ispring

Services Web iSpring: Présentation des processus de sécurité

Date de révision : Août 2022

Avertissement

Ce document est fourni à titre d'information uniquement. Il représente les pratiques actuelles d'iSpring en matière de protection des données des clients à la date d'émission du présent document, lesquelles sont susceptibles d'être modifiées sans préavis. Ce document ne crée aucune garantie, représentation, engagement contractuel, condition ou assurance de la part d'iSpring, de ses affiliés, fournisseurs ou concédants de licence.

Sommaire

Introduction

Aider à protéger la confidentialité, l'intégrité et la disponibilité des données de nos clients est de la plus haute importance pour iSpring, tout comme le maintien de la confiance des clients. L'objectif de ce document est de répondre à la question « Comment iSpring m'aide à protéger mes données ? ».

Plus précisément, les processus de sécurité physique et opérationnelle d'iSpring sont décrits pour l'infrastructure réseau et serveur sous le contrôle d'iSpring ainsi que pour les implémentations de sécurité spécifiques aux services.

Aperçu des services Web iSpring

iSpring fournit les services Web suivants :

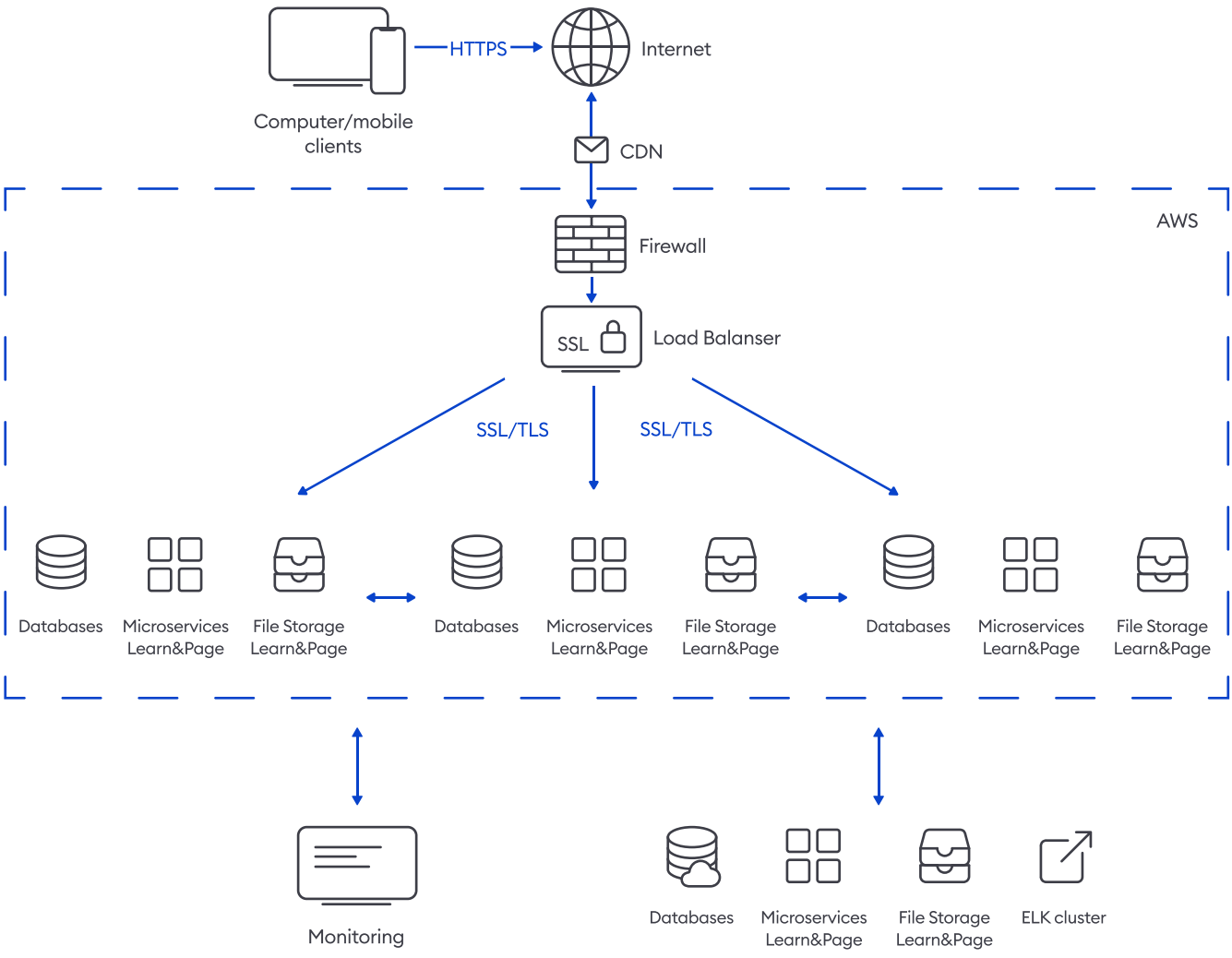
1. **iSpring Learn** est un système de gestion de l'apprentissage (Learning Management System - LMS) hébergé permettant d'enseigner et d'évaluer les employés ou les élèves en ligne.
2. **iSpring Space** est un portail permettant de stocker des cours eLearning et de collaborer sur ceux-ci en équipe.
3. **iSpring Market** est une plateforme basée sur le cloud pour vendre des cours en ligne.

Ces deux services Web sont étroitement intégrés à iSpring Suite, un outil auteur de contenu eLearning, et aux applications mobiles d'iSpring.

Principes de conception sécurisés

Les services Web iSpring ont été conçus pour assurer un hébergement sécurisé des données personnelles des utilisateurs et la livraison du contenu, des bases de données et des analyses des utilisateurs sur un réseau non fiable. Lors du développement du logiciel, les considérations de sécurité ont prévalu sur les préoccupations de convivialité.

Diagramme du réseau



Installations sécurisées

iSpring fait appel à des fournisseurs d'hébergement fiables ayant des normes de sécurité élevées pour exécuter les composants et services d'iSpring Learn LMS et iSpring Space. iSpring ne dépend pas d'un seul fournisseur d'hébergement, il est donc possible de passer d'un fournisseur d'hébergement principal à un fournisseur secondaire en cas de problème inattendu.

Nous utilisons les fournisseurs d'hébergement suivants pour les services Web iSpring :

- **Liquid Web** (consultez les certifications Liquid Web)
- **Amazon Web Services** (consultez le programme de conformité AWS) (certifié ISO 27001)
- **FirstColo** (certifié ISO 27001)
- **Leaseweb** (certifié ISO 27001)

Nos hébergeurs restreignent l'accès physique à leurs serveurs conformément aux normes SSAE 16 et ISO 27001.

Réseau sécurisé

iSpring utilise des pare-feu logiciels (au niveau du système d'exploitation) qui sont configurés pour empêcher les attaques par déni de service (DoS) et enregistrer les connexions refusées. Tous les pare-feu sont configurés par défaut en mode déni avec quelques ports ouverts pour permettre le trafic entrant.

Plateforme sécurisée

Les serveurs iSpring fonctionnent sur Debian Linux avec les derniers correctifs de sécurité installés. Des tests de pénétration ont été effectués pour tous les serveurs, et les journaux système sont constamment audités pour identifier toute activité suspecte.

Secure Shell (SSH) prend en charge l'accès à distance authentifié et crypté par le personnel iSpring. Toute tentative d'accès non autorisé aux serveurs (par exemple, les attaques par dictionnaire) est surveillée et automatiquement bloquée par le système de prévention des intrusions.

Surveillance

iSpring utilise un système de surveillance automatisé pour assurer un haut niveau de performance et de disponibilité des services. Le système de surveillance interne effectue des contrôles périodiques des composants et services iSpring Learn et iSpring Space afin de surveiller leurs principales mesures opérationnelles. Des alarmes sont configurées pour avertir le personnel iSpring par email, messagerie instantanée (Jabber) et SMS lorsque les seuils d'alerte précoce des principales métriques opérationnelles sont franchis. Un calendrier d'astreinte est utilisé pour garantir que le personnel est toujours disponible pour répondre aux problèmes opérationnels. Une documentation est tenue à jour pour aider et informer le personnel sur le traitement des incidents ou des problèmes. Des ingénieurs d'assistance technique sont en service 24h/24, 7j/7 et 365 jours par an.

Stockage et sauvegarde

iSpring utilise une protection continue des données plutôt que des sauvegardes régulières sur iSpring Learn LMS et iSpring Space afin d'éviter toute perte de données et toute interruption de service en cas de problèmes matériels. Toutes les données iSpring Learn et iSpring Space sont stockées de manière redondante dans plusieurs emplacements physiques. C'est aussi bien le cas pour les fichiers uploadés par les clients que pour leurs données stockées dans des bases de données. Toutefois, les bases de données des clients sont également sauvegardées quotidiennement.

Accès des employés

iSpring exige que les employés ayant un accès potentiel aux données des clients fassent l'objet d'une validation approfondie de leurs antécédents (comme le permet la loi) en fonction de leur poste et du niveau d'accès aux données.

iSpring ne donne accès aux serveurs iSpring Learn ou à sa console d'administration qu'aux employés iSpring qui ont des besoins professionnels légitimes pour de tels privilèges. Lorsqu'un employé ne nécessite plus ces privilèges pour des besoins professionnels, son accès est immédiatement révoqué, même s'il continue à être un employé d'iSpring. Tous les accès aux serveurs iSpring Learn par les employés d'iSpring sont consignés et audités de façon régulière.

Gestion de la continuité des activités

Les services Web iSpring ont été conçus pour tolérer les pannes de système ou de matériel avec un impact minimal sur le client. Tous les services Web iSpring sont déployés en configuration 1+1, de sorte qu'en cas de défaillance du centre de données primaire, il existe une option de réacheminement du trafic vers un centre de données secondaire. Nous utilisons un service DNS dynamique avec une fonction de basculement actif pour réacheminer automatiquement le trafic d'un serveur temporairement indisponible vers un serveur de secours.

Cryptage des données

Les services Web iSpring utilisent une connexion sécurisée (cryptée) lorsque cela est possible et n'affecte pas les performances globales pour les utilisateurs finaux.

Les types suivants de connexions des utilisateurs aux services Web iSpring sont protégés par un cryptage SSL/TLS de 256 bits :

- Toutes les données sensibles telles que les mots de passe, les informations de contact et de facturation sont toujours transférées via SSL. Les informations non sensibles sont transférées via le protocole HTTP ordinaire sans cryptage. Si la sécurité du contenu est une préoccupation, il est possible d'activer l'option **Force HTTPS** qui rend toutes les connexions cryptées par SSL.

Seules des connexions cryptées sont utilisées pour transférer des données entre les serveurs iSpring :

- Tous les messages électroniques provenant des services Web iSpring sont envoyés via TLS.

- La réplication des bases de données entre les serveurs de bases de données est effectuée via SSL.
- Tous les transferts de fichiers entre les serveurs de stockage sont effectués via SSL et SFTP.

Politique en matière de mots de passe

Les services Web iSpring exigent que chaque mot de passe comporte au moins six caractères, au moins une lettre majuscule et au moins un chiffre. Cette exigence permet d'éviter que les comptes ne soient configurés avec des mots de passe courts et courants qui sont facilement compromis par une attaque par dictionnaire.

Délais d'inactivité

Un utilisateur peut quitter un PC public sans se déconnecter et laisser un PC personnel sans surveillance. Les services Web iSpring répondent à ce type de menace en appliquant des délais d'inactivité. Les utilisateurs sont automatiquement déconnectés des services Web iSpring si leur connexion reste inactive pendant plusieurs minutes.

Compatibilité avec les pare-feu

Les services Web iSpring sont compatibles avec les pare-feu. L'outil auteur iSpring Suite communique avec le LMS iSpring Learn par le biais d'une connexion HTTP ordinaire (port 80) et d'une connexion HTTPS sécurisée (port 443).

iSpring Suite génère uniquement du trafic HTTP et HTTPS sortant vers les ports 80 et 443. Comme la plupart des pare-feu sont déjà configurés pour autoriser le trafic Web sortant, les utilisateurs n'ont pas besoin de configurer leur pare-feu manuellement.

Mise hors service du périphérique de stockage

La politique iSpring implique un processus de mise hors service des supports amovibles et des périphériques de stockage. Ce processus est conçu pour éviter que les données des clients ne soient exposées à des personnes non autorisées. Lorsqu'un périphérique de stockage atteint la fin de sa durée de vie opérationnelle, un employé iSpring spécialement formé lance un processus de mise hors service de ce périphérique. iSpring utilise les techniques décrites dans le document DoD 5220.22-M (« National Industrial Security Program Operating Manual ») ou NIST 800-88 (« Guidelines for Media Sanitization ») pour détruire les données dans le cadre du processus de mise hors service. Si un dispositif matériel ne peut être mis hors service, il sera démagnétisé ou détruit physiquement conformément aux pratiques standard de l'industrie.

Protection de la vie privée des clients

iSpring comprend que toutes les entreprises qui externalisent la prestation de services sont préoccupées par le respect de la vie privée. iSpring applique une politique de confidentialité rigoureuse qui interdit la divulgation non autorisée d'informations personnelles ou d'entreprise à un tiers.

Divulgation des informations de l'utilisateur

Pour fournir les services Web, iSpring doit recueillir certaines informations personnelles des utilisateurs, notamment le nom/prénom, l'adresse email et les mots de passe au niveau du compte. iSpring s'engage à ne pas divulguer ces informations confidentielles à un tiers et à ne pas les utiliser autrement que pour fournir les services convenus par tous les moyens. Avec le consentement de ses clients, iSpring envoie des messages de mise à jour des services aux utilisateurs des services Web iSpring aux adresses email qu'ils ont fournies lors de leur inscription. De plus amples informations sur la politique de confidentialité d'iSpring sont disponibles à l'adresse https://www.ispring.fr/politique-de-confidentialite.

Conclusion

Les services Web iSpring sont des solutions fiables pour la création de contenu eLearning, la diffusion sécurisée, le suivi et le partage de contenu. Les processus de sécurité iSpring protègent toutes les informations confidentielles contre toute divulgation non autorisée à un tiers. La protection continue des données, la surveillance étendue et l'équilibrage des charges garantissent un fonctionnement ininterrompu. L'utilisation d'un cryptage sophistiqué assure la sécurité des informations confidentielles. Le fait que les services Web iSpring soient compatibles avec les pare-feu permet d'intégrer cette solution de manière transparente à l'infrastructure de réseau et de sécurité existante de toute entreprise.