Rapport sécurité liée au projet d'intégration.

De Dryver Cédric
Bombaert Andréas
Schamroth Arthur
Dieuzeide Gael
Brichant Vincent
Carlier Louis

Projet d'intégration :
Application citoyenne

Introduction :

Dans le cadre de notre projet d'intégration, nous avons besoin d'avoir une application qui nécessite une sécurité rigoureuse afin de protéger nos utilisateurs. Nous utilisons plusieurs services afin d'avoir une gestion plus simple de nos comptes utilisateurs, mais aussi une sécurité renforcée, mais que nous ne maitrisons pas totalement. Nous n'utilisons pas de serveurs pour notre application, mais nous utilisons une base de données via le service de Google : Firebase. Nous enregistrons quelques informations utilisateurs, mais principalement des données liées à notre application (Coordonnés GPS, etc.). Donc en finalité, peu d'informations qui peuvent mettre en danger nos utilisateurs.

I. Gestion des comptes utilisateurs.

Pour notre application, nous avons besoin de compte utilisateurs, pour plusieurs raisons, par exemple pour la gestion des points dans l'application, ou pour avoir une meilleure modération, etc. Pour cette gestion des comptes utilisateurs, nous utilisons un service qui nous permet de sous-traiter automatiquement cette tâche. Ce service se nomme Auth0, et il est utilisé par beaucoup de grosses entreprises, gérant ainsi plus de 10 000 clients, et ils sont en partenariat avec plusieurs géants, tels que Microsoft ou AWS.

Une autre qualité d'utiliser Auth0 c'est que nous dépendons de leur sécurité, ce qui peut être à double tranchant, car ils ont mis en place beaucoup de protocoles et de solutions pour renforcer leur sécurité et donc celles de leurs clients, mais si un attaquant réussit à exploiter une faille, alors beaucoup d'utilisateurs seraient touchés par cette attaque, sans que nous puissions y faire quelque chose. Mais ils ont bien conscience de ce problème et ils ont mis en priorité le fait d'assurer une sécurité fiable pour leurs clients.

A) Conformité

Auth0 dispose de plusieurs certificats de sécurité et de réglementations qui permettent d'assurer que leur sécurité a été évalué approuvé par des organisations qui sont spécialistes dans ce domaine. Ils possèdent ces certifications :

- SOC 2 Type 2
- ISO 27001 et 27018.

Le SOC (Contrôles système et d'organisation) est un rapport de contrôle interne créé par l'American Institute of Certified Public Accountants (AICPA), qui examine les services fournis par une organisation de services afin que les utilisateurs finaux puissent évaluer et traiter les risques associés à un service externalisé.

L'ISO 27001 et la norme la plus connue de la famille des ISO. Elle spécifie les exigences relatives aux systèmes de management de la sécurité des informations, afin d'avoir la certitude que l'organisation qui la possède, a une facilité sur le management de la sécurité d'actifs sensibles (données financières, documents de propriété intellectuelle, données relatives aux personnels ou informations confiées par des tiers).

L'ISO 27018 concerne la protection des données à caractères personnels dans le cloud computing (car Auth0 est basé sur le cloud). Elle assure que les mesures de protections des informations personnelles sont bien appliquées dans le contexte des environnements de sécurité de l'information d'un fournisseur de services publics et des services de cloud computing.

Auth0 indique aussi qu'il respecte certaines règlementations, comme le RGPD pour l'Europe et le HIPAA pour l'Amérique.

B) Surveillance de la sécurité

Auth0 dispose d'un SIEM (Security Information and Event Management) qui collecte des données de leurs services afin de les analyser et les appliquer dans du Machine Learning avec détection automatique. Cela permet d'avoir un centre d'opération 24/7 qui surveille en permanence et fournit des alertes en temps réel a Auth0 afin d'intervenir au plus vite.

C) Réponses aux incidents

L'équipe des opérations de sécurité d'Auth0 maintient une fonction d'analyse numérique légale et de réponse aux incidents (DFIR). Leurs processus de réponse aux incidents, contiennent des « Escalations path » (ce qui signifie que si un problème ne peut pas être résolu dans un délai convenu, il est rapidement porté à un niveau de responsabilité approprié pour une résolution adéquate) pour les membres seniors et pour les membres du personnel exécutif, et il est testé chaque année.

D) Gestion de vulnérabilités

Auth0 réalise des scans journaliers et hebdomadaires automatiques de vulnérabilité sur tous leurs serveurs et instances. Ils effectuent aussi des tests d'intrusions tiers au moins tous les 6 mois. À chaque nouvelle fonctionnalité, ils effectuent des tests d'intrusion tiers de bout en bout, et ils ont aussi mis en place un programme de White Hat, qui permet d'avoir un programme de divulgation responsable (RDP) qui encourage les chercheurs « white Hat » à enquêter sur les services et aussi les produits de Auth0.

E) Cryptage des données au repos et en transit

Auth0 a comme responsabilité des données d'identité « critique », et assure qu'elles ne tombent jamais entre les mains de personnes extérieures. Ils ne stockent aucun mot de passe en texte clair, ils sont toujours hachés grâce à Bcrypt, et ils ont renforcé leur sécurité face aux « Rainbows tables » qui est une des failles de Bcrypt. Ils ont donc établi un système de salage, qui consiste à ajouter une donnée supplémentaire afin d'empêcher que deux informations identiques conduisent à la même empreinte.
Ils ont choisi Bcrypt car les résultats de cette méthode atteignent les propriétés fondamentales d'une fonction de mot de passe sécurisé telles que définies par ses concepteurs (Niels Provos and David Mazières) :

- Il est résistant à la pré-image.
- L'espace pour le salage est suffisamment grand pour atténuer les attaques de précalcule, tels que les Rainbow tables.
- Il a un cout adaptable

Les concepteurs de Bcrypt pensent que la fonction conservera sa force et sa valeur pendant de nombreuses années. Sa conception mathématique donne l'assurance aux cryptographes de sa résistance aux attaques.

En ce qui concerne le cout adaptable, nous pourrions dire que Bcrypt est une fonction de hachage adaptative, car nous sommes en mesure d'augmenter le nombre d'itérations effectuées en fonction d'un facteur clé transmis : le coût. Cette adaptabilité permet de compenser l'augmentation de la puissance informatique, mais elle a un coût d'opportunité, il faut choisir entre la rapidité et la sécurité.

Assez parlé de Bcrypt, intéressons-nous maintenant aux données. Certaines données au repos et en mouvement sont cryptées. Toutes les communications réseaux utilisent la couche de transport sécurité (TLS) avec un cryptage AES (Advanced Cryptage Standard) d'au moins 128 bits.

La connexion utilise TLS, et elle est chiffrée et authentifiée à l'aide d'AES_128_GCM et utilise ECDHE_RSA comme mécanisme d'échange de clés.

F) Protection DDoS

Tous les services Auth0 ont des fonctionnalités intégrées de limitation de débit et de blocage automatisé pour atténuer les attaques par déni de service ou d'authentification. L'infrastructure Auth0 est aussi protégée contre les attaques volumétriques de leurs fournisseurs de cloud, en plus d'un service d'atténuation DDoS dédié. De plus, pour protéger la plateforme, le système Auth0 impose des limites de débit aux APIs et aux appels de base de données.

II. Gestion des données

Comme expliqué dans l'introduction, notre application utilise les services de Firebase lorsqu'il s'agit de stocker des données. Firebase étant un service Google, la sécurité est prise très au sérieux à travers plusieurs points.

A) RGPD & CCPA

Firebase gère le RGPD de la manière suivante : le client est responsable du contrôle des données et par conséquent du respect des droits d'individus, en l'occurrence nos utilisateurs.

Le RGPD et le CCPA (California Consumer Privacy Act) imposent des règles aux contrôleurs de données et leurs sous-traitants, c'est-à-dire que, dans ce cas, pour toutes les données des utilisateurs que Firebase fournit à Google, Google se doit d'appliquer à la lettre les règles du RGPD.

En plus du RGPD, les services Firebase sont régis par les conditions d'utilisation Google Cloud et les conditions d'achat Google. La liste complète de ces conditions d'utilisation est disponible sur le site de Firebase.

B) Conformité

Firebase est, comme Auth0, certifié selon certaines normes de confidentialité et de sécurité avec pour les processus d'évaluation :

- L'ISO 27001
- SOC1
- SOC2
- SOC3

Et pour les processus de certification :

- ISO27017
- ISO27018

Toutes ces normes sont respectées pour le premier service que nous utilisons sur Firebase, à savoir le Cloud Firestore.

Pour revenir sur l'ISO 27017, elle fournit des conseils en termes de contrôle et de mise en œuvre de services cloud aux entreprises, mais également aux clients. Elle fournit ces conseils par rapport aux contrôles décrits dans la norme ISO 27002.

En ce qui concerne la base de données Realtime Firestore elle n'est couverte que par les processus d'évaluation cités ci-dessus.

Firebase est également tenu de se conformer aux exigences de protection des données par rapport à l'Espace économique européen, du Royaume-Uni ou de la Suisse vers les USA, etc. Firebase doit donc avoir une base légale pour les transferts de données conformément aux lois ou la plateforme est utilisée.

C) Traitement de données

Les services Firebase traitent les données personnelles de certaines manières en fonction des services utilisés, pour les services que nous utilisons voilà leurs caractéristiques :

- Realtime Firebase :

Données personnelles	**Manière dont les données aident**
Adresses IP et Agents utilisateurs	**Comment ça marche :** la base de données utilise les données personnelles pour aider les clients à comprendre les tendances d'utilisation et les pannes de plateforme
	Conservation : La base de données conserve les données pendant quelques jours à moins que le client choisisse de l'enregistrer plus longtemps

- Cloud Firebase

Données personnelles	**Manière dont les données aident**
Adresses IP	**Comment ça marche :** La base de données utilise les adresses IP pour exécuter des fonctions de gestion d'événements et d'HTTP
	Conservation : Les adresses IP sont gardées temporairement pour fournir le service

D) Sécurité

Les données sont chiffrées lorsqu'elles transitent grâce à HTTPS, mais également lorsque les données sont au repos (c'est valable pour les deux services Firebase que nous utilisons).

Firebase utilise des mesures de sécurité étendues pour minimiser l'accès :

- Les employés qui ont un objectif professionnel à atteindre les données personnelles ont un accès restreint
- L'accès des employés aux systèmes contenant des données personnelles est enregistré
- L'accès aux données personnelles est uniquement autorisé aux employés se connectant avec l'authentification 2 facteurs.

De plus, nous pouvons contrôler si nos services Data Firebase peuvent-être utilisés par Google pour analyse approfondie, des idées et recommandations sur des services non Firebase Google.

III – Service, Réseau et communications

Notre application comporte une partie client-side et une base de données. Nous ne possédons aucun serveur. Cela signifie plusieurs choses : Nous ne pouvons mettre en place des sécurités sur l'isolation des services et des réseaux. De plus, nous n'avons pas mis en place de site web, car tout ce fait via l'application mobile, donc nous ne pouvons pas obtenir de certificat SSL ainsi que chiffrer les communications, car les seules communications sont des appels à la base de données et des appels à différentes API tels que Google ou le service Auth0. Ces services de sécurité ne sont pas mis en place à notre échelle, mais sont présentes dans les services que nous utilisons, mais leur documentation n'est pas open-source, car cela engendrerait des risques pour les services en question, mais on suppose que via certains certificats (tels qu'ISO 27001) certifie que nos services possèdent une isolation des service et réseau conforme, et que nous pouvons leurs faire confiance.

A) SSL – TLS

Pour ce qui est des certificats de chiffrement des données, nous ne disposons d'aucun certificat, car nos données ne passent pas par un serveur, mais nos services disposent de certificat sur le chiffrement des données qu'ils nous envoient. Auth0 dispose d'un ensemble sécurisé de combinaison de version SSL / TLS / cipher suite combinations.

B) Redondance des atouts critique

Nous n'utilisons pas non plus d'outils tels que les RAIDs car nous ne gérons pas directement la base de données, et il n'existe pas de documentation sur l'utilisation de RAID pour Firebase, de même sur l'utilisation d'un HAPROXY, mais ils assurent une redondance via leur multiplicité de points de présence à travers le monde, nos données sont répliquées sur les appareils de stockage de plusieurs sites. Cependant, pour Auth0, ils expliquent qu'ils veillent à ce que leurs dépendances critiques soient redondante. Ils détectent rapidement les pannes et ainsi leurs failover est rapide. Leur architecture implémente des composants redondants à tous les niveaux à tous les niveaux : DNS, Centre de données, Couche d'application et au stockage. Ils ont mis en place une stratégie de haute disponibilité afin de pouvoir assurer un accès constant à leurs services cloud.

C) Politiques, DRP, RPO/RTO

Pour nos politiques au niveau DRP, RPO et RTO, nous ne possédons rien, car nous dépendons toujours de nos services et aucun désastre ne peut arrêter notre activité, car nous ne possédons aucune infrastructure. Si un des services que nous utilisons venait à cesser de fonctionner à cause d'un désastre, nous devons compter sur leurs plans de reprise d'activité ainsi que leurs procédures en cas de panne. Mais si nous devons compter sur la certification ISO 22301 du côté de nos services, ni Firebase, ni Auth0 ne possède cette certification.

C’est également le cas pour les objectifs de reprise d’activité et les objectifs de perte de données maximale admissible, nous ne sommes pas affectés par ces principes, de plus si l’un de nos services venait à affecter le bon fonctionnement de notre application, le coût serait à l’heure actuelle minime, car ils assurent une redondance forte de nos données.

IV – RGPD de notre application

Notre application respecte le GDPR sous plusieurs aspects :

A) Localisation

La permission pour accéder à la localisation de l'utilisateur est demandée à chaque fois qu'un utilisateur utilise l'application pour la première fois et il peut changer son choix à tout moment. De plus la localisation de l'utilisateur n'est utilisée que lorsqu'il utilise l'application et elle n'est enregistrée sous aucune forme.

Seul Google peut potentiellement utiliser la localisation à d'autres fins, mais ça nous ne pouvons rien faire à notre échelle.

B) Gestion des données des comptes

Les informations des comptes seront gardées uniquement à des fins de bon fonctionnement de l'application, elles ne seront conservées que le temps dont nous en avons besoin et l'utilisateur pourra supprimer son compte à n'importe quel moment où il le décidera. Il pourra également modifier les données de son compte à tout moment et si l'utilisateur vient à ne plus utiliser l'application nous finirons par supprimer ses données inutilisées après un certain temps.

C) Sécurité des données

Nous aurons une personne qui se chargera de la sécurité des données en temps réel et nous aurons mis en place plusieurs solutions de sécurité afin d'éviter que les données des utilisateurs soient interceptées par des personnes mal intentionnées.

D) Solutions mises en place

Nous allons faire une section dans l'application où l'utilisateur aura accès à toutes les informations concernant le stockage de ses données ainsi que la sécurité liée à celles-ci. L'utilisateur pourra ensuite contacter les administrateurs si un point ne lui plait pas ou s’il souhaite effacer ses données de notre base de données.

V – Gestionnaire de source

Nous utilisons comme gestionnaire de source GitHub, qui permet de travailler a plusieurs sur une même application sans risque de conflit, cependant notre repository est en public, pour que vous puissiez voir notre travail. Mais comme le repository est en public, nous avons donc nos clés de nos API qui sont aussi en public. Nous nous en sommes rendu compte trop tard, et nous avons mis nos clés dans notre. Git ignore afin qu'elles restent cachées. Nous avons installé un outil permet de vérifier les pull requests afin de détecter si certaines clés ou informations qui sont censés être caché, et nous le notifie dans le cas contraire. Ainsi, grâce à GitGuardian nous n'avons plus à nous soucier qu'une personne tierce récupère nos clés sensibles.