Politique de sécurité

La sécurité est une priorité d'Azopio et afin de délivrer le plus haut standard de protection nous avons mis en place une politique de sécurité mettant en valeur l'expertise et l'expérience de nos partenaires ainsi que l'implémentation de technologies ultra-sécurisés et de méthodes reconnues:

- Notre infrastructure technique est complètement redondante et hébergée en France par OVH;
- Tous les transferts de données se font en SSL;
- Azopio et ses partenaires sont conformes aux normes PCI-DSS (Payment Card Industry Data Security Standard) Niveau 1;

1. Le plus haut niveau de sécurité pour notre infrastructure technique à travers OVH

Des datacentres placés sous haute protection:

L'accès à l'enceinte des bâtiments d'OVH est strictement surveillé. Afin de résister à toute forme d'intrusion ou d'aléa, chaque périmètre est sécurisé par des clôtures équipées de barbelés. Un système de vidéo-surveillance et de détection de mouvements fonctionne également en continu. L'activité dans les centres de données et à l'extérieur des bâtiments est monitorée puis enregistrée sur des serveurs sécurisés, tandis que des équipes de surveillance se relaient 24h/24, 7j/7.
Afin de contrôler et de surveiller l'accès à l'enceinte d'OVH, des procédures de sécurité strictes sont en place. Chaque membre du personnel d'OVH est équipé d'un badge RFID nominatif auquel sont associés ses droits d'accès. Ceux-ci sont régulièrement reconsidérés, en fonction des attributions de chacun. Pour accéder aux locaux, chaque employé d'OVH doit tout d'abord soumettre son badge à une vérification, puis traverser un sas sécurisé.

Gestion des risques d'incendie:

Chaque salle de chaque datacentre est équipée d'un système de détection et d'extinction d'incendie ainsi que de portes coupe-feu. OVH respecte la règle APSAD R4 pour l'installation des extincteurs portatifs et mobiles, et possède le certificat de conformité N4 pour tous ses datacentres.

Sécurité réseau:

OVH déploie son réseau en fibre optique à travers le monde et sa technologie est installée et maintenue par ses propres équipes d'ingénieurs.
OVH a fait le choix de construire son réseau de manière totalement redondée: plusieurs boucles de sécurisation ont ainsi été mises en place, afin d'éliminer tout risque d'indisponibilité.

Sécurité serveur:

Une présence humaine est assurée 24/7/365 dans les centres de données par les équipes d'OVH, afin d'assurer une maintenance permanente.

Alimentation électrique:

Les centres de données d'OVH sont alimentés par deux arrivées électriques indépendantes l'une de l'autre et sont également équipés d'onduleurs. Des groupes électrogènes d'une autonomie de 48 heures permettent de pallier une éventuelle panne du réseau de fourniture d'électricité.

Protection anti-DDoS:

OVH intègre une protection contre tous les types d'attaques DDoS à son service d'hébergement dédié.

2. Tous les transferts de données en SSL

SSL (Secure Sockets Layer) est la technologie de sécurité standard pour établir une liaison cryptée entre un serveur web et un navigateur. Ce lien garantit que toutes les données échangées entre le serveur web et les navigateurs restent privées et intégrales. SSL est une norme de l'industrie et est utilisé par des millions de sites internet permettant de protéger les transactions en ligne de leurs clients.

3. Conformité aux normes PCI et mise en place de des meilleures pratiques PCI

Azopio a mise en place les pratiques PCI suivantes:

- Les données du titulaire de carte de paiement ne sont jamais envoyées sans SSL ;
- Nous n'enregistrons, ni stockons les données de carte sensibles (numéro de carte complet ou valeur de vérification (CVV/CVC));
- Nous protégeons nos clients en gardant notre site à l'abri des attaques sur les éléments dynamiques;