# Aperçu de la sécurité de Biings

## Introduction

Notre mission chez Biings est d'aider les entreprises à maintenir un environnement de travail sain grâce à des pratiques managériales préventives. La sécurité des données de nos clients est une responsabilité extrêmement importante pour Biings Technologies. Nos efforts sont tournés vers la protection de nos clients contre les derniers dangers. Nous utilisons les mêmes serveurs que nos clients pour stocker nos données sensibles d'absence et de RH, nous avons donc également un intérêt a garder nos standard de sécurité aussi haut que possible. Aligner nos objectifs avec les vôtres est la meilleure façon de maintenir une relation de confiance et de sécurité.

## Sécurité Organisationnelle

### Contrôle des accès

Tous nos employés et contractants doivent signer une clause de confidentialité avant d'avoir accès à notre code source et autre données. Aucun contrôle des antécédents n'est effectué sur nos employés.

Les seuls employés ayant accès aux données des clients sont ceux situés dans les bureaux de Morges.

Tout le monde chez Biings est formé et informé sur les questions de sécurité et les meilleures pratiques à appliquer (changement de mots de passe réguliers inclus) ainsi que sur la façon dont nous programmons et gérons les tickets de support client. Nous gardons des traces de toutes les connexions à nos comptes et nos serveurs. L'accès à nos locaux de Morges est également régulé par des cartes d'accès personnelles.

Notre hébergeur (Infomaniak) n'a pas accès aux données présentes sur nos serveurs.

## Surveillance, journalisation et alertes du système

Biings utilise un serveur dédié sécurisé par des firewall et surveillé avec soin. Notre infrastructure logicielle est mise jours régulièrement avec les derniers patch de sécurité.

Nous avons également des alertes en place si le serveur utilise excessivement des ressources. Ces alertes sont envoyées directement a notre équipe afin d'inspecter manuellement les causes du problème.

Nous utilisons des outils qui ont fait leurs preuves afin de surveiller les activités suspicieuses sur nos serveurs.

## Directives de développement

Nos pratiques de développement portent une attention toute spéciale au top 10 des risques de sécurité publiés par la fondation OWASP

Biings, en tant qu'application web et serveur, est construit grâce à des frameworks open source qui comportent déjà des couches de sécurité fortes et qui sont régulièrement testés et mis-à-jours pour combler d'éventuelles vulnérabilités.

## Backups

Toutes les données sont sauvegardées quotidiennement dans plusieurs sites différents en Suisse. Pa défaut toutes les sauvegardes sont conservée pour une durée maximum de 30 jours.

Des instantanés de nos serveurs sont régulièrement effectués en cas de désastre nécessitant une récupération rapide des données et fonctions de ceux-ci.

# Protection des données et confidentialité

## Emplacement des données

Biings utilise un serveur localisé en Suisse dont l'hébergeur est Infomaniak. Pour des raisons de sécurité, l'endroit exact où se trouve le serveur n'est pas public.

## Sécurité des comptes Biings

Bien que nous ne requérons pas de mot de passe complexe, nous demandons toujours un nombre minimum de caractères lors de la création ou du changement de mots de passes.

Nous limitons et gardons une trace des connexions échouées, nous interdisons également l'énumération des utilisateurs afin de ralentir une éventuelle tentative d'intrusion.

## Cryptage en transit et au repos

Lorsque nous utilisons un réseau public nous utilisons un cryptage avancé. Nous utilisons des certificats SSL/TLS délivré par GANDI.net. La connection utilise un cryptage AES_128_GCM, avec SHA2 pour l'authentification et ECDHE_RSA en tant que mécanisme d'échange des clés.

Les données sur les absences, les suivis et les données RH ne sont pas cryptées au repos — elles sont actives dans notre base de données et sujette aux mêmes protections et surveillance que nos autres systèmes. Tous les mots de passes sont hashed et salted avec l'algorithme de cryptage Blowfish.

## Sécurité physique

Hébergés dans les data center de classe III+ de chez Infomaniak, nos serveurs sont protégés par plusieurs sas d'entrée, une identification biométrique (qui analyse les veines dans le pouce), de la reconnaissance faciale ainsi qu'un système de surveillance non-stop.

Seul le personnel autorisé à accès au data center. Du personnel est également présent 24/7/365.

## Forces de l'ordre

Biings ne partagera pas vos données avec les forces de l'ordres à moins qu'une ordonnance du tribunal nous y force. Nous rejetons par défaut toute demande des forces de l'ordres locales où fédérales si elles ne sont pas accompagnées d'une telle ordonnance. Et à moins qu'il ne nous soit légalement interdit de le faire nous vous informerons de toutes requêtes de ce genre.

### Rétention des données et suppression

Toutes vos données serons immédiatement inaccessible après une annulation. Lorsque vous supprimez votre compte, nous vous transférerons toutes les données en notre possession et nous nous assurerons avec vous qu'elles soient supprimées de tous nos serveurs. Vos données ne pourrons pas être récupérées une fois qu'elles ont étés supprimées.

## Gestion des incidents et reprise après sinistre

Dans l'éventualité d'un incident, nous contacterons le propriétaire de votre compte et travaillerons avec vous tout du long.

Lorsqu'une brèche de sécurité est détectée, par nos équipes ou systèmes de gestions, nous vous préviendrons dans les plus brefs délais et vous informerons des données potentiellement compromises.

Nous gardons des sauvegardes de secours dans des locaux différents. Elles sont sauvegardées au moins une fois par jours.

Dans le cas d'un incident grave notre équipe est formée afin de restaurer le système grâce à ces sauvegardes de secours.

### En cas d'attaque ransomware

Si nous sommes victime d'une attaque ransomware, nous gèlerons immédiatement les accès aux données actuellement en production, nous informerons également tout les clients ayant été impacté par cette attaque. Nous contacterons également les autorités compétentes.

Par la suite nous mettrons en place un nouveau serveur sur le cloud afin de restaurer les données selon notre dernière sauvegarde afin de permettre a nos clients d'utiliser nos services dans les plus brefs délais. Certaines données peuvent être perdue.

L'étape la plus important va-t-être de chercher les éventuelles vulnérabilités en cause et de les corriger dans la mesure du possible. Bien évidement nos clients serons tous mis au courant de l'avancement de la situation au fur et à mesure.

# Conclusion

Nous sommes entrés dans le secteur en 2013 et avons travaillé avec des entreprises qui requièrent un haut niveau de sécurité. La sécurité n'est pas uniquement une affaire de technologies, c'est une affaire de confiance. Nous avons redoublé d'efforts afin de gagner la confiance de nos client. Protéger les données RH stockées dans Biings est une responsabilité importante que nous avons envers nos clients, et nous continuons à l'honorer afin de maintenir cette relation de confiance.

## Vous souhaitez en savoir plus ?

Posez nous votre question sur notre site web si vous souhaitez aborder directement le sujet avec nous et nous vous répondrons dans les plus brefs délais.

swiss made software
+hosted in switzerland