Livre blanc sécurité :

Google Apps, une offre de messagerie et de collaboration sécurisée

Google

Livre blanc sécurité : Google Apps, une offre de messagerie et de collaboration sécurisée

Table des matières

Pour plus d'informations sur Google Apps, consultez le site **www.google.com/a**

Introduction

Devant la multiplication des offres de services hébergés par des tiers ces dernières années, les entreprises accordent de plus en plus d'attention à la sécurité des services en ligne. L'émergence de différents concepts et définitions du cloud computing (informatique en nuage) a non seulement mis en exergue des questions liées à la propriété et à la protection des données, mais a également levé le voile sur la manière dont différents fournisseurs de technologies cloud computing élaborent et mettent en place leurs services. Tous les acteurs, experts en sécurité, utilisateurs finals et entreprises, réfléchissent aux implications du modèle cloud computing pour la sécurité.

Google Apps (comprenant Gmail, Google Agenda, Google Documents et d'autres applications Web) propose des produits et services conviviaux destinés aux entreprises. Ces services, caractérisés par des environnements informatiques redondants et une allocation dynamique des ressources, permettent aux clients d'accéder virtuellement à leurs données, à tout moment et n'importe où, à partir de périphériques Internet. Cet environnement informatique, souvent appelé « cloud » (nuage), permet à de nombreux clients de partager et d'utiliser les ressources d'unité centrale, de mémoire et de stockage, et leur offre en outre des avantages en termes de sécurité.

Google fournit des services sur le cloud fiables grâce à l'expérience tirée de la gestion de ses propres activités, et propose de la même façon des services essentiels, tels que la Recherche Google. Les contrôles de sécurité, qui isolent les données lors du traitement dans le cloud, ont, dès le début, été développés parallèlement à la technologie principale. La sécurité est, par conséquent, un composant clé de chacun des éléments de cloud computing, tels que la compartimentation, l'attribution des serveurs, le stockage des données et le traitement.

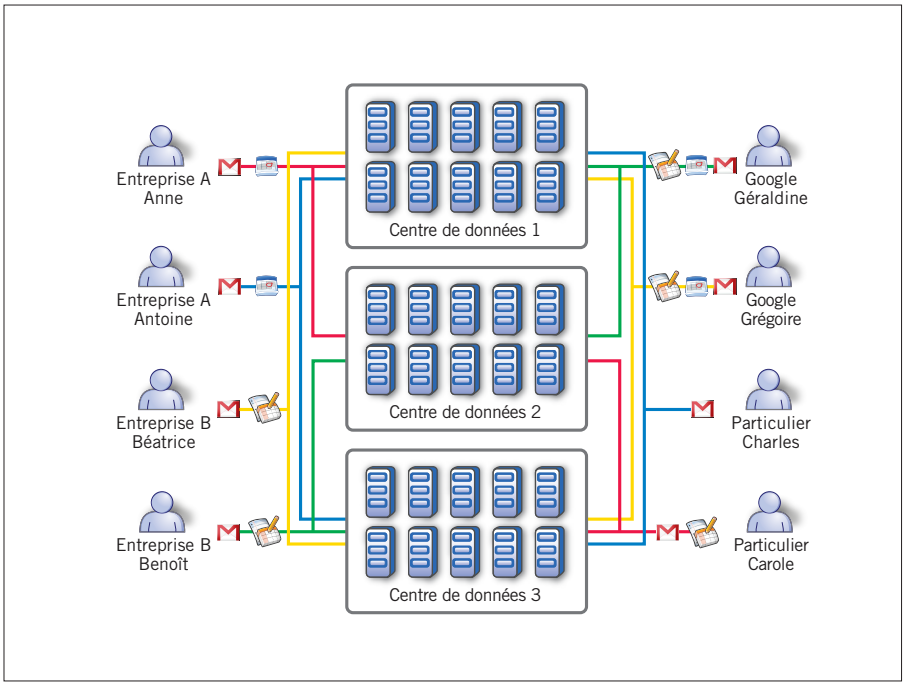

Figure 1 : Environnement distribué multiblocs de Google

Ce livre blanc explique comment Google crée une plate-forme basée sur la sécurité pour proposer ses produits Google Apps, en abordant des sujets tels que la sécurité des informations, la sécurité physique et la sécurité opérationnelle. Cet exposé a pour objet de démontrer que la sécurité fait partie intégrante du cloud computing de Google et représente un élément clé de ses processus de conception et de développement. Les règles décrites dans ce livre blanc sont celles qui étaient en vigueur au moment de sa rédaction. Certaines caractéristiques peuvent changer au fil du temps, dans la mesure où nous intégrons régulièrement de nouveaux produits et fonctionnalités dans Google Apps.

Présentation

La vision de la sécurité de Google s'articule autour d'une stratégie multicouches, proposant des contrôles à différents niveaux du traitement des données (stockage, accès et transferts). Cette stratégie comprend les dix éléments suivants :

- Politique générale de sécurité de Google
- Sécurité organisationnelle
- Classification et contrôle des actifs
- Sécurité par le personnel
- Sécurité physique et environnementale
- Sécurité opérationnelle
- Contrôle des accès
- Développement et maintenance des systèmes
- Reprise sur sinistre et plan de continuité de l'activité
- Conformité réglementaire

Politique générale de sécurité de Google

Google s'engage à garantir la sécurité de toutes les informations stockées sur ses systèmes informatiques. Cet engagement est exposé dans le Code de conduite de Google, consultable sur le site Web de Google à l'adresse **http://investor.google.com/corporate/code-of-conduct.html**. Les grandes lignes de la philosophie de sécurité de Google sont également présentées sur la page suivante : **http://www.google.com/intl/fr/corporate/security.html**.

L'ensemble des règles de sécurité couvrant la sécurité physique et la sécurité des comptes, des données, des services de l'entreprise, des systèmes réseau et informatiques, des services d'applications, de la gestion des modifications, du système de réponse après incident et des centres de données constitue le fondement de l'engagement de Google en matière de sécurité. Ces règles sont régulièrement révisées afin de garantir leur efficacité et leur adéquation.

Tous les employés de Google doivent se conformer à ces règles de sécurité. Ils se voient en outre remettre un livret sur la sécurité, qui décrit les aspects les plus importants des règles de sécurité des informations, tels que l'utilisation sans risques d'Internet, le télétravail sécurisé et la manière de libeller et de traiter les données sensibles. D'autres consignes sont régulièrement fournies sur des sujets utiles, notamment dans le domaine des technologies émergentes, telles que l'utilisation en toute sécurité de périphériques mobiles et de logiciels de partage entre homologues (P2P). Les directives de ces documents sont présentées sous une forme simple, conformément au principe fondamental de Google selon lequel les règles écrites ne sont efficaces que si leurs informations sont assimilées.

Sécurité organisationnelle

Sécurité des informations

Google emploie à plein temps une équipe chargée de la sécurité des informations. Intégrée dans l'organisation Génie logiciel et opérations de Google, elle est composée d'experts mondiaux parmi les plus reconnus en matière de sécurité des informations, des applications et des réseaux. Cette équipe s'occupe de la maintenance des systèmes de défense du périmètre de l'entreprise, de la mise au point de processus d'examen de la sécurité et de l'élaboration d'une infrastructure de sécurité personnalisée. Elle joue également un rôle essentiel dans le développement, la documentation et l'implémentation des règles et normes de sécurité de Google.

Le personnel chargé de la sécurité des informations de Google exécute les activités spécifiques suivantes :

- Révision des plans de sécurité des réseaux, systèmes et services Google à l'aide d'un processus rigoureux à plusieurs phases
- Examen de la sécurité au niveau conception et implémentation
- Services de conseil en continu sur les risques de sécurité associés à un projet donné et proposition de solutions aux enjeux de sécurité
- Surveillance des réseaux Google à la recherche d'activités suspectes, et application de processus formels de réponse sur incident afin d'identifier, d'analyser et d'écarter rapidement les menaces visant la sécurité des informations

- Mise en conformité avec les règles définies par le biais d'évaluations de la sécurité et d'audits internes réguliers
- Élaboration de cours sur la conformité avec les règles de sécurité Google et formation des employés, notamment dans les domaines de la sécurité des données et de la programmation sécurisée
- Recrutement d'experts en sécurité extérieurs afin d'évaluer régulièrement la sécurité de l'infrastructure et des applications
- Exécution d'un programme de gestion des vulnérabilités pour mettre au jour les problèmes propres aux réseaux, tout en s'assurant que les problèmes connus devant être résolus le sont dans les délais impartis

L'équipe de sécurité des informations travaille également officiellement avec la communauté de sécurité externe à Google :

- Publication de nouvelles techniques de sécurisation de la programmation, dans le souci de rester au fait des dernières tendances et préoccupations liées à la sécurité
- Collaboration avec des éditeurs de logiciels et des professionnels de la maintenance afin d'identifier et de résoudre les vulnérabilités des logiciels libres et fermés tiers
- Élaboration de normes internationales sur la confidentialité
- Mise à la disposition du public de documents de formation sur les problèmes de sécurité des informations, tels que la sécurité des navigateurs (**http://code.google.com/p/browsersec/wiki/Main**)
- Organisation et participation à des projets libres tels que skipfish, un outil actif de reconnaissance de la sécurité des applications Web entièrement automatisé (**http://code.google.com/p/skipfish**)
- Création d'un cursus de formation dans les meilleures universités
- Organisation et participation à des conférences universitaires

Une liste des publications relatives à la sécurité et à la confidentialité rédigées par les employés de Google est disponible à l'adresse **http://research.google.com/pubs/SecurityCryptographyandPrivacy.html**.

Audit interne global et conformité globale
En plus de l'équipe à plein temps en charge de la sécurité des informations, Google conserve également plusieurs fonctions axées sur la conformité légale et réglementaire à l'échelle mondiale. Google dispose d'un poste Conformité globale assurant la conformité légale et réglementaire, ainsi que d'une fonction Audit interne global en charge de la revue et de l'adhérence d'audit aux exigences de conformité formulées, telles que la loi Sarbanes-Oxley et les normes PCI (Payment Card Industry).

Sécurité physique
Google gère une équipe internationale, installée aux États-Unis, qui se consacre à la sécurité physique des locaux de Google et de son centre de données. Nos responsables de la sécurité, hautement qualifiés, suivent des formations dans la protection d'environnements similaires de type infrastructure sous haute sécurité.

Classification et contrôle des actifs

Accès aux informations
Google dispose de pratiques et de contrôles complets pour assurer la sécurité des informations des clients.

Les applications Google fonctionnent dans un environnement distribué mutualisé. Au lieu d'isoler les données de chaque client sur une machine ou sur un ensemble de machines, les données Google Apps de tous les clients Google (particuliers, entreprises et même les propres données de Google) sont réparties sur une infrastructure partagée composée de nombreuses machines homogènes Google et situées dans les différents centres de données de Google.

Google Apps utilise un système de fichiers distribué destiné à stocker d'importantes quantités de données sur un grand nombre d'ordinateurs. Les données structurées sont alors stockées dans une grande base de données distribuée, au sommet du système de fichiers. Les données sont morcelées et répliquées sur plusieurs systèmes de sorte qu'aucun système ne représente un point de défaillance unique. Des noms de fichiers aléatoires sont attribués aux paquets de données, ceux-ci n'étant pas enregistrés en texte clair de manière à n'être pas lisibles par l'homme. Pour plus d'informations, veuillez télécharger le résumé à l'adresse http://labs.google.com/papers/gfs.html.

Les couches de l'application Google et la pile de stockage requièrent que les demandes provenant d'autres composants soient authentifiées et autorisées. L'authentification entre services s'appuie sur un protocole de sécurité reposant sur un système Google qui permet de répartir les canaux authentifiés entre les services d'application. La confiance entre les instances de ce courtier d'authentification provient des certificats d'hôte x509 émis vers chaque hôte de production Google par une autorité de certification interne à Google.

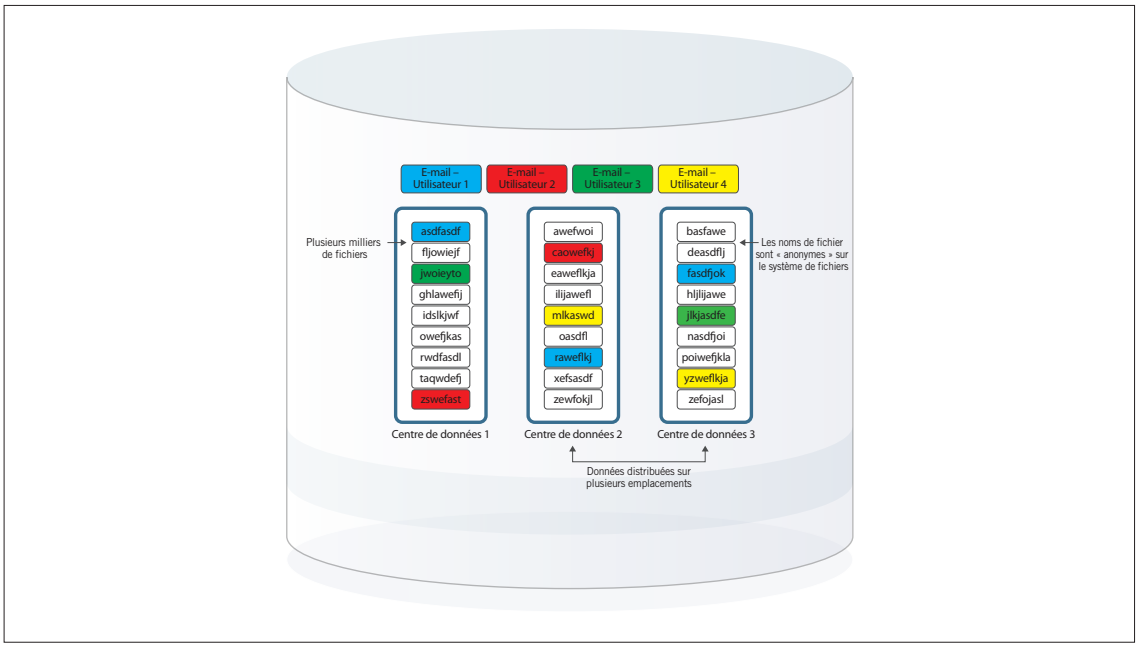

Figure 2 : Architecture du système de fichiers Google (GFS)

Par exemple, un service frontal Gmail effectue un appel de procédure à distance vers un service principal Gmail pour demander un message d'une boîte de réception d'un utilisateur particulier. Le service principal Gmail authentifie et traite cette demande uniquement si le demandeur est effectivement un service exécuté sous une identité autorisée à accéder aux services principaux de Gmail. Le service principal Gmail s'authentifie à son tour pour accéder aux fichiers du système de fichiers distribué de Google et, s'il y parvient, n'obtient l'accès qu'en fonction des listes de contrôle d'accès (ACL).

L'accès des ingénieurs en charge de l'administration des applications de production aux environnements de production est régi de manière similaire. Un système centralisé de gestion des groupes et des rôles permet de définir et de contrôler l'accès des ingénieurs aux services de production, à l'aide d'une extension du protocole de sécurité mentionné ci-dessus, qui authentifie les ingénieurs via l'utilisation d'un certificat x509 personnel émis à leur intention.

La règle requiert que l'accès administratif à l'environnement de production à des fins de débogage et de maintenance s'appuie sur des connexions authentifiées de clé publique SSH (shell sécurisé). Dans les deux cas de figure, l'appartenance à un groupe octroyant l'accès aux services ou aux comptes de production est définie à la demande.

Les contrôles de sécurité décrits précédemment reposent sur l'intégrité de la plate-forme de production Google. Cette plate-forme est elle-même fondée sur :

- des protections de sécurité physique de l'environnement de centre de données de Google ;
- l'intégrité de l'environnement du système d'exploitation de production Google ;
- un accès au niveau administrateur système (racine) limité et à la demande aux hôtes de production, accordé à un groupe spécialisé d'employés dont l'accès est surveillé.

Ces aspects des pratiques de sécurité de Google sont expliqués plus en détail dans les sections suivantes du présent document.

Données supprimées

Après la suppression d'un message, d'un compte, d'un utilisateur ou d'un domaine par un utilisateur ou un administrateur Google Apps et la confirmation de cette suppression (par exemple, vidage de la corbeille), les données en question ne sont plus accessibles depuis l'interface Google Apps de l'utilisateur.

Les données sont ensuite supprimées des serveurs actifs et des serveurs de réplication de Google. Les pointeurs vers les données sur les serveurs actifs et de réplication de Google sont supprimés. Les données sans référence seront remplacées par d'autres données des clients au fil du temps.

Mise au rebut des supports

Une fois qu'ils sont retirés des systèmes Google, les disques contenant les informations des clients suivent un processus de destruction des données avant de quitter les locaux de Google. La règle exige, dans un premier temps, que le disque soit effacé par des personnes habilitées. L'opération consiste en une écriture complète du lecteur avec des zéros (0x00), suivie d'une lecture complète pour s'assurer que l'unité est vierge.

Puis, une autre personne habilitée doit procéder à une deuxième inspection afin de confirmer que le disque a bien été effacé. Ces résultats sont consignés par numéro de série du lecteur pour le suivi.

Enfin, le disque effacé est enregistré dans l'inventaire pour être réutilisé et redéployé. Si le lecteur ne peut pas être effacé en raison d'un incident matériel, il doit être stocké de manière sécurisée jusqu'à sa destruction. Un audit est pratiqué toutes les semaines sur chaque site afin de veiller au bon respect des règles d'effacement des disques.

Sécurité par le personnel

Les employés Google doivent adopter une conduite en accord avec la politique de l'entreprise en ce qui concerne la confidentialité, la déontologie, l'utilisation appropriée et l'adhésion aux normes professionnelles.

À l'embauche, Google se renseigne sur la formation et les fonctions précédemment occupées par une personne, et procède à des contrôles de référence internes et externes. Lorsque le droit du travail ou les réglementations légales l'autorisent, Google peut également effectuer des contrôles en matière de condamnation, de solvabilité, d'immigration et de sécurité. L'étendue de ces contrôles dépend du poste visé.

Une fois embauchés par Google, tous les employés doivent signer un accord de confidentialité, accuser réception des règles du guide de l'employé de Google et accepter de s'y conformer. L'accent est mis sur la confidentialité des informations et données des clients dans le guide et au cours de l'orientation de la nouvelle recrue.

Les employés reçoivent une formation sur la sécurité dans le cadre de leur embauche. En outre, chaque employé Google se doit de lire et comprendre le code de conduite de l'entreprise et de suivre une formation à ce sujet. Le code met en évidence le fait que Google attend de ses employés qu'ils exercent leur activité en toute légalité, selon la déontologie et en toute intégrité, dans le respect mutuel des utilisateurs, des partenaires et même des concurrents. Le code de conduite de Google est consultable par tous à l'adresse **http://investor.google.com/corporate/code-of-conduct.html**.

Selon la fonction occupée par un employé, d'autres plans de formation et règles de sécurité peuvent s'appliquer. Les employés Google en charge de la gestion des données des clients doivent satisfaire aux exigences requises par ces règles. La formation sur les données des clients insiste sur l'utilisation appropriée des données conjointement aux processus métier, ainsi que sur les conséquences de toute violation.

Chaque employé Google a l'obligation de communiquer d'éventuels problèmes de sécurité et de confidentialité au personnel de la sécurité Google désigné. L'entreprise propose des mécanismes de signalement confidentiels pour permettre aux employés de signaler en tout anonymat une violation de la confidentialité dont ils ont pu être témoins.

Sécurité physique et environnementale

Contrôles de sécurité

Les centres de données Google sont répartis géographiquement et mettent en œuvre différentes mesures de sécurité physique. Les mécanismes technologiques et sécuritaires utilisés dans ces différents sites peuvent varier en fonction des conditions locales, telles que l'emplacement des bâtiments et les risques régionaux. Les contrôles standard de sécurité physique mis en œuvre dans chaque centre de données Google utilisent des technologies connues et suivent les meilleures pratiques du secteur : systèmes personnalisés de contrôle d'accès par carte électronique, systèmes d'alarme, caméras intérieures et extérieures et vigiles. L'accès aux zones où sont installés ou stockés des systèmes ou des composants de ces systèmes est différencié de celui des parties publiques, telles que les halls. La surveillance des caméras et des alarmes installées dans chacune de ces zones est centralisée pour permettre de détecter toute activité suspecte. En outre, les locaux sont régulièrement inspectés par des vigiles à bicyclette, sur Segways ou mini véhicule électrique (T3 motion).

Les locaux Google sont équipés de caméras haute résolution avec analyse vidéo et d'autres systèmes permettant de détecter et de traquer les intrus. Les enregistrements d'activité et les images sont conservés pour un examen ultérieur, le cas échéant. D'autres dispositifs de sécurité, tels que les caméras thermiques, les clôtures de périmètre et la biométrie peuvent être utilisés, si nécessaire.

L'accès à toutes les installations du centre de données est limité aux employés Google autorisés, aux visiteurs approuvés et aux tierces parties agréées dont la tâche est de gérer le centre de données. Google administre

une règle d'accès visiteur et un ensemble de procédures mentionnant que les responsables de centres de données doivent approuver les visiteurs à l'avance afin que ceux-ci pénètrent dans les zones internes spécifiques souhaitées. La règle concernant les visiteurs s'applique également aux employés Google qui n'ont habituellement pas accès aux locaux du centre de données. Google pratique un audit trimestriel des personnes ayant accès à ces centres de données afin de s'assurer que seul le personnel habilité accède à chacun des niveaux.

Google limite l'accès à ses centres de données selon la fonction et non la hiérarchie. Par conséquent, même les cadres haut placés de Google n'ont pas accès à ses centres de données.

Contrôles environnementaux

Les clusters informatiques de Google sont conçus dans le sens de la résilience et de la redondance, afin de permettre de minimiser les points individuels de défaillance et de réduire l'impact des incidents courants de matériel et les risques pour l'environnement. Doubles circuits, commutateurs, réseaux et autres dispositifs requis sont utilisés pour garantir la redondance. L'infrastructure des locaux des centres de données a été conçue pour être robuste, tolérante aux pannes et faire preuve d'une maintenabilité concurrente.

Alimentation électrique Pour un fonctionnement en continu, 24 h/24 et 7 j/7, les systèmes électriques des centres de données Google incluent des systèmes redondants. Une source d'alimentation principale et auxiliaire, de capacité égale, est disponible pour chaque composant critique du centre de données. Lors de la première défaillance de la source d'alimentation principale, due à une baisse de tension, une extinction, une surtension, une sous-tension ou à une condition de fréquence hors tolérances, un onduleur est prévu pour fournir de l'énergie jusqu'à ce que les générateurs de secours prennent le relais. Les générateurs de secours diesel sont en mesure de fournir une alimentation électrique suffisante pour faire fonctionner le centre de données à pleine capacité pendant un certain temps.

Climat et température Le refroidissement par circulation d'air est requis pour maintenir une température de service constante pour les serveurs et autre matériel informatique. Le refroidissement empêche la surchauffe et réduit les risques d'interruption de service. Les climatiseurs de la salle informatique sont alimentés par des systèmes électriques normaux et de secours.

Détection et lutte contre l'incendie Des équipements automatiques de détection et de lutte contre l'incendie permettent d'éviter l'endommagement du matériel informatique. Les systèmes de détection d'incendie utilisent des capteurs de chaleur, de fumée et d'eau placés dans les plafonds du centre de données et sous le faux-plancher. En cas d'incendie ou en présence de fumée, le système de détection se déclenche et émet des alarmes audibles et visibles dans la zone concernée, au niveau de la console des opérations de sécurité et du bureau de surveillance à distance. Des extincteurs manuels sont également répartis dans les centres de données. Les techniciens des centres de données reçoivent une formation sur la prévention d'incendie et l'extinction de feux naissants, à l'aide notamment d'extincteurs.

Plus d'informations

Des informations complémentaires et une visite guidée vidéo des centres de données Google sont disponibles sur la page **http://www.google.com/corporate/green/datacenters/summit.html**.

Sécurité opérationnelle

Prévention contre les logiciels malveillants

Les logiciels malveillants représentent un vrai danger pour les environnements informatiques d'aujourd'hui. Une offensive efficace d'un logiciel malveillant peut compromettre l'intégrité d'un compte, entraîner le vol de données et, éventuellement, conduire à un accès non autorisé à un réseau. Google prend très au sérieux ces menaces à l'encontre de ses réseaux et de ses clients et applique un certain nombre de méthodes pour prévenir, détecter et éradiquer les logiciels malveillants.

La stratégie consiste dans un premier temps à prévenir l'infection à l'aide d'analyseurs manuels et automatisés afin de passer au peigne fin l'index de recherche de Google et vérifier la présence de sites Web susceptibles de contenir logiciels malveillants ou risques de phishing. Des informations complémentaires à propos de ce procédé sont disponibles sur la page **http://googlewebmastercentral.blogspot.com/2008/10/malware-we-dont-need-no-stinking.html**. Les listes noires résultant de ces procédures d'analyse ont été intégrées dans différents navigateurs Web et dans la barre d'outils Google afin de renforcer la protection des internautes contre les sites suspects. Ces outils, accessibles au public, sont également utilisés par les employés Google.

En outre, Google a recours à plusieurs antivirus dans Gmail, sur les serveurs et les postes de travail afin de capturer les logiciels malveillants ayant échappé aux signatures antivirus. Le personnel d'assistance est formé pour identifier et éradiquer les logiciels malveillants risquant d'infecter le réseau Google, et transmet les cas inhabituels à l'équipe en charge de résoudre les incidents.

Surveillance

Le programme de surveillance de la sécurité de Google s'intéresse aux informations recueillies sur le trafic réseau interne, les actions des employés sur les systèmes et aux connaissances extérieures en matière de vulnérabilités.

En de nombreux points de notre réseau global, une inspection du trafic interne est pratiquée afin de détecter tout comportement suspect, tel que la présence de trafic indiquant des connexions à un réseau de zombies. Cette analyse est effectuée à l'aide d'une combinaison d'outils Open Source et commerciaux destinés à la capture et à l'analyse du trafic. Un système de corrélation propriétaire s'appuyant sur le meilleur de la technologie Google prend également en charge cette analyse. L'analyse du réseau est complétée par l'examen des journaux système afin d'identifier tout comportement inhabituel, tel que l'activité non prévue dans les comptes d'anciens employés ou les tentatives d'accès aux données des clients.

Les techniciens de la sécurité Google placent des alertes de recherche sur les référentiels de données publics en quête d'incidents liés à la sécurité susceptibles de nuire à l'infrastructure de l'entreprise. Ils passent activement en revue les rapports de sécurité entrants et surveillent les listes de diffusion publiques, les messages des blogs et les systèmes de forum électronique. L'analyse automatisée du réseau, transmise au personnel de sécurité Google, permet de déterminer à quel moment une menace inconnue risque de se présenter. L'analyse réseau est complétée par l'analyse automatisée des journaux système.

Gestion des vulnérabilités

Google emploie une équipe à temps plein chargée de veiller à ce que les vulnérabilités soient gérées le plus rapidement possible. L'équipe de sécurité Google effectue des analyses à la recherche de menaces pour la sécurité à l'aide d'outils commerciaux, d'actions intensives automatisées et manuelles contre l'intrusion, de processus d'assurance qualité, de revues de sécurité logicielle et d'audits externes. L'équipe de gestion des vulnérabilités est responsable du suivi de ces dernières.

Lorsqu'une faille avérée nécessitant un dépannage a été identifiée par l'équipe de sécurité, elle est consignée, priorisée en fonction de sa gravité et attribuée à un propriétaire. L'équipe de gestion des vulnérabilités assure le suivi de ces cas jusqu'à leur résolution.

Google gère également des relations et des interfaces avec les membres de la communauté de recherche sur la sécurité pour assurer le suivi de cas signalés dans les services Google et les outils Open Source. Pour en savoir plus sur le signalement des problèmes de sécurité, consultez la page **http://www.google.com/intl/fr/corporate/security.html.**

Gestion des incidents

Google dispose d'un processus de gestion des incidents s'appliquant aux événements de sécurité susceptibles de nuire à la confidentialité, à l'intégrité et à la disponibilité de ses systèmes ou de ses données. Ce processus précise le déroulement des actions, les procédures de notification, d'escalade, d'atténuation et de documentation. Le programme de gestion des incidents de sécurité Google s'articule autour des recommandations NIST sur la gestion des incidents (NIST SP 800-61).

Le personnel clé est formé en investigation numérique et en gestion des justificatifs en préparation d'un événement, y compris l'utilisation d'outils tiers et propriétaires. Les tests des plans de résolution des incidents sont pratiqués pour des zones clés, telles que les systèmes stockant des informations client sensibles. Ces tests tiennent compte d'une variété de scénarios, notamment les menaces internes et les failles de sécurité des logiciels.

Pour une résolution rapide des incidents de sécurité, l'équipe Google est disponible pour tous les employés 24 h/24 et 7 j/7. En cas d'incident concernant la sécurité des informations, l'équipe Google répond en consignant et en priorisant l'incident selon sa gravité. Les événements ayant une répercussion directe sur les clients sont traités avec la plus grande priorité. Une personne ou une équipe se consacre à la résolution du problème et se procure, le cas échéant, l'aide des spécialistes du produit ou des experts en la matière. Les autres responsabilités sont différées jusqu'à la résolution du problème.

Les ingénieurs de la sécurité Google effectuent des investigations rétrospectives, si nécessaire, afin de déterminer la cause d'événements isolés, les tendances communes à plusieurs événements, et d'élaborer de nouvelles stratégies pour empêcher la récurrence d'incidents similaires.

Sécurité du réseau

Google utilise plusieurs niveaux de défense pour protéger le périmètre réseau contre des attaques externes. Seuls les services et protocoles autorisés répondant aux exigences de sécurité de Google sont habilités à balayer le réseau de l'entreprise. Les paquets non autorisés sont automatiquement écartés.

La stratégie de la sécurité réseau de Google comprend les éléments suivants :

- Contrôle de la dimension et de la création du périmètre réseau ; application de la ségrégation des réseaux à l'aide de pare-feu normalisés et de la technologie ACL
- Gestion systématique des règles de pare-feu réseau et ACL utilisant la gestion des changements, le contrôle par les pairs et les tests automatisés
- Restriction de l'accès aux dispositifs en réseau au personnel autorisé
- Acheminement de tout le trafic via des serveurs frontaux personnalisés qui permettent de détecter et d'arrêter les requêtes malveillantes
- Création de points d'agrégation internes afin d'améliorer la surveillance
- Examen des fichiers journaux afin d'exploiter les erreurs de programmation (par exemple, les failles XSS) et génération d'alertes de haute priorité si un événement est détecté

Sécurité du système d'exploitation
Conçus en interne du début à la fin, les serveurs de production de Google sont basés sur une version dépouillée et durcie de Linux qui a été personnalisée pour inclure les composants nécessaires à l'exécution d'applications Google, telles que les services requis pour administrer le système et traiter le trafic utilisateur. Le système est conçu pour que Google soit en mesure de conserver le contrôle de l'ensemble de la pile matérielle et logicielle et pour garantir la sécurité de l'environnement d'application.

Les serveurs de production de Google sont basés sur un système d'exploitation durci standard, et les correctifs de sécurité sont déployés de manière uniforme sur l'ensemble de l'infrastructure de l'entreprise. La maintenance de cet environnement homogène est assurée par des logiciels propriétaires qui surveillent en permanence les systèmes en quête de modifications binaires. Si une modification détectée est différente de l'image Google standard, le système revient automatiquement à son état officiel. Ces mécanismes d'autorétablissement sont conçus pour permettre à Google de surveiller et de résoudre des événements déstabilisants, de recevoir des notifications sur les incidents et de ralentir les méfaits potentiels sur le réseau.

À l'aide d'un système efficace de gestion des modifications permettant la fourniture d'un mécanisme centralisé pour l'enregistrement, l'approbation et le suivi des modifications concernant tous les systèmes, Google réduit les risques de modifications non autorisées apportées au système d'exploitation Google standard.

Contrôle des accès

Contrôles d'authentification
Google requiert l'utilisation d'un identifiant utilisateur unique pour chaque employé. Ce compte permet d'identifier l'activité de chaque personne sur le réseau Google, y compris l'accès aux données des employés ou des clients. Ce compte unique est utilisé pour chaque système de Google. Après son embauche, un employé se voit attribuer un identifiant utilisateur par les ressources humaines et dispose d'un ensemble de droits par défaut décrits ci-après. Lorsque l'emploi d'une personne prend fin, la règle exige la désactivation de l'accès du compte au réseau Google depuis le système des ressources humaines.

Lorsque des mots de passe servent à l'authentification (par exemple, pour la connexion à des postes de travail), les systèmes appliquent les règles rigoureuses de mot de passe de Google, notamment la date d'expiration du mot de passe, les restrictions relatives à la réutilisation d'un mot de passe et un niveau de sécurité du mot de passe suffisant.

Google utilise très largement des mécanismes d'authentification à deux facteurs, tels que les certificats et les générateurs de mots de passe à usage unique.

Contrôles d'autorisation
Les droits et les niveaux d'accès sont basés sur la fonction et le rôle occupés par l'employé. Un droit d'accès minimal et l'accès à des informations potentiellement utiles à l'utilisateur sont également pris en compte.

Les employés Google ne disposent que d'un ensemble limité d'autorisations par défaut pour accéder aux ressources de l'entreprise, telles que la messagerie électronique, le portail interne de Google et les informations RH. Les demandes d'accès complémentaire suivent un processus formel impliquant une requête et une approbation de la part d'un propriétaire de données ou de système, d'un gestionnaire ou d'autres responsables, conformément aux règles de sécurité énoncées par Google. Les approbations sont gérées par les outils de flux de travail qui conservent les enregistrements d'audit de toutes les modifications. Ces outils contrôlent à la fois les modifications des paramètres d'autorisations et le processus d'approbation afin de garantir l'application cohérente des systèmes d'acceptation.

Les paramètres d'autorisation d'un employé permettent de contrôler l'accès à toutes les ressources, y compris les données et les systèmes des produits Google Apps.

Comptabilité

La règle de Google consiste à enregistrer l'accès administratif à chaque système de production Google et à toutes les données. Ces fichiers journaux sont consultables par l'équipe de sécurité Google selon les besoins.

Développement et maintenance des systèmes

La stratégie de Google se doit d'envisager les propriétés et les implications de sécurité des applications, des systèmes et des services utilisés ou fournis par Google tout au long du cycle de vie d'un projet.

La règle de sécurité des applications, systèmes et services de Google prévoit que les équipes et les personnes mettent en œuvre les mesures de sécurité appropriées dans les applications, les systèmes et les services en cours de développement, en fonction des risques et préoccupations de sécurité identifiés. La règle mentionne que Google dispose d'une équipe de sécurité dont la mission est de fournir des lignes directrices de sécurité et d'assurer l'évaluation des risques.

Google met en œuvre un certain nombre de mesures visant à garantir que les produits logiciels et services qu'il propose aux utilisateurs sont conformes aux normes les plus strictes sur la sécurité logicielle. Cette section décrit l'approche actuelle de Google en matière de sécurité logicielle ; celle-ci peut s'adapter et évoluer avec le temps.

Consultation et revue de sécurité

S'agissant de la conception, du développement et du fonctionnement des applications et services, l'équipe de sécurité Google propose les catégories principales de services de consultation suivantes aux équipes techniques et de production Google :

- Revues de sécurité au niveau de la conception : évaluations au niveau de la conception des risques de sécurité d'un projet et mesures d'atténuation correspondantes, tout en considérant leur caractère approprié et leur efficacité.
- Revues de sécurité au niveau de l'implémentation : évaluation au niveau de l'implémentation des artefacts de code pour mesurer leur fiabilité par rapport aux menaces de sécurité applicables.
- Consultation de sécurité : consultation en continu des risques de sécurité associés à un projet donné et solutions éventuelles aux problèmes de sécurité, souvent sous forme d'exploration de l'espace de conception dans les phases initiales des cycles de vie des projets.

Google reconnaît qu'une multitude de types de problèmes de sécurité interviennent au niveau de la conception du produit. C'est pourquoi ils doivent être pris en considération et résolus lors de la phase de conception du produit ou du service. La finalité essentielle de la revue de sécurité au niveau conception est de garantir la prise en compte de ces considérations. Dans ce cadre, la revue de sécurité au niveau de la conception se fixe les objectifs suivants :

- Fournir une évaluation de haut-niveau des risques de sécurité associés au projet, sur la base d'une recherche des menaces réelles
- Procurer aux décideurs du projet les informations nécessaires afin qu'ils puissent faire des choix éclairés en matière de gestion des risques et intégrer les considérations de sécurité dans les objectifs d'un projet
- Fournir des lignes directrices quant au choix et à la mise en œuvre correcte de contrôles de sécurité planifiés (par exemple, protocoles d'authentification ou cryptage)
- S'assurer que l'équipe de développement dispose de la formation adéquate eu égard aux classes de vulnérabilités applicables, aux schémas d'attaque et aux stratégies d'atténuation appropriées

Lorsque des projets impliquent des fonctionnalités ou des technologies innovantes, l'équipe de sécurité est chargée de rechercher et d'explorer les menaces, les schémas d'attaque potentiels et les classes de vulnérabilités spécifiques des technologies et fonctionnalités en question.

Le cas échéant, Google sous-traite à des entreprises tierces de consultation de sécurité pour compléter les compétences de l'équipe de sécurité et obtenir une revue indépendante afin de valider les revues de sécurité internes.

Sécurité dans le contexte du cycle de vie des logiciels Google

La sécurité est au cœur de notre processus de conception et de développement. L'organisation technique de Google ne requiert pas que les équipes de développement de produits suivent un processus de développement logiciel particulier ; au contraire, les équipes choisissent et mettent en œuvre des processus adaptés aux besoins du projet. Dans ce cadre, un certain nombre de processus de développement logiciel sont utilisés chez Google, allant des méthodologies de développement Agile Software à des processus plus classiques, par étapes.

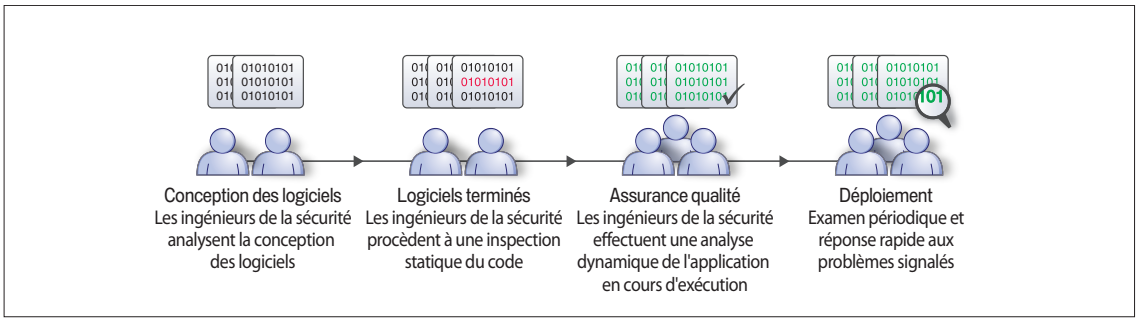

Figure 3 : Stratégie de développement et de maintenance systèmes de Google

Les processus de revue de la sécurité de Google sont prévus pour fonctionner dans la structure choisie. Leur réussite dépend de la culture technique en matière de qualité de Google et de quelques exigences définies par la direction technique des processus de développement de projet :

- Documentation de conception revue par les pairs
- Conformité aux lignes directrices de style de codage
- Revue de code par les pairs
- Tests de sécurité multicouches

Les mandats ci-dessus représentent la culture d'ingénierie logicielle de Google, dans laquelle les objectifs clés sont la qualité, la fiabilité et la maintenabilité des logiciels. Tandis que la finalité première de ces mandats est d'encourager la création d'artefacts logiciels irréprochables en matière de qualité logicielle, l'équipe de sécurité Google suggère également qu'ils représentent des « moteurs » significatifs et évolutifs en faveur de la réduction de l'incidence de failles de sécurité dans la conception logicielle :

- L'existence d'une documentation de conception suffisamment détaillée constitue une condition préalable du processus de revue de sécurité au niveau de la conception, dans la mesure où lors des premières phases du projet, c'est en général le seul artefact disponible pour élaborer les évaluations de sécurité.
- Bon nombre de classes de failles de sécurité au niveau implémentation s'apparentent finalement à des défauts fonctionnels courants, à faible risque. La plupart des failles au niveau implémentation sont le résultat d'omissions très simples de la part du développeur.
- Avec des développeurs et des réviseurs de code formés aux schémas de vulnérabilité en vigueur et aux méthodes permettant de les éviter, une culture du développement basée sur la revue par les pairs, insistant sur la création d'un code de haute qualité est un moteur important et évolutif vers une base de code sécurisée.

Les ingénieurs logiciels de l'équipe de sécurité Google collaborent avec d'autres ingénieurs Google sur le développement et la validation de composants réutilisables conçus et implémentés pour permettre aux projets logiciels d'éviter certaines classes de vulnérabilités. Parmi les exemples figurent les couches d'accès aux données conçues pour résister aux failles d'injection de langage de requête, ou les structures de modèles HTML avec défenses intégrées contre les vulnérabilités XSS (comme le mécanisme d'**échappement automatique** de la bibliothèque libre **Google CTemplate**).

Formation à la sécurité

Reconnaissant l'importance d'une main-d'œuvre technique formée aux pratiques de codage sécurisé, l'équipe de sécurité Google met en place une campagne de communication et un programme de formation à l'intention des ingénieurs, dont le contenu actuel est le suivant :

- Formation des nouveaux ingénieurs à la sécurité
- Création et gestion d'une documentation complète sur les pratiques sécurisées de codage et de conception
- Références ciblées et contextuelles à la documentation et aux supports de la formation (par exemple, des outils automatisés de test des vulnérabilités fournissent aux ingénieurs des références à la documentation de formation et de fond en rapport avec les bugs ou classes de bugs spécifiques mis en évidence par l'outil)
- Présentations techniques sur les rubriques relatives à la sécurité
- Newsletter sur la sécurité distribuée à l'ensemble des ingénieurs et destinée à informer la main-d'œuvre technique Google des menaces, schémas d'attaque, techniques d'atténuation, bibliothèques liées à la sécurité, meilleures pratiques et lignes directrices, etc. recensés récemment

- Le sommet de la sécurité, conférence récurrente à l'échelle de Google, qui réunit les ingénieurs des différentes équipes Google travaillant sur la sécurité et propose des présentations techniques détaillées sur les sujets de sécurité

Tests et revue de sécurité au niveau implémentation
Google applique un certain nombre d'approches pour continuer de réduire l'incidence de failles de la sécurité au niveau implémentation dans ses produits et services :

- Revues de sécurité au niveau implémentation : réalisées par les membres de l'équipe de sécurité Google, généralement lors des dernières phases du développement de produits, les revues de sécurité au niveau implémentation visent à valider la résistance d'un artefact logiciel aux menaces de sécurité applicables. Ces revues sont généralement constituées d'une réévaluation des menaces et contremesures identifiées lors de la revue de sécurité au niveau conception, de revues ciblées sur le code critique pour la sécurité, de revues de code sélectives permettant d'évaluer la qualité du code du point de vue de la sécurité, et de tests de sécurité ciblés.
- Tests automatisés des failles dans certaines classes de vulnérabilités pertinentes. Pour ces tests, nous utilisons aussi bien des outils développés en interne que des outils disponibles sur le marché.
- Tests de sécurité réalisés par des ingénieurs de la qualité logicielle dans le contexte des actions menées en matière de test et d'évaluation de la qualité logicielle globale du projet.

Reprise sur sinistre et plan de continuité de l'activité

Afin de réduire l'interruption de service due à une panne de matériel, à une catastrophe naturelle ou autre, Google met en œuvre un programme de reprise sur sinistre sur tous les sites de ses centres de données. Ce programme inclut plusieurs composants destinés à réduire le risque de point de défaillance unique, dont les suivants :

- Réplication et sauvegarde des données : pour garantir la disponibilité en cas de sinistre, les données Google Apps sont répliquées sur plusieurs systèmes au sein d'un même centre de données, mais aussi dans un centre de données secondaire.
- Google gère un ensemble de centres de données répartis géographiquement, conçu pour garantir la continuité de service en cas de sinistre ou autre incident se produisant dans une région particulière. Les connexions à grande vitesse entre les centres de données permettent un basculement rapide. La gestion des centres de données est également distribuée afin de fournir une couverture permanente indépendante du lieu et d'assurer l'administration système.

Outre la redondance des données et la dispersion régionale des centres de données, Google dispose également d'un plan de continuité de l'activité pour son siège à Mountain View en Californie. Ce plan tient compte des sinistres majeurs, tels qu'un séisme ou une crise sanitaire publique, et suppose que les personnes et les services peuvent être indisponibles pendant un maximum de 30 jours. Ce plan est conçu pour assurer la continuité des opérations des services destinés à nos clients. Notre plan de reprise sur sinistre fait l'objet de tests réguliers.

Conformité réglementaire

Processus d'accès aux informations légales
Google applique des processus légaux standard pour répondre aux requêtes d'informations utilisateur de la part de tiers. Des informations peuvent uniquement être obtenues par des parties tierces par le biais de processus légaux tels que les mandats de perquisition, les ordonnances du tribunal, les citations à comparaître, via l'exemption statutaire ou encore avec le consentement de l'utilisateur. À réception d'une demande de divulgation d'informations, l'équipe juridique Google examine la demande et vérifie sa conformité avec la loi en vigueur. Si la requête est légalement recevable, la règle de Google mentionne qu'il faut notifier l'utilisateur ou l'organisation dont les informations font l'objet d'une demande, sauf en cas d'urgence ou d'interdiction légale.

Confidentialité
Google applique une règle de confidentialité très stricte pour assurer la protection des données de ses clients. Cette règle est détaillée sur la page **http://www.google.com/a/help/intl/fr/users/privacy.html** et est valable dans le cadre de chaque application de Google Apps. Pour en savoir plus sur les règles et pratiques du centre de confidentialité Google, accédez à la page **http://www.google.com/privacy.html**.

En deux mots, Google n'est pas propriétaire des données de ses clients et nous pensons qu'il doit en demeurer ainsi.

Google adhère aux principes suivants concernant les données de ses clients :

- Google ne partagera pas les données avec d'autres, sauf indication contraire dans les **Règles de confidentialité** Google.
- Google propose aux clients des fonctionnalités leur permettant d'**emporter les données** s'ils souhaitent utiliser des services externes conjointement à Google Apps ou arrêter d'utiliser tous les services Google.

Le contenu des utilisateurs est analysé ou indexé uniquement dans les cas suivants, afin de fournir aux clients un service de haute qualité :

- Certaines données utilisateur, telles que les e-mails et les documents, sont analysées et indexées, de sorte que les utilisateurs au sein du domaine d'un client puissent les rechercher dans leurs propres comptes Google Apps.
- Les e-mails sont analysés pour que Google puisse procéder au filtrage anti-spam et à la détection de virus.
- Les e-mails sont analysés de sorte que Google puisse afficher en contexte les publicités pertinentes dans certaines circonstances.
- Excepté lorsque les utilisateurs choisissent de rendre des informations publiques, les données Google Apps ne font pas partie de l'index général google.com.

Les procédures d'analyse et d'indexation sont automatisées et n'impliquent pas d'interaction humaine. Google peut également supprimer tout contenu non conforme aux **Conditions d'utilisation** des produits Google Apps.

Safe Harbor

Google adhère aux principes de sphère de sécurité (Safe Harbor) des États-Unis relatifs aux avis, au choix, au transfert continu, à la sécurité, à l'intégrité des données, à l'accès et à l'application, et est inscrit au **programme Safe Harbor du Département du commerce américain**.

SAS 70

Google a obtenu une attestation de conformité à la norme SAS 70 Type II et s'efforcera d'obtenir des attestations similaires pour les produits de messagerie et de collaboration Google Apps, ainsi que pour ses produits de sécurité et de conformité, fournis par Postini. Un audit SAS 70 est une évaluation indépendante pratiquée par une société d'audit externe qui valide l'adhésion de l'entreprise concernée aux contrôles qu'elle s'est défini, et confirme que ceux-ci fonctionnent de manière efficace. Une fois qu'elle a terminé, la société d'audit produit un rapport détaillant la conformité de l'entreprise à ces contrôles.

Personnalisation des fonctionnalités de sécurité

Outre les différents contrôles de sécurité décrits précédemment que Google met en place pour assurer la sécurité et la confidentialité des données des clients, Google Apps fournit également d'autres options de sécurité pouvant être utilisées par les administrateurs de domaine d'un client. Nous nous efforçons de proposer davantage de choix aux clients dans la gestion des contrôles de sécurité de leur domaine.

Authentification unique (SSO)

Google Apps offre le service d'authentification unique (Single Sign-On, SSO) aux clients de Google Apps for Business, Google Apps for Education, Google Apps for Government et Google Apps for ISPs. Ces versions de Google Apps disposent d'une API d'authentification unique, basée sur le standard SAML, que les administrateurs peuvent intégrer dans un système LDAP ou d'autres systèmes d'authentification unique. Cette fonctionnalité permet aux administrateurs d'utiliser le mécanisme d'authentification de leur choix, tel que les certificats, les jetons matériels, la biométrie et autres.

Longueur et niveau de sécurité du mot de passe

Les administrateurs peuvent définir la longueur minimale des mots de passe des utilisateurs de leur domaine et contrôler leur complexité à l'aide d'indicateurs (pour identifier les mots de passe qui respectent les critères de longueur, mais ne sont pas suffisamment complexes).

Les indicateurs de niveau de sécurité d'un mot de passe peuvent évaluer en temps réel le niveau de sécurité d'un mot de passe, et permettent aux administrateurs de repérer les mots de passe susceptibles d'être moins sécurisés avec le temps en fonction de l'émergence de nouveaux schémas d'attaque.

Déconnexion unique au niveau de l'administrateur

Les administrateurs peuvent réinitialiser les cookies de connexion d'un utilisateur pour empêcher l'accès non autorisé à son compte. Cette opération déconnecte cet utilisateur de toutes les sessions actives de navigateur Web et nécessite une nouvelle authentification lors de la prochaine tentative d'accès de l'utilisateur à Google Apps.

Combinée à la capacité existante des administrateurs à réinitialiser les mots de passe utilisateur, cette fonctionnalité consistant à réinitialiser les cookies de connexion des utilisateurs améliore la sécurité du cloud en cas de vol ou de perte du périphérique.

Connexions de navigateur sécurisées (HTTPS)
Google Apps for Business, Google Apps for Education, Google Apps for Government et Google Apps for ISPs proposent aux administrateurs de domaine de forcer tous les utilisateurs de leur domaine à utiliser le protocole HTTPS (Hypertext Transfer Protocol Secure) pour les services tels que Gmail, Google Documents, Google Agenda, Google Sites, etc. Les informations envoyées via HTTPS sont cryptées à partir du moment où elles quittent Google et jusqu'à ce qu'elles soient reçues par l'ordinateur du destinataire.

Transfert de messages sécurisé contrôlé par des règles (TLS pour SMTP)
Avec la fonction TLS (Transfer Layer Security) contrôlée par des règles pour SMTP (Simple Mail Transfer Protocol), les administrateurs peuvent définir des règles conçues pour envoyer et recevoir des messages entre domaines spécifiques. Par exemple, un administrateur peut spécifier que tous les messages externes envoyés par les membres de l'équipe de comptabilité à leur banque doivent être sécurisés avec TLS ou différés si TLS n'est pas possible. De même, un administrateur peut mandater une connexion TLS sécurisée entre leur domaine et leur conseiller juridique externe, leurs auditeurs ou autres partenaires avec lesquels les employés peuvent avoir des communications sensibles.

Google Recherche d'archives
Google est conscient que les services d'archives peuvent aider les clients à respecter les différentes exigences de l'industrie. En mettant en œuvre Google Message Discovery, géré par Postini, les clients peuvent créer pour leur organisation un référentiel de messagerie centralisé et disponible à la recherche permettant d'explorer les archives pour localiser et exporter des e-mails. Le produit peut enregistrer et indexer tous les messages en fonction de règles de conservation définies par le client. Les clients peuvent identifier les messages pertinents et conserver, rechercher et exporter les données à partager, selon les besoins, avec des fournisseurs externes.

Conclusion

Google s'engage à conserver en toute sécurité les informations stockées sur ses systèmes informatiques. Chacun des dix composants de la stratégie de sécurité multicouches de Google est soutenu et défendu dans toute l'organisation. Google Apps propose des contrôles à chaque niveau du stockage, de l'accès et du transfert des données. Des millions d'organisations, y compris Google, travaillent avec Google Apps, et Google investit dans cette confiance jour après jour. Avec Google Apps, les utilisateurs peuvent être assurés que Google valorise la confidentialité, l'intégrité et la disponibilité de leurs données.

Google

WP64-1005