La sécurité de vos données est fondamentale

Version Décembre 2020

Dans un monde numérique où la protection des données a été trop souvent prise à la légère, chez Talkspirit nous sommes déterminés à faire tous les efforts nécessaires pour garantir la sécurité de nos données, des vôtres et de celles de chacun de vos utilisateurs.

Cet engagement indéfectible nous vaut aujourd'hui la confiance de plus de 500 clients parmi lesquels :

Notre niveau d'exigence est particulièrement élevé quelque soit le domaine : sécurité applicative, sécurité des infrastructures et sécurité physique.

Voici le détail de nos actions.

Sécurité applicative

Code applicatif

L'ensemble du code applicatif est stocké dans des repositories de gestion de code Git sur le service SAAS Github.

Données clients

Seuls les utilisateurs membres de votre organisation ou invités à votre plateforme peuvent accéder à vos données. Nous ne faisons aucun traitement sur vos données qui sont et restent votre propriété.

Etanchéité

L'étanchéité des données est garantie au niveau logiciel. Notre API est faite en PHP sur le framework Symfony.

Suppression des donnés client

Talkspirit offre la possibilité au propriétaire d'une plateforme de supprimer l'intégralité des données de sa plateforme, à tout moment. Dans les 24h suivant la demande de suppression, Talkspirit supprime de façon définitive toutes les informations. Les sauvegardes des services Talkspirit sont détruites sous 1 an.

Restitution des données clients.

Le propriétaire de la plateforme peut exporter à tout moment l'intégralité des contributions échangées hors publications privées en dehors des groupes et conversations de tchat. Un export des fichiers hébergés sur la plateforme est également possible, sur demande.

Authentification à la plateforme

Tous les mots de passe des utilisateurs sont stockés cryptés et salés.
L'authentification des applications Front (site Web, applications de bureau et mobile) à l'API permettant d'accéder aux données, se fait via le protocole oAuth 2.

Les administrateurs peuvent par ailleurs intégrer leur plateforme Talkspirit à divers fournisseurs d'authentification unique : Google, MS Azure, LinkedIn ou encore un service proposant une authentification unique SAML (tel que OneLogin, Okta ou un annuaire LDAP).

Imputabilité, traçabilité

Consignation de l'accès

Nous disposons de journaux d'accès détaillés consignant chaque connexion à un compte ainsi que le type d'appareil utilisé et l'adresse IP de la connexion. Ces journaux sont disponibles sous la forme d'un flux compatible avec les outils SIEM du marché à l'aide d'un connecteur json.

Gestion des logs

Les journaux des serveurs sont journalisés hebdomadairement puis sauvegardés pendant 1 an sur un serveur distant. Les logs des accès aux serveurs sont envoyés en temps réel vers la solution Logs Data Platform d'OVHcloud avec une rétention de 45 jours.

Les logs applicatifs sont journalisés sur 20 jours glissants sur les serveurs.

Gestion des incidents

La remontée des alertes se fait selon le niveau de gravité de l'incident.

Les dysfonctionnements logiciels remontés par nos utilisateurs sont gérés par une équipe Support au travers une assistance en ligne intégrée au produit Talkspirit.

Ces incidents sont également partagés sur la plateforme Talkspirit de l'entreprise pour une visibilité partagée par tous.

Dans le cas d'une violation de sécurité, Talkspirit vous informe rapidement de tout accès non autorisé à vos données.

Audit fonctionnel et amélioration continue

Nous faisons appel à des prestataires spécialisés pour effectuer régulièrement des audits de sécurité de nos services et vérifier que nos pratiques en matière de sécurité sont rigoureuses.

Le dernier audit a été réalisé par la société Acceis au mois de juillet 2020.

Les équipes de développement priorisent leur travail pour résoudre tout problème de sécurité qui pourrait survenir au cours du développement.

Sécurité des infrastructures

Infrastructure

Datacenter

Notre infrastructure est hébergée chez OVHcloud, prestataire français, dans le centre de données de Roubaix. OVHcloud garantit les plus hauts niveaux de sécurité.

Le datacenter répond aux normes de sécurité les plus strictes ; il est certifié SAS70 Type II, ISO27001, SOC 1, SOC 2 et SSAE16.

Serveurs

Les serveurs sont sous Linux Debian. Le logiciel Talkspirit utilise

- Nginx
- PHP
- Redis
- MongoDB
- Elasticsearch
- Centrifugo
- Onlyoffice
- Jitsi

L'infrastructure est hébergée dans la partie private cloud d'OVHcloud qui garantit une redondance matériel et réseau. La partie Jitsi est hébergée dans le public cloud d'OVHcloud afin de pouvoir répondre aux pics de trafic liés à la vidéo.

Les serveurs sont systématiquement réinstallés et toutes les données clients supprimées lorsqu'un serveur est remplacé chez notre hébergeur.

Cloisonnement des environnements

Chaque nouvelle version de Talkspirit est testée sur un environnement de staging qui est complètement isolé de la production. Les mêmes règles de déploiement d'accès et d'installation de logiciels sont respectées.

Protection réseau

Prévenir les attaques

L'hébergeur OVHcloud nous offre un service protection Anti-DDOS à la pointe.
Par ailleurs, les pare-feu sont configurés selon les meilleures pratiques de l'industrie.

Chiffrement du trafic

Les services Talkspirit prennent en charge les dernières suites de chiffrement sécurisé et les protocoles recommandés pour crypter tout le trafic.

- Le transfert des données entre Talkspirit et les postes des utilisateurs est sécurisé via un certificat SSL AES-128 bit.
- A distance l'accès aux serveurs par nos équipes Infrastructure se fait uniquement par clefs via SSH au travers d'un vpn. L'accès SSH par mot de passe est désactivé.

Nous surveillons étroitement l'évolution du paysage cryptographique et nous nous efforçons d'effectuer rapidement les mises à niveau permettant de répondre aux menaces émergentes au fur et à mesure de leur découverte, et nous mettons en œuvre les meilleures pratiques au fil de leur évolution.

Installations, mise à jour et correctifs

Nos serveurs sont mis à jour de façon continue avec les derniers correctifs de sécurité.

L'installation des serveurs, leur mise à jour ainsi que les déploiements des logiciels sont entièrement automatisés :

- Les serveurs sont installés via des scripts Ansible. Les scripts sont testés de manière régulière à travers une machine Vagrant.`
- Le logiciel est déployé de manière automatique sous forme d'un package Debian envoyé par le service CircleCi lorsque les différents tests automatiques ont été réalisés. Chaque déploiement génère un artifact qui permet de faire un rollback sur une version précise du logiciel. La mise en production est tracée

Sauvegarde

Base de données

Une sauvegarde quotidienne est réalisée de la base de données sur 7 jours glissants sur le serveur. Une autre sauvegarde est réalisée quotidiennement sur le cloud d'object storage d'OVHcloud qui permet une rétention de 52 semaines. L'ensemble des sauvegardes sont chiffrées.

Fichiers

Les fichiers clients sont répliqués sur la solution d'object storage d'OVHcloud de manière quotidienne. Ils sont donc sauvegardés sur des sites distants.

Gestion des incidents

Monitoring

Les problèmes de dysfonctionnement hardware sont gérés par l'équipe Infrastructure de l'entreprise. La remontée des incidents se fait via 2 outils.

Le service Pingdom qui permet le monitoring du site à travers différents endroits dans le monde.
Le système d'alertes d'AlertManager qui permet un monitoring système et logiciel.
Le monitoring de Pingdom est accessible via Talkspirit.status.io.
En interne, l'équipe Infrastructure dispose de l'application Pushover sur téléphone mobile afin d'être averti des dysfonctionnements et pouvoir agir 24h/24.

Communication

La page Talkspirit.status.io. est le support de communication que nous utilisons en cas d'incident majeur ou de maintenance sur la plateforme.

Performance et disponibilité

La bande passante disponible est de 1 Gbs.

Les performances de la plateforme et sa disponibilité sont publiquement accessibles sur la page https://status.talkspirit.com/ Il n'est pas possible de filtrer cette page sur une instance en particulier.

Sécurité physique

Personnel

Notre personnel est qualifié. Nos équipes sont formées aux bonnes pratiques sur la confidentialité et la sécurité.

Intervention du personnel extérieur

Seules les personnes habilitées d'OVHcloud peuvent accéder au datacenter et à la connectivité réseau.

Surveillance et contrôle d'accès

Nous limitons l'accès de notre personnel aux services et données.

Seules les équipes Infrastructure et DevOps peuvent intervenir sur l'infrastructure de production. Et chaque membre du personnel n'accède qu'aux services qui lui sont nécessaires pour réaliser son travail (les mots de passe d'accès à l'ensemble des services SAAS utilisés sont nominatifs).

Nous nous engageons en outre à nous assurer que les Données client ne sont pas vues par quiconque ne devant pas y avoir accès. Le fonctionnement des services Talkspirit nécessite que certains employés aient accès aux systèmes qui stockent et traitent les Données client. Par exemple, pour pouvoir diagnostiquer un problème que vous rencontrez, nous pouvons nous trouver dans l'obligation d'accéder à vos Données client. Il est interdit à ces employés d'utiliser ces autorisations pour consulter les données client sauf nécessité absolue. Nous avons mis en place des contrôles techniques afin que tout accès aux données client soit consigné.