



¿QUÉ
PREOCUPA?

PREVENCIÓN DE FUGA DE INFORMACIÓN-DLP: O CÓMO VENDER LA SEGURIDAD A TU CEO

En los últimos meses estamos viviendo episodios cada vez más preocupantes de fugas de información y espionaje industrial dignos de las mejores novelas de John le Carré. Parece que, por fin, todo el mundo ha asumido que el mayor activo de cualquier compañía es, precisamente, dicha información, y frecuentemente nos encontramos con situaciones tales como robos de dispositivos portátiles de altos directivos, venta de información a la competencia, etc. En este sentido, a todos se nos viene inmediatamente a la memoria el episodio de espionaje protagonizado por Ferrari y McLaren-Mercedes en el mundo de la Fórmula 1, como caso reciente más notorio.

Con el paso del tiempo, los profesionales también nos hemos dado cuenta de que el verdadero problema en la seguridad de la información no se encuentra tanto en el exterior como dentro de nuestras empresas y, más concretamente, en el uso inadecuado o no autorizado de información sensible por parte de empleados.

El modelo tradicional de seguridad en las TI está basado en la protección perimetral, introduciendo capas de acceso a la red desde fuera hacia dentro

contenidos, que pueden cubrir parte de la solución, no son fiables y cuentan con un gran número de vulnerabilidades que imposibilitan conseguir un grado aceptable de protección.

DLP

En estas situaciones son donde cobran sentido las aplicaciones para la Prevención de Fuga de Información o *Data Loss Prevention*. Estas soluciones están concebidas para ayudar a las compañías a conocer y controlar la información que es utilizada y que, llegado el caso, sale al exterior a través de diversos medios: correo-e, web, FTP o incluso dispositivos portátiles de almacenamiento tales como memorias o discos USB. Mediante la firma de los contenidos a proteger y su correspondiente clasificación seremos capaces de detectar cuándo se está haciendo uso de información sensible y qué destino tienen estos datos.

Dependiendo de la solución que deseemos implementar nos encontramos con tecnologías que analizan el tráfico de la red en busca de patrones que coincidan con los datos clasificados como

Toda esta situación de cierta inquietud en el uso de la información, aunque parezca paradójico, está ayudando mucho a aquellos que nos dedicamos a la seguridad en el ámbito de las TI, ya que preocupa cada vez más a los propietarios de las compañías –y, en general, a aquellos con responsabilidad sobre el negocio– el riesgo de que información corporativa pueda llegar a ser utilizada por la competencia o que datos personales de clientes queden expuestos. De hecho, muchas veces son ellos mismos los que se interesan por el grado de protección de la compañía frente a estas amenazas y nos preguntan qué estamos haciendo para darles solución.

Convencer al Comité de Dirección sobre la necesidad de la puesta en marcha de un proyecto de DLP es mucho más sencillo de explicar por su finalidad que otras iniciativas de protección. El hecho de que una aplicación vaya a evitar o, al menos detectar, fugas de datos o información estratégica analizando el tráfico de la red y revisando todo lo que sale de ella, y que además nos ayude a cumplir con la legislación vigente es el sueño de cualquiera. ¿Quién no se ha encontrado con el difícil reto de explicar a su Director General lo que es un *firewall*, un *appliance anti-spam* o un dispositivo IDS para justificar el coste, normalmente elevado, de este tipo de soluciones? Sin embargo, una aplicación de DLP “se vende sola” porque tiene un fin claramente comprensible para cualquiera.

En definitiva, las tecnologías para la prevención de fugas de información han venido a dar un soplo de aire fresco a los departamentos de seguridad, alineando completamente las necesidades del negocio con las inquietudes y responsabilidades de los Directores de Seguridad y de TI, así como aportando transparencia a sus procesos de gestión y control. No obstante, debemos ser conscientes, y transmitirlo así a nuestra Dirección,

Con el paso del tiempo, los profesionales también nos hemos dado cuenta de que el verdadero problema en la seguridad de la información no se encuentra tanto en el exterior como dentro de nuestras empresas y, más concretamente, en el uso inadecuado o no autorizado de información sensible por parte de empleados.

que dificulten o imposibiliten ataques en forma de denegación de servicio, *hacking*, *mail-bombing*, etc., que afecten a nuestra infraestructura y que puedan llegar a comprometer aquellos sistemas críticos para el buen funcionamiento de la corporación. El nivel de sofisticación de los dispositivos que protegen nuestra red hace cada vez más difícil para un atacante externo hacerse con el control de algún servicio para conseguir acceder a datos de su interés, por lo que ¿no sería más sencillo conseguirlos desde dentro? Evidentemente, el nivel de seguridad existente en una red para los usuarios autorizados, *a priori*, no es tan estricto. Además, el hecho de que los empleados habitualmente trabajen con la información objeto de control hace que se priorice la funcionalidad en detrimento, en muchos casos, de la seguridad.

Pero no sólo nos enfrentamos a un problema privado, por decirlo de alguna manera, sino que existen normas reguladoras y leyes estatales que obligan a las empresas a velar por la salvaguarda de la información almacenada, enfrentándose en caso de incumplimiento a graves sanciones económicas, sin contar con el deterioro en su reputación e imagen de marca. Hay ejemplos claros de esto en la Ley de Protección de Datos o en las normas Sarbanes-Oxley, HIPAA o GLBA, entre otras, que exigen a las compañías controlar en todo momento qué personal no autorizado pueda tener acceso y utilizar información clasificada.

Descrito el escenario inicial nos encontramos con un problema complejo de solucionar: ¿cómo controlar la información que es manejada por los empleados y cómo evitar que estos datos sean utilizados o sacados de la red sin autorización? Si bien es cierto que existen técnicas, como el filtrado de

sensibles, o bien aplicaciones cliente instaladas en los servidores y estaciones de trabajo que inspeccionan en tiempo real la información que está siendo utilizada. Cada una de ellas tiene ventajas e inconvenientes, pero deben ser utilizadas de forma complementaria para obtener un porcentaje de efectividad satisfactorio y reducir al máximo el

Explicar y convencer al Comité de Dirección de la necesidad de poner en marcha un proyecto de DLP es, por su finalidad, mucho más sencillo de explicar que otras iniciativas de protección. El hecho de que una aplicación vaya a evitar, o al menos detectar, fugas de datos o información estratégica analizando el tráfico de la red y revisando todo lo que sale de ella, y que además ayude a cumplir con la legislación vigente, es el sueño de cualquiera.

número de falsos positivos o negativos.

El principal problema que tienen estos proyectos no es tanto técnico como organizativo, ya que exige de la compañía que quiera implantarla la correcta identificación de las fuentes de información y su clasificación. Esto suele representar el 80% del tiempo de cualquier proyecto de esta índole y requiere de la colaboración de todos los propietarios de los datos, ya que son ellos los que fijarán los distintos niveles de criticidad en los mismos. Es por ello que muchas veces, la fase inicial consiste en una labor de monitorización de la información que viaja por la red y que nos puede servir de ayuda para identificar los orígenes de los datos así como los usuarios que están haciendo uso de ellos.

de que estas soluciones, como cualquier otra tecnología, no son infalibles y que los resultados dependerán mucho del grado de implicación de todas las áreas de negocio. Pero también es cierto que puede ser un buen punto de partida para aquellas empresas que no posean una política de clasificación bien definida, ya que, como se ha indicado anteriormente, ésta es fundamental para el correcto funcionamiento de la solución implantada. ■



David Moreno
Responsable de Seguridad TI
david.moreno@
grupocortefiel.com
GRUPO CORTEFIEL