Sécurité et protection contre les vulnérabilités dans Google Apps : une étude détaillée

Livre blanc Google - Février 2007

La sécurité dans Google Apps

POUR PLUS D'INFORMATIONS

En ligne : www.google.com/a
E-mail : apps-enterprise@google.com

La protection des applications réseau contre d'éventuelles tentatives de piratage est un élément clé du bon fonctionnement de tout système informatique. En matière de messagerie et de collaboration, les enjeux sont décuplés. Google investit des milliards de dollars dans ses équipes, dans les procédures et dans les technologies pour garantir la sécurité et la confidentialité des données dans Google Apps. Une équipe dédiée à la sécurité et composée de professionnels expérimentés a été mise en place. Cette équipe est chargée de concevoir les systèmes de sécurité en amont et de procéder à des audits à tous les niveaux (conception, codification, produit fini) afin d'en garantir la conformité avec les standards très stricts de Google en matière de sécurité et de confidentialité des données. L'infrastructure qui héberge Google Apps et des centaines de milliers de données utilisateur est aussi utilisée pour gérer les données de millions de consommateurs et les milliards de dollars investis dans des transactions publicitaires. Avec Google Apps, vos informations sont en sécurité.

Introduction

Google est en charge de l'organisation de l'information mondiale : la sécurité des données de dizaines de millions d'utilisateurs s'inscrit au cœur de cette mission. Google prend très au sérieux cette responsabilité et a mis en place des moyens considérables pour gagner la confiance de ses utilisateurs et pour en rester digne. En effet, ce n'est que grâce à des produits sûrs qu'il est possible de conserver la confiance des utilisateurs et de créer des produits novateurs qui serviront les besoins et les intérêts des futurs utilisateurs.

Conséquence de cette prise de conscience, Google propose au travers de Google Apps des produits sûrs et fiables. Les produits et les services offerts combinent des solutions technologiquement avancées avec les règles en matière de sécurité les plus performantes du marché. Des milliards de dollars en capital sont investis pour garantir aux données et aux applications l'environnement le plus sûr et le plus fiable possible. Google se concentre en particulier sur plusieurs aspects clés pour ses clients professionnels :

- Sécurité organisationnelle et opérationnelle : règles et procédures à mettre en place pour garantir la sécurité à toutes les étapes des opérations (conception, déploiement, phase opérationnelle).
- Sécurité des données : stockage des données des clients en lieu sûr et sur des serveurs et dans des applications sécurisés.
- Protection contre les menaces : protection des utilisateurs et de leurs informations contre les risques d'attaques malveillantes et le piratage.
- Accès sécurisé : accès aux données réservé aux seuls utilisateurs autorisés et sécurité des canaux d'accès.
- Confidentialité des données : confidentialité des données à caractère sensible.

Le présent document décrit la stratégie de Google en matière de sécurité et les nombreuses mesures mises en œuvre aux plans physique, logique et opérationnel pour garantir une sécurité et une confidentialité maximale des données.

Sécurité organisationnelle et opérationnelle

Les piliers sur lesquels Google s'appuie sont ses collaborateurs et les procédures mises en place. Équipes, procédures, technologie : seule la conjonction de ces trois facteurs permet d'assurer un environnement informatique responsable et sécurisé. La sécurité n'est pas un élément que l'on se contente de vérifier a posteriori. Bien au contraire, elle doit faire partie intégrante des produits et de l'architecture et de l'infrastructure des systèmes en amont. Chez Google, une équipe dédiée à plein temps est chargée de développer, de documenter et de mettre en œuvre des règles exhaustives en la matière. Certains experts mondiaux dans le domaine de la sécurité des informations, des applications et des réseaux l'ont rejointe.

Cette équipe se divise en différents secteurs fonctionnels : protection du périmètre, protection des infrastructures, protection des applications, détection et prévention des failles du système. Google a attiré des spécialistes de la sécurité ayant fait carrière dans les entreprises du Fortune 500. Leur objectif est d'élaborer des mesures préventives visant à intégrer la notion de sécurité dès la phase de développement du code source et du système et à répondre de façon dynamique aux problèmes ponctuels.

.

Méthodologie de développement
La sécurité est l'une des priorités de Google dès la conception d'un nouveau produit. Les équipes techniques et les équipes produit reçoivent une formation approfondie en la matière. La méthodologie de développement repose sur un plan composé de plusieurs étapes et comprenant des points de contrôle réguliers ainsi que des audits complets.

L'équipe Google de sécurité des applications est impliquée dans toutes les phases de développement du produit, depuis sa conception et l'audit de son code source jusqu'au lancement final du produit, en passant par les étapes de test fonctionnel et de test du système. Durant tout ce processus, Google fait appel à un certain nombre de technologies commerciales et propriétaires. Il est également du ressort de l'équipe concernée de s'assurer que des procédures de développement sécurisées sont mises en place pour garantir la sécurité du client.

Sécurité opérationnelle
L'objectif principal de l'équipe de sécurité de Google est d'assurer la sécurité des systèmes opérationnels tant au niveau du traitement des données qu'à celui de la gestion des systèmes. Des audits réguliers sont menés sur les opérations effectuées dans les centres de données et les menaces potentielles à l'encontre des actifs physiques et logiques de Google sont en permanence évaluées.

L'équipe de sécurité est également en charge de la sensibilisation et de la formation de tous les collaborateurs de la société afin qu'ils exercent leur activité dans un souci constant de sécurité et de professionnalisme. Préalablement à l'embauche de tout nouveau collaborateur, le passé professionnel de celui-ci est passé au peigne fin. Tous les membres de l'équipe sont formés de façon approfondie et leurs connaissances font l'objet de mises à jour régulières.

Communauté des acteurs en matière de sécurité et consultants
Google travaille également en étroite collaboration avec la communauté des différents acteurs en matière de sécurité et fait sienne l'expérience des meilleurs experts mondiaux dans ce domaine. Un positionnement à la pointe des nouveautés dans le secteur, une capacité de réaction très rapide face à toute menace potentielle et une aptitude à tirer le meilleur parti de l'expertise de tous les acteurs concernés à l'intérieur et à l'extérieur de l'entreprise sont les fruits de cette collaboration. Google conduit cette communauté élargie dans la voie de la divulgation responsabilisée. Pour plus d'informations sur ce programme et sur les experts clés avec lesquels Google est en dialogue permanent, consultez le site **http://www.google.com/corporate/security.html**.

En dépit de cette protection à tous les niveaux, de nouvelles menaces peuvent voir le jour, menaces que Google est en mesure de contrer rapidement. L'équipe de sécurité audite toutes les infrastructures afin d'identifier les menaces potentielles et coopère avec les équipes techniques pour résoudre immédiatement tout problème éventuel. Les utilisateurs de Google Apps Édition Premier sont informés de tout risque potentiel dès que possible par e-mail.

Sécurité des données
La mission première des équipes de sécurité est la sécurité des données appartenant aux entreprises ou aux utilisateurs. L'un des principes sur lequel repose toute l'activité de Google est la confiance, confiance qui constitue la clé de voûte du succès de Google en tant qu'entreprise. Tous ses collaborateurs sont nourris du principe même de responsabilité envers l'utilisateur final. La protection des données est au cœur de la mission de Google, dont la sécurisation des milliards de dollars échangés lors des transactions publicitaires et des transactions d'achat d'une part et la protection des technologies de communication et de collaboration d'autre part constituent les deux enjeux majeurs.

Pour plus d'informations sur ces principes fondateurs de notre entreprise, consultez notre code de conduite à la page **http://investor.google.com/conduct.html**.

Sécurité physique

Google gère l'un des plus vastes réseaux de centres de données distribués au monde et prend toutes les mesures nécessaires à la protection des données et des contenus relevant de la propriété intellectuelle de ces centres. Situés partout dans le monde, certains centres sont la seule propriété de Google, qui en assure entièrement la gestion de façon qu'aucune tierce partie ne puisse y avoir accès. Leurs emplacements géographiques ont été choisis de manière à se prémunir contre les catastrophes naturelles. Seuls quelques collaborateurs triés sur le volet bénéficient d'un accès hautement contrôlé et audité aux installations et aux serveurs qui y sont hébergés. La gestion de la sécurité est assurée depuis chaque site localement et de façon centralisée à partir des centres de sécurité de Google.

Les installations locales sont conçues non seulement en vue d'une efficacité maximale mais aussi afin d'assurer la meilleure sécurité et fiabilité possible. De nombreux niveaux de redondance permettent d'assurer la poursuite des opérations et des services même dans les circonstances les plus difficiles et les plus extrêmes. Ceci inclut des niveaux multiples de redondance à l'intérieur d'un même centre, des sauvegardes d'opérations effectuées par des générateurs et des systèmes assurant une complète redondance entre différents sites. Des moyens de contrôle à la pointe de la technologie sont utilisés pour gérer les centres localement et à distance et des systèmes de basculement automatique ont été prévus pour protéger les systèmes.

Sécurité logique

Dans un environnement informatique basé sur le Web, la sécurité logique des données et des applications est un élément aussi crucial que la sécurité physique. Google met en place tous les moyens possibles pour que ses applications soient parfaitement sûres, que les données soient gérées de façon sécurisée et responsable et que tout accès extérieur et non autorisé à des données appartenant à une entreprise ou à un client soit impossible. Dans ce but, Google fait appel à un certain nombre de techniques standard dans l'industrie ainsi qu'à certains concepts tout à fait uniques et novateurs, comme le recours à des technologies spécialisées plutôt qu'à des technologies généralistes.

L'essentiel de la technologie proposée par Google a été conçu pour offrir des fonctionnalités spécialisées. Par exemple, la couche du serveur Web est spécialement conçue et mise en œuvre pour mettre à disposition de l'utilisateur les seules fonctionnalités nécessaires au bon fonctionnement d'une application spécifique. Elle est donc moins vulnérable aux attaques de tous bords que la plupart des logiciels commerciaux.

Toujours en vue d'améliorer la sécurité de ses produits, Google a modifié les bibliothèques principales. L'infrastructure Google consistant en un système d'applications dédiées plutôt qu'en une plate-forme généraliste, certains services offerts par le système d'exploitation Linux peuvent être limités ou désactivés. Ces modifications visent à améliorer les capacités système nécessaires à une certaine tâche et à désactiver ou à supprimer toutes les parties du système qui ne sont pas indispensables.

Les serveurs Google sont également protégés par plusieurs niveaux de pare-feu. Le trafic est surveillé de façon à détecter des attaques éventuelles et toute tentative est rapidement détournée.

Accès aux informations

Les données relatives à la messagerie électronique ne sont pas enregistrées dans un système de fichiers ou de base de données traditionnel mais stockées dans un format destiné à en optimiser les performances. Elles sont réparties sur un certain nombre de volumes logiques et physiques, ce qui en garantit la redondance et permet des accès à la demande. Les intrusions éventuelles sont ainsi découragées. Les systèmes de protection physique décrits plus haut garantissent que tout accès physique aux serveurs est impossible. L'accès aux systèmes de production est réservé aux collaborateurs qui utilisent le protocole crypté SSH (shell sécurisé). Une connaissance approfondie de la structure des données et de l'infrastructure propriétaire de Google est nécessaire pour avoir accès aux données des utilisateurs finaux. Cette couche de sécurité est un élément parmi d'autres grâce auquel Google Apps assure la protection des données sensible.

L'architecture distribuée de Google est conçue pour offrir un niveau de sécurité et de fiabilité bien supérieur à une architecture traditionnelle monobloc. Les données sont réparties sur plusieurs serveurs, clusters et centres de données. Ainsi, elles sont en parfaite sécurité et tout risque de perte potentielle est éliminé.

Seules les informations d'identification permettent l'accès aux données utilisateur. De cette façon, il est impossible à un client d'avoir accès aux données d'un autre client s'il ne connaît pas les informations de connexion de ce dernier. Ce système, dont l'efficacité a été prouvée, est utilisé par des dizaines de millions d'internautes faisant un usage quotidien de leur messagerie électronique, de leur agenda et de plusieurs documents, mais également par Google qui en a fait sa principale plate-forme, fréquentée par ses quelque 10 000 collaborateurs.

Redondance

L'architecture de réseau et d'applications utilisée par Google est conçue pour une fiabilité optimale. La plate-forme informatique en grille de Google assure une réaction rapide à des pannes de matériel fréquentes grâce à un système de basculement des logiciels très performant. Tous les systèmes Google sont intrinsèquement redondants de par leur conception. Chaque sous-système est également conçu pour ne pas dépendre d'un serveur logique ou physique unique pour son fonctionnement.

Les données sont répliquées plusieurs fois sur les serveurs actifs organisés en cluster, si bien que si un incident se produit sur un serveur, les données sont toujours accessibles par l'intermédiaire d'un autre système. De plus, les données utilisateur sont répliquées dans différents centres de données. Ainsi, dans le cas d'une panne ou d'un accident à grande échelle affectant l'intégralité d'un centre de données, un second centre de données serait en mesure de prendre la relève et de fournir aux utilisateurs les services qu'ils attendent.

Protection contre les menaces

Les virus transmis dans les e-mails, les attaques de phishing et les spams sont les menaces les plus fréquentes auxquelles les entreprises doivent faire face. Des rapports montrent que plus des deux tiers des e-mails sont des spams et que de nouveaux virus sont diffusés sur Internet chaque jour par les messageries électroniques. Parer à ces attaques peut sembler une tâche insurmontable et même les entreprises dotées d'un système de filtrage contre les spams et les virus déploient des efforts permanents pour ne pas se laisser dépasser. De plus, les applications en réseau sont la cible d'attaques malveillantes visant à les infiltrer ou à nuire à leur bon fonctionnement. Le système de protection à toute épreuve proposé par Google met les utilisateurs à l'abri des attaques visant les données et dissimulées dans le contenu de leurs messages et de leurs fichiers.

Protection contre les virus et les spams

Le filtre mis à disposition des clients de Google Apps contre les spams et le phishing est l'un des plus puissants sur le marché actuel. Google a développé des filtres haute technologie capables d'apprendre à reconnaître les spams à leur structure. Ces filtres sont mis à l'épreuve en permanence dans des milliards d'e-mails. Google peut donc identifier efficacement les spams, les attaques de phishing et les virus, et ainsi s'assurer que la boîte de réception, l'agenda et les documents des utilisateurs sont correctement protégés.

Le système antivirus de l'interface Web de Google permet de se protéger contre les tentatives malveillantes de propagation d'un virus dans une entreprise ou sur un réseau interne. À l'inverse de ce qui se produit pour les applications de messagerie clientes traditionnelles, les messages ne sont pas téléchargés vers votre bureau. La détection des virus éventuels s'effectue au niveau du serveur et Gmail n'autorise pas l'utilisateur à ouvrir une pièce jointe tant que celle-ci n'a pas été analysée et que toute menace n'a pas été écartée. Par conséquent, les virus propagés par e-mail ne peuvent pas exploiter la vulnérabilité du côté client et les utilisateurs ne peuvent pas ouvrir à leur insu un document contenant un virus.

Attaques contre les applications et les réseaux

Outre le filtrage du contenu des données pour la détection de spam et de virus, Google applique une stratégie permanente d'auto-protection et de protection de ses clients contre les attaques malveillantes. Les pirates informatiques tentent par tous les moyens de pénétrer dans les applications accessibles sur Internet ou de nuire à leur bon fonctionnement. Refus de service, usurpation d'adresse IP, failles XSS, corruption de paquets sont autant d'exemples d'attaques lancées quotidiennement contre les réseaux. Google, l'un des plus importants fournisseurs

de services Web au niveau mondial, met en œuvre des moyens considérables dans la lutte contre les menaces en tous genres. Tous les logiciels sont analysés avec divers programmes antivirus commerciaux et propriétaires conçus pour les réseaux et les applications. L'équipe de sécurité Google travaille avec des collaborateurs externes afin de tester et d'améliorer son infrastructure de sécurité et sa position sur le marché de la sécurité des applications.

Accès sécurisé

Quel que soit le niveau de sécurité garanti par un centre de données, les données, une fois téléchargées vers un ordinateur local, deviennent vulnérables. Des études ont démontré que l'ordinateur portable moyen contient plus de 10 000 fichiers et des milliers de messages téléchargés. Imaginez qu'un tel ordinateur portable d'entreprise tombe entre les mains d'un utilisateur malveillant. Cet utilisateur non autorisé pourrait très simplement avoir accès aux secrets industriels et au contenu relevant de la propriété intellectuelle de votre entreprise. Google Apps, en évitant le stockage en local des données sur un ordinateur portable, permet de minimiser ce risque.

Protection de l'utilisateur final

La conception Web de Google Apps permet aux utilisateurs d'accéder à leurs données où qu'ils soient, tandis que ces dernières sont stockées sur les serveurs sécurisés de Google. Plutôt que de stocker leurs e-mails sur un ordinateur de bureau ou un ordinateur portable, les utilisateurs disposent d'une interface hautement interactive et de grande qualité pour le courrier électronique, l'agenda et la messagerie instantanée tout en continuant à utiliser un navigateur Web.

De même, des applications comme Google Documents permettent aux utilisateurs de contrôler parfaitement les informations auxquelles ils ont accès. Les documents demeurent sur le serveur mais les utilisateurs bénéficient de fonctionnalités d'édition très étendues par l'intermédiaire du navigateur Web. Les utilisateurs peuvent également contrôler plus étroitement l'octroi des droits d'accès à ces documents et définir une liste d'utilisateurs habilités à les modifier ou à les lire. Ces droits s'appliquent automatiquement à tous les accès au document, ce qui permet d'éviter les problèmes de transfert d'e-mails à l'extérieur de l'entreprise. Enfin, les produits Google offrent une fonctionnalité de suivi des modifications à un niveau de granularité très fine, permettant ainsi de déterminer quel utilisateur a fait quel changement et à quel moment.

Google Apps protège également les données pendant leur transmission pour veiller à ce que les utilisateurs puissent y avoir accès en toute sécurité sans crainte que des données confidentielles soient interceptées sur le réseau. L'accès à la console administrative Web de Google Apps et à la plupart des applications destinées à l'utilisateur final est possible grâce à une connexion SSL (Secure Socket Layer). Google offre un accès HTTPS à la plupart des services de Google Apps. Il est possible de personnaliser cette fonctionnalité de façon à ne proposer l'accès HTTPS que pour quelques services clés tels que la messagerie électronique et l'agenda. Ainsi, tous les accès aux données et toutes les interactions sont cryptés.

À aucun moment Google ne stocke des mots de passe ou des données client sur le système de l'utilisateur. Les cookies servent à conserver les informations relatives aux sessions et apportent plus de confort à l'utilisateur, mais ils ne peuvent pas contenir d'informations sensibles ni être utilisés pour essayer d'accéder à un compte utilisateur.

À vous de décider

Outre la protection des données des entreprises et des utilisateurs, Google offre aux entreprises la possibilité d'intégrer les méthodologies en matière de sécurité, d'accès, d'audits et d'authentification dans Google Apps. Une API d'identification unique SAML 2.0 permet aux utilisateurs d'accéder à Google Apps par l'intermédiaire des mécanismes d'authentification déjà existants dans leur entreprise. Un utilisateur peut par exemple se connecter par l'intermédiaire d'Active Directory mais ses informations de connexion ne sont pas transmises par les serveurs Google lors de l'accès aux outils Web. Les entreprises sont ainsi encouragées à renforcer leurs règles en matière de niveau de sécurité et de fréquence de changement des mots de passe.

De plus, Google propose une console d'administration et une API destinées à la gestion des utilisateurs. Les administrateurs ont à tout moment la possibilité de désactiver l'accès à un compte ou de supprimer ce compte. Cette possibilité de donner ou de retirer l'accès à un utilisateur à travers une API peut également être intégrée à vos procédures internes.

Google permet aussi d'installer un pare-feu sur le système de messagerie afin de protéger la messagerie électronique et la messagerie instantanée. Tous les mails entrants et sortants sont alors interceptés par ce pare-feu et il est possible d'auditer et d'archiver les e-mails et de mettre en place des contrôles supplémentaires.

Confidentialité des données

Google prend très à cœur la confidentialité des données professionnelles et personnelles et sait que les données hébergées par les applications sont sensibles et confidentielles. Avec Google Apps, aucune information n'est en danger. Vous pouvez consulter les règles de confidentialité légales destinées à protéger tous les services à la page **http://www.google.com/privacypolicy.html**. Conformément à ces règles et à celles de chacun des services présents dans Google Apps, à aucun moment les collaborateurs de Google ne peuvent avoir accès aux données confidentielles des utilisateurs. Google garantit que ces règles ne peuvent être modifiées de façon à porter préjudice aux clients et/ou aux utilisateurs sans leur consentement exprès et par écrit.

Conclusion

Google Apps constitue une plate-forme sûre et fiable pour vos données. Elle fait appel aux technologies les plus récentes et aux meilleures pratiques en matière de gestion de centres de données, de sécurité des applications en réseau et d'intégrité des données. Lorsque vous confiez vos données à Google, vous pouvez le faire en toute confiance et en sachant que Google va s'investir au niveau technologique comme financier pour assurer les infrastructures nécessaires à la sécurité, la confidentialité et l'intégrité de vos données.

Pour plus d'informations sur Google Apps, accédez au site suivant : **http://www.google.com/a** ou envoyez un e-mail à **apps-enterprise@google.com.**