Resumen de la solución

Cómo evitar las fugas de datos en su empresa

En la mayoría de las organizaciones se producen fugas de datos. A veces los responsables son personas que pertenecen a la empresa, pero en su mayor parte los autores de los robos son agentes externos, y para sacar la información de la empresa se emplean múltiples formas y diversos canales. Las organizaciones intentan detener este flujo, cada una por sus motivos y con mayor o menor éxito. Intel Security encargó el estudio *Intel Security 2016 Data Protection Benchmark Study* (Estudio comparativo de protección de datos, 2016) para saber quiénes son las personas que se ocultan detrás de estos robos, qué tipos de datos se roban y qué vías se emplean para su filtración.

En el *Informe de McAfee Labs sobre amenazas: septiembre de 2016*, analizamos los datos del estudio y explicamos nuestras conclusiones. Entre otras cosas, observamos lo siguiente:

- El intervalo entre una fuga de datos y su detección es cada vez mayor.
- Los proveedores de servicios sanitarios y los fabricantes son presas fáciles.
- El método habitual de prevención de pérdida de datos es cada vez más ineficaz contra los nuevos objetivos de robo.
- La mayoría de las empresas no vigila el segundo método más frecuente de fuga de datos.
- La prevención de pérdida de datos se implementa por las razones correctas.
- La visibilidad es crucial.

Políticas y procedimientos recomendables para una prevención de pérdida de datos eficaz

Para impedir la transferencia inadvertida o deliberada de datos confidenciales a personas no autorizadas, es fundamental que las organizaciones elaboren políticas y procedimientos de prevención de pérdida de datos. Las iniciativas de prevención de pérdida de datos que tienen éxito empiezan en la fase de planificación, en la que se definen las necesidades de la empresa. Es en esta fase, por ejemplo, cuando deben adaptarse las políticas de clasificación y fuga de datos a las políticas de privacidad e intercambio de datos de la organización. Si las necesidades de la empresa se establecen con claridad, es más fácil centrar la iniciativa de prevención de pérdida de datos y evitar que cambie constantemente de ámbito.

intel Security

Resumen de la solución

El siguiente paso importante de la iniciativa es identificar los datos confidenciales de la organización. Las tecnologías de análisis de servidores y endpoints permiten clasificar archivos en función de expresiones regulares, diccionarios y tipos de datos no estructurados. Los productos de prevención de pérdida de datos a menudo llevan incorporada la clasificación de categorías típicas de datos confidenciales, como datos de tarjetas de pago o información médica personal, que puede acelerar el proceso de detección. También es posible crear clasificaciones personalizadas para identificar tipos de datos exclusivos de la organización.

Esta fase se complica con las aplicaciones autorizadas y no autorizadas por el departamento de TI y sus correspondientes datos en la nube. Con los datos en la nube autorizados por TI, la identificación de los datos confidenciales puede y debe formar parte del proceso de suscripción al servicio en la nube. Cuando es el caso, clasificar este tipo de datos puede ser relativamente sencillo.

Sin embargo, es frecuente que los grupos funcionales de las organizaciones soslayen al departamento de TI para satisfacer sus objetivos empresariales y se suscriban a los servicios en la nube por su cuenta. Si TI no conoce estos servicios y los datos que hay detrás, la posibilidad de fuga de datos crece. Como consecuencia, durante esta fase es importante trabajar con los grupos funcionales para identificar las ubicaciones de los datos en la nube y utilizar el proceso anterior para clasificarlos.

Tras completar el proceso de descubrimiento de datos confidenciales, pueden implementarse productos de prevención de pérdida de datos en la red de confianza y en todos los endpoints para obtener visibilidad y control de los datos importantes en reposo y en movimiento. Deben implementarse políticas para detectar el movimiento o el acceso imprevisto a datos confidenciales. Hay eventos, como la transferencia de datos confidenciales a dispositivos USB o a través de la red a una ubicación externa, que pueden formar parte de un proceso empresarial normal o bien constituir una acción deliberada o inadvertida que provoque una fuga de datos.

La probabilidad de fugas de datos puede reducirse con una formación bien elaborada que sensibilice sobre la seguridad. Los usuarios pueden aprender las medidas apropiadas para transferir datos confidenciales mediante pantallas informativas, que les permitirían formarse en las políticas de protección de datos durante su jornada laboral normal. Por ejemplo, una pantalla de notificación informaría al usuario de que su transferencia de datos confidenciales infringe las normas y le presentaría alternativas, como tachar los datos confidenciales antes de intentar transferirlos otra vez.

Normalmente, los propietarios de los datos saben mejor cómo utilizarlos que otros grupos de la organización. Deberían ser ellos los encargados de clasificar los incidentes de pérdida de datos. Separar las funciones entre los propietarios de los datos y el equipo de seguridad reduce la posibilidad de que un solo equipo burle las políticas de protección de datos.

Tras establecer los movimientos de datos permitidos e incorporar las directivas que los rigen en los productos de prevención de pérdida de datos, pueden activarse las directivas que bloquean las transferencias no autorizadas de datos confidenciales. Una vez activado el bloqueo, los usuarios ya no pueden realizar acciones que infrinjan las directivas. Estas pueden matizarse con mayor o menor flexibilidad según las necesidades de la empresa para asegurar que los usuarios desempeñen sus tareas sin perder seguridad.

A medida que la iniciativa de prevención de pérdida de datos avance, es importante validar y reajustar las directivas a intervalos programados. A veces son demasiado restrictivas o laxas, y afectan a la productividad o suponen un riesgo para la seguridad.

Cómo puede ayudarle Intel Security a protegerse frente a la fuga de datos

McAfee DLP Discover

El primer paso para proteger los datos convenientemente es saber dónde reside la información y qué datos hay exactamente. McAfee DLP Discover protege contra la filtración de datos mediante la simplificación del primer paso gracias a estas funciones:

- Identificación de clasificaciones para la detección en el entorno de confianza, bien mediante el empleo de las clasificaciones incorporadas (por ejemplo, HIPAA, PCI, SOX) o bien mediante la creación de otras personalizadas.
- Análisis y revisión de inventario utilizando las clasificaciones identificadas, con el fin de descubrir qué tipos de datos residen en el entorno de confianza y dónde se encuentran. Revisión de las infracciones de las directivas existentes en la interfaz de McAfee DLP Discover.
- Análisis de reparación para localizar los datos almacenados en ubicaciones no autorizadas y traslado de dichos datos a una ubicación autorizada.
- Análisis de inventario y reparación en recursos locales, como los compartidos de red, o en recursos en la nube, como Box.
- Creación de nuevas directivas de protección de datos según lo que se haya descubierto en los análisis de McAfee DLP Discover.

McAfee DLP Endpoint

McAfee DLP Endpoint supervisa e impide la fuga de datos en la oficina, desde otro lugar y en la nube. Supervise rápidamente los eventos en tiempo real, aplique directivas de seguridad que se administran de manera centralizada y genere detallados informes forenses y de proliferación, sin que se vean afectadas las operaciones cotidianas.

- Una vez finalizada la fase de Discovery, cree directivas de protección de datos para comunicar las infracciones. De esta forma, facilita la información necesaria para saber cómo se desplazan los datos en la organización y permite la aplicación de reglas de bloqueo. McAfee DLP incluye clasificaciones incorporadas (por ejemplo, HIPAA, SOX, PCI e ITAR) que pueden utilizarse para identificar datos dentro de la organización.
- Cree pantallas informativas para que los usuarios conozcan las directivas de protección de datos cuando realicen transferencias de datos cotidianas. Estos cuadros emergentes informativos y personalizables son extremadamente útiles y reducen los riesgos en las transferencias de datos realizadas por los empleados.
- Consulte el Administrador de incidentes para identificar las propiedades de los datos que se transfieren a ubicaciones no autorizadas; por ejemplo, cómo y quién realiza las transferencias.
- Tras crear las directivas de protección de datos y adaptar los requisitos organizativos, active el bloqueo de transferencias de datos no autorizadas.
- Permita las clasificaciones manuales, para que los usuarios puedan clasificar los documentos que hayan creado. Ellos que son los propietarios podrán entender mejor su nivel de confidencialidad, si el motor de clasificación automático no puede detectar los datos estructurados. McAfee DLP Endpoint incorpora esta característica sin necesidad de utilizar otras herramientas de terceros.
- Para aumentar la protección, cree e implemente una regla de protección de acceso de aplicaciones que utilice McAfee Threat Intelligence Exchange para evitar que las aplicaciones desconocidas puedan acceder a datos confidenciales. De esta forma, se permite a las aplicaciones autorizadas transferir datos confidenciales, pero se limita el acceso a esos datos a las aplicaciones no verificadas o maliciosas.

McAfee DLP Monitor

McAfee DLP Monitor permite recopilar, rastrear e informar sobre los datos que se transfieren en toda la red. Descubra fácilmente las amenazas desconocidas para los datos y tome medidas para protegerlos.

- Active las directivas y reglas incorporadas adecuadas para detectar las posibles infracciones en la red.
- Cree reglas y directivas personalizadas adicionales, por ejemplo, para supervisar las transferencias de datos confidenciales en la nube.
- Realice análisis forenses para correlacionar los eventos de riesgo actuales y pasados, detectar tendencias de riesgos e identificar amenazas. McAfee DLP Monitor permite a los expertos en seguridad comprender rápidamente la situación y desarrollar las reglas y directivas necesarias para corregir las posibles anomalías.
- Cree otros filtros de captura para excluir datos irrelevantes y adapte las reglas para reducir los falsos positivos.
- Configure alertas para enviar notificaciones a los remitentes, destinatarios, propietarios de datos y administradores de sistemas, cuando se infrinjan las directivas.

McAfee DLP Prevent

McAfee DLP Prevent protege frente a la pérdida de información garantizando que solo salga de la red cuando sea conveniente, ya sea a través del correo electrónico, el correo web, la mensajería instantánea, wikis, blogs, portales, HTTP/HTTPS o transferencias FTP. Su capacidad para identificar y mitigar rápidamente los intentos de filtración suele marcar la diferencia entre mantener a salvo sus datos más valiosos o ser noticia por robo de información.

- Integre McAfee DLP Prevent con proxies web o con agentes de transferencia de mensajes mediante directivas incorporadas, para impedir transferencias de datos no autorizadas a través de gateways del correo electrónico o proxies web.
- Cree reglas de McAfee DLP Prevent para permitir o bloquear documentos confidenciales según el porcentaje de coincidencia.
- Utilice las plantillas que incluye DLP para proteger los datos confidenciales y evitar que se transfieran a la nube.
- Consulte los informes sobre incidentes de seguridad y ajuste las directivas para reducir los falsos positivos y maximizar la continuidad del negocio.
- Configure alertas para enviar notificaciones a los remitentes, destinatarios, propietarios de datos y administradores de sistemas, cuando se infringen las directivas.

Más información

Comunidad Intel Security Expert Center

- McAfee Data Loss Prevention

914_0816_brf_preventing-data-leak-organization

McAfee. Part of Intel Security.
Avenida de Bruselas n.º 22
Edificio Sauce
28108 Alcobendas
Madrid, España
Teléfono: +34 91 347 8500
www.intelsecurity.com