Juillet 2018

Questions fréquentes
Sécurité

Jamespot.

AVANT-PROPOS

La sécurité des systèmes d'information est un sujet d'importance croissante dans le domaine des données numériques et des risques accrus qu'elles peuvent engendrer. Jamespot aide depuis plus de dix ans les organisations à mieux communiquer et collaborer au quotidien, et nous avons vu monter le niveau stratégique et opérationnel des informations qui circulent sur les plateformes de nos clients. Dans le même temps, les attaques sur les systèmes d'informations grand public ou d'entreprises se sont multipliées dans le monde, modifiant de manière irréversible le besoin de sécurité accrue (cybercriminalité).

C'est pourquoi nous avons mis en place des mesures de sécurité fortes afin de se prémunir au maximum contre tout risque potentiel. Le risque zéro n'existe pas, mais face à ce défi permanent c'est un processus continu d'amélioration, d'anticipation des risques et des failles, de tests d'intrusions, que nous avons mis en place pour s'assurer d'un niveau de sécurité optimal pour vous.

Cet objectif, nous pouvons l'atteindre avec et grâce à vous. Tout d'abord, en vous donnant toute l'information nécessaire. Savoir se protéger, c'est connaître ses propres limites : c'est pourquoi nous mettons à votre disposition ce document qui répond aux questions autour de la sécurité.
Ensuite, et c'est sans doute le plus important, par notre vigilance pour réagir rapidement en cas de doute ou de risque et mettre en place un « patch de sécurité » si quelqu'un de malveillant réussit à déjouer les systèmes mis en place.

Nous comptons également sur vous pour rester vigilant et nous prévenir au plus vite si un tel évènement se produit.

La sécurité est en effet l'affaire de tous.

FAQ SÉCURITÉ

AVANT-PROPOS 2

FAQ SÉCURITÉ 3

1. ORGANISATION 4
1.1 Jamespot serait-il informé (par contrat) d'incidents de sécurité survenus chez ses propres sous-traitants? 4
1.2 Jamespot dispose-t-il d'une procédure documentée de gestion des incidents sécurité ? 4
1.3 En cas d'évènement ayant mis en péril les données personnelles des utilisateurs de la plateforme, comment sont avertis les clients, par qui, avec quelle rapidité ? 4

2. ACCÈS À LA PLATEFORME 4
2.1 A quoi sert HTTPS ? 4
2.2 Verisign 4
2.3 Les mots de passe sont créés par les utilisateurs : y-a-t-il une indication du degré de résistance du mot de passe saisi ? 4
2.4 Y a-t-il possibilité de mener une campagne de mesure de la résistance des mots de passe générés par les utilisateurs (sans bien sûr en avoir connaissance) ? 5
2.5 Quel est le protocole utilisé pour chiffrer/hasher les mots de passe ? 5

3. SAUVEGARDE 5

4. HABILITATION 5
4.1 Existe-t-il des collaborateurs de Jamespot qui, à l'insu du client, peuvent surpasser les droits et accéder à la plateforme et aux données (droits Super Utilisateur/Super Administrateur) ? 5
4.2 Sous-traitance 5

5. MAINTENANCE 6
5.1 Les interventions opérées par Jamespot sont-elles enregistrées dans une main courante ? 6
5.2 Quels sont les personnels ou catégories de personnels Jamespot qui sont habilités à réaliser les opérations de maintenance ? 6
5.3 Des tiers peuvent-il être amenés à accéder à la plateforme et aux données ? 6

6. SÉCURITÉ PHYSIQUE 6
6.1 Sécurité réseau : Si le flux est chiffré entre l'utilisateur et le frontal Web, l'est-il entre le frontal Web et le back-end ? 6
6.2 Sécurité applicative 6
6.2.1 Historisation des actions des utilisateurs 6
6.2.2 Politique d'application des correctifs de sécurité (fréquence, rapidité, impact sur l'opérationnel, information des clients en cas de difficultés, etc.). Même question concernant la base de données. 6
6.2.3 Respect des recommandations de l'OWASP concernant le développement sécurisé (ou d'une autre référence équivalente) ? 6
6.2.4 Veille sécurité 7
6.2.5 En cas de bug sécurité connu de Jamespot (mais non encore résolu), les clients seraient-ils informés ? 7
6.3 Sécurité dans les documents 7
6.3.1 Un utilisateur dépose en banque documentaire un Word avec un cheval de Troie : détection ? 7
6.3.2 Un utilisateur peut-il déposer un exécutable ? 7
6.4 Audits de sécurité 7
6.4.1 Jamespot fait-il réaliser des audits de sécurité, des tests d'intrusion, des revues de code ? Si oui, précisions. 7

1. ORGANISATION

1.1 Jamespot serait-il informé (par contrat) d'incidents de sécurité survenus chez ses propres sous-traitants?

Oui, les incidents survenus sur les matériels gérés par les sous-traitants font contractuellement l'objet d'une alerte mail. Les résolutions d'incidents sont documentées et nous sont envoyés.

1.2 Jamespot dispose-t-il d'une procédure documentée de gestion des incidents sécurité ?

Les incidents sont tracés dans notre outil de gestion des incidents disponible dans notre outil de support accessible à l'adresse : http://ecosysteme.jamespot.pro .
Dans cet outil, on a plusieurs espaces de suivi. On peut ouvrir un accès au client, afin de suivre les incidents qu'il déclare, liés à son espace personnel.

Jamespot utilise un espace interne, pour tracer les problèmes et évolutions transverses.

1.3 En cas d'évènement ayant mis en péril les données personnelles des utilisateurs de la plateforme, comment sont avertis les clients, par qui, avec quelle rapidité ?

En cas de problème avéré sur les données, les clients seraient prévenus par le support Jamespot dans les plus brefs délais.

2. ACCÈS À LA PLATEFORME

2.1 A quoi sert HTTPS ?

HTTPS permet de sécuriser la communication entre vos utilisateurs et nos serveurs.
Cela permet :

- de certifier que vos utilisateurs dialoguent effectivement avec le réseau que vous avez mis en place, et non pas avec un clone qui capterait des informations.
- de chiffrer les transferts entre le navigateur et le serveur pour éviter toute écoute même physique lors des échanges d'information.

2.2 Verisign

Verisign est le plus connu et le plus répandu des fournisseurs de certificats.
Acheter un certificat chez eux permet de vous assurer que le support HTTPS sera reconnu sur tous les navigateurs, mais vous pouvez aussi bien faire appel à d'autres fournisseurs de certificats.

Enfin, vous pouvez utiliser le certificat multi-domaine de Jamespot (certificat wildcard), qui assure le chiffrement des transferts, et vous assure que vous dialoguez avec une plateforme Jamespot (valable par définition pour toutes les plateformes Jamespot, ce qui peut donc provoquer une alerte par ouverture d'une boîte de dialogue qui peut effrayer certains utilisateurs).

2.3 Les mots de passe sont créés par les utilisateurs : y-a-t-il une indication du degré de résistance du mot de passe saisi ?

Jamespot a implémenté un mécanisme d'indication du degré de résistance du mot de passe.

2.4 Y a-t-il possibilité de mener une campagne de mesure de la résistance des mots de passe générés par les utilisateurs (sans bien sûr en avoir connaissance) ?

Vous pouvez mettre en place un projet de cette nature.

2.5 Quel est le protocole utilisé pour chiffrer/hasher les mots de passe ?

Le stockage des mots de passe est encodé et stocké en SHA256 plus SALT.

3. SAUVEGARDE

Les serveurs de production sont des VMs déployées dans VSphere, suivant l'offre SDDC (Software Defined Datacenter) de OVH.
Les VMs sont situées sur des espaces de stockages en RAID-1 ou RAID-10, pour garantir un stockage doublé.
Les données sont sauvegardées tous les soirs, et envoyées chiffrées chez Online pour conserver une copie pendant 7 jours à un autre emplacement.

Enfin, si un client veut disposer, en plus, de sa propre sauvegarde (par exemple dans l'hypothèse d'une faillite de Jamespot), une option payante d'export SQL sur un compte SSH est disponible.

4. HABILITATION

4.1 Existe-t-il des collaborateurs de Jamespot qui, à l'insu du client, peuvent surpasser les droits et accéder à la plateforme et aux données (droits Super Utilisateur/Super Administrateur) ?

La plateforme de supervision de Jamespot permet d'accéder à tous les comptes de tous les réseaux sociaux gérés par Jamespot.
Cette fonctionnalité est utilisée à titre d'aide à l'utilisateur qui le demande, ou de reproduction de bugs dans l'environnement client.

4.2 Sous-traitance

Jamespot fait appel à des sociétés tierces pour assurer l'hébergement physique des données et des traitements.
Les conditions de réalisation de ces contrats sont conformes aux règles de l'art et du droit français et européen.

5. MAINTENANCE

5.1 Les interventions opérées par Jamespot sont-elles enregistrées dans une main courante ?

Les interventions de maintenance sont déployées depuis un référentiel de sources Subversion, afin de déployer systématiquement les mêmes modifications sur l'ensemble des serveurs qui composent le Datacenter principal chez OVH.

5.2 Quels sont les personnels ou catégories de personnels Jamespot qui sont habilités à réaliser les opérations de maintenance ?

L'équipe de développement de Jamespot est seule habilitée à réaliser ces opérations.

5.3 Des tiers peuvent-il être amenés à accéder à la plateforme et aux données ?

Seul l'hébergeur peut être amené à effectuer des opérations de réparation en cas de dégradation des serveurs.

6. SÉCURITÉ PHYSIQUE

6.1 Sécurité réseau : Si le flux est chiffré entre l'utilisateur et le frontal Web, l'est-il entre le frontal Web et le back-end ?

Les données sont effectivement chiffrées lorsqu'elles transitent entre les différents hébergeurs. Elles ne sont pas chiffrées à l'intérieur du réseau privé virtuel d'un même Datacenter.

6.2 Sécurité applicative

6.2.1 Historisation des actions des utilisateurs

Un journal des accès est disponible pour les administrateurs. Il recense l'ensemble des traces d'accès de tous les utilisateurs pendant un an.

6.2.2 Politique d'application des correctifs de sécurité (fréquence, rapidité, impact sur l'opérationnel, information des clients en cas de difficultés, etc.). Même question concernant la base de données.

Les serveurs du Datacenter peuvent être mis à jour en cas de mise à disposition de correctifs de failles critiques délivrées sur notre distribution Linux.

6.2.3 Respect des recommandations de l'OWASP concernant le développement sécurisé (ou d'une autre référence équivalente) ?

Les plateformes Jamespot répondent aux exigences des besoins métiers. Pour cela, les plateformes sont adaptables et intégrables avec d'autres systèmes.

On distingue donc deux profils d'utilisateurs : les administrateurs ont des droits qui surpassent les exigences de sécurité, afin de mettre en œuvre cette extensibilité.

Les droits accordés aux utilisateurs standard du système sont en revanche conformes aux recommandations de sécurité de ce référentiel.

6.2.4 Veille sécurité

Jamespot suit la communication ANSSI (http://www.cert.ssi.gouv.fr) pour les alertes, et les réponses aux attaques informatiques.

6.2.5 En cas de bug sécurité connu de Jamespot (mais non encore résolu), les clients seraient-ils informés ?

Par défaut, on ne communique pas les bugs aux Administrateurs, sauf après leur correction.

6.3 Sécurité dans les documents

6.3.1 Un utilisateur dépose en banque documentaire un Word avec un cheval de Troie : détection ?

Nous n'effectuons pas de détection de Virus dans les fichiers binaires déposés.

6.3.2 Un utilisateur peut-il déposer un exécutable ?

Un utilisateur peut déposer un exécutable sur la plateforme.

6.4 Audits de sécurité

6.4.1 Jamespot fait-il réaliser des audits de sécurité, des tests d'intrusion, des revues de code ? Si oui, précisions.

Jamespot sous-traite des audits de sécurité, aussi bien automatiques que humains, et plus généralement, Jamespot est accompagné dans ses démarches sécurité par des professionnels mandatés.

Tout client peut demander à effectuer un audit de sécurité (tests d'intrusion). Il en assumera la charge, mais Jamespot s'engage à l'aider dans sa mise en œuvre de l'audit.


Contactez-nous :
info@jamespot.com
www.jamespot.com
blog-jamespot.com