Resumen exhaustivo de protección de seguridad y vulnerabilidad para Google Apps

Informe de Google de febrero de 2007

Seguridad de Google Apps

MÁS INFORMACIÓN:

Online www.google.com/a
Correo electrónico apps-enterprise@google.com

Proteger las aplicaciones basadas en red contra posibles hackers es clave para garantizar el éxito de cualquier sistema, y en el caso del correo electrónico y las colaboraciones, la importancia es primordial. Google invierte miles de millones de dólares en tecnología, personal y procesos para garantizar que los datos de Google Apps estén a salvo, seguros y mantengan su privacidad. El equipo dedicado de profesionales de la seguridad de Google es responsable de la seguridad desde el inicio, de la revisión de todo el diseño, el código y el producto final para asegurar que cumple los estándares de seguridad y privacidad de Google. La misma infraestructura que se utiliza para alojar Google Apps y proteger cientos de miles de datos de usuarios se utiliza también para administrar millones de datos de usuarios y miles de millones de dólares en transacciones publicitarias. Con Google Apps, la información está segura y a salvo.

Introducción

Como parte de la misión de organizar la información proveniente de todo el mundo, Google es responsable de salvaguardar los datos de decenas de millones de usuarios. Nos tomamos muy en serio esta responsabilidad y Google ha hecho una gran labor para ganarse y mantener la confianza de sus usuarios. Google comprende que los productos seguros son necesarios para mantener la confianza del usuario y se esfuerza en crear productos innovadores que cumplan con las necesidades del usuario y que funcionen en su propio interés.

Google Apps se beneficia de este extenso conocimiento operacional para generar productos seguros y fiables. Para garantizar a nuestros clientes la protección de sus datos, los productos y servicios de Google combinan soluciones de tecnología avanzada con prácticas de seguridad pioneras en el sector. Invertimos miles de millones de dólares para garantizar el entorno más seguro y fiable para los datos y las aplicaciones. Google se centra especialmente en varios aspectos de seguridad que son cruciales para los clientes comerciales:

- Seguridad organizativa y operacional. Políticas y procedimientos para garantizar la seguridad en todas las fases del diseño, implantación y operaciones en curso.
- Protección de datos. Garantizamos la protección de los datos del cliente en instalaciones, servidores y aplicaciones seguras.
- Evitar amenazas. Protegemos a los usuarios y su información de ataques malintencionados y de posibles hackers.
- Acceso seguro. Garantizamos que solamente los usuarios autorizados puedan acceder a los datos y que el canal de acceso sea seguro.
- Privacidad de datos. Garantizamos que la información confidencial se mantenga privada y confidencial

Este documento muestra la estrategia de seguridad de Google, que consiste en tomar un gran número de medidas de seguridad física, lógica y operacional para garantizar la máxima protección y privacidad de datos.

Seguridad organizativa y operacional

La base de la estrategia de seguridad de Google está en las personas y en los procesos. La seguridad se consigue mediante una combinación de profesionales, procesos y tecnología que, si se combinan correctamente, conducen a una informática responsable y segura. La seguridad no es algo que se pueda simplemente validar y dar luego por hecho sino que se diseña desde un principio en los mismos productos, en la arquitectura, en la infraestructura y en los sistemas. Google cuenta con un equipo de seguridad a tiempo completo para desarrollar, documentar e implementar una exhaustiva política de seguridad. Este equipo está formado por algunos de los mayores expertos del mundo en protección de información, aplicaciones y redes.

El equipo de seguridad está dividido en áreas funcionales como defensa de perímetro, defensa de las infraestructuras, detección de vulnerabilidad y reacción. Muchos de los profesionales de Google cuentan con experiencia en puestos de responsabilidad en seguridad de la información en las empresas de la lista Fortune 500. Este equipo centra gran parte de sus esfuerzos en medidas preventivas para garantizar que el código y los sistemas estén protegidos desde un principio, pero también está preparado para reaccionar de forma dinámica ante cualquier problema de seguridad

.

Metodología de desarrollo
La seguridad de Google es primordial desde que se empieza con el primer borrador del diseño de un producto. Los equipos de ingeniería y producto de Google reciben un extenso entrenamiento en los conceptos básicos de seguridad. Asimismo, la metodología de desarrollo de Google está estructurada en varios pasos, con puntos de control y auditorías completas.

El equipo de seguridad de las aplicaciones de Google está presente en todas las fases del ciclo de vida del desarrollo del producto, incluida la revisión del diseño, la auditoría del código, las pruebas de sistema y funcionalidad y la aprobación final para el lanzamiento. Google utiliza un gran número de tecnologías patentadas y comerciales para garantizar la seguridad de las aplicaciones en todos los ámbitos. Asimismo, el equipo de seguridad de las aplicaciones de Google es el responsable de garantizar que se sigan procesos de desarrollo seguros para garantizar la protección del cliente.

Seguridad operacional
El equipo de operaciones de seguridad de Google se dedica a mantener la seguridad de los sistemas operacionales , incluida la gestión de datos y la administración de sistemas. Este grupo audita regularmente las operaciones de los centros de datos y lleva a cabo una evaluación constante de amenazas contra los recursos físicos y lógicos de Google.

Este grupo también es responsable de garantizar que todos los empleados sean seleccionados y formados como es debido para realizar su trabajo de forma segura y profesional. Google realiza una ardua labor para controlar y verificar el historial de un profesional antes de que se una a nuestra organización. Todo el personal encargado de mantener los procesos y procedimientos de seguridad ha recibido formación específica sobre las prácticas y no dejan de realizar cursos para mantenerse al día.

Asesorías y comunidad sobre seguridad
Además de los procesos descritos anteriormente, Google trabaja activamente con la comunidad de seguridad y aprovecha la sabiduría colectiva de los mejores y más brillantes especialistas del mundo. Gracias a ello, Google se mantiene a la cabeza en las tendencias de seguridad, puede reaccionar rápidamente ante las amenazas emergentes y se beneficia de la experiencia de los profesionales dentro y fuera de la empresa. Google se compromete activamente con esta extensa comunidad de la seguridad revelando información de forma responsable. Visita **http://www.google.com/corporate/security.html** para obtener más información sobre este programa y sobre algunos de los expertos clave con los cuales Google mantiene una comunicación continua.

Incluso con todos estos niveles de protección, pueden aparecer vulnerabilidades desconocidas, y Google está equipado para responder rápidamente a alertas de seguridad y este tipo de vulnerabilidades. El equipo de seguridad de Google audita toda la infraestructura ante vulnerabilidades potenciales y trabaja directamente con los ingenieros para corregir inmediatamente cualquier error que se detecte. Los clientes de Google Apps edición premier reciben notificaciones sobre las cuestiones de seguridad que afecten a los usuarios tan pronto como es posible por correo electrónico.

Protección de datos
La seguridad de los datos de usuario y de la empresa es el objetivo de los equipos de operaciones y seguridad de Google. La actividad de Google se basa en la confianza de los usuarios y, por lo tanto, es una de las claves del éxito continuado de Google como corporación. Todos los empleados de Google asimilan el valor de la responsabilidad hacia el usuario final. La protección de datos es el núcleo de lo que representa Google. En Google cuidamos mucho la protección de los miles de millones de transacciones publicitarias y comerciales, y aplicamos el mismo cuidado a nuestras tecnologías de comunicación y colaboración.

Podrás ver lo fundamental que es para nuestra identidad consultando nuestro código de conducta en **http://investor.google.com/conduct.html.**

Seguridad física
Google realiza operaciones en una de las mayores redes de centros de datos distribuidos por todo el mundo y realiza una ardua labor para proteger la información y la propiedad intelectual en estos centros. Google realiza operaciones en centros de datos de todo el mundo; muchos de ellos son propiedad absoluta de Google y se gestionan para garantizar que no haya acceso exterior de terceros. La localización geográfica de los centros de datos se ha seleccionado especialmente para evitar desastres naturales. Solamente algunos miembros de Google tienen acceso a estas instalaciones y a los servidores que contienen, acceso que está estrictamente vigilado y auditado. La seguridad se supervisa y controla tanto localmente en el sitio como centralmente en los centros de operaciones internacionales de seguridad de Google.

Las instalaciones se han diseñado no sólo para obtener una máxima eficiencia, sino también para ofrecer seguridad y fiabilidad. Los múltiples niveles de redundancia garantizan el funcionamiento y la disponibilidad de servicio incluso en las circunstancias más adversas y extremas. Cada centro incluye varios niveles de redundancia, copias de seguridad alimentadas por generadores para las operaciones continuas y redundancia plena en múltiples centros dispersos. Se utilizan sistemas de seguridad de última generación para supervisar los centros, tanto de forma local como a distancia, así como sistemas automatizados de recuperación tras fallos para proteger los equipos.

Seguridad lógica
En la informática basada en la web, la seguridad lógica de los datos y las aplicaciones es tan importante como la seguridad física. Google llega al límite para garantizar aplicaciones seguras, una gestión de datos segura y responsable y la inexistencia de accesos externos no autorizados a los datos de clientes o usuarios. Para alcanzar este objetivo, Google utiliza un gran número de técnicas estándar del sector y algunos enfoques únicos e innovadores. Uno de ellos es el de aprovechar la tecnología de propósito específico en lugar del software de propósito general.

La mayor parte de la tecnología de Google está destinada a ofrecer funciones de propósito específico en lugar de funciones de propósito general. Por ejemplo, el nivel de servidor web está especialmente diseñado e implementado por Google para exponer únicamente las funciones necesarias para realizar operaciones en aplicaciones específicas. Por lo tanto, no es tan vulnerable ante los ataques de todo tipo a los que la mayoría del software comercial es susceptible.

Google también ha realizado modificaciones en las bibliotecas básicas por razones de seguridad. La infraestructura de Google es un sistema de aplicaciones dedicado y no una plataforma informática de propósito general, por ello, parte de los servicios ofrecidos por el sistema operativo estándar Linux pueden quedar limitados o inhabilitados. Estas modificaciones se centran en aumentar las funciones del sistema necesarias para una tarea concreta y en inhabilitar o eliminar todos los aspectos del sistema no necesarios.

Los servidores de Google también están protegidos por múltiples niveles de cortafuegos para protegerlos contra los ataques. El tráfico se inspecciona minuciosamente para hacer frente a los intentos de ataque, y todos ellos se tratan con el fin de proteger los datos del usuario.

Accesibilidad a la información
Los datos como los mensajes de correo electrónico se guardan en un formato codificado optimizado para el rendimiento, en lugar de almacenarlos en un sistema de archivos o en una base de datos tradicional. Los datos se extienden por un gran número de volúmenes físicos y lógicos para la redundancia y conveniencia de acceso para evitar la manipulación. Las protecciones físicas de Google descritas anteriormente garantizan la imposibilidad de acceder físicamente a los servidores. Todos los accesos a los sistemas de producción están dirigidos por el personal y utilizan encriptado SSH (estructura de seguridad). Para conseguir un acceso significativo a los datos del usuario final sería necesario el conocimiento especializado de las estructuras de datos y la infraestructura patentada de Google . Éste es uno de los mucho niveles de protección para garantizar la seguridad de datos confidenciales de Google Apps.

La arquitectura distribuida por Google está diseñada para ofrecer un mayor nivel de seguridad y fiabilidad frente a la arquitectura tradicional. Los datos de los usuarios individuales se distribuyen en un gran número de servidores, clústeres y centros de datos anónimos. De esta forma se garantiza que la información esté segura frente a posibles pérdidas, e incluso más protegida.

Los datos de usuario son solamente accesibles mediante las credenciales pertinentes, lo cual garantiza que ningún cliente tiene acceso a los datos de otro cliente sin los datos de identificación. Este sistema probado da servicio a diario a decenas de millones de usuarios con correo electrónico, calendarios y documentos y, además, es una herramienta que Google utiliza como plataforma principal para dar servicio a sus más de 10.000 empleados.

Redundancia
La arquitectura de redes y aplicaciones de Google está diseñada para ofrecer la máxima fiabilidad y operatividad. La plataforma informática basada en cuadrículas de Google soluciona los constantes fallos de hardware, y el sólido software de recuperación tras fallos resiste a estas interrupciones. Todos los sistemas de Google poseen un diseño redundante y los subsistemas no dependen de ningún servidor físico o lógico concreto para su funcionamiento continuo.

Los datos se replican varias veces en los clústeres de servidores activos de Google y, por lo tanto, en caso de que un equipo falle, los datos seguirán siendo accesibles a través de otro sistema. Asimismo, los datos de los usuarios se replican en distintos centros de datos. Como resultado, si falla un centro de datos completo o se ve implicado en una catástrofe, se activará inmediatamente un segundo centro de datos para dar servicio a los usuarios.

Evitar amenazas
Los virus de correo electrónico, los ataques de suplantación de identidad (phishing) y el spam son las principales amenazas de hoy en día contra la seguridad de las empresas. Los informes demuestran que más de dos tercios del correo que se recibe es spam y cada día surgen nuevos virus de correo electrónico que se distribuyen a través de Internet. Mantener el control de esta situación puede ser una tarea abrumadora, e incluso las compañías con filtros contra spam y antivirus dedican muchos esfuerzos a mantenerlos actualizados para enfrentarse a las nuevas amenazas. Asimismo, las aplicaciones basadas en redes son el objetivo de ataques malintencionados que tratan de manipular datos o interrumpir el servicio. El sistema de evasión de amenazas de máxima categoría de Google protege a los usuarios de ataques a sus datos y el contenido de sus mensajes y archivos.

Protección contra virus y spam:
Los clientes de Google Apps se benefician de los filtros contra spam y phising más potentes del sector. Google ha desarrollado filtros de tecnología avanzada que obtienen información de los patrones que se incluyen en mensajes identificados como spam; estos filtros se guían continuamente gracias a miles de millones de mensajes de correo. En consecuencia, Google puede identificar spam, ataques de phishing y virus con mucha precisión y garantizar que las bandejas de entrada, los calendarios y los documentos de los usuarios estén protegidos.

A través de la interfaz web de Google, la protección de virus bloquea la amenaza de que los usuarios distribuyan inconscientemente un virus por la red interna de la compañía. A diferencia de las aplicaciones de correo electrónico tradicionales basadas en el cliente, los mensajes no se descargan al escritorio. Por el contrario, se escanean en el servidor para detectar la presencia de virus y Gmail no permite que el usuario abra un documento adjunto hasta que haya sido analizado y se haya mitigado la amenaza. Como resultado, los virus de correo electrónico no pueden aprovechar las vulnerabilidades de seguridad por parte del cliente y los usuarios no pueden abrir por error un documento que contenga virus.

Ataques contra aplicaciones y redes
Google filtra el contenido de los datos para evitar spam y virus, pero además se protege a sí mismo y a sus clientes de forma continua contra ataques malintencionados. Los hackers siempre buscan formas de introducirse o hacer caer las aplicaciones basadas en la web. Algunos de los ataques más comunes que sufren a diario las redes son la denegación de servicio, la suplantación de IP (spoofing), los comandos cruzados (XSS) y la manipulación de paquetes. Google, al ser uno de los principales proveedores del mundo

de servicios basados en la web, ha conseguido proteger sus activos frente a estas y otras amenazas. Se escanea todo el software utilizando una serie de soluciones propias y patentadas de escaneado de redes y aplicaciones. Asimismo, el equipo de seguridad de Google trabaja con empresas externas para probar y mejorar la posición de seguridad de las infraestructuras y aplicaciones de Google.

Acceso seguro
Por muy protegida que esté la información en el centro de datos, ésta es vulnerable una vez el usuario la ha descargado en su equipo local. Los estudios demuestran que los equipos portátiles tienen de media más de 10.000 archivos y miles de mensajes descargados. Imagina que uno de estos portátiles corporativos cae en manos de un usuario malintencionado. Con sólo montar un disco, este usuario no autorizado puede acceder a la propiedad intelectual e información confidencial de tu empresa. Con Google Apps las compañías podrán reducir este riesgo evitando el almacenamiento local de datos en los equipos portátiles de los usuarios.

Protección del usuario final
El diseño basado en la web de Google Apps garantiza que los usuarios tengan un acceso rápido a sus datos desde cualquier lugar a la vez que los datos se mantienen protegidos en los servidores de Google. En lugar de guardar los mensajes de correo electrónico en un equipo de sobremesa o en un portátil, los usuarios disponen de interfaces altamente interactivas para correo electrónico, calendarios, y mensajería instantánea mediante un navegador web.

De forma similar, las aplicaciones como Google Docs permiten a los usuarios un gran nivel de control sobre la información. Estos documentos permanecen en el servidor, pero los usuarios cuentan con un gran número de funciones de edición a través del navegador web. Además, pueden controlar minuciosamente quién tiene acceso a estos documentos y establecer una lista de editores y lectores. Estos permisos se aplican a cualquier acceso al documento y evitan que un documento interno se reenvíe fuera de la empresa por correo electrónico. Finalmente, estos productos registran las modificaciones de manera exhaustiva y ofrecen la opción de ver quién realizó los cambios y cuándo lo hizo.

Google Apps también protege la transmisión de datos por la red, de manera que los usuarios pueden estar seguros que los datos confidenciales no se intercepten. El acceso a la consola administrativa basada en la web de Google Apps y a la mayoría de aplicaciones de usuario final está protegido por una conexión de Secure Socket Layer (SSL). Google ofrece acceso HTTPS a la mayoría de servicios de Google Apps, y el producto se puede configurar para permitir solamente el acceso HTTPS a los servicios clave, como el correo electrónico o el calendario. Con esta funcionalidad, todos los accesos del usuario y todas las interacciones de datos estarán encriptados.

Google nunca utiliza cookies para almacenar contraseñas o datos del usuario en su equipo. Las cookies se utilizan para guardar la información de la sesión y a conveniencia del usuario, pero nunca se utilizan para guardar información confidencial que pueda utilizarse para entrar en la cuenta del usuario.

Te damos el control
Además de ofrecer estas protecciones para los datos de la compañía y el usuario, Google ofrece a las empresas el control para integrar en Google Apps la seguridad de la empresa, los accesos, auditorías, y metodologías de autentificación. Google Apps ofrece una única API de acceso basada en SAML 2.0 que permite a las compañías utilizar los mecanismos de autentificación ya existentes para que los usuarios accedan a Google Apps. Las empresas podrán, por ejemplo, utilizar la autentificación Active Directory para registrar a un usuario y las credenciales no se transmitirán por los servidores de Google para acceder a las herramientas basadas en la web. Esto permite a las empresas seguir reforzando la seguridad de las contraseñas y las políticas de frecuencia de cambio.

Asimismo, Google ofrece una consola de administración y una API para la administración de usuarios. El administrador tiene la capacidad de cancelar o eliminar inmediatamente el acceso a una cuenta bajo petición, lo cual también puede utilizarse en los procesos internos para otorgar y retirar autorizaciones a un usuario a través de la API.

En lo referente al correo electrónico y a la mensajería instantánea, Google también ofrece la posibilidad de utilizar una pasarela de correo previa al sistema de correo. En esta configuración, todo el correo entrante y saliente pasa por el sistema del cliente, y ofrece la posibilidad de auditar y archivar el correo, así como de configurar controles de supervisión.

Privacidad de datos

Google da mucha importancia a la privacidad del usuario y de la compañía, y es consciente de que los datos almacenados en las aplicaciones son confidenciales y privados. Google garantiza con Google Apps que la seguridad de la información no está en peligro. Puedes visitar la política de privacidad de Google legalmente vinculante que protege todos los servicios en **http://www.google.com/privacypolicy.html**. Según está política y otras relacionadas sobre los servicios individuales incluidos en Google Apps, los empleados de Google en ningún caso tendrán acceso a los datos confidenciales de los usuarios. Google también garantiza que esta política no será alterada de ninguna forma perniciosa sin el consentimiento expreso por escrito del cliente o usuario.

Conclusión

Google Apps ofrece una plataforma segura y fiable para tus datos, te ofrece las últimas tecnologías y las mejores prácticas para la administración de centros de datos, seguridad en las aplicaciones de redes e integridad de la información. Cuando confías los datos de tu empresa a Google puedes hacerlo con total seguridad, sabiendo que todo el peso de la inversión en tecnología e infraestructura de Google está dedicado a garantizar la seguridad, privacidad e integridad de tus datos.

Para obtener más información sobre Google Apps visita **http://www.google.com/a** o envía un mensaje a **apps-enterprise@google.com**.