PROGENDA

Politique de Sécurité

Infrastructure et services externes

Nos services sont hébergés sur un ensemble de serveurs dédiés fournis par la société française OVH. Cette société est donc soumise au droit européen sur la protection des données et couverte par différentes certifications de sécurité : PCI-DSS, ISO/IEC 27001 et SOC 1 et 2.

Nos données sont répliquées à plusieurs niveaux : au niveau du serveur premièrement, via l'existence d'un système RAID (« Redundant Array of Independent Disks »). Ce système fournit chacun de nos serveurs de deux disques durs clones. En cas de défaillance de l'un des deux disques, celui-ci peut être remplacé sans interruption de service pour le serveur, le disque dur restant assurant seul les opérations.

Au niveau centre de données (« datacenter »), l'ensemble de nos bases de données (serveurs de fichiers, bases de données relationnelles et non-relationnelles, caches et moteurs d'indexation) sont répliquées sur plusieurs serveurs, garantissant ainsi un service continu même en cas de crash de serveur.

Nos serveurs applicatifs sont également dupliqués et placés derrière un répartiteur de charge (« load balancer ») qui s'assure que chacun des serveurs reçoive une part égale de requêtes à traiter et qui, en cas de défaillance de l'un des serveurs, redirigera automatiquement les requêtes vers les serveurs restants.

Enfin, toutes les connexions entrantes publiques sont placées derrière une protection anti-DDOS, fournie par la firme Cloudflare, qui figure parmi les leaders du marché.

Un service d'archivage (« backup ») quotidien sauvegarde également l'entièreté de notre base de données et l'exporte sur un système de stockage externe à notre centre de données principal.

Nous disposons d'un serveur central faisant office de journal des événements (« log »). Toutes les requêtes (provenant des patients, des médecins, du personnel de nos clients ou de notre personnel) y sont enregistrées. Cela permet de savoir qui a accédé à une certaine page à un moment bien précis ou de retracer toute la navigation d'un visiteur en particulier. Certaines données (mots de passe, token, etc.) sont filtrées pour ne pas être enregistrées dans nos logs.

Tous nos serveurs sont surveillés par un partenaire externe (New Relic) qui analyse la performance de nos services et nous avertit par plusieurs moyens de communication en cas de surcharge de l'un de nos serveurs. Cette société n'a pas accès aux données de nos bases de données.

Les différentes erreurs générées sur nos serveurs (page introuvable, erreur dans un mot de passe, envoi d'email ou de SMS à des adresses ou numéros erronés, etc.) sont également gérées par un fournisseur externe (la société néerlandaise AppSignal). Celui-ci enregistre l'adresse de la page, l'heure, le navigateur web utilisé, etc. mais les données personnelles (par exemple les données de formulaire) ne lui sont pas envoyées. Les erreurs générées sur les navigateurs sont elles traitées par la société Sentry. A nouveau, aucune donnée personnelle n'est traitée, il ne s'agit que d'informations concernant nos codes.

Pour plus de détails sur nos services, veuillez vous référer au registre des activités de traitement présent dans la Convention de traitement des données à caractère personnel.

Sécurité de l'application

Progenda intègre toutes les techniques modernes de sécurisation des applications web. Afin de ne pas affaiblir l'intégrité de nos mesures de sécurité, la liste ci-dessous n'est pas exhaustive.

Toutes nos pages sont protégées par une liste blanche stricte de règles « Content Security Policy ». Ces règles décrivent les origines possibles du code s'exécutant sur vos pages et les connexions autorisées. Elles servent de protection supplémentaire en cas de faille dans notre code ou celui de nos fournisseurs.

Toutes les actions qui entraînent un changement d'état sont protégées par un token CSRF. Ces actions nécessitent toujours une méthode HTTP appropriée (POST, PUT, PATCH ou DELETE). Les requêtes depuis une origine externe autorisée (CORS) sont filtrées par une liste blanche stricte et sont limitées à certaines pages contenant uniquement de l'information publique. Nous interdisons l'intégration de Progenda dans une Iframe, afin d'éviter tout click-jacking. Tous les liens ouvrant de nouveaux onglets sont protégés par un attribut « noopener », empêchant une prise de contrôle de la page initiale par la page ouverte.

Notre système de sessions est basé sur des cookies qui ne peuvent être lus par du code s'exécutant sur le navigateur (« HttpOnly »), qui ne peuvent être envoyés au travers d'une connexion non-sécurisée (« Secure ») et qui ne peuvent être envoyés lors d'une requête depuis une page étrangère à Progenda (« SameSite »).

Les mots de passe de nos utilisateurs sont hashés avec l'algorithme BCrypt avant d'être enregistrés en base de données. L'accès à notre API se fait à l'aide de jetons (« tokens »)

générés depuis l'interface d'administration. Après génération, le token est également hashé avec l'aide de BCrypt avant d'être enregistré. Ces tokens sont révocables depuis l'interface.

Toutes les requêtes s'adressant aux serveurs de Progenda doivent être établies au travers d'une connexion chiffrée (HTTPS). Les requêtes en clair sont redirigées. Notre domaine est protégé par une politique HSTS, interdisant au navigateur d'utiliser une connexion non-sécurisée. Cette information a été inscrite dans le code source des navigateurs utilisant des listes de domaines protégés (« preload »).

Nous n'autorisons plus les protocoles de chiffrement antérieurs à TLS 1.1. Cela signifie également que les versions de Internet Explorer antérieures à Internet Explorer 11 ne sont plus supportées.

Les autorités habilitées à générer un certificat pour nos domaines sont inscrites dans le champ DNS CAA. Nous monitorons la publication de nouveaux certificats pour nos domaines via le programme Certificate Transparency. Nos champs DNS sont également protégés par l'extension DNSSEC.

Les connexions entre notre fournisseur Cloudflare et nos serveurs « origine » sont également chiffrées. Seuls les serveurs de Cloudflare peuvent accéder au service web sur nos serveurs, protégeant l'identité de nos serveurs aux yeux des robots parcourant le net.

Nos emails sont signés et authentifiés via le protocole DKIM. Les adresses habilitées à envoyer des emails en notre nom sont spécifiées via le champ SPF. Ces deux mesures sont imposées de manière stricte par notre champ DMARC. Tout email ne respectant pas les conditions ne peut atteindre la boîte de réception du destinataire.

Plusieurs politiques anti-DoS ont été mises en place : pour chaque requête HTTP, toutes les procédures trop longues ou qui peuvent être exécutées plus tard sont placées en tâche de fond, afin de garantir une réponse rapide et de ne pas remplir le pool de requêtes. Toutes nos boucles n'opérant pas sur des collections sont limitées par des compteurs supplémentaires, afin d'éviter toute boucle infinie. Nos expressions régulières (regex) n'utilisent pas de backtracking.

La prise de rendez-vous est protégée par plusieurs mesures de sécurité, telles que des captchas, l'enregistrement de l'adresse IP sur chaque rendez-vous pris, la limitation du nombre de rendez-vous sur base de l'adresse IP ou de l'adresse email ou l'utilisation de whitelist et de blacklist de personnes pouvant prendre rendez-vous (au choix de l'utilisateur).

Nous avons également mis en place des politiques de suppression de données afin d'éviter toute perte de données involontaire. Ainsi, selon le type de ressource à supprimer, celle-ci sera uniquement marquée comme supprimée, marquée comme supprimée et à supprimer réellement à une date ultérieure ou bien supprimée immédiatement.

Toutes les données au coeur de Progenda sont également exportables depuis l'interface. Nous considérons que tout client désirant arrêter le service doit pouvoir récupérer ses données aussi

facilement que possible et que l'accès aux données ne doit pas constituer un frein au départ du client.

Nous avons évalué les deux mesures de sécurité HPKP et SRI comme étant inutiles au vu des mesures déjà en place et/ou dangereuses pour la stabilité du système.

Procédures internes et formations

Les équipes de Progenda (techniques et non-techniques) sont sensibilisées à la sécurisation des données de manière régulière. Nous avons une approche holistique de la sécurité : plusieurs éléments sécurisés de manière individuelle peuvent représenter une faille de sécurité lorsqu'ils se combinent.

Cette vision est communiquée de manière transversale dans l'entreprise, afin de responsabiliser chacun sur ses propres actions en tant que maillon d'une chaîne de sécurité. Une telle sensibilisation nous permet de mettre en place une défense en profondeur. De manière concrète, son application implique par exemple un principe de moindre privilège, autant dans le produit que dans les procédures qui l'entourent.

Elle entraîne également une sensibilisation à la mise à jour continue des différents appareils et logiciels utilisés dans le cadre professionnel, qui sera vérifiée de manière régulière.

Nous avons de plus réalisé une analyse de risque (basée sur une approche développée par Microsoft, « Threat Modeling Web Applications »), en incluant tous les membres de l'équipe, en listant l'ensemble des risques auxquels nous étions sujet et en les catégorisant (probabilité x impact du risque).

Les équipes de développement sont formées au travers de conférences internationales ayant comme thème principal la sécurité informatique. La participation à un minimum de deux conférences par an est obligatoire.

Chaque ligne de code est analysée à la fois par plusieurs développeurs (via un système de « code reviews ») et par différents systèmes d'analyse statique de code. Une suite de tests automatique est lancée pour chaque modification dans le code. Des systèmes d'analyse de dépendances sont également mis en place.

Pour chaque incident impactant de manière critique l'utilisation des services de Progenda (tel qu'une panne de serveur), nous rédigeons un compte-rendu interne (« Post-mortem »). Ces compte-rendus sont détaillés autant que possible et non-culpabilisants (le but n'étant pas d'attribuer la faute en interne, mais de faire partager l'apprentissage par erreur). Ils disposent de conclusions et d'actions à prendre suggérées et sont organisés dans un dossier accessible à tous.

L'activation d'une authentification multi-facteurs (« 2FA ») est obligatoire pour tous les membres de l'équipe sur les services qui la proposent. La gestion des comptes utilisateurs et des mots de passe sur les services externes utilisés par nos équipes est gérée de manière centrale et chiffrée au travers d'un gestionnaire de mots de passe. Le principe de moindre privilège est à nouveau d'application.

PROGENDA

Agenda en ligne adapté au monde médical

Confirmations et rappels par emails & SMS

Prise de rendez-vous via internet

Référencement optimisé & site web

Essai gratuit →

Ou appelez-nous au 02 318 42 02!