DLP: PREVENCIÓN DE FUGA DE INFORMACIÓN (DATA LOSS PREVENTION)

Torres Martínez Miguel Ángel
migueltorres18@hotmail.es
Especialización en Seguridad Informática
Universidad Piloto de Colombia

Abstract — *Incidents of data loss or data leakage are presented incrementally in all organizations, result in sanctions, economic losses, and loss of image. These events are generated mostly by employees who send accidentally or not, sensitive information to outside areas that are not trusted.*

Solutions DLP (Data Loss Prevention) use sophisticated pattern matching techniques and user identity to identify and prevent unauthorized communication of sensitive information through the network perimeter.

Key words—*Loss information, Patterns of behavior, Prevention, Security policy, Sensitive data.*

Resumen—*Los incidentes relacionados con pérdida de información o fuga de datos se presentan de forma incremental en todas las organizaciones, lo cual conlleva multas, sanciones, pérdidas económicas y de imagen. Estos eventos son generados en su mayoría por empleados o funcionarios internos que envían de manera accidental o no, información sensible a zonas externas que no son de confianza.*

Las soluciones de DLP (Data Loss Prevention) utilizan técnicas sofisticadas de coincidencia de patrones y de identidad de usuarios para identificar e impedir la comunicación no autorizada de información sensible a través del perímetro de la red.

Índice de Términos—*Datos sensibles, Fuga de información, Patrones de comportamiento, Política de seguridad, Prevención.*

I. INTRODUCCIÓN

La fuga y pérdida de información confidencial es uno de los problemas críticos que enfrenta toda organización, dicha información es considerada como un activo muy valioso, el cual está propenso a ser robado o manipulado de forma indebida por medio de correos electrónicos, mensajería instantánea, impresión o copia en dispositivo de almacenamiento USB.

En Colombia muchas empresas e instituciones deben cumplir con regulaciones y controles para cumplir con la protección de información confidencial, por ejemplo la ley datos personales, PCI[1] (Payment Card Industry), circular 051, ley SOX[2] (Sarbanes-Oxley) dependiendo de su razón social y el nicho de mercado en el que están inmersos. Una herramienta efectiva que ofrece mecanismos para salvaguardar la información es la solución de prevención de fuga de información (Data Loss Prevention DLP).

Los productos DLP ayudan a detectar y prevenir en tiempo real la fuga de información sensible que se pueda producir en la organización, bien sea de forma no intencional o con algún objetivo específico. Adicionalmente permite educar y notificar a los empleados sobre la manera más adecuada de manipular la información confidencial, por consiguiente se obtiene una mejor cultura de seguridad de la información en toda la organización.

II. ANTECEDENTES

La primera plataforma construida como una solución en la detección de fugas de información confidencial, llamada Vontu, fue publicada en enero de 2004. La empresa fabricante de este producto fue adquirida posteriormente por Symantec, con lo cual se produjo un nivel de maduración cada vez más importante.

Este fue el primer producto que cambio la percepción acerca de la protección de la

[1] PCI DSS, Payment Card Industry Data Security Standard, Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago.

[2] SOX Ley Sarbanes Oxley, Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista

información, ya que no se centraba en los patrones tradicionales considerados hasta el momento, que consistían en identificar los servicios que se podían publicar y los que se restringían (firewalls[3]), o en patrones de comportamiento correlacionados para detectar incidentes que atentaran contra la seguridad de la información (IDS[4] e IPS[5]). El concepto se centraba en el contenido de la información sensible con el fin de prevenir que dicha información pueda salir de la infraestructura de la organización.

Posteriormente surgieron otros productos relacionados con la prevención de fugas de información, como Provilla, la cual fue adquirida por la empresa Trend Micro y redefinida como DLP "TrenMicro LeakProof" y Onigma de quien actualmente es propietario McAfee llamada actualmente "McAfee Data Loss Prevention" [8].

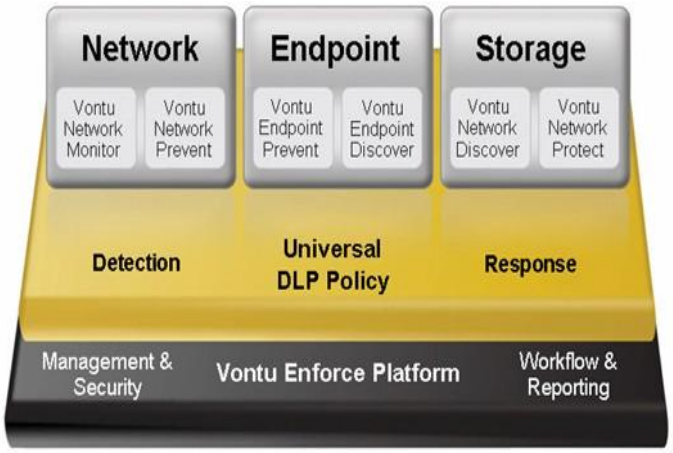

Figura 1. Plataforma de Vontu Enforce Symantec, tomado de: *http://www.symantec.com*.

III. DEFINICIÓN

DLP (Prevención de Fuga de Información - Data Loss Prevention (DLP) es un término de seguridad informática que comprende un conjunto de herramientas destinadas a evitar el envío de información sensible, confidencial o crítica, fuera del entorno de la organización, adicionalmente describe las soluciones tecnológicas que detectan, monitorean y evitan que la información clasificada como confidencial sea transmitida y usada de forma indebida hacia el exterior de las organizaciones.

Esto se logra a través de la inspección de contenidos, el análisis del contexto de seguridad de los flujos de información, es decir propietarios, destinatarios, custodios, contexto de la información, propósitos de transmisión, medios y tiempos de comunicación.

IV. CARACTERÍSTICAS

La infraestructura DLP ofrece una solución robusta orientada a la detección, monitoreo, protección y administración de información sensible dependiendo de su categorización, del medio de almacenamiento y de los propietarios identificados:

- Detecta información sensible localizándola en su medio de almacenamiento, creando un inventario de datos, y sus propietarios con el fin de administrar y simplificar el tratamiento de la información asociada.

- Supervisa el modo en que se utiliza la información confidencial por parte de los usuarios, los procesos organizacionales involucrados y su visibilidad.

- Protege la información por medio de la aplicación automatizada de políticas de seguridad con el fin de proteger los datos de manera anticipada y evitar las posibles fugas de información.

- Administra políticas globales de pérdida de datos en toda la organización, identifica incidentes de seguridad y elabora informes de forma centralizada por medio de una plataforma unificada y centralizada.

[3] Firewall, dispositivo que hace parte de un sistema o una red, está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

[4] IDS, Sistema de Detección de Intrusiones (Intrusion Detection System) programa de detección de accesos no autorizados a un computador o a una red.

[5] IPS, Sistema de Prevención de Intrusos, software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

V. FUNCIONAMIENTO

La protección de la información se realiza basados en la clasificación de la información, proceso mediante el cual se categorizan los datos para poder ser tratados dependiendo de su ubicación y manipulación:

A. Información en uso (data in use)

Son los datos que son accedidos o manipulados en tiempo real por usuarios o programas, su protección se realiza por medio de la instalación de agentes en las estaciones que se desean proteger. Los agentes controlan el acceso a la información, su copia en dispositivos de almacenamiento externos y su impresión en físico.

B. Información en transmisión (data in motion)

Consiste en los datos que se encuentran en trasmisión a través de cualquier medio, su protección se realiza implementando dispositivos o software que analicen los paquetes de red en busca de patrones, para determina si el contenido de la información transmitida se encuentra autorizada.

Algunos protocolos que son continuamente monitoreados son SMTP[6], HTTP[7], HTTPS[8], FTP[9] y Telnet[10]. Con esto se logra identificar, por ejemplo, si un empleado envía correos desde su cuenta corporativa hacia cuentas externas con información confidencial, la herramienta de DLP bloquea el correo saliente, notifica al usuario de la infracción cometida y crea un incidente para que los dueños de la información sean enterados de dicha acción.

C. Información almacenada (data in rest)

Hace referencia a los datos que se encuentran almacenados en cualquier medio y que son accedidos de forma esporádica, su protección se realiza navegando por los repositorios de datos de la organización. Por ejemplo, el módulo de descubrimiento de data in rest puede navegar en los recursos compartidos de la organización, para identificar la existencia de archivos con información de clientes o transacciones financieras y ubicarlos en su correspondiente sitio de alojamiento.

VI. BENEFICIOS

Controla el flujo de datos confidenciales entre centros de cómputo, plataformas, sistemas, entidades clientes, proveedores y usuarios finales.

Redefine el flujo de los datos confidenciales en los procesos internos con el fin de identificar responsables y custodios de la información.

Monitorea y protege la información que es publicada en los recursos web públicos.

Apoya la implementación de las políticas globales de seguridad de la información definidas por la organización.

VII. TIPOS

Con el fin de abarcar la protección en toda la infraestructura de una organización, los productos de DLP son ubicados tanto en el perímetro de red, es decir en la frontera donde se delimita el tráfico interno de la organización; como al interior de la red, en los puntos (servidores, equipos, portátiles) en donde reside información catalogada como confidencial. De esta manera, los tipos de DLP son:

A. DLP de Red

Se encuentran ubicados en el perímetro de la red, o en segmentos de red identificados estratégicamente para monitorear el tráfico de datos en puntos críticos. Se encargan de detectar correos electrónicos, servicios de mensajería, y servidores web.

B. DLP de Host

Son agentes instalados localmente en servidores, estaciones de trabajo, portátiles y dispositivos

[6] SMTP, Simple Mail Transfer Protocol (Protocolo para transferencia simple de correo).

[7] HTTP, Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto).

[8] HTTPS, Hypertext Transfer Protocol Secure (Protocolo seguro de transferencia de hipertexto).

[9] FTP, File Transfer Protocol, (Protocolo de Transferencia de Archivos)

[10] Telnet, Teletype Network (Protocolo de red que permite el acceso remoto a equipos de la Red.

móviles. Están orientados a controlar la fuga de información por medio de dispositivos de almacenamiento externos.

VIII. FABRICANTES

De acuerdo a la información publicada por Gartner, las principales empresas líderes fabricantes de soluciones de DLP para el año 2014 son: CA Tecnologies, McAfee, RSA, Symantec, Trustware, Verdasys y Websense.

El estudio identifica las empresas más importantes, utilizando parámetros de categorización basados en el posicionamiento, la estrategia de mercado y la eficacia en el desempeño de los objetivos. Los productos de prevención de fuga de información (Data Loss Prevention) más destacados son:

Figura 2. Gráfico de las empresas líderes en Data Loss Prevention, según Gartner, tomado de: http://www.gartner.com.

Controla el flujo de datos confidenciales entre centros de cómputo, plataformas, sistemas, entidades clientes, proveedores y usuarios finales.

De acuerdo al estudio "Magic quadrant for content-aware data loss prevention" publicado por la empresa consultora Gartner, "en el año 2014 más del 50% de las empresas utilizará alguna característica en sus políticas de seguridad a la hora de realizar una prevención de fuga de información (Data Loss Prevention) en sus datos sensibles. Sin embargo sólo el 30% de estas dispondrá de una solución o estrategia DLP global basada en el contenido" [2].

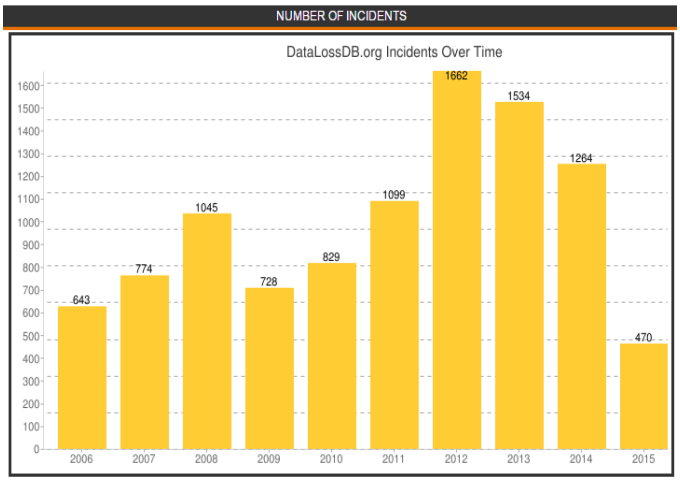

Figura 3. Número de Incidentes empresariales relacionados con Pérdida de Datos durante la última década, tomado de: http://www.datalossdb.org/statistics.

IX. IMPLEMENTACIÓN

La implementación de una herramienta de DLP no es una tarea sencilla, debido a la gran cantidad de información almacenada en servidores, equipos, carpetas y archivos. A pesar de que la herramienta puede realizar la identificación de contenido clasificado como confidencial, también se pueden realizar ajustes para incluir información como gráficos, formulas o esquemas.

El éxito en la implementación de una plataforma de DLP radica en el análisis inicial de los flujos de datos, la clasificación de la información, el análisis de riesgos y la configuración de la herramienta.

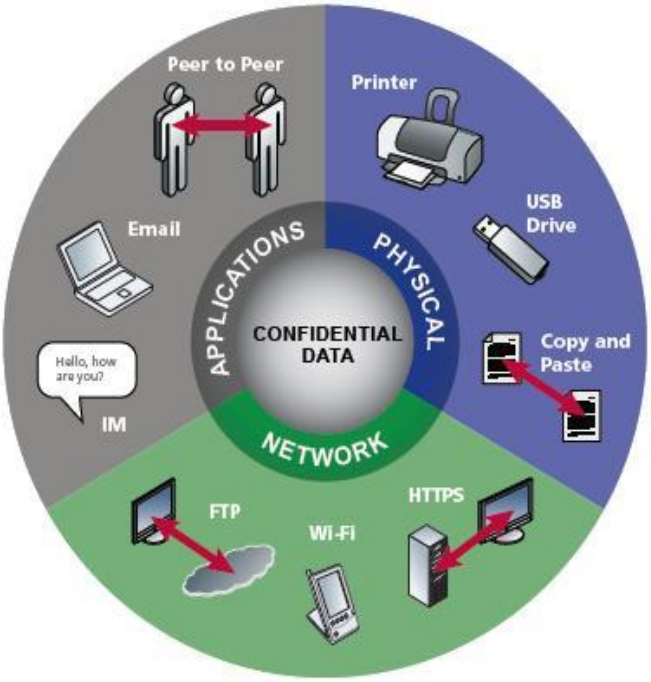

Figura 4. Data Loss Prevention – How DLP technologies work, tomado de: http://blog.skodaminotti.com/.

A. *Consideraciones Previas*

Antes de implementar la herramienta, es necesario realizar actividades previas de consultoría en las que se considere la clasificación de la información y la definición de roles y responsabilidades.

- Clasificación de información: La categorización de la información se puede realizar por medio del descubrimiento de activos críticos por medio de la herramienta DLP, con ello se construyen los patrones de detección, los cuales deben ser afinados para evitar fallos, como por ejemplo, bloqueo de acciones legitimas o posibilitar fugas de información.

La información encontrada se encuentra almacenada en archivos con diversos formatos, los cuales se analizan de acuerdo a su contenido. Los archivos que no permiten el acceso a su contenido, por encontrarse cifrados, son verificados por medio del hash asociado para identificar su autenticidad.

- Roles y responsabilidades: Se deben especificar y documentar para determinar los usuarios autorizados para la manipulación de la información sensible, de esta forma la herramienta de DLP garantizan el cumplimiento de las necesidades de la organización.

B. *Gestión centralizada*

La gestión centralizada se realiza por medio de una consola destinada a la gestión de las políticas de seguridad de la organización. Los módulos contenidos en la solución de DLP deben acceder a la base de datos central para obtener acceso a los patrones de comportamiento permitido y restringido definidos previamente.

C. *Monitoreo y prevención*

Las herramientas DLP trabajan en modo monitoreo y en modo prevención. En modo monitoreo se registran los eventos en los que se presenta fuga de información, representados en incidentes y eventos con el fin de realizar seguimiento a los patrones de comportamiento de los usuarios. En modo prevención, se realizan bloqueos de determinadas acciones en función de las políticas de seguridad ya establecidas.

Las buenas practicas definidas por las empresas proveedoras de DLP recomiendan que se ejecute la herramienta en modo monitoreo durante algunos meses antes de aplicar el modo prevención. Esto con el fin de realizar afinar los patrones de detección y las políticas de seguridad para evitar posibles denegaciones de servicio.

D. *Despliegue e integración*

La integración de la solución DLP con otras herramientas de seguridad es un aspecto importante con el fin de brindar una capa de seguridad perimetral más robusta para la organización, de esta manera la combinación con firewalls e IDSs brinda mayor eficacia en la detección y contención de actividad sospechosa. En otros casos, por ejemplo, con soluciones de antivirus, se deben realizar ajustes para que los agentes de DLP no sean identificados como software malintencionado.

X. CONCLUSIONES

Una solución DLP cubre necesidades de seguridad importantes en las empresas, ya que en la actualidad la información es uno de los activos más importantes y no se debe permitir escenarios de fugas de la información, la cual esta almacenada en medios digitales.

La principal característica de la tecnología DLP con respecto a otras herramientas de seguridad es la capacidad de analizar distintos protocolos y formatos de almacenamiento y su contenido, para determinar las adecuadas formas de uso, transmisión y almacenamiento, de acuerdo a las políticas de seguridad establecidas.

Las políticas definidas en DLP no solo bloquean la impresión, el copiado de datos a dispositivos externos o el envío de información por Internet, sino que establece medidas de control y monitoreo para los flujos de datos, permitiendo realizar estas acciones a los usuarios autorizados, conservando un registro histórico de las actividades realizadas.

REFERENCIAS

[1] Aced Emilio, “La Privacidad en entornos 'Data Loss Prevention"', disponible en http://www.redseguridad.com/opinion/articulos/la-privacidad-en-entornos-data-loss-prevention.

[2] Alonso Cebrián Rubén, “Fuga de información en empresas líderes en Data Loss Prevention”, disponible en http://blog.elevenpaths.com/2013/08/fuga-de-informacion-en-empresas-lideres.html.

[3] Cano Gabarda Florencio, “Introducción a la tecnología “Data Loss Prevention (DLP)”, disponible en http://www.seinhe.com/introduccion-a-la-tecnologia-data-loss-prevention-dlp/.

[4] DataLossdb open security foundation, “Data Loss Statistics”, disponible en http://www.datalossdb.org/statistics.

[5] Ing. Cardozo González Luis Fran y Ing. García Severiche Bladimiro, “Prevención de perdida de datos - Data Loss Prevention”, disponible en http://www.seinhe.com/blog/14-introduccion-a-la-tecnologia-data-loss-prevention-dlp.

[6] Karl-Heinz Holtschmit, “Data Loss Prevention”, http://www.isaca.org/chapters7/Monterrey/Events/Documents/20101206%20Data%20Loss%20Prevention.pdf.

[7] Kino Makino, “OpenDLP. Data Loss Prevention open source. Monitoriza las fugas de información.”, disponible en http://kinomakino.blogspot.com/2015/03/opendlp-data-loss-prevention-open.html.

[8] Symantec Corporation “La solución de prevención contra la pérdida de datos líder del mercado”, disponible en http://www.symantec.com/es/mx/data-loss-prevention/.

[9] Tomlin Jay, “How share file works to prevent Data Loss and meet compliance requirements”, disponible en http://blogs.citrix.com/2015/05/12/how-sharefile-works-to-prevent-data-loss-and-meet-compliance-requirements/.