Technische und organisatorische Maßnahmen zum Datenschutz

der

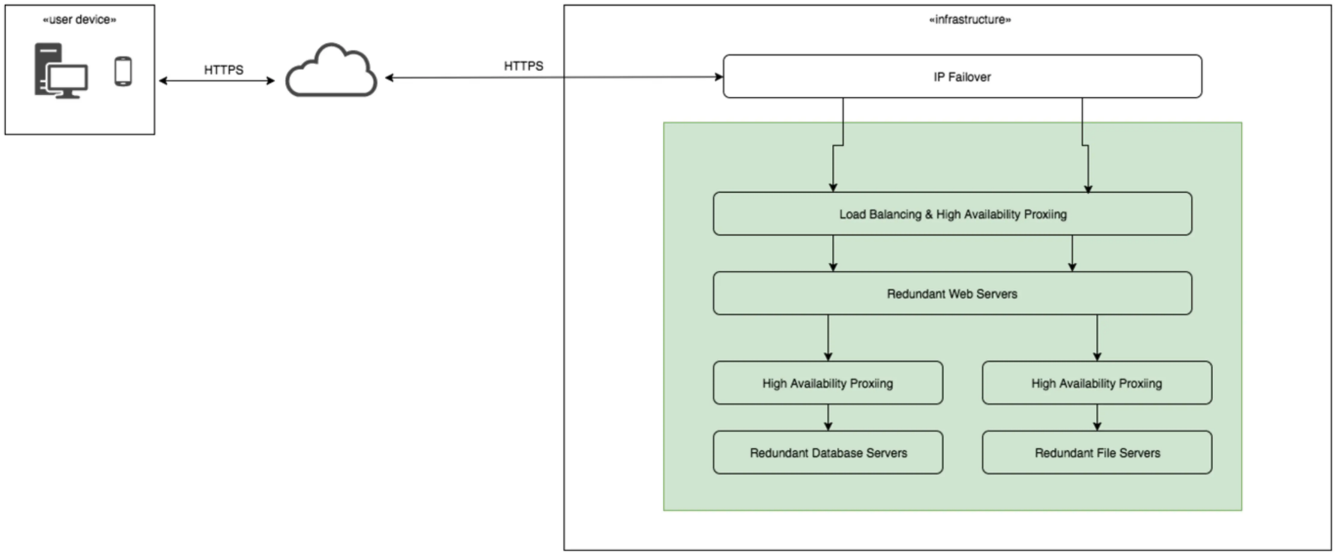
fynk GmbH
Heinrichsgasse 2/8
A-1010 Wien

1. Einleitung

Dieses Dokument soll eine Übersicht über die technischen und organisatorischen Maßnahmen bieten, die fynk im Rahmen seiner Rolle als Auftragsdatenverarbeiter vornimmt, um die Daten des Vertragspartners zu schützen. Dabei hält sich die Struktur des Dokuments an die Vorgaben die sich aus der DSGVO ergeben. Vorab werden allgemeine Informationen bereitgestellt, die das Verständnis der weiteren Angaben erleichtern sollen.

1.1 Systemarchitektur

fynk greift zum Betrieb der Applikation auf die Infrastruktur und Dienstleistungen von Amazon Web Services EMEA Sarl, 38 avenue John F. Kennedy, L-1855, Luxemburg (im folgenden „AWS“) und Microsoft Deutschland GmbH, Walter-Gropius-Straße 5, 80807 München (im folgenden „Azure“) zurück. AWS und Azure sind nach ISO27001 zertifiziert. Zur Wahrung der Datensicherheit setzt fynk unter anderem auf eine softwarebasierte Verschlüsselung aller Datenträger welche Kundendaten beinhalten. Die Architektur ist auf Sicherheit, Skalierbarkeit und hohe Verfügbarkeit ausgelegt, jede für den Betrieb zwingend erforderliche Komponente ist zumindest einfach redundant. Die Systemarchitektur ist in der folgenden Grafik dargestellt.



1.2 Rollen bei fynk mit Datenzugriff

Aus organisatorischer Sicht gibt es mehrere Anwendungsfälle die einen Datenzugriff seitens fynk auf Kundendaten erfordern. Dabei gilt es zu unterscheiden, in welcher Form der Datenzugriff erfolgt:

1.2.1 Zugriff in der Applikation

Um Kunden bei der Einrichtung des Accounts zu helfen und um Fehlerfälle nachvollziehen zu können, können Kundenbetreuer und ggf. Entwickler sich in den Firmen-Account des Kunden einloggen. Hierbei wird jede Aktion (z.B. Datenzugriff und Datenveränderung) die der individuelle User durchführt geloggt.

1.2.2 Zugriff via Datenbank

Um Kunden bei der Einrichtung des Accounts zu helfen und um Fehlerfälle nachvollziehen zu können, können Kundenbetreuer und ggf. Entwickler sich mit der Datenbank verbinden. Hierfür werden individuelle User verwendet, die Datenbankabfragen werden protokolliert.

1.2.3 Zugriff via Server

Für Wartungsarbeiten und Infrastrukturmaßnahmen können Systemadminstratoren von fynk auf die Server auf denen die Kundendaten liegen zugreifen. Dabei werden persönliche User verwendet (kein Sammeluser) und Login und Logout Zeitpunkte auf den Servern geloggt.

2. Vertraulichkeit

2.1 Zutrittskontrolle

fynk greift zum Betrieb der Applikation auf die Infrastruktur und Dienstleistungen von AWS und Azure zurück. Für die Rechenzentren von AWS und Azure werden derzeit folgende Sicherheitsmaßnahmen zur Zutrittskontrolle eingesetzt:

- elektronisches Zutrittskontrollsystem mit Protokollierung
- dokumentierte Schlüsselvergabe an Mitarbeiter und Colocation-Kunden für Colocation Racks (jeder Auftraggeber ausschließlich für seinen Colocation Rack)
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- 24/7 personelle Besetzung der Rechenzentren
- Videoüberwachung an den Ein- und Ausgängen

2.2 Zugangskontrolle

2.2.1 Nutzer

fynk bietet mehrere Arten der Authentifizierung für Nutzer. Prinzipiell kann der Kunde selbst das Schutzniveau konfigurieren. Es gibt sowohl die Möglichkeit einer einfachen Authentifizierung vie E-Mail und Passwort. Als auch die Möglichkeit der Aktivierung von Zwei-Faktor-Authentifizierung mittels Authenticator App.

Das Passwort kann mit Zugriff auf die bei der Registrierung angegeben Email-Adresse zurückgesetzt werden. Dafür wird je nach Einstellung bei der Registrierung automatisch ein Passwort generiert oder es kann ein eigenes Passwort gewählt werden. Das Passwort kann mit Zugriff auf die bei der Registrierung angegeben Email-Adresse zurückgesetzt werden.

Die Passwortrichtlinie für Nutzer ist: Mindestens 8 Zeichen

2.2.3 Kundenbetreuer

Der Login der Kundenbetreuer ist mit Email, Passwort und zwei Faktor-Authentifizierung gesichert. Die vorgegebene Passwortrichtline von fynk lautet:

- Mindestens 11 Zeichen länge
- Zumindest drei Arten von Zeichen (Großbuchstabe, Kleinbuchstabe, Zahl, Sonderzeichen)
- Passwortrotation alle 6 Monate
- Die letzten 10 Passwörter dürfen nicht verwendet werden

2.2.4 Serveradministratoren

fynk verhindert den unbefugten Zugang zur fynk Infrastruktur einerseits durch den Einsatz von RSA-Schlüsseln. Autorisierte fynk-Administratoren haben einen persönlichen Schlüssel mit dem sie sich zu den Servern verbinden können, die sie für Ihre Arbeit brauchen. Bei der Schlüsselvergabe folgen wir dem Least-Privilege Prinzip, Mitarbeiter bekommen nur Zugang zu Systemen die sie unbedingt brauchen. Andererseits wird der Zugang zur fynk Infrastruktur mittels durchgehender Zwei-Faktor-Authentifizierung mittels FIDO-Schlüsseln sichergestellt.

2.3 Zugriffskontrolle

2.3.1 Nutzer

Die Zugriffskontrolle wird vom System entsprechend der Konfiguration durch den Kunden umgesetzt. fynk bietet ein Rollen- und Berechtigungssystem welches Kunden in der Applikation selber Konfigurieren können. Die Vergabe und periodische Überprüfung der vergebenen Berechtigungen obliegen dem Kunden. Zugriffe von Nutzern in der Applikation werden protokolliert.

2.3.2 Kundenbetreuer

Für Kundenbetreuer obliegt die Zugriffskontrolle fynk. Durch organisatorisches Onboarding und Offboarding Prozesse wird sichergestellt, dass vergebene Berechtigungen aktuell sind.

Zusätzlich werden regelmäßig alle vergebenen Berechtigungen überprüft. Zugriffe von Kundenbetreuern werden protokolliert.

2.3.3 Systemadministratoren

Für Systemadministratoren obliegt die Zugriffskontrolle fynk. Durch organisatorisches Onboarding und Offboarding Prozesse bei neuen Mitarbeitern bzw. bei Abgängen wird sichergestellt, dass vergebene Berechtigungen aktuell sind. Zusätzlich werden monatlich alle vergebenen Berechtigungen überprüft. Login-Zeitpunkte von Systemadministratoren werden auf allen Servern protokolliert.

Alle Mitarbeiter von fynk sind auf das Datengeheimnis verpflichtet, diese Verpflichtung behält ihre Wirkung auch nach einer Kündigung.

3. Integrität

3.1 Weitergabekontrolle

fynk folgt bei der Weitergabekontrolle dem Least-Privilege Prinzip: Daten werden nach Möglichkeit nicht weitergegeben. Die Produktivdaten liegen ausschließlich in Produktion- und Backupsystem. In Ausnahmefällen werden Produktivdaten in ein Testsystem eingespielt, hier gibt es einen definierten Prozess nach dem vorgegangen wird und der sicherstellt, dass die Daten sobald die notwendigen

Tests erfolgt sind, wieder gelöscht werden. Daten werden immer über verschlüsselte Kanäle übertragen, welche unbefugtes Lesen, Kopieren, Verändern oder Entfernen technisch verhindern. Backups werden vor der Übertragung verschlüsselt.

3.2 Eingabekontrolle

In der Applikation wird jede Anfrage von eingeloggten Nutzern protokolliert. Dadurch können Veränderungen oder Löschungen von Daten nachvollzogen werden. Das gilt auch für Mitarbeiter von fynk. Auf den Servern werden Login-Zeitpunkte von Systemadministratoren protokolliert.

4. Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeit

Hohe Verfügbarkeit ist kritisch für den Erfolg von fynk. AWS und Azure bieten sowohl auf Hardware-Ebene als auch auf Software-Ebene höchste Standards bezüglich Verfügbarkeit.

Die Architektur der Applikation ist auf „High Availability“ ausgelegt. „Single Points of Failure“, also Soft- und Hardware-Komponenten die bei einem Ausfall die Verfügbarkeit von fynk einschränken werden durch redundante Infrastruktur vermieden.

Durch eine erprobte Backupstrategie vermeiden wir Datenverluste weitestgehend. Datenbankbackups werden alle 2 Stunden abgelegt, Dateien alle 24 Stunden. Dabei kombinieren wir Vollspeicherungen mit inkrementellen Backups. Backups werden auf 3 verschiedenen Maschinen repliziert und zumindest halbjährlich testweise auf einem Testsystem eingespielt.

Durch die Dienstleistungen von AWS erfüllt fynk die höhsten Anforderungen bezüglich Netzwerksicherheit und DDoS Prävention.

4.2 Belastbarkeit

Die Belastbarkeit von fynk wird durch regelmäßige Kapazitäts- und Ressourcenplanung in der Infrastruktur sichergestellt.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Datenschutz-Management

fynk nutzt Software für das Datenschutz-Management. Hier werden relevante Dokumente abgespeichert und etwaige Änderungen im Datenschutz dokumentiert.

Mitarbeiter werden zumindest jährlich oder bei relevanten Neuerungen geschult.

5.2 Incident-Response-Management

Datenschutzrechtlich relevante Vorfälle werden nach einem definierten Prozess behandelt. Sollten Kundendaten betroffen sein werden die Kunden entsprechend der vertraglichen Regelungen benachrichtigt. Wenn durch den Vorfall behördliche Meldepflichten entstehen wird fynk diesen entsprechen.

5.3 Datenschutzfreundliche Voreinstellungen

Die Applikation unterstützt Datenschutzprozesse an vielen Stellen. Die Voreinstellungen sehen minimale Datenerfassung und automatisierte Datenlöschung nach entsprechenden Fristen vor. Fynk unterstützt Kunden bei der Konfiguration des Systems entsprechend den spezifischen Anforderungen bzgl. Datenschutz.

6. Auftragskontrolle

Zur Sicherstellung der Auftragskontrolle, also dass fynk die Daten der Kunden ausschließlich im Sinne der Kunden verwendet, wird ein Vertrag zur Auftragsdatenverarbeitung geschlossen, in dem Rechte und Pflichten beider Parteien definiert sind.