sowie unterschiedliche VPCs (Virtual Private Clouds) verwendet werden. Ein direkter Netzwerkzugriff zwischen VPCs in verschiedenen AWS-Accounts ist nicht möglich.

Personio speichert Daten ausschließlich in AWS-Rechenzentren in der Europäischen Union. Alle Front-End- und Back-End-Systeme, die von Personio betrieben werden, sind redundant ausgelegt und über mehrere Verfügbarkeitszonen verteilt. So ist sichergestellt, dass selbst beim Ausfall einer Verfügbarkeitszone der Betrieb der Personio-Applikation uneingeschränkt möglich ist.

Jede Verfügbarkeitszone ist an mehrere Internet-Service-Provider angeschlossen und wird durch mehrere Stromkreise versorgt. Sie sind über High-Speed-Links miteinander verbunden, so dass die Applikationen, die auf mehrere Zonen verteilt sind, LAN-Verbindungen nutzen können, um zwischen den Zonen zu kommunizieren. Dies ermöglicht eine optimale Performance aller Systeme, die von der Personio-Applikation genutzt werden.

Das folgende Diagramm zeigt eine typische Netzwerkarchitektur in AWS. Zu sehen ist eine VPC innerhalb einer AWS-Region, die über drei Verfügbarkeitszonen verteilt ist. In jeder Verfügbarkeitszone können verschiedene Subnetze erstellt werden, die entweder öffentlich oder privat sind.



Wir haben ein ähnliches Netzwerk aufgebaut und Best Practices angewendet, um sicherzustellen, dass die Kundendaten nur innerhalb der privaten Subnetze zugänglich sind. Das bedeutet, dass sich unsere gesamte Infrastruktur innerhalb eines privaten Netzwerks (ohne öffentliche IPs) befindet und daher nicht direkt vom Internet aus zugänglich ist. Nur die öffentlich zugänglichen Teile der Infrastruktur, wie z. B. Load Balancer, befinden sich im öffentlichen Netzwerk, da sie für das Routing des Kundenverkehrs verwendet werden.

Intrusion detection / Malware detection / **Logging von sicherheitsrelevanten Ereignissen**

Personio verwendet ein Intrusion Detection System (IDS). Es besteht aus Agents und einem zentralen Master, der die Verfügbarkeit der Agents überwacht und im Falle von Anomalien von den Agents informiert wird.

Das IDS überwacht:

- Logdateien auf ungewöhnliche oder unbekannte Einträge
- Änderungen an Systemdateien (File Integrity Monitoring) sowie AWS-eigene Konfigurationen
- Sämtliche Login-Versuche sowie Rechte-Änderungen innerhalb der Systeme
- Änderungen im Device-Filesystem und den geladenen Kernel-Modulen, um den Anschluss unautorisierter Hardware zu erkennen

- Netzwerktraffic
  - Bekannte Exploits und Rootkits
  - Spoofing
- Alle Änderungen am IDS selbst inkl. Restarts oder Ausfall von Agents
- Durch IAM-Benutzer ausgelöste API-Events innerhalb der AWS-Account-Umgebungen
- Ungenutzte Dienste oder Benutzer auf den jeweiligen Systemen
- Änderungen bei genutzten (Netzwerk-)Ports

Werden sicherheitsrelevante Anomalien auf einem System erkannt, werden diese automatisch den zuständigen Mitarbeitern bei Personio mitgeteilt, die daraufhin eine manuelle Prüfung der Anomalie vornehmen. Besonders kritische Anomalien wie z. B. bei der Erkennung eines Rootkits werden automatisch unterbunden. Weiterhin unterstützt das IDS ein Security Policy Enforcement, das den Anforderungen von PCI DSS 3.0 entspricht. Dieses wird genutzt, um sichere Konfigurationen der laufenden Dienste zu erzwingen sowie mögliche Sicherheitsrisiken (beispielsweise nicht genutzte Systemzugänge) zu erkennen.

Logging / Audit Trail

Personio nutzt in seinen AWS-Umgebungen Logging für verschiedene Bereiche. Diese umfassen:

- System-Ereignisse
- Error Logging
- Benutzer-Aktivitäten
- Anmeldungen sowie Anfragen an Datenbank-Systeme
- Sonstige Security-relevanten Ereignisse / Audit Logging

Durch die Verwendung von AWS Cloudtrail hat Personio die Möglichkeit, sämtliche Events innerhalb der genutzten Cloud-Umgebungen aufzuzeichnen und dadurch nicht nur transparente Benutzer- und Ressourcen-Aktivitäten zu schaffen, sondern auch ein hohes Transparenz-Level zur forensischen Analyse möglicher Sicherheitsvorfälle bereitzustellen.

Die Informationen, die durch Cloudtrail gesammelt werden, werden durch das IDS ausgewertet, um Anomalien zeitnah zu erkennen.

Change Management

Personio verwaltet Konfigurationen von Systemen und Software mittels „Infrastructure as Code“. Der zugehörige Code wird in Repositories einer Versionsverwaltung abgelegt, um Änderungen zeitlich und inhaltlich nachvollziehbar zu machen.

Bevor Änderungen in die Betriebsumgebung eingespielt werden, werden diese in einer Staging-Umgebung, die identisch zur Betriebsumgebung aufgebaut ist, getestet. Dies gilt sowohl für Konfigurationsänderungen als auch für System- und Software-Updates.

Backups

Personio erstellt mindestens tägliche Backups aller Daten, die zum Betrieb der Infrastruktur notwendig sind, sowie aller Daten, die von Kunden in der Personio Applikation eingegeben oder hochgeladen werden.

Performance und Auto Scaling

Personio nutzt sowohl horizontale als auch vertikale Auto-Scaling-Funktionen, die von AWS bereitgestellt werden, um die bestmögliche Leistung zu ermöglichen. Dadurch ist es möglich, vollständig automatisiert Ressourcen zu den Netzwerken zuzuschalten, wenn die vorhandenen Ressourcen nicht mehr ausreichend sind.

Monitoring

Personio nutzt verschiedene Monitoring-Tools, um eine maximale Verfügbarkeit und Performance der Applikation sicherzustellen. Diese überwachen mindestens folgende Parameter:

Verfügbarkeit

- Erreichbarkeit der Applikation
- Erreichbarkeit von Backend-Systemen und -Diensten

Ressourcen

- Auslastung von CPUs
- Auslastung von Netzwerk-Interfaces
- Auslastung von persistenten und flüchtigen Speichern

Performance

- Application Performance Index (Apdex)
- Antwortzeiten der Applikation
- Antwortzeiten von Backend-Systemen
- Abfragezeiten für Datenbankinhalte

Security

- Siehe Abschnitt „Intrusion Detection / Malware Detection / Logging von sicherheitsrelevanten Ereignissen“
- Update-Status von Systemen

Monitoring

- Error logs
- Zugriffslogs

Zusätzlich zu diesem automatisierten Monitoring überwachen Mitarbeiter vom DST einschlägige Online-Medien und Blogs auf das Bekanntwerden von Sicherheitslücken, um zeitnah auf diese reagieren zu können.

Security Audits und Penetrationtests

Personio führt in regelmäßigen Abständen sowohl interne als auch externe Sicherheitstests durch. Zudem wird die Sicherheit der Personio-Applikation regelmäßig durch einen externen, unabhängigen Anbieter auf mögliche Schwachstellen überprüft (Ergebnisse des letzten Penetrationstest sowie den Datenschutz-Auditreport erhalten Sie auf Anfrage, eine Zusammenfassung des letzten Datenschutz-Audits finden Sie auf unserer Datenschutz-Website unter Downloads). Weiterhin werden auch interne Audits durchgeführt, bei denen nicht nur die technischen, sondern auch die organisatorischen Maßnahmen innerhalb des Unternehmens auf ihre Wirksamkeit hin untersucht werden.

Abschließend möchten wir Sie gerne auf unsere Datenschutz-Website personio.de/datenschutz hinweisen, auf der Sie weiterführende Informationen und Dokumente zum Thema einsehen bzw. anfordern können. Sollten dennoch Fragen ungeklärt bleiben, wenden Sie sich gerne an datenschutz@personio.de

Personio