ANLAGE ./A ZU DEN AGB

ALLGEMEINE DATENSICHERHEITSRICHTLINIEN (ADSR) DER LDB LABORDATENBANK GMBH

1. Ansprechpartner für Support und Technik

Für jeden Kunden wird ein primärer Ansprechpartner (First-Level-Support) und ein sekundärer Ansprechpartner definiert der als Vertretung und für den Second-Level-Support zur Verfügung steht, sodass eine optimale Betreuung durchgehend gewährleistet ist.

2. Nutzung der Labordatenbank

Die Labordatenbank ist eine Webanwendung und für die Nutzer mit einem Web Browser unter einer eindeutigen Webadresse erreichbar. Weitere Information zur Nutzung der Labordatenbank und den unterstützen Web Browsern finden Sie in der Labordatenbank Anleitung unter:

Labordatenbank Anleitung: https://labordatenbank.at/manualpages

Unterstützte Browser: https://labordatenbank.at/manualpages/view/24

3. Verfügbarkeit der Labordatenbank Cloud

Die Labordatenbank Cloud ist auf zwei unabhängige Verfügbarkeitszonen verteilt und auf eine Verfügbarkeit von > 99,95% ausgelegt. Das entspricht einer Downtime von weniger als 5 Std. pro Jahr.

Verfügbarkeitszonen (Availability Zones) sind eigenständige Rechenzentren die viele Kilometer voneinander getrennt sind und mit redundanter Stromversorgung, Vernetzung und Konnektivität, so entwickelt wurden, dass sie von Ausfällen in anderen Verfügbarkeitszonen isoliert sind.

Die Labordatenbank Cloud läuft im Rechenzentrum von Amazon AWS in Frankfurt und ist dort parallel auf die Verfügbarkeitszonen eu-central-1a und eu-central-1b verteilt. Die Labordatenbank Cloud ist so aufgebaut, dass sie den Ausfall einer Verfügbarkeitszone standhält und verfügbar bleibt.

Die Labordatenbank wird alle 10 Minuten auf Funktionalität geprüft. Ist die Labordatenbank nicht erreichbar, so wird automatisch Ihr Labordatenbank Ansprechpartner kontaktiert, sodass eine entsprechende Reaktion gestartet werden kann.

Weiter unten ist die Serverarchitektur der Labordatenbank schematisch dargestellt.

4. Schutz vor Zugriff durch Dritte

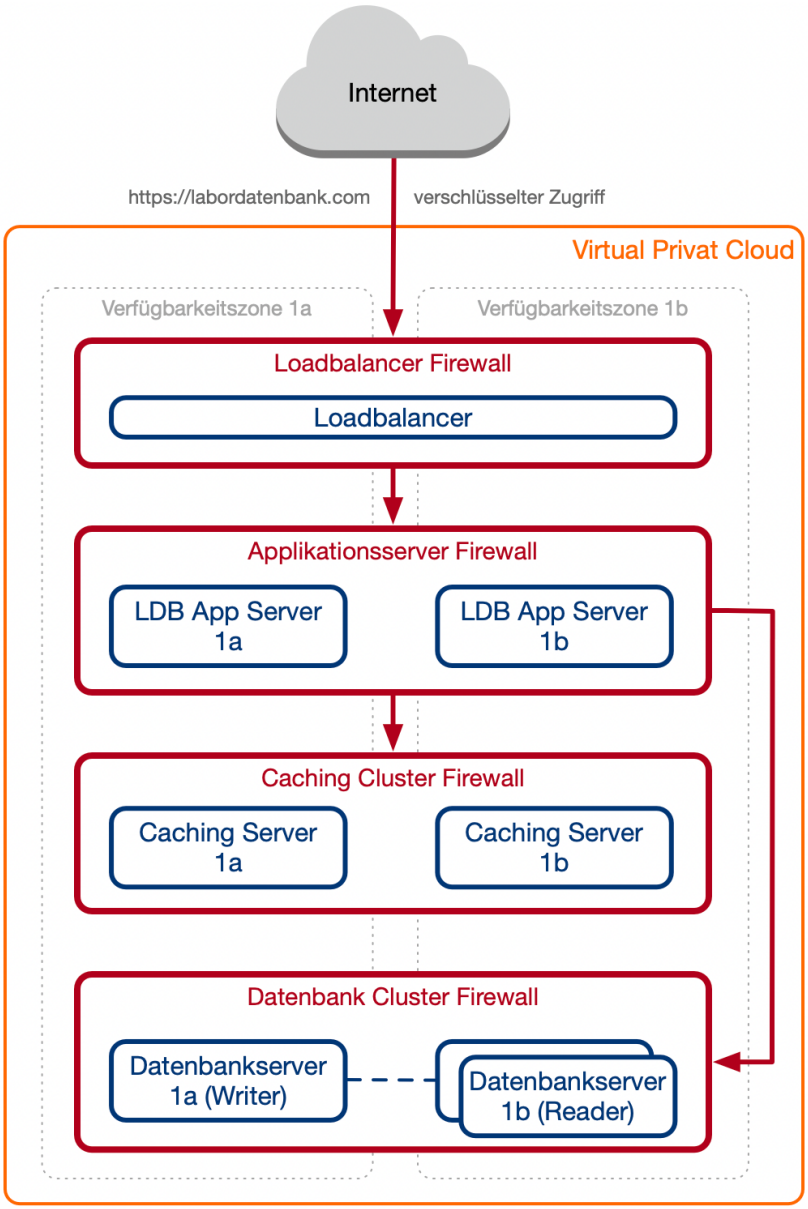
Eine Firewall rund um die Labordatenbank Cloud gewährleistet, dass nur verschlüsselte Zugriffe auf die Labordatenbank möglich sind. Der Zugriff auf die Firewall wird von einem Load Balancer gesteuert, der die Last der Anfragen auf mehrere Anwendungsserver in unterschiedlichen Verfügbarkeitszonen verteilt und nur verschlüsselte Verbindungen über HTTPS mit einer RSA-Verschlüsselung und einer Schlüssellänge von 2.048 Bit zulässt.

Die Anmeldung zur Labordatenbank erfolgt über eine Benutzerauthentifizierung mit Login, Passwort und einem weiteren Sicherheitsfaktor (2-Faktor-Authentifizierung) mit Authenticator Apps wie Authy, Google Authenticator, Microsoft Authenticator, etc. oder mit Security Keys wie YubiKeys, SoloKeys, Google Titan, etc. Die Verschlüsselung der Passwörter erfolgt mit Hilfe des Algorithmus Argon2ID, der nach aktuellem Stand der Technik ungebrochen ist.

Jeder Versuch einer Anmeldung wird mit IP-Adresse und Uhrzeit protokolliert. Versucht jemand mehrmals hintereinander sich mit einem falschen Passwort anzumelden, so wird die Anmeldung zur Labordatenbank für einen definierten Zeitraum gesperrt.

Darüber hinaus ist die Labordatenbank innerhalb der Virtual Privat Cloud (VPC), durch eine Hierarchie von Firewalls geschützt. Der Zugriff vom Internet auf die Labordatenbank erfolgt HTTPS verschlüsselt über einen Loadbalancer. Der Loadbalancer verfügt über eine eigene Firewall welche ausschließlich HTTPS Verbindungen annimmt, eine Sicherheitsprüfungen vornimmt und nur zulässige Datenpakete an die Applikationsserver weitergibt.

Die Applikationsserver enthalten die Labordatenbank Anwendung, aber keine persistenten Daten. Die Applikationsserver sind auf zwei Verfügbarkeitszonen verteilt und durch eine eigene Firewall geschützt.



Der Caching und Datenbank Cluster ist ebenfalls auf zwei Verfügbarkeitszonen verteilt und beide verfügen jeweils über eine eigene Firewall die nur über die geschützten Applikationsserver erreichbar sind (ein direkter Zugriff vom Internet auf den Caching und Datenbank Cluster ist ausgeschlossen).

Die persistenten Daten der Labordatenbank werden im Datenbank Cluster verschlüsselt gespeichert. Dabei verwendet jede Labordatenbank Instanz eine eigene Datenbank mit eigenem Datenbank-Account, sodass ein Zugriff auf Daten von einem anderen Labordatenbank Kunden technisch ausgeschlossen ist.

Für die Verschlüsselung der Datenbanken wird AES-256-GCM verwendet, ein symmetrischer Algorithmus basierend auf Advanced Encryption Standard (AES-256) und Galois Counter Mode

(GCM) mit 256-bit Schlüssel, der von Kryptographen als Quantenresistent angesehen wird. Somit sind die Daten auch vor einem theoretischem zukünftigen groß angelegten Quatencomputerangriff geschützt.

5. Datensicherung der Labordatenbank Cloud

Eine vollständige Datensicherung der Labordatenbank erfolgt laufend auf Amazon S3. Um unseren Kunden absolute Sicherheit zu gewährleisten, wird bei der Labordatenbank jede Sekunde ein inkrementelles Backup erstellt. Darüber hinaus wird täglich ein vollständiges Backup erstellt.

Alle Tagesbackups werden für eine Woche aufgehoben. Nach einer Woche wird ein vollständiges Backup pro Woche bis auf Widerruf, für zumindest die nächsten 10 Jahre aufbewahrt.

Alle in der Labordatenbank hinterlegten Dateien (z.B. wenn Sie Bilder oder Dokumente in der Labordatenbank hochladen) und die täglich erstellten Datenbank Backups werden als verschlüsselte Dateien auf Amazon S3 gespeichert und sind auf eine Datenbeständigkeit von 99,999999999% über ein Jahr ausgelegt (diese Zuverlässigkeitsstufe entspricht einem jährlich zu erwartenden Datenverlust von 0,000000001%). Diese Datenbeständigkeit wird erreicht, indem jede Datei redundant auf drei voneinander unabhängigen räumlich getrennten Rechenzentren (Verfügbarkeitszonen) gespeichert wird.

Alle Dateien werden verschlüsselt gespeichert, wobei jede Datei mit einem eigenen Schlüssel verschlüsselt wird (alle Schlüssel werden mit einem eigenen Masterschlüssel verschlüsselt, welcher laufend geändert wird). Für die Verschlüsselung der Backups wird ebenfalls der 256-bit Advanced Encryption Standard (AES-256) verwendet. Für dieses Verfahren ist kein praktisch durchführbarer Angriff bekannt.

6. Updates zur Labordatenbank

Die Labordatenbank wird laufend gewartet und weiterentwickelt. Während andere Datenbanksysteme keine oder nur spärliche Updates pro Jahr zur Verfügung stellen, gibt es bei der Labordatenbank laufend aktuelle Updates. Die meisten Updates dienen der weiteren Systemverbesserung, Erfüllung normativer Richtlinien und der Entwicklung neuer Funktionen.

Weiters wird die Sicherheit der Labordatenbank von unserer Technik laufend geprüft und verbessert. Mit der Sicherstellung laufender Updates sind auch die Sicherheitseinstellungen immer auf dem aktuellen Stand.

Labordatenbank Versionsverzeichnis: https://labordatenbank.at/updates

7. Erstellung und Unterzeichnung von Berichten

Prüfberichte werden mit der Labordatenbank als PDF erstellt und mit der Labordatenbank unterschrieben.

Das Unterschreiben von Berichten ist nur durch eigens berechtigte Nutzer und Passworteingabe möglich. Durch das Unterschreiben des Berichts wird ein digitaler Schlüssel erstellt, der jeden unterschriebenen Bericht vollständig und eindeutig identifiziert. Dieser Schlüssel wird in der Labordatenbank hinterlegt und kann jederzeit zur Validierung von Berichten herangezogen werden.

Als Teil der Labordatenbank Enterprise Cloud, können Berichte, Angebote und Rechnungen in der Labordatenbank mit einem Zertifikat für elektronische Signaturen unterschrieben werden. Die Labordatenbank verwendet dafür das erweiterte PAdES (PDF Advanced Electronic Signatures) Verfahren. Damit erfüllt die elektronische Unterschrift in der Labordatenbank die fortgeschrittenen Anforderungen der Europäischen Union entsprechend der ETSI EN 319 142 des Europäischen Telekommunikation Standard Institut.

Falls Sie noch nicht über ein Zertifikat verfügen, können Sie ein Zertifikat bei Trust-Liste der Europäischen Union (EUTL) https://helpx.adobe.com/de/document-cloud/kb/european-union-trust-lists.html oder Adobe Approved Trust List (AATL) https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html für Ihr Land bestellen.

8. Anforderungen der ISO 17025 und ISO 9001

Die Labordatenbank erfüllt die Anforderungen der ISO 17025 und ISO 9001 und ist für den Einsatz in akkreditierten Laboren geeignet.

9. Datenschutzerklärung Labordatenbank

Die LDB verpflichtet sich, im Rahmen der Zusammenarbeit mit ihren Kunden das Datengeheimnis sowie sämtliche jeweils geltenden nationalen und europäischen Datenschutzbestimmungen einzuhalten, die für die LDB als Auftragsverarbeiter im Sinne der DSGVO und des österreichischen Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 ab 25.5.2018 gelten.