Universidad Autónoma de Nuevo León

Facultad de Ingeniería Mecánica y Eléctrica

Materia: Arquitectura de Computadoras

Data Lost Prevention

Maestro: Enrique Manuel Castillo Morales

Alumno: Héctor Mauricio Flores Martínez

Matrícula: 1897759

Grupo: 007

Hora: Martes N4 - N6

Fecha de entrega: 23/05/2022

Índice

1. Data Lost Prevention

Data Loss Prevention (DLP), en una traducción literal, prevención de la pérdida de datos. Las soluciones DLP se utilizan en el proceso de monitoreo de sucesos que pueden ocasionar la filtración de información. Los productos centrados en DLP posibilitan la prevención y la corrección de vulnerabilidades cuando se las diagnostican. Existen diferentes tipos de soluciones DLP, cada una orientada a un propósito específico, pero con el mismo objetivo: prevenir la pérdida de datos.

Los productos de software de DLP utilizan reglas empresariales para imponer el cumplimiento de la normativa y clasificar y proteger la información confidencial y crítica, de modo que los usuarios no autorizados no puedan compartir accidental o maliciosamente datos que puedan poner en peligro a la organización.

La implementación de soluciones DLP debe ser precedida de un estudio centrado en las necesidades del negocio. El resultado de éste deberá mostrar los puntos de vulnerabilidad, posibilitando el establecimiento de un conjunto de soluciones para atender las necesidades evidenciadas.

Figura 1: Blue Coat Data Loss Prevention DLP1700

1.1. ¿Cómo funciona la prevención de la pérdida de datos?

El software de DLP supervisa, detecta y bloquea los datos sensibles para que no salgan de la organización. Esto significa que es necesario supervisar tanto la entrada a las redes corporativas, como los datos que intentan salir de la red.

La mayoría de los productos de software de DLP se centran en acciones de bloqueo. Por ejemplo, si un empleado intenta reenviar un correo electrónico de la empresa en contra de la política de la misma fuera del dominio corporativo, o subir un archivo corporativo a un servicio de almacenamiento en la nube para consumidores, como Dropbox, se le denegará el permiso.

Además, el software de DLP puede bloquear los ordenadores de los empleados para que no lean ni escriban en unidades de memoria USB para evitar copias no autorizadas.

La detección se centra principalmente en el correo electrónico entrante, buscando archivos adjuntos e hipervínculos sospechosos para los ataques de phishing.

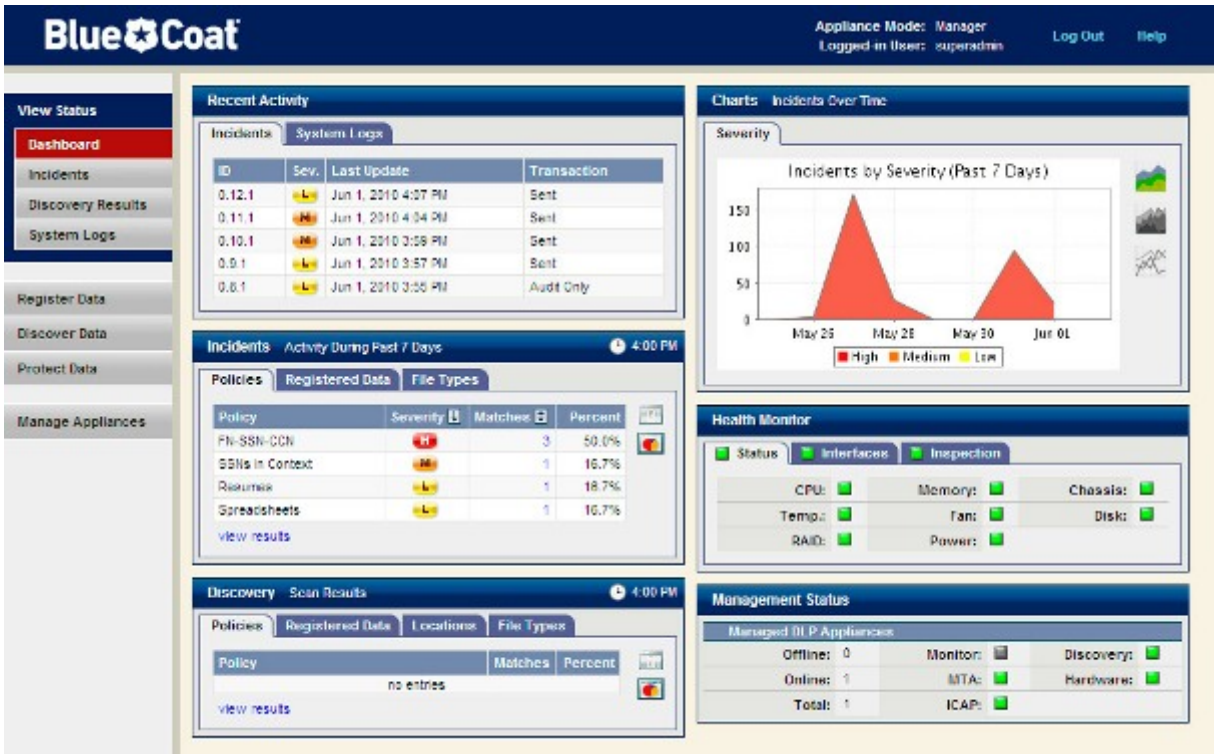

Figura 2: Imagen del software del DLP Blue Coat

La mayoría de los programas de DLP ofrecen a las organizaciones la opción de marcar los contenidos incoherentes para que el personal los examine manualmente o bloquearlos directamente.

1.2. ¿Porqué es importante la prevención de la pérdida de datos?

La pérdida de datos puede, en el mejor de los casos, costar a las empresas una multa considerable –si no masiva– y, en el peor de los casos, dejar a una organización fuera del negocio o incluso llevar a alguien a la cárcel.

La pérdida de datos podría costar definitivamente a la gerencia su trabajo. Los CEO y CIO de Equifax y Target renunciaron en desgracia después de las grandes violaciones de datos que perjudicaron a sus empresas y les costaron millones en multas.

La monitorización de recursos por parte de un DLP no se limita exclusivamente a la red interna de la organización, ya que estas herramientas son capaces de extender su supervisión a dispositivos móviles, tanto Android como iOS. Los DLP son capaces de comprobar a qué correos corporativos se ha accedido. Además, tienen capacidad de comprobar y detener la transmisión de datos confidenciales desde la organización a aplicaciones de almacenamiento en la nube o redes sociales.

Para que la implantación de un DLP en la organización sea lo más sencilla posible, incorporan plantillas preconfiguradas según distintas normas o estándares como el RGPD, LPI, LSSI o PCI-DSS.

1.3. ¿Cómo podemos prevenir la pérdida de los datos?

La prevención de la pérdida de datos en la red abarca una serie de técnicas de seguridad de datos. Entre ellas se encuentran:

- **Identificación de datos.** La DLP solo es útil si se sabe qué es y qué no es sensible. Las empresas deben utilizar una herramienta automatizada de descubrimiento y clasificación de datos para garantizar una identificación y categorización fiables y precisas de los datos, en lugar de dejar que sean los humanos quienes decidan.

- **Proteger los datos en movimiento.** Los datos se mueven bastante internamente, y las violaciones externas a menudo se basan en esto para desviar los datos. El software de DLP puede ayudar a garantizar que los datos no se desvíen a un lugar al que no deberían ir.

- **Proteger los datos en reposo.** Esta técnica protege los datos cuando no están en movimiento, como los que residen en bases de datos, otras aplicaciones, repositorios en la nube, computadoras, dispositivos móviles y otros medios de almacenamiento.

- **Prevención de la pérdida de datos en el punto final.** Este tipo de funcionalidad de DLP protege los datos en el nivel de los dispositivos finales, no solo las computadoras, sino también los teléfonos móviles y las tabletas. Puede bloquear los datos para que no se copien o cifrar todos los datos mientras se transfieren.

- **Detección de fugas de datos.** Esta técnica consiste en establecer una línea de base de la actividad normal y, a continuación, buscar activamente comportamientos inusuales.

2. Tipos de Data Loss Prevention

Network DLP Disponibles en las plataformas de software o hardware, integrada a los puntos de salida de datos de la red corporativa. Una vez instalada, la solución monitorea, rastrea y genera informes de todos los datos de tráfico en la red. Este es el tipo de DLP ideal para explorar todo el contenido que pasa por los puertos y protocolos de la empresa. Proporciona informes importantes que ayudan a garantizar la seguridad de la información en la organización, como: qué datos están siendo utilizados, por quién están siendo accedidos y hacia dónde van. La información recopilada por el Network DLP se guarda en una base de datos que se puede administrar fácilmente.

Storage DLP ¿Usted sabe cuáles son los datos que sus colaboradores almacenan y comparten? ¿Cuántas de estas informaciones se consideran sigilosas y pueden estar en riesgo de fugas? Estas son preguntas que el almacenamiento DLP ayuda a responder. Es un sistema que permite ver archivos confidenciales almacenados y compartidos por quienes tienen acceso a la red corporativa. Así, es posible identificar puntos sensibles y prevenir la filtración de información. Es una buena solución para controlar datos almacenados en la nube, por ejemplo.

Endpoint DLP En el pasado eran los disquetes, hoy en día son los pendrives: herramientas externas que ayudan a transportar archivos de manera práctica y rápida. Sin embargo, pueden poner en riesgo la seguridad de la empresa y facilitar la filtración de datos de forma accidental o intencional. Para evitar esto, es necesario tener una solución que ayude a prevenir la pérdida de datos a través de dispositivos extraíbles. La solución DLP más adecuada para ello son las opciones Endpoint. Estas se instalan en todas las estaciones de trabajo y dispositivos utilizados por los empleados de la empresa para supervisar e impedir la salida de datos sensibles por dispositivos extraíbles, aplicaciones para compartir o áreas de transferencia.

Referencias

[1] Ostec, "Dlp: ¿qué es y cómo funciona?" 2015, fecha de consulta: 21 de Mayo de 2022. [Online]. Available: https://ostec.blog/es/seguridad-perimetral/dlp-que-es-y-como-funciona/

[2] A. Patrizio, "Prevención de pérdida de datos (dlp)," 2022, fecha de consulta: 21 de Mayo de 2022. [Online]. Available: https://www.computerweekly.com/es/definicion/Prevencion-de-perdida-de-datos-DLP

[3] B. Coat, "Blue coat data loss prevention dlp1700 appliance safeguard your sensitive company data," 2022, fecha de consulta: 21 de Mayo de 2022. [Online]. Available: https://www.edgeblue.com/DLP1700.asp

[4] INCIBE, "Dlp protege tus datos contra fugas de información," 2019, fecha de consulta: 21 de Mayo de 2022. [Online]. Available: https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion