Dernière mise à jour : octobre 2021

Présentation du programme de sécurité

HubSpot

Table des matières

Présentation du programme de sécurité de HubSpot

L'entreprise et les produits

HubSpot est la première plateforme d'inbound marketing, de vente, de service client, et de gestion de contenu et des opérations au monde. Depuis 2006, l'entreprise s'attache à accélérer le mouvement inbound. Aujourd'hui, plus de 100 000 clients dans plus de 120 pays s'appuient sur ses logiciels, ses services et ses solutions de support pour transformer la façon dont ils attirent et interagissent avec leurs clients, et les fidélisent.

Les produits HubSpot sont proposés sous la forme de solutions SaaS, ou logiciels en tant que service. Ces dernières sont mises à la disposition des clients par le biais d'applications web spécialement conçues à cet effet, d'interfaces de programmation d'application (API) et de plug-ins d'e-mails.

Attention portée à la sécurité et aux risques

La protection des données des clients est le principal objectif de HubSpot en matière de sécurité. C'est pour cette raison que l'entreprise a décidé d'investir dans des ressources et des outils de contrôle adaptés pour offrir des services et un niveau de protection adéquats à ses clients. Ces investissements comprennent la mise en place d'équipes exclusivement chargées de la sécurité de l'entreprise et des produits, responsables du programme exhaustif de gestion de la sécurité et du processus de gouvernance de HubSpot. Ces équipes se concentrent sur l'élaboration de nouveaux outils de contrôle et la mise à jour de ceux déjà en place, ainsi que sur la mise en œuvre et la gestion du champ d'action de HubSpot en matière de sécurité et de risques. Leur mission inclut également le développement d'une structure de support visant à faciliter une gestion efficace des risques. Le responsable de la sécurité supervise la mise en œuvre des mesures de sécurité au sein de HubSpot et de ses produits.

Objectifs en matière de sécurité et de gestion des risques

HubSpot a développé un champ d'action sécuritaire en se basant sur les meilleures pratiques du secteur des SaaS. Les principaux objectifs de l'entreprise comprennent :

- La confiance et la protection des clients : constamment proposer des services et produits de qualité supérieure aux clients, tout en préservant la confidentialité de leurs informations.
- La disponibilité et la continuité du service : garantir la disponibilité constante des services et des données à toute personne autorisée, et minimiser proactivement les risques liés à la sécurité susceptibles d'en affecter la continuité.
- L'intégrité des informations et du service : s'assurer que les données des clients ne sont jamais corrompues ni modifiées d'aucune façon.
- La conformité avec les normes : HubSpot axe son programme de sécurité d'entreprise autour des directives les plus exigeantes du secteur en matière de cybersécurité, notamment les contrôles de sécurité critique du Center for Internet Security (CIS, Centre pour la sécurité sur internet). Les contrôles qui gouvernent la disponibilité, la confidentialité et la sécurité des données des clients sont conçus pour être conformes au certificat SOC 2, conformément aux principes de services de confiance (TSP) établis par l'American Institute of Certified Public Accountants (AICPA).

Contrôles de sécurité de HubSpot

Afin de protéger les données qui lui sont confiées, HubSpot adopte une stratégie de défense en profondeur, en mettant en œuvre plusieurs couches de contrôles de sécurité dans l'ensemble de son organisation. Les sections suivantes décrivent un sous-ensemble des contrôles qui font l'objet des questions les plus fréquentes.

Infrastructure produit de HubSpot

Sécurité de l'infrastructure cloud

HubSpot n'héberge aucun système produit dans ses bureaux. L'entreprise sous-traite l'hébergement de son infrastructure produit à un des fournisseurs d'infrastructure cloud leaders du marché, Amazon Web Services (AWS). Ce fournisseur garantit une disponibilité du service 99,95 à 100 % du temps et les installations appliquent une redondance à l'ensemble des services d'alimentation électrique, de réseau et de ventilation.

L'infrastructure produit AWS de HubSpot est hébergée dans l'est des États-Unis ou en Allemagne. AWS applique un programme de sécurité soumis à des audits, ainsi que des protections de sécurité physiques, environnementales et infrastructurelles. Les plans de continuité des activités et de récupération en cas de sinistre ont été validés de manière indépendante dans le cadre des certifications SOC 2 Type 2 et ISO 27001.

La documentation de conformité est disponible publiquement sur la page de conformité dans le cloud AWS.

HubSpot dispose également dans sa base de connaissances d'un article comprenant les questions fréquentes posées au sujet de l'infrastructure reposant sur le cloud, disponible ici.

Sécurité des réseaux et protection du périmètre

L'infrastructure produit de HubSpot applique plusieurs couches de filtres et d'inspection de toutes les connexions sur l'ensemble de la plateforme.

Des listes de contrôle des accès au niveau du réseau sont mises en place pour empêcher tout accès réseau non autorisé à l'infrastructure interne de l'entreprise. Des pare-feu sont configurés pour refuser les connexions réseau qui ne sont pas explicitement autorisées par défaut, et le suivi du trafic est assuré pour déceler les activités anormales.

Les changements apportés à la sécurité du réseau sont activement surveillés et soumis à des processus de contrôle des modifications. Les ensembles de règles des pare-feu sont révisés tous les ans afin de s'assurer que seules les connexions nécessaires sont configurées.

Gestion de la configuration

L'automatisation permet à HubSpot de s'adapter aux besoins des clients. L'infrastructure produit est un environnement fortement automatisé qui permet d'étendre les capacités dès que cela est nécessaire. Les instances de serveur sont étroitement contrôlées, du provisionnement au déprovisionnement, afin que les déviations des lignes de base des configurations soient détectées et annulées à une cadence prédéfinie. Si un serveur de production dévie ou s'éloigne de la configuration de la ligne de base, celle-ci sera rétablie sous 30 minutes.

Les configurations de tous les types de serveurs sont intégrées dans des images et des fichiers de configuration. La gestion de la configuration au niveau des serveurs se fait par l'intermédiaire de ces images et scripts de configuration lorsque le serveur est construit. Les modifications apportées à la configuration et aux images standards sont effectuées via un processus contrôlé de gestion des changements. Chaque type d'instance comprend sa propre configuration renforcée, en fonction de son déploiement.

La gestion des correctifs est généralement effectuée avec des outils automatisés de gestion des configurations ou en supprimant les instances de serveurs qui ne sont plus conformes à la ligne de base attendue et en créant une instance de remplacement.
Une gestion rigoureuse et automatisée de la configuration est intégrée à la gestion quotidienne de l'infrastructure HubSpot.

Alertes et surveillance

HubSpot automatise l'intégralité de ses procédures de production et investit aussi fortement dans des capacités automatisées de surveillance, d'alerte et de réponse pour

gérer les problèmes potentiels en continu. L'infrastructure produit de HubSpot est conçue pour alerter les ingénieurs et les administrateurs lorsque des anomalies surviennent. Les taux d'erreurs, les abus, les attaques d'applications et d'autres anomalies déclenchent notamment des réponses et des alertes automatiques qui sont adressées aux équipes concernées afin qu'elles puissent les analyser et les corriger. Si des activités inattendues ou malveillantes se produisent, des systèmes automatisés font appel aux bons intervenants pour une résolution rapide du problème.

De nombreux déclencheurs automatisés sont également intégrés au système pour répondre immédiatement aux situations imprévisibles. Le blocage du trafic, la mise en quarantaine, la fin des processus et d'autres fonctionnalités similaires sont déclenchés si des seuils prédéfinis sont atteints. La plateforme HubSpot peut ainsi parer à une grande variété de situations indésirables.

Protection des applications

Défenses des applications web

Tous les contenus de clients hébergés sur la plateforme sont protégés par un pare-feu d'applications web (WAF). La configuration du WAF repose sur une combinaison de normes sectorielles et de règles personnalisées offrant la possibilité d'activer ou de désactiver automatiquement certains outils de contrôle, afin de garantir un niveau de protection optimal aux clients. Ces outils assurent un suivi actif et en temps réel du trafic au niveau des applications. Ils permettent en outre de recevoir des alertes ou de bloquer un comportement malveillant lorsqu'il est détecté, selon le type et la fréquence de ce dernier.

Les règles appliquées pour détecter et bloquer le trafic malveillant s'alignent sur les directives des meilleures pratiques documentées par l'Open Web Application Security Project (OWASP), notamment son Top 10 et des recommandations similaires. Des dispositifs de protection contre les attaques par déni de service (DDoS) sont également incorporés pour s'assurer que les sites web des clients et les autres éléments des produits HubSpot sont disponibles en permanence.

Gestion du développement et des sorties

L'un des avantages majeurs de HubSpot tient à un ensemble de fonctionnalités au développement rapide. Les produits sont constamment optimisés grâce à une approche de distribution continue et moderne du développement logiciel.

Du nouveau code est proposé, approuvé, intégré et déployé plusieurs milliers de fois par jour. Les vérifications des codes, les tests, le cas échéant, et l'approbation des fusions sont effectués avant le déploiement. L'approbation est contrôlée par des propriétaires de référentiel désignés. Une fois approuvé, le code est automatiquement soumis à l'environnement d'intégration continue de HubSpot, où s'effectuent les processus de compilation, de packaging et de test.

Chaque déploiement archive les codes de production existants pour parer à toute détection d'échec par les hooks post-déploiement. L'équipe en charge du déploiement gère les notifications liées à l'intégrité des applications. En cas d'échec, une procédure de restauration est immédiatement lancée.

HubSpot utilise un système exhaustif de séparation des logiciels et de gestion du trafic pour contrôler les fonctionnalités basées sur les préférences des clients (bêta privée, bêta publique, lancement complet). L'entreprise effectue des mises à jour transparentes et, en tant qu'application SaaS, les lancements n'entraînent aucun temps d'arrêt. Les modifications importantes de fonctionnalités sont communiquées par le biais de messages dans l'application et/ou d'articles portant sur les mises à jour de produits.

Lors de la dernière phase de test, le nouveau code est déployé dans un environnement d'assurance qualité HubSpot dédié et distinct, avant d'être exécuté dans l'environnement de production. La segmentation au niveau du réseau empêche tout accès non autorisé entre ces deux environnements.

Analyses de vulnérabilité, tests d'intrusion et programme de recherche de bugs

L'équipe de sécurité de HubSpot adopte une approche à plusieurs niveaux pour les analyses de vulnérabilité et utilise un ensemble d'outils reconnus dans le secteur pour garantir une analyse complète de l'environnement technologique.

Les analyses de vulnérabilité sont configurées pour déceler quotidiennement les vulnérabilités exploitables. Des analyses permanentes, qui font appel à des listes d'inclusion d'analyses flexibles, et des signatures de détection des vulnérabilités en mise à jour constante aident HubSpot à parer à de nombreuses menaces de sécurité.

HubSpot fait appel à des parties tierces reconnues dans le secteur pour effectuer des tests d'intrusion annuels. L'objectif de ces programmes consiste à déceler de manière itérative toute faille présentant un risque de sécurité et à traiter les éventuels problèmes dans les meilleurs délais. Les tests d'intrusion sont effectués au niveau des applications et du réseau de la plateforme HubSpot.

Outre les analyses de vulnérabilités internes et les tests d'intrusion indépendants, HubSpot gère également un programme de recherche de bugs, dans le cadre duquel des chercheurs en sécurité informatique indépendants sont invités à déceler des failles dans les produits HubSpot. Les membres de la communauté et les clients HubSpot peuvent également effectuer des tests de sécurité sur des portails d'essai. Pour obtenir de plus amples informations sur le programme de recherche de bugs de HubSpot, merci de consulter https://bugcrowd.com/hubspot.

Protection des données des clients

Séparation logique des locataires

HubSpot propose une solution SaaS hautement évolutive et multi-locataire. L'interface utilisateur et les API HubSpot limitent l'accès au contenu autorisé exclusivement.
La plateforme HubSpot réalise une segmentation logique des données à l'aide d'un identifiant de portail unique, qu'elle associe à toutes les données et à tous les objets spécifiques à un client. Les informations sont disponibles via l'interface utilisateur ou les API afin d'être produites pour un portail HubSpot précis, sans aucun risque d'accès entre portails ou de pollution des données.

Les règles d'autorisation sont incorporées dans l'architecture de conception et validées en continu. En outre, HubSpot enregistre les authentifications d'application et les

modifications associées, la disponibilité des applications et les vues de page effectuées par les utilisateurs.

Informations confidentielles

Les produits HubSpot offrent une expérience de marketing, de vente, de service client, de gestion de contenu et de gestion des opérations intégrée. Les données collectées par leur intermédiaire correspondent aux informations recueillies dans le cadre d'interactions avec des leads ou des clients, celles disponibles dans les annuaires publics et grâce à des sources tierces fiables.

Les outils de HubSpot permettent aux clients de définir le type d'informations pouvant être recueillies et stockées en leur nom. Conformément aux Conditions d'utilisation et à la Politique d'utilisation acceptable de HubSpot, les clients doivent s'assurer qu'ils recueillent uniquement des informations pertinentes pour leurs processus relatifs au marketing, à la vente, au service client, à la gestion de contenu et aux opérations. Les produits HubSpot ne doivent pas être utilisés pour collecter ou capturer des données sensibles, telles que des numéros de cartes de crédit ou de débit, des informations financières personnelles, des numéros de sécurité sociale, de passeport ou de permis de conduire, ni toute information liée à l'état de santé ou à la situation professionnelle ou financière.

Davantage d'informations sur la classification des données utilisées et prises en charge par le système HubSpot sont disponibles dans le tableau de classification des données du rapport SOC 2 de l'entreprise.

Chiffrement en transit et au repos

Chaque interaction sensible avec les produits HubSpot, comme les appels d'API ou les sessions authentifiées, est chiffrée en transit à l'aide des protocoles TLS 1.2 ou 1.3 et de clés de 2 048 bits ou supérieures. Le protocole TLS (Transport Layer Security) est également activé par défaut pour les clients qui hébergent leurs sites web sur la plateforme HubSpot.

Merci de consulter le guide de configuration de site web et l'article de la base de connaissances intitulé SSL et sécurité du domaine dans HubSpot pour plus d'informations sur la configuration du protocole TLS.

HubSpot s'appuie sur plusieurs technologies pour garantir le chiffrement des données stockées au repos. Les données de la plate-forme sont stockées avec un chiffrement AES-256. Les mots de passe utilisateurs sont hachés en respectant les meilleures pratiques du secteur et sont chiffrés au repos. Certaines fonctionnalités d'e-mail offrent une couche de chiffrement supplémentaire, aussi bien au repos qu'en transit.

Gestion des clés

Les clés de chiffrement en transit et au repos sont gérées de manière sécurisée par la plateforme HubSpot. Les clés privées TLS pour le chiffrement en transit sont contrôlées par le biais du partenaire de diffusion de contenu de HubSpot. Les clés de chiffrement de volume et de champ pour les données au repos sont stockées dans un système de gestion des clés renforcé. La fréquence de rotation des clés dépend du caractère sensible des données chiffrées. De manière générale, les certificats TLS sont renouvelés tous les ans.

Actuellement, HubSpot ne peut pas utiliser de clés de chiffrement fournies par des clients.

Sauvegarde des données et récupération après sinistre

Fiabilité et récupération du système

HubSpot s'engage à assurer la disponibilité de ses systèmes en déployant tous les efforts commercialement raisonnables pour atteindre une disponibilité du service de 99,95 % pour son service d'abonnement au cours d'un mois civil donné. Veuillez vous référer à la Section 7 des Conditions spécifiques liées aux produits pour en savoir plus.

De plus, HubSpot fournit des mises à jour en temps réel et un historique des données sur le statut et la sécurité de son système sur son site dédié.

Tous les services des produits HubSpot sont conçus avec une redondance complète. L'infrastructure des serveurs est répartie de manière stratégique sur de multiples zones de disponibilité distinctes et sur des réseaux cloud virtuels et privés auprès des fournisseurs d'infrastructure de HubSpot. De plus, tous les composants web, d'applications et de bases de données sont déployés avec un minimum d'instances ou de conteneurs de serveurs de support N+1.

Récupération après sinistre

HubSpot applique un plan de récupération après sinistre qui est testé tous les ans dans le cadre de ses contrôles SOC 2. Veuillez vous référer au rapport SOC 2 de l'entreprise, qui peut être téléchargé sur la page hubspot.fr/security, pour en savoir plus.

Stratégie de sauvegarde

SAUVEGARDES DES SYSTÈMES

Une sauvegarde des systèmes est effectuée régulièrement en respectant des fréquences et des calendriers bien établis. Sept jours d'enregistrement sont conservés pour toutes les bases de données de manière à faciliter les restaurations éventuelles. Les sauvegardes sont suivies pour s'assurer de leur bonne exécution, et des alertes sont générées si des exceptions se produisent. Tout échec est communiqué, analysé et résolu.

Les données sont sauvegardées chaque jour dans leur propre région. De plus, les sauvegardes sont copiées périodiquement dans une région AWS différente à des fins de récupération en cas d'indisponibilité du centre régional principal. Des processus de surveillance et d'alerte sont en place pour les échecs de réplication, et sont gérés en conséquence.

Tous les ensembles de données de production sont hébergés dans un système de stockage de fichiers haute disponibilité, comme le système S3 d'Amazon.

STOCKAGE PHYSIQUE DES SAUVEGARDES

Dans la mesure où HubSpot fait appel à des services de cloud publics pour l'hébergement, la sauvegarde et la récupération, l'entreprise n'intègre pas d'infrastructure ou de moyen de stockage physique dans ses produits. HubSpot ne produit et n'utilise généralement pas de supports imprimés (papier ou ruban, par exemple) dans le cadre de l'offre de ses produits à ses clients.

DISPOSITIFS DE PROTECTION DES SAUVEGARDES

Par défaut, toutes les sauvegardes sont protégées par le biais de restrictions de contrôle d'accès aux réseaux des infrastructures produits de HubSpot, et de listes de contrôle d'accès aux systèmes stockant les fichiers de sauvegarde.

OPTIONS DE SAUVEGARDE OFFERTES AUX CLIENTS

La plateforme HubSpot propose de nombreuses options aux clients qui souhaiteraient également effectuer une copie de leurs données. Le portail HubSpot contient de nombreuses fonctionnalités d'export, et la bibliothèque d'API publiques peut être utilisée pour synchroniser les données avec des systèmes tiers. Pour en savoir plus sur la sauvegarde de données, consultez l'article de la base de connaissances portant sur l'export de contenu.

Contrôle des identités et des accès

Gestion des utilisateurs des produits

Les produits HubSpot peuvent prendre en charge des règles d'autorisation détaillées. Les clients ont la possibilité de créer et de gérer les utilisateurs de leurs portails, ainsi que d'attribuer les privilèges appropriés à ces comptes et de limiter leur accès aux fonctionnalités de données.

Pour en savoir plus sur les rôles utilisateurs, merci de consulter le guide HubSpot relatif aux rôles utilisateurs et aux autorisations.

Dispositifs de protection pour les identifiants de connexion aux produits

Les produits HubSpot proposent aux utilisateurs plusieurs façons de se connecter à leurs comptes : le système de connexion HubSpot intégré, l'option « S'identifier avec Google » ou l'authentification unique (SSO). Une politique relative aux mots de passe est appliquée de façon uniforme au système de connexion intégré. Elle stipule que les mots de passe doivent être composés d'au moins 8 caractères et contenir des lettres majuscules et minuscules, des caractères spéciaux, des espaces et des chiffres. Les utilisateurs du système de connexion intégré de HubSpot ne peuvent pas modifier cette politique.

Tous les clients de HubSpot disposent de la fonctionnalité « S'identifier avec Google ». Un SSO plus avancé basé sur SAML et intégré à n'importe quel fournisseur d'identité basé sur SAML est disponible avec tous les produits Entreprise de HubSpot.

Les clients qui ont recours à un service d'authentification unique ont la possibilité de configurer une telle connexion pour leurs utilisateurs. Des instructions pour la configuration

d'une authentification unique sont disponibles dans cet article de la base de connaissances et dans HubSpot Academy. Les utilisateurs qui se connectent à l'aide de l'authentification unique ou de Google peuvent définir une politique relative aux mots de passe par l'intermédiaire de leur service SSO ou de leurs comptes Google.

Par ailleurs, il est recommandé aux clients qui utilisent le système de connexion intégré de HubSpot de configurer la double authentification, qui peut être activée par les administrateurs via leur portail HubSpot pour l'ensemble des utilisateurs.

Autorisation des API produits

L'accès aux interfaces de programmation d'application (API) se fait soit au moyen d'une clé d'API, soit par le biais du protocole d'autorisation OAuth (version 2). Les clients ont la possibilité de générer des clés API pour leurs portails. Ces clés sont conçues pour établir des prototypes d'intégrations personnalisées dans les meilleurs délais. L'implémentation du protocole OAuth de HubSpot représente une approche plus rigoureuse d'authentification et d'autorisation des requêtes d'API. De plus, toutes les intégrations présentées exigent l'application de ce protocole. Les autorisations relatives aux requêtes générées par le protocole OAuth sont établies dans des domaines d'application définis. Pour plus d'informations sur l'utilisation des API, merci de consulter le portail des développeurs sur le site web de HubSpot.

Accès à l'infrastructure de production

L'accès aux systèmes de HubSpot est strictement contrôlé et suit le principe du moindre privilège. Les salariés de HubSpot se voient accorder l'accès en fonction d'un modèle de contrôle des accès basé sur les rôles.

L'accès quotidien est strictement limité aux personnes qui en ont besoin dans le cadre de leur fonction. Pour les accès d'urgence (réponse aux alertes et résolution des problèmes, par exemple) et l'accès aux fonctions administratives, le système de HubSpot applique une méthode appelée JITA (Just in Time Access) selon laquelle il est possible de demander l'accès à des fonctions spécifiques pour une durée limitée. Chaque requête JITA est enregistrée, et les fichiers journaux font l'objet d'un suivi continu pour détecter les requêtes

anormales. Une fois que la session à durée limitée prend fin, l'accès au compte expire et est révoqué automatiquement.

Par ailleurs, les connexions réseau directes aux appareils de l'infrastructure produit par SSH ou protocoles similaires sont interdites. Les ingénieurs doivent s'identifier par le biais d'un bastion ou d'un serveur de rebond avant de pouvoir accéder aux environnements de contrôle qualité ou de production. L'authentification au niveau des serveurs s'effectue par l'intermédiaire de clés SSH uniques à chaque utilisateur et d'un processus de double authentification qui requiert l'utilisation de jetons.

Les accès des salariés à des ressources liées à la production et à l'entreprise sont sujets à une réévaluation quotidienne automatisée et à au moins une réévaluation semestrielle manuelle.

Accès des salariés de HubSpot aux portails des clients

Les membres du support client, du service client et d'autres équipes en relation avec les clients peuvent effectuer une requête JITA pour accéder aux portails des clients pour une période de temps limitée. Les demandes d'accès sont restreintes aux responsabilités de leur poste et associées aux activités de support et d'assistance apportées aux clients. Ces demandes sont limitées au portail d'un client précis pour une période de 24 heures maximum. Toutes les demandes d'accès, connexions, requêtes, consultations de page et autres informations du même ordre sont enregistrées.

Authentification et autorisation de l'entreprise

L'accès au réseau de l'entreprise, à distance ou dans les bureaux, exige une authentification à plusieurs facteurs (MFA), et toutes les applications SaaS utilisées par HubSpot exigent une authentification unique (SSO) avec MFA afin de faciliter les contrôles d'accès centralisés.

Les politiques liées aux mots de passe respectent les meilleures pratiques du secteur en matière de longueur, de complexité et de fréquence de rotation.

HubSpot a conçu des systèmes de support complets pour rationaliser et automatiser ses activités de gestion et de conformité de la sécurité. Parmi ses nombreuses fonctions, le système analyse plusieurs fois par jour l'infrastructure produit et de l'entreprise afin de s'assurer que les autorisations sont adéquates, de gérer les événements liés aux salariés,

de révoquer des comptes et des accès si nécessaire, de compiler les fichiers journaux des demandes d'accès et de capturer des preuves de conformité pour chacun des contrôles de sécurité technologique de l'entreprise. Par périodes de 24 heures, ces systèmes internes examinent l'infrastructure et vérifient que celle-ci correspond aux configurations approuvées.

Sécurité de l'organisation et de l'entreprise

Vérifications des antécédents et intégration des salariés

Les salariés de HubSpot aux États-Unis font l'objet d'une vérification complète d'antécédents avant de recevoir une proposition d'embauche formelle. Des vérifications concernant plus particulièrement les qualifications professionnelles et scolaires ainsi que les antécédents judiciaires sont effectuées pour les salariés potentiels. En dehors des États-Unis, des vérifications des antécédents professionnels sont effectuées. La vérification des références est laissée à la discrétion du responsable du recrutement.

Lors de leur embauche, tous les salariés doivent lire et accepter la Politique d'utilisation acceptable d'entreprise de HubSpot et les principes de bon sens de HubSpot, qui définissent les responsabilités des salariés en matière de sécurité et de protection des supports et des données de l'entreprise, y compris, mais sans s'y limiter, la protection des appareils portables et des équipements professionnels.

Gestion des politiques

Afin d'aligner tous les salariés de HubSpot sur la protection des données, l'entreprise documente et applique plusieurs politiques et procédures écrites. Elle applique une politique de sécurité des informations écrites principale, qui couvre les exigences en matière de gestion des données, les considérations liées à la confidentialité et les réponses aux violations, parmi de nombreux autres sujets.

Les politiques sont revues et approuvées au moins une fois par an, et stockées dans le wiki de l'entreprise. Les politiques qui exigent une attestation des employés sont incorporées dans les formations annuelles obligatoires.

Formation de sensibilisation à la sécurité

HubSpot considère que ses salariés sont en première ligne et s'assure qu'ils sont bien formés pour leur rôle. Une formation de sensibilisation à la sécurité, qui aborde les meilleures pratiques en matière de sécurité générale, est proposée à tous les nouveaux salariés de HubSpot lors de leur embauche, et sur une base annuelle. HubSpot informe également ses équipes des actualités et des initiatives récentes du secteur par le biais d'articles dans sa base de connaissances interne.

Après la formation initiale, des contenus plus spécialisés sont disponibles en fonction du rôle et des accès des salariés. Par exemple, HubSpot propose le programme Security Advocates, un programme centré sur la sécurité, grâce auxquels les développeurs des équipes produits peuvent bénéficier de formations supplémentaires liées à la sécurité, aux risques fréquents, aux menaces et aux défis en la matière.

Gestion des risques

HubSpot dispose d'un programme de gestion des risques en entreprise, qui inclut une politique documentée, des évaluations continues des risques et un registre formel des risques. Les activités de mitigation et de résolution des risques sont suivies grâce à un système de tickets et examinées à une cadence définie.

Davantage de détails sur le programme d'évaluation et de gestion des risques sont disponibles dans le rapport SOC 2, qui peut être téléchargé sur la page hubspot.fr/security.

Gestion des prestataires

HubSpot fait appel à plusieurs fournisseurs de services tiers afin d'accroître la capacité des produits HubSpot à répondre aux besoins des clients en matière de marketing, de vente, de service client, de gestion de contenu et d'opérations. L'entreprise poursuit un programme de gestion des prestataires afin de garantir la mise en place de contrôles de sécurité et de respect de la confidentialité adéquats. Ce programme inclut l'inventaire, le suivi et l'examen des programmes de sécurité des prestataires qui travaillent pour HubSpot.

Des dispositifs de sécurité appropriés sont évalués au regard du service fourni et du type de données échangées. Le respect continu des protections attendues est géré dans le cadre de la relation contractuelle de HubSpot avec ces derniers. Les équipes de HubSpot chargées de la sécurité, des aspects juridiques et de la conformité travaillent en lien avec les parties prenantes commerciales dans le cadre du processus d'examen de la gestion des prestataires.

HubSpot fournit également la liste de ses sous-traitants ultérieurs dans son Accord sur le traitement des données.

Dispositifs de protection physique

La sécurité des bureaux HubSpot est assurée de plusieurs façons. Des agents de sécurité sont présents dans l'ensemble des succursales à travers le monde afin de créer un environnement sûr pour les salariés. L'ouverture des portes est contrôlée à l'aide de jetons RFID associés à chaque individu, qui sont automatiquement mis hors service en cas de perte ou lorsqu'ils ne sont plus nécessaires (cessation de contrat de travail, utilisation peu fréquente, etc.). La vidéosurveillance et de nombreux autres dispositifs de sécurité sont mis en œuvre dans les bureaux HubSpot.

Dispositifs de protection du réseau de l'entreprise

Des pare-feu d'applications à la gestion centralisée sont déployés pour une disponibilité élevée dans les bureaux de HubSpot. Les réseaux pour les invités sont séparés du réseau de l'entreprise, et disposent de pare-feu distincts. Des pare-feu sont configurés pour filtrer le trafic réseau entrant non autorisé et pour refuser les connexions réseau entrantes qui ne sont pas explicitement autorisées par une règle.

HubSpot effectue des vérifications de conformité du système avant d'autoriser la connexion d'un appareil à son réseau entreprise. Les appareils non autorisés sont déconnectés immédiatement ou transférés vers des VLAN de confinement.

Dispositifs de protection des points de terminaison, protection anti-virus et protection contre les logiciels malveillants

HubSpot utilise des outils de détection des menaces et de réponse sur les points de terminaison (EDR) pour protéger ses systèmes. L'entreprise dispose ainsi d'une visibilité complète sur les comportements système anormaux, et elle est en mesure d'enquêter et de réagir rapidement grâce à des déclencheurs d'événements automatisés ou à l'isolation manuelle d'un système. Sa plateforme EDR est intégrée à d'autres outils de la pile de sécurité pour créer un écosystème optimisé de plusieurs outils qui défend efficacement l'entreprise.

Gestion des incidents

Réponse aux incidents

L'équipe du centre d'opérations de sécurité de HubSpot fournit une couverture 24h/24, 7j/7 et 365 jours par an pour répondre rapidement à tous les événements liés à la sécurité et la confidentialité. Le programme de réponse rapide aux incidents de HubSpot est réactif et reproductible. Des types d'incidents, basés sur l'historique des tendances, sont prédéfinis et créés afin de faciliter le suivi opportun des incidents, l'affectation cohérente des tâches, la transmission et la communication. De nombreux processus automatisés alimentent le système de réponse aux incidents, y compris les activités malveillantes ou les alertes liées à des anomalies ou aux prestataires, les requêtes des clients, les événements liés à la confidentialité, etc.

Pour répondre à un incident, HubSpot détermine tout d'abord, dans la mesure du possible, l'exposition de l'information ainsi que la source du problème de sécurité. Le cas échéant, l'entreprise fournit des comptes rendus réguliers pour garantir une résolution appropriée de l'incident.

Le responsable de l'information et de la sécurité examine tous les incidents liés à la sécurité, qu'ils soient suspectés ou avérés, puis HubSpot contacte les clients concernés pour leur proposer la solution la plus adaptée à la nature de l'incident.

HubSpot dispose également d'une équipe interne de détection des menaces qui travaille en continu pour déceler toutes les vulnérabilités et s'assurer que les meilleures pratiques sont mises en place pour sécuriser les produits de l'entreprise.

Conformité

Loi Sarbanes-Oxley (SOX)

HubSpot étant une entreprise cotée en bourse, ses principaux contrôles informatiques sont audités de manière récurrente, conformément à la loi Sarbanes-Oxley.

Des informations publiques relatives aux mesures prises par HubSpot pour se conformer à cette loi et les rapports financiers annuels de l'entreprise sont disponibles dans le cadre des déclarations fournies à la SEC. Plus d'informations sont disponibles sur la page des relations avec les investisseurs : https://ir.hubspot.com/

Contrôles de systèmes et d'organisation (SOC 2)

HubSpot se soumet tous les ans à des audits SOC 2 Type 2 et SOC 3 rigoureux pour attester des contrôles mis en place et qui gouvernent la disponibilité, la confidentialité et la sécurité des données de ses clients, conformément aux principes de services de confiance (TSP) établis par l'American Institute of Certified Public Accountants (AICPA). HubSpot est fier de l'excellence de ses contrôles et vous invite à contacter votre représentant HubSpot pour obtenir une copie du rapport SOC 2 Type 2. Le rapport SOC 3 est disponible publiquement et peut être téléchargé sur la page des dispositifs de sécurité de HubSpot : https://hubspot.fr/security.

Traitement et stockage des données sensibles

Veuillez consulter les Conditions d'utilisation (https://legal.hubspot.com/fr/terms-of-service) pour en savoir plus sur les types de données interdites. Les produits HubSpot ne doivent pas être utilisés pour collecter ou capturer des données sensibles, telles que des numéros de cartes de crédit ou de débit, des informations financières personnelles, des numéros de sécurité sociale, de passeport ou de permis de conduire, ou tout autre numéro

d'identification de même nature, ni toute information liée à l'état de santé ou à la situation professionnelle ou financière.

De nombreux clients travaillant dans le domaine de la santé utilisent HubSpot pour les besoins des équipes en contact direct avec la clientèle, sans incorporer de données sensibles liées à la santé des patients. Toutefois, HubSpot ne doit pas être considéré comme une solution pour le traitement ou le stockage électronique d'informations de santé protégées. L'entreprise n'est pas conforme à la loi HIPAA et n'est pas certifiée HITRUST.

De même, les clients de HubSpot règlent leur facture par carte de crédit, mais HubSpot ne stocke pas, ne traite pas et ne collecte pas les informations de carte de crédit soumises par ses clients et n'est pas conforme à la norme PCI-DSS. HubSpot fait appel à des prestataires fiables et conformes à la norme PCI pour les paiements par carte de crédit, afin que ses transactions soient gérées en toute sécurité.

Confidentialité

La confidentialité des données des clients est l'une des préoccupations principales de HubSpot. Comme indiqué dans la Politique de confidentialité de HubSpot, l'entreprise ne vend jamais les données personnelles à des tiers. Les mesures de protection décrites dans le présent document et les autres dispositifs mis en place visent à garantir que les données demeurent confidentielles et inaltérées. Les produits HubSpot ont été conçus avec pour préoccupation principale les besoins des clients et les questions de confidentialité. Le programme de HubSpot pour le respect de la confidentialité intègre les meilleures pratiques, les besoins des clients et de leurs contacts ainsi que les exigences réglementaires.

Conservation et suppression des données

Les données des clients sont conservées tant que ceux-ci restent actifs. La plateforme HubSpot fournit aux clients actifs des outils qui leur permettent de supprimer leurs données (voir la section « Suppression ou restitution des données personnelles » de l'Accord sur le traitement des données de HubSpot), ou de les exporter (voir l'article de la base de connaissances qui explique comment exporter du contenu et des données).

Les données des anciens clients sont supprimées des bases de données actives sur demande écrite de ces derniers ou après un laps de temps prédéfini suivant la résiliation de l'ensemble des contrats. Les données des utilisateurs des outils gratuits sont effacées lorsque le portail n'est plus activement utilisé, et les données liées aux anciens clients des versions payantes sont supprimées après un délai de 90 jours suivant la fin de toute relation.

Les informations stockées dans les réplicas, les instantanés et les sauvegardes ne sont pas supprimées de façon active, mais purgées naturellement au fil du cycle de vie des données. HubSpot conserve certaines données telles que les fichiers journaux et métadonnées connexes afin de répondre à des exigences de sécurité, de conformité ou statutaires.

Actuellement, HubSpot ne permet pas à ses clients de définir des politiques personnalisées de rétention des données.

Gestion du programme de respect de la confidentialité

L'équipe juridique, l'équipe de sécurité et de nombreuses autres équipes collaborent pour s'assurer que le programme du respect de la confidentialité est mis en œuvre de manière continue et efficace. Pour en savoir plus sur l'engagement de l'entreprise à respecter la confidentialité des données, merci de consulter :

- La Politique de confidentialité de HubSpot
- La Politique de confidentialité relative à l'utilisation du produit HubSpot
- L'Accord sur le traitement des données de HubSpot

Réponse aux violations

Les politiques en matière de signalement des violations, ainsi que les processus et les obligations de HubSpot en la matière sont détaillés dans la section « Réponse aux incidents » du rapport SOC.

Les obligations de HubSpot liées aux violations de données personnelles sont également détaillées dans son Accord sur le traitement des données.

RGPD

La plateforme HubSpot comporte des fonctionnalités qui permettent aux clients de facilement satisfaire aux exigences du Règlement général sur la protection des données (RGPD), notamment la capacité d'effectuer une suppression conforme au RGPD, en réponse à des demandes d'accès à des données personnelles (veuillez consulter l'article de la base de connaissances ici). Vous pouvez vous référer à la page RGPD de HubSpot ici.

Portée et utilisation du présent document

La transparence vis-à-vis des méthodes employées pour offrir les services HubSpot à ses clients est une valeur chère à l'entreprise. Ce document a été conçu en tenant compte de cette transparence. HubSpot améliore en permanence les mesures de protection mises en œuvre. À ce titre, les informations et les données contenues dans le présent document, et toute communication connexe, ne sont pas destinées à créer une obligation contractuelle ou contraignante entre HubSpot et toute autre partie, ni à modifier, altérer ou réexaminer les accords établis entre les parties.