



Déclaration de sécurité

SphinxOnline 4.22

Dernière mise à jour : 22/03/2021

LE SPHINX DEVELOPPEMENT

Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France

Tél : 04.50.69.82.98 - Fax : 04.50.69.82.78

Email : contact@lesphinx.eu Web : www.lesphinx.eu

SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34



Table des matières

| | | |
|------|--|----|
| 1 | Introduction..... | 3 |
| 2 | Infrastructure | 4 |
| 2.1 | Hébergement | 4 |
| 2.2 | Réseau et protocoles de communications | 4 |
| 2.3 | Contrôle des accès systèmes..... | 5 |
| 2.4 | Protection anti-virus..... | 5 |
| 2.5 | Sécurité des postes de travail sensibles..... | 5 |
| 2.6 | Disponibilité..... | 5 |
| 2.7 | Continuité des services..... | 6 |
| 2.8 | Surveillance | 6 |
| 2.9 | Gestion des Sauvegardes | 7 |
| 2.10 | Gestion des Mises à jours..... | 7 |
| 3 | Solution SphinxOnline | 8 |
| 3.1 | Protection des accès :..... | 8 |
| 3.2 | Gestion des Incidents | 9 |
| 3.3 | Sécurité des échanges | 10 |
| 3.4 | Portabilité des données :..... | 10 |
| 3.5 | Traçabilité | 10 |
| 3.6 | Cookies | 10 |
| 4 | Sécurité administrative et organisationnelle | 11 |
| 4.1 | Gestion des failles de sécurité..... | 11 |
| 4.2 | Mesures de contrôles et de suivi | 11 |



1 Introduction

La société Sphinx Développement édite et distribue depuis plus de 30 ans des solutions logicielles dédiées à l'enquête et l'analyse de données. Depuis maintenant plus de 15 ans, Le Sphinx propose des services hébergés pour permettre à ses clients de réaliser des projets d'enquêtes en ligne en toute autonomie. Un ensemble d'applications est ainsi accessible directement via Internet pour permettre de paramétrer les questionnaires, diffuser les enquêtes, héberger l'ensemble des données collectées et partager des résultats sous forme de rapports interactifs.

Ce document a pour objectif de lister et décrire l'ensemble des mesures prises et les dispositifs mis en place pour répondre à ces objectifs de disponibilité, confidentialité et d'intégrité.



2 Infrastructure

2.1 Hébergement

Les serveurs sont hébergés dans le Datacenter de la société OVH qui en assure la sécurité physique. Les données sont stockées à Roubaix, Strasbourg et Gravelines en France.

La fourniture et l'exploitation des infrastructures (Datacenter, serveurs, réseaux) assurée par OVH sont certifiées ISO 27001:2013.

L'infogérance des serveurs est assurée par nos services. Notre hébergeur n'a pas accès aux données stockées sur nos serveurs et fournit les garanties nécessaires quant à la non-intrusion d'individu dans leurs centres de données.

2.2 Réseau et protocoles de communications

Les serveurs de productions sont isolés dans une DMZ et sont protégés contre les intrusions par un pare-feu réseau.

La zone DMZ n'est accessible que sur le protocole TCP sur les ports 80 et 443.

Les flux arrivant sur le port 80 (http) sont automatiquement redirigés vers le port 443 (https).

OVH intègre une solution de mitigation qui protège l'infrastructure d'une attaque massive en déni de service sans bloquer les flux légitimes.

Toutes les données échangées entre les logiciels clients (navigateur internet ou Sphinx IQ/IQ2) et le serveur sont cryptées via le protocole TLS.

SSL est désactivé. La version 1.2 du protocole TLS est présenté prioritairement, et les versions TLS 1.1 et inférieures peuvent être acceptées si le navigateur de l'utilisateur ne supporte pas les versions supérieures.

Les certificats sont générés à partir de clés 2048bits et signés avec l'algorithme sha256.



2.3 Contrôle des accès systèmes

L'accès aux serveurs est réservé au personnel du service exploitation (<8 personnes) et se fait à travers d'une connexion VPN (tunnel IPsec ou SSL avec authentification à double facteur)

Les accès administrateur des domaines, administrateur de machine physique et administrateur de machine virtuelles sont distincts. Chacun de ces accès est nominatif.

Les mots de passe de ces administrateurs respectent la politique suivante et doivent :

- comporter au moins un chiffre, une minuscule, une majuscule, un caractère spécial
- être différents des 24 mots de passe précédents
- être changés tous les 6 mois

Au bout de 5 tentatives d'accès infructueuses, l'authentification au compte est impossible durant 60 minutes.

Les droits d'accès sont revus à minima semestriellement sur le principe du moindre privilège. En cas de cessation de contrat, les accès sont révoqués immédiatement.

Les mots de passe des administrateurs locaux de chaque machine sont changés pour des mots de passes distincts de 22 caractères minimum comportant au moins un chiffre, une minuscule, une majuscule et un caractère spécial.

2.4 Protection anti-virus

Une protection antivirus logicielle est installée sur tous les serveurs. L'administration de celle-ci est centralisée. Les alertes sont remontées en temps réel et la protection vérifiée quotidiennement.

Les stratégies en place incluent notamment :

- une analyse complète chaque semaine
- la protection en temps réel
- une mise à jour quotidienne de la base de signature

2.5 Sécurité des postes de travail sensibles

Les postes de travail sensibles (développeurs, administrateurs, service support, ...) sont protégés par mot de passe, les disques sont chiffrés (BitLocker) le verrouillage de l'ordinateur est automatique après 10 minutes d'inactivité.

L'intégralité des postes bénéficie d'une protection anti-virus.

2.6 Disponibilité



Un taux de disponibilité des serveurs Sphinx est garanti à hauteur de 99.9% sur 365 jours. Ce taux ne tient pas compte des interruptions liées à des maintenances programmées. Ces dernières ont lieu 1 à 2 fois par mois en moyenne entre 3h00 et 4h00 du matin (UTC +1). Si elles doivent être effectuées en dehors de ce créneau horaire, les détails de l'intervention sont communiqués aux propriétaires des comptes ou au responsable de l'administration de ceux-ci dans un délai préalable de deux semaines.

2.7 Continuité des services

Les dispositifs de continuité de service sont décrits dans le plan de continuité de service.

Ce document est confidentiel mais il couvre les points suivants :

- Contexte et infrastructure
- Aide au diagnostic et seuils de déclenchement des interventions
- Scénario de panne
- La Perte de Connectivité réseau : Vrack, configuration VLAN , ...
- Défaillance matériel serveur physique : Host, contrôleur de domaine, serveur de backup
- La défaillance de la machine virtuelle remplissant le rôle de pare-feu ou la perte de la configuration de celle-ci

En cas de défaillance du serveur, le service sera rétabli sur une autre machine dans un délai maximum de 8 heures suivant la notification de la panne.

La perte de données maximale est de 24 heures.

Les serveurs étant actuellement hébergés par la société OVH (<https://www.ovh.com>), la continuité des services SPHINX est donc assujettie à celle de l'accès internet fourni par OVH. En cas d'interruption de ce service, pour quelque cause que ce soit, la société LE SPHINX DEVELOPPEMENT s'engage à faire tout son possible pour trouver un nouveau fournisseur.

Les données sont stockées sur des regroupements de disques en RAID 5 ou Raid 50. Un système de monitoring permet d'alerter nos équipes en cas de défaillance d'un disque.

2.8 Surveillance

Les applications, les systèmes et le réseau sont monitorés 24h sur 24 et 7 jours sur 7. Des tests d'accès distants aux applications, à l'international sont réalisés de façon récurrente par la société INTERNETVISTA (www.internetvista.com).

Nos équipes interviennent de 8h à 23h, 7 jours sur 7 en cas d'alerte remontée par les différents outils de monitoring.



2.9 Gestion des Sauvegardes

Les données sont sauvegardées quotidiennement et sont conservées pendant une durée maximale de 6 mois.

Elles peuvent être récupérées sur demande, et ce jusqu'à 2 mois après l'expiration de l'abonnement. Ces sauvegardes sont chiffrées via l'algorithme AES (256 bits).

Les données de sauvegardes sont répliquées quotidiennement entre les infocentres de Roubaix, Strasbourg et Gravelines.

2.10 Gestion des Mises à jours

Les mises à jour des systèmes d'exploitation sont effectuées dans un délai maximum de 7 jours après la mise à disposition des correctifs. L'approbation des mises à jours est effectuée manuellement (fonctionnalités WSUS).



3 Solution SphinxOnline

3.1 Protection des accès :

La sécurité des comptes utilisateurs est assurée par login/mot de passe.

Les mots de passe sont stockés sur les serveurs de manière chiffrée non réversible (HASH PBKDF2 HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 itérations).

Les mots de passe doivent respecter certaines contraintes de complexité minimales (8 caractères alphanumériques et caractères spéciaux) et doivent être changés à minima tous les 6 mois.

Les 5 derniers mots de passe ne peuvent pas être réutilisés.

Après 5 tentatives infructueuses d'accès, la connexion au compte est bloquée pendant 5 minutes.

Une authentification à double facteur est disponible. Celle-ci permet à l'utilisateur de protéger l'accès au compte avec un deuxième code à usage unique généré par une application tierce.

L'accès aux enquêtes et/ou modules complémentaires peut également être protégé par mot de passe. Cette protection est active par défaut.

Par défaut les sessions sont limitées dans le temps selon les durées suivantes :

- 8 heures glissantes pour les profils utilisateurs

- 45 minutes non glissantes pour les profils administrateurs

Les administrateurs de la solution ont la possibilité de se connecter sur un compte utilisateur. Ce type d'accès n'est autorisé qu'en cas de demande d'assistance ou suspicions d'atteinte à la confidentialité ou l'intégrité des données. La durée de validité de ce type d'accès est fixée à 20 minutes.

Au-delà de ces délais, les jetons utilisés sont révoqués et ne peuvent plus être réutilisés.



3.2 Gestion des Incidents

Le service de support technique est accessible au 04 50 69 82 98 du lundi au jeudi de 8h30 à 12h30 et de 14h à 18h et le vendredi de 8h30 à 12h30 et de 14h à 17h (heure de Paris).

Le délai de correction court à compter de la découverte du problème.

Les délais d'intervention pour effectuer une mise à jour corrective dépendent du type d'anomalie.

| ANOMALIE FONCTIONNELLE | | |
|------------------------|---|---|
| Type | Définition | Délais de correction |
| Bloquante | Désigne toute anomalie rendant impossible l'utilisation d'une fonctionnalité, sans solution de contournement. | Sous 8 heures ouvrées |
| Majeure | Désigne toute anomalie impliquant un fonctionnement en mode dégradé d'au moins une fonctionnalité. | Sous 72 heures ouvrées |
| Mineure | Désigne toute anomalie disposant d'une solution de contournement, sans dégradation du fonctionnement global. | Mise à disposition lors des mises-à-jour mineures |

| FAILLE DE SECURITE | | | |
|--------------------|--------------------|-------------------------|--|
| Niveau de risque | Impact | Facilité d'exploitation | Délais de correction |
| Critique | Critique | Facile à modéré | Sous 8 heures ouvrées |
| | Majeur | Facile | |
| Majeur | Critique | Elevée | Sous 72 heures ouvrées |
| | Majeur | Modérée à élevée | |
| | Important | Facile | |
| Important | Critique ou Majeur | Difficile | Mise à disposition au plus tard lors de la prochaine mise-à-jour mineure |
| | Important | Modérée à élevée | |
| | Mineur | Facile | |
| Mineur | Important | Difficile | Mise à disposition au plus tard lors des mises-à-jour mineures |
| | Mineur | Modérée à difficile | |



3.3 Sécurité des échanges

Lors de la publication ou de l'importation d'une enquête à partir du logiciel client Sphinx IQ2, les fichiers échangés entre le serveur et le logiciel sont stockés dans une archive chiffrée (algorithme AES 128 bits). L'échange de fichiers n'est effectué qu'après vérification du couple login/mot de passe de l'utilisateur (requête chiffrée en AES 256 bits).

3.4 Portabilité des données :

Il est possible d'exporter les données d'enquêtes, campagnes d'emailing ou SMS dans différents formats standards comme .csv ou .xls.

3.5 Traçabilité

Les requêtes et les connexions sont consignées dans des journaux d'événements applicatifs. Ces journaux enregistrent toutes les connexions, enregistrements, modifications, actions de navigation des répondants...

Ces journaux sont conservés pendant une période d'un an puis sont automatiquement supprimés.

3.6 Cookies

La solution SphinxOnline utilise uniquement des cookies techniques nécessaires au bon fonctionnement des applications pour les objectifs suivants :

- Garantie de sécurité : authentification, contrôle d'accès, ...
- Préférences : Choix de langue, répertoire de travail courant, options d'affichages, ...

Ces cookies ne sont communiqués à aucun tiers et ne font pas l'objet d'une exploitation à des fins publicitaires ou de ciblage.



4 Sécurité administrative et organisationnelle

4.1 Gestion des failles de sécurité

La société SPHINX DEVELOPPEMENT est tenue à une obligation de moyen pour assurer l'intégrité du réseau et des systèmes contre tout acte de malveillance extérieur ou toute attaque informatique connue.

En cas de tentative, ou de suspicion d'atteinte à la sécurité de l'information ou de vol de données personnelles. Nous nous engageons à avertir le propriétaire du compte dans les 8 heures ouvrées à compter de la découverte du problème.

Nos équipes suivent quotidiennement les alertes émises par le CERT-FR et, lorsque c'est nécessaire, prennent les mesures adéquates pour se prémunir des vulnérabilités évoquées dans ces alertes, ce qui peut impliquer l'application de correctifs ou la mise en place des recommandations.

4.2 Mesures de contrôles et de suivi

Un audit de configuration et des tests d'intrusion sur la solution sont réalisés chaque année par un cabinet externe spécialisé dans la sécurité informatique. De 2018 à 2020, le cabinet Oppida a été mandaté. La synthèse du dernier rapport de contre audit est disponible sur demande.

Les éventuelles failles critiques remontées lors de ces audits sont corrigées dans les plus brefs délais.

Un document interne recense toutes les failles connues, les améliorations envisageables et évolution possible en terme de sécurité.

Les informations sont issues de :

- Bulletin de sécurité (fournisseurs, CERT-FR, ANSSI, ...)
- Remontées et besoin clients
- Synthèse d'audit
- Problématiques liées aux évolutions logicielles et/ou matérielles
- ...

Chaque élément de ce document catégorisé en fonction de plusieurs critères (exploitabilité, difficulté de mise en œuvre, criticité, probabilité, ...). Une révision mensuelle de ce document est effectuée pour mettre à jour les éléments au regard de l'état de l'art en matière de sécurité et pour définir les actions à venir.