McAfee
An Intel Company

PROTEGER LA INFORMACIÓN

Guía de solución

De acuerdo con el informe de McAfee "Data Loss by the Numbers" (La pérdida de información en cifras), de todos los tipos de datos generales, la información que habitualmente corre mayores riesgos incluye los nombres y las direcciones, los números de DNI o equivalentes y los de las tarjetas de crédito[1].

Security Connected

El marco Security Connected de McAfee permite integrar distintos productos, servicios y asociaciones para reducir los riegos de forma efectiva, eficiente y centralizada. Basado en más de dos décadas de prácticas de seguridad probadas, el enfoque Security Connected ayuda a las organizaciones de todos los tamaños y segmentos, de todas las zonas geográficas, a mejorar sus condiciones de seguridad, optimizar la seguridad para conseguir una mayor rentabilidad y alinear estratégicamente la seguridad con las iniciativas empresariales. La arquitectura de referencia Security Connected ofrece una ruta concreta desde las ideas hasta la implantación. Utilícela para adaptar los conceptos de Security Connected a sus riesgos, infraestructura y objetivos empresariales. En McAfee dedicamos todos nuestros esfuerzos a la búsqueda constante de nuevas soluciones y servicios que garanticen la total seguridad de nuestros clientes.

En la operación Shady RAT (Remote Administration Tool, herramienta de administración remota), McAfee accedió a un servidor de comandos y control malicioso que se había utilizado en múltiples ataques dirigidos. Más de 70 organizaciones fueron el objetivo de los ataques que utilizaban este sistema, y los operadores habían estado robando información durante al menos seis años. La filtración más larga de información confidencial de una sola organización duró 28 meses, y el promedio fue de casi nueve meses. En total robaron más de un petabyte de información[1].

Protección de los datos valiosos

Desafíos

No es ninguna sopresa que tanto los empleados maliciosos como los agresores externos deseen apoderarse de información confidencial como la propiedad intelectual, los registros financieros y los datos personales. La información es valiosa y, por tanto, es un objetivo. Además, corre peligro a causa de empleados negligentes y poco cuidadosos, y de otros usuarios de confianza con derechos de acceso elevados como los socios comerciales y los consultores. Dado que la información ayuda a hacer negocios, debe ser accesible y utilizable para que su valor no disminuya. Es esencial encontrar el equilibrio justo entre los permisos de acceso y la reducción de riesgos.

Las dificultades surgen cuando las organizaciones saben cuánta información confidencial tienen. Con independencia del volumen, en raras ocasiones la información se encuentra en un solo lugar: está extendida a lo largo de almacenes de datos estructurados como las bases de datos o no estructurados como los servidores de archivos, los ordenadores portátiles, los mensajes de correo electrónico, las unidades extraíbles (unidades USB) y otros. Normalmente pueden acceder a dicha información múltiples usuarios que pertenecen a grupos diferentes y se encuentran en distintas partes del mundo. En muchos casos, quienes necesitan acceder a ella pueden ser socios de negocio u otros grupos que la organización no controla.

La mayoría de las organizaciones es consciente de los resultados de la falta de protección adecuada de la información. Los problemas pueden ser la desventaja competitiva causada por el robo de propiedad intelectual, las multas de las autoridades reguladoras, o las demandas judiciales colectivas y los costes relacionados con las filtraciones. Aunque las consecuencias están claras, implantar una solución puede ser un desafío. Los problemas técnicos más habituales que las organizaciones sufren cuando intentan elaborar una estrategia de protección de la información eficaz incluyen:

- Descubrir dónde está la información.
- Clasificar la información.
- Imponer el cumplimiento de las directivas para proteger la forma en que se maneja la información.
- Supervisar en tiempo real el acceso a las redes y a los endpoints.
- Realizar el análisis forense de los datos relacionados con los usuarios que interactúan con la información.
- Gestionar las soluciones de cifrado distribuidas.
- Reducir los ataques a las bases de datos.

En el año 2006 robaron el ordenador portátil propiedad de un analista de datos. Contenía información personal y médica de aproximadamente 26,5 millones de militares activos y veteranos[2].

Afortunadamente, estos problemas técnicos no tienen por qué atormentar a las organizaciones. En la actualidad existen distintas soluciones integradas de protección de la información, desarrolladas con el objetivo de abordar los riesgos de la seguridad y facilitar la puesta en marcha de los controles para protegerla, sin poner obstáculos a los usuarios con complicados mecanismos de acceso a la información.

¿Qué tienen en común Britney Spears, George Clooney, Arnold Schwarzenegger, Maria Shriver y Farrah Fawcett? La información médica confidencial de todos ellos se robó a un prestador de servicios sanitarios y posteriormente se vendió a periódicos sensacionalistas.

Soluciones

Existen varias soluciones para proteger la información que ofrecen la ventaja añadida de reducir los costes y la complejidad. Algunas son controles de red o de endpoints, y otras son específicas para los datos o para la gestión general de la seguridad. Si bien muchas de estas soluciones pueden ser eficaces, especialmente cuando operan en un marco Security Connected, hay cuatro tecnologías que son clave: la prevención de pérdida de datos (DLP, Data Loss Prevention), los controles para proteger las unidades de almacenamiento extraíbles, el cifrado y la supervisión de la actividad de las bases de datos (DAM, Database Activity Monitoring).

Prevención de pérdida de datos

Las soluciones DLP deben descubrir y registrar la información confidencial con independencia del formato y, a intervalos regulares, informar a la solución DLP y a los controles relacionados de los cambios, por ejemplo, de sistemas de almacenamiento de datos nuevos. Una estrategia DLP eficaz combinará controles basados en la red y en el host para proteger a las organizaciones frente a la pérdida de datos tanto por negligencia como deliberadamente. Los ejemplos incluyen la carga de información, el envío fuera de la organización mediante la mensajería instantánea o el correo electrónico, e incluso la copia de la información en dispositivos extraíbles. Desde el punto de vista operativo, la solución DLP debe contar con una gestión centralizada que englobe tanto el descubrimiento, la creación de directivas, el análisis y la respuesta como otros controles como los gateways de Internet para imponer de forma más amplia el cumplimiento de las normativas.

Control de dispositivos y medios de almacenamiento extraíbles

Una de las formas más sencillas y habituales de filtrar información por negligencia o con malas intenciones es utilizar dispositivos extraíbles como unidades USB, reproductores MP3, DVDs, etc. Las soluciones de esta categoría deben imponer qué tipos de dispositivos pueden utilizarse, así como el tipo de información que puede transferirse mediante conexiones físicas o inalámbricas como Bluetooth e infrarrojas. Dado que los dispositivos USB son pequeños y cuentan con gran capacidad de almacenamiento, las funciones de cifrado son esenciales cuando la información está contenida en dispositivos móviles. Estas soluciones deben cifrar los datos de forma transparente y automática cuando la información aprobada se transfiere a una unidad USB autorizada. Para optimizar la gestión de la seguridad, las soluciones DLP y la administración de unidades USB deben estar centralizadas, dado que sus controles están estrechamente relacionados.

Cifrado

El cifrado reduce considerablemente la utilidad de los datos perdidos o robados. Además del cifrado de unidades USB, se pueden añadir capas de protección adicionales como el cifrado completo de los discos de Macs y PCs. Los archivos y las carpetas, incluidos los archivos de red, deben cifrarse, especialmente si puede hacerse de forma automática y transparente, dado que se comparten y mueven a través de toda la organización. Utilizando soluciones de cifrado gestionadas de forma centralizada con los controles de protección de la información señalados anteriormente, el despliegue, la administración y la creación de directivas pueden ser más eficientes y constantes en las distintas soluciones, y da como resultado un menor coste total de propiedad.

Supervisión de la actividad de las bases de datos

Descubrir todas las bases de datos de una organización puede ser tan difícil como encontrar la información confidencial. Las soluciones de supervisión de la actividad de las bases de datos deben ser capaces de identificarlas y de proveer protección específica, incluso en los sistemas donde no se hayan aplicado parches. Estas soluciones deberían sacar partido de la combinación de la aplicación virtual de parches, la protección frente a ataques específicos y conocidos, así como de la capacidad de terminar sesiones que violen las directivas de seguridad, como es el caso de los ataques de día cero. Estos controles deben funcionar tanto en las bases de datos físicas como en los entornos virtualizados y de servicios distribuidos en Internet. Al aprovechar el marco Security Connected de McAfee en todos los controles de protección de la información como DLP, la protección de los dispositivos extraíbles, el cifrado y DAM, la actividad de las bases de datos, es posible reducir los riesgos y los costes, y mejorar la rentabilidad de la inversión.

Consideraciones sobre las buenas prácticas

- Utilice una estrategia para enfrentarse tanto los ataques externos como a los empleados negligentes o con malas intenciones.
- Implante controles específicos para la protección de datos y refuércelos con controles de redes y endpoints de apoyo.
- Saque partido de las soluciones que permiten el análisis en tiempo real y forense.
- Apruebe directivas y controles para proteger la información que aborden el almacenamiento de datos críticos, los endpoints, los dispositivos extraíbles y los puntos de filtración habituales como el correo electrónico, la mensajería instantánea y la Web.
- Aproveche las ventajas del cifrado, especialmente en dispositivos como los ordenadores portátiles y las unidades USB, para reducir el riesgo de que la información confidencial de los dispositivos perdidos o robados pueda recuperarse.
- Proteja las bases de datos con controles optimizados para imponer el cumplimiento de las directivas en materia de datos estructurados.

Dados la complejidad, el tiempo, el dinero y los recursos que se necesitan para realizar pruebas exhaustivas de los parches de las bases de datos, en promedio solo se aplican a las de producción dos o tres veces al año.

Motivaciones de valor

Las soluciones adecuadas para proteger la información deben ofrecer valor operativo ayudando a las organizaciones a centrarse en evitar gastos, no en el sentido de prevención que tiene el término, si no en el de las estadísticas reales de pérdidas de datos. En este momento, el coste promedio de una fuga de datos es de 214 dólares por cada registro[3]. Las soluciones adecuadas para proteger la información deben:

- Ayudar a limitar los gastos legales, las multas y los costes por incumplimiento de las normativas en el caso de que se produzca una fuga de datos.
- Identificar rápidamente las vías de filtración de los datos en combinación con las directivas corporativas.
- Disminuir la necesidad de realizar las diligencias debidas y de pagar gastos legales preliminares en el caso de exista una citación judicial de terceros (si se manejan datos de terceras partes).

Material relacionado de la arquitectura de referencia Security Connected

Nivel II

- Protección de centros de datos
- Protección de la información frente a amenazas internas
- Control y supervisión de los cambios

Nivel III

- Protección de la propiedad intelectual
- Protección del correo electrónico
- Protección de soportes extraíbles
- Imponer el cumplimiento de las normativas a los endpoints

Si desea obtener más información sobre la arquitectura de referencia Security Connected, visite: www.mcafee.com/mx/enterprise/reference-architecture/index.aspx.

Acerca del autor

Brian Contos, CISSP (Certified Information Systems Security Professional), es Director de la estrategia global de seguridad de McAfee. Es un experto en seguridad reconocido, con casi 20 años de experiencia en ingeniería y gestión de la seguridad. Es autor de varios libros como *Enemy at the Water Cooler* (El enemigo en casa) y *Physical and Logical Security Convergence* (Convergencia de la seguridad física y lógica). Ha trabajado en organismos públicos y en empresas Forbes Global 2000 en todo el continente americano, Europa, Oriente Medio y Asia. Es ponente invitado en importantes eventos del sector como RSA, Interop, SANS, OWASP y SecTor. Además, escribe en publicaciones sectoriales y de negocios como *Forbes, New York Times* y *The Times* de Londres. Brian es miembro distinguido del Ponemon Institute y se licenció en la Universidad de Arizona.

brian_contos@mcafee.com || http://siblog.mcafee.com/author/brian-contos/ || @BrianContos

[1] http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf
[2] http://en.wikipedia.org/wiki/Laptop_theft
[3] http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

McAfee
An Intel Company

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com