Fuga de información: ¿una amenaza pasajera?

Autor: Federico Pacheco, Gerente de Investigación y Educación de ESET Latinoamérica
Fecha: 19 de Enero de 2011

ESET Latinoamérica, Av. Del Libertador 6250, 6to. Piso
Buenos Aires, C1428ARS, Argentina
Tel. +54 (11) 4788 9213 – Fax. +54 (11) 4788 9629
info@eset-la.com, www.eset-la.com

Índice

Introducción

Entre los temas más discutidos y controversiales ocurridos durante 2010 se encuentra sin duda la **fuga de información,** a partir del controvertido caso *Wikileaks*. Sin embargo es interesante destacar que **el tema no es nuevo para la industria de la seguridad de la información**, solo que hoy en día parece ser difícil evitarlo en las mesas de discusión sobre la **privacidad y la confidencialidad** en las empresas y también en el ámbito personal. Justamente estos dos últimos conceptos permiten ilustrar la idea principal que se analizará.

La confidencialidad se refiere a la característica que implica que la información sea accedida solamente por los usuarios autorizados. Por su parte, **la privacidad** habla más bien de una garantía de confianza respecto a la propia información y su uso, diferenciándose de lo público y de lo secreto.

Por tanto, la fuga de información es lo que ocurre cuando algún dato o activo de información que tenga valor para una organización, pasa a manos ajenas, **perdiendo la cualidad de confidencialidad** que le fue asignada. Esto se puede ver representado, por ejemplo, en documentos que pasan a ser accesibles por personas no autorizadas, o también por cualquier dato secreto que alguien interno le facilite a un externo sin pasar por un medio digital. Se desarrollarán a continuación los conceptos necesarios para entender en mayor profundidad la fuga de información, partiendo de algunos casos representativos de los últimos años, y atravesando las clasificaciones básicas del problema: por su naturaleza (técnica o humana) y por el contexto en que se da (corporativo o personal); además de presentar los consejos asociados a cada uno de los contextos.

Casos relevantes

Uno de los casos con mayor repercusión fue el de *Wikileaks*, una organización sin fines de lucro que desde 2006 permite que personas que tengan cierta información sensible de interés público puedan publicarla en dicho sitio web, preservando el anonimato y garantizando la publicación tal cual esta fue ingresada. El sitio llegó a los grandes medios en **noviembre de 2010**, cuando comunicó a la prensa internacional una colección de más de **250.000 cables** entre el Departamento de Estado estadounidense y sus embajadas por el mundo, transformándose en **la mayor filtración de documentos secretos de la historia**, además de haber afectado al país.

En los últimos años se han dado a conocer otros casos relevantes, como el del **banco** HSBC, que en **marzo de 2010** declaró la fuga de datos de **15.000 clientes suizos**, luego de que un ex-empleado del área informática les llevará los datos a autoridades impositivas de Francia.

En enero del mismo año tuvo lugar la *Operación Aurora*, un ataque masivo ocurrido contra más de 30 empresas como Google, Adobe y Juniper; destacado por ser uno de los ataques más importantes en materia de robo de información, aunque finalmente no tuvo éxito.

En **diciembre de 2009**, la red social *Tuenti* fue afectada por el robo de 4.000 cuentas de usuario y sus contraseñas, por parte de un atacante enojado con la empresa.

En **julio de 2008** si bien no se dieron a conocer casos como los anteriormente mencionados, se produjo una importante cantidad de incidentes de seguridad basados en la vulnerabilidad del protocolo DNS descubierta por el especialista de seguridad Dan Kaminsky, que sirvió de base para realizar ataques de phishing, propagación de malware y otros. Ese año, según un informe de incidentes de Verizon, el 39% de los incidentes de seguridad involucraron a *partners* y terceras partes de las empresas, y el 31% de los ataques **incluyeron algún código malicioso** (en ese entonces el protagonista era el gusano Nuwar).

En **agosto de 2007** el sitio global de búsquedas laborales *Monster* sufrió el robo de **1,6 millones de datos con información personal** de los usuarios registrados. Los atacantes ingresaron a las bases de datos con contraseñas que habían sido obtenidas previamente mediante un troyano.

Con estos pocos ejemplos se puede ver que no ha sido poco común encontrar casos de filtración de información en los últimos años, lo cual es parte de lo que ha hecho reaccionar a muchas organizaciones y gobiernos a favor de la seguridad informática.

La naturaleza del problema

En principio, es posible separar el tema en dos grandes ramas, la primera relacionada con la tecnología, y la segunda con las personas. Esta clasificación obedece a un aspecto fundamental de la información, que es su medio de propagación (sistemas o personas) y el lugar donde se almacena (dispositivos de almacenamiento o la memoria de cada individuo).

Aspectos técnicos

Desde el punto de vista técnico **el problema radica en la dificultad de administrar y gestionar la enorme cantidad de datos que procesan las organizaciones**. En este sentido, teniendo en cuenta que cada nivel de usuarios deberá acceder a distintos archivos y datos, y que estos además viajarán por las

redes y se almacenarán en distintas ubicaciones dentro y fuera del centro de cómputos; la complejidad de la situación aumenta exponencialmente. Esta diversidad de posibles ubicaciones de los datos hace que lo que se deba proteger no esté centralizado y se requieran medidas y tratamientos diferentes para cada caso. Por supuesto que todos los componentes tecnológicos forman parte de este aspecto, desde el hardware hasta el software y las redes.

En muchos casos uno de los aliados técnicos de la fuga de información es el malware, que en sus distintas formas y tipos permite acceder a equipos, explotar vulnerabilidades y afectar la privacidad de forma directa. De hecho, como caso particular, **el spyware está diseñado para espiar los sistemas** en los cuales se logra alojar, haciendo que, por ejemplo, las contraseñas de un usuario sean capturadas, o su información estadística de navegación sea tomada sin su consentimiento para fines económicos. En el mismo sentido, dentro del software malicioso que produce este tipo de resultados, existen los denominados *keyloggers*, que son dispositivos de software o hardware que capturan silenciosamente lo tecleado por el usuario. Si bien este aspecto técnico debe resolverse principalmente con un software antivirus adecuado, también es indispensable que el usuario conozca los peligros a los que se expone, dado que en muchos casos la falta de concientización es la que promueve la exposición directa a las amenazas.

Además en ocasiones **puede darse una fuga no intencional**, por deberse a un error técnico que hace que quede expuesta determinada información, ya sea en Internet o dentro de las empresas. También es necesario particularizar el caso de la omisión, en el cual una falla de configuración podría derivar en resultados similares a los antedichos, pero con asignación de responsabilidades más clara.

Para enfrentar los problemas derivados del aspecto técnico aparecieron mecanismos, conocidos con distintas siglas, entre las que se encuentran: *Data Loss Prevention* (DLP), *Data Leak Prevention* (también DLP), *Information Leak Detection and Prevention* (ILDP), *Information Leak Prevention* (ILP), *Content Monitoring and Filtering* (CMF) y *Information Protection and Control* (IPC). Todos estos mecanismos tienen como objetivo el monitoreo y control de los datos digitales que circulan en una infraestructura tecnológica, ya sea por medio de filtrado de contenidos web, por aplicación de políticas en el uso de determinados datos previamente identificados como sensibles, o por el bloqueo de la conexión de dispositivos no marcados como confiables.

Estas tecnologías no funcionan solas, sino que **deben ser minuciosamente configuradas**, para lo cual se requiere previamente conocer el **valor de la información**, que se obtiene luego de realizar un estudio de **valuación de activos**, o bien al menos un reconocimiento de los activos de información importantes, de manera que se reconozca el valor que tiene aquello que se desea proteger. Esto puede originar que muchas empresas dispongan de un sistema que técnicamente proteja contra la fuga de información, pero que al no tener realizado un estudio que determine el valor de sus datos, dicho sistema no tenga la efectividad que podría llegar a tener. Más allá de esto, **la información se debe clasificar** en función de su nivel de requerimientos de confidencialidad, integridad y disponibilidad, cosa que también ayudaría a

implementar un sistema como los mencionados. Si bien esto último pertenece a la rama de la seguridad administrativa, es más difícil encontrar este nivel de madurez en las empresas pequeñas y medianas, al tiempo que en las grandes compañías suele ser una práctica común, por lo que pueden estar naturalmente mejor preparadas para enfrentar problemas relacionados con estos procesos previos.

La aplicación de una política cuya contramedida pueda implantarse por medios técnicos, se puede ejemplificar con una persona que recibe un documento con información confidencial, al que por su nivel jerárquico tiene permitido acceder, que lo imprime y lo deja olvidado sobre la mesa de una oficina. Si alguien encontrara este papel, se haría de dicha información confidencial, en tanto que la persona no sería en principio acusada, ya que hay varias otras que poseen acceso a ese documento. Ahora bien, si por procedimientos definidos en la política de seguridad de la organización, dicho documento incluyera de manera automatizada el nombre de la persona que lo envía a la impresora, la situación cambiaría, y probablemente el desmemoriado individuo del ejemplo no vuelva a cometer el error de dejar en cualquier parte un documento. Esto también se relaciona con el hecho de que en las empresas no todas las personas cuentan con el mismo nivel de acceso a los recursos, y lógicamente aquellos con mayor cargo jerárquico tendrán mayor nivel de responsabilidad por su acceso a documentos e información más sensible que quienes realizan otro tipo de tareas.

Aspectos humanos

En este aspecto, si bien lo normal no es que una persona desee robar información intencionalmente, no se puede negar que la posibilidad exista. Lo que sí es posible afirmar es que cualquiera que esté involucrado en la fuga intencional de información pertenecerá al grupo de **empleados disconformes** con la empresa, o que se hayan visto perjudicados por la misma, situación que es conveniente que intente conocer para evitar permanecer desprevenidos. Esto sin contar el **espionaje interno** que puede existir por parte de empleados que lo realizan en función de **intereses externos**, perjudicando a la propia organización a la que pertenecen.

De todos modos, esto no implica que la fuga pueda darse solo por malas intenciones del propio empleado, ya que en muchos casos un atacante intenta conseguir información utilizando técnicas de Ingeniería Social, buscando engañar al usuario. De esta manera, los usuarios simplemente pueden ser víctimas de algún fraude o engaño que podrían dejar expuesta a la empresa por impericia. Además, algo tan simple como una infección de malware transportado en un *pendrive* podría introducir un riesgo importante en una empresa si no cuenta con un sistema que pueda prevenirlo de manera eficiente.

En las empresas, para facilitar la trazabilidad de las acciones de los usuarios, se suelen incluir procedimientos mediante los que se garantiza que el uso de los activos de información es **efectivamente auditado** y que es posible **generar registros** (*logs*) de las acciones importantes que se hayan definido, que si bien es un proceso técnico, implica un conocimiento de los individuos respecto a su grado de

responsabilidad en lo que realizan dentro de una empresa. El conocimiento de **la vinculación entre las personas y sus accesos puede evitar en gran medida la fuga de información**, ya que en caso de filtrarse hacia el exterior, se podría señalar de manera directa a todos aquellos que tuvieron acceso y se podría analizar su uso previo al incidente, obteniendo posibles conclusiones y responsables. De cualquier manera, dada la imposibilidad de monitorear a las personas más allá de la esfera laboral, es estrictamente necesario que exista un alto grado de concientización y que las políticas de seguridad estén correctamente aplicadas para garantizar que quienes manejen información confidencial tengan **asumidos los riesgos** relacionados con su filtración.

Acciones y contramedidas

Si bien resulta difícil que ciertos problemas sean mitigados en su totalidad, es posible estudiarlos desde distintos ángulos a fin de que puedan reducirse las posibilidades de ocurrencia y se disminuyan los riesgos. Tal es el caso de la fuga de información, sobre la cual se describirán en principio algunas formas de protección en ámbitos de empresas y personales.

En entornos corporativos

Al hablar de acciones de seguridad en empresas, la lógica indica que para la mayoría de las actividades **es necesario basarse en estándares**, normalmente de alcance internacional, y normativas vinculadas a lo que se quiera organizar. Comúnmente se tiende a pensar que esto solo es necesario en grandes empresas y no aplica a pequeñas y medianas, sin embargo las normativas internacionales suelen tener suficiente flexibilidad como para que sean adaptadas a todo ámbito de negocios, con los ajustes e interpretaciones necesarios para cada caso. Con este mismo razonamiento también se puede deducir que la fuga de información no es patrimonio de las grandes corporaciones, solo que éstas están más expuestas por su mayor cantidad de personal, complejidad de sus sistemas y procesos, y valor percibido en el mercado.

Respecto a las normas mencionadas anteriormente, la fuga de información está contemplada dentro de la gestión de la seguridad, y como tal se describen contramedidas y técnicas en distintos estándares. Así pues, se apela con frecuencia a la serie de normas ISO 27000, que está especialmente dedicada a seguridad de la información. Dentro de esta familia se encuentran específicamente algunas normas como lo son la 27001, referida a los **requisitos para implementar un sistema de gestión de seguridad**, la 27002 que define las **mejores prácticas**, la 27004 que habla sobre las métricas, la 27005 que trata sobre la **gestión de riesgos**, entre otras.

También existe normativa específica para ciertas industrias, como lo es la norma PCI DSS (*Payment Card Industry Data Security Standard*) para lo referido a las empresas relacionadas con la operación de tarjetas

de crédito, o Basilea II para la industria bancaria. También existen estándares relacionados con la tecnología en general, como COBIT (*Control Objectives for Information and related Technology*) o ITIL (*Information Technology Infrastructure Library*).

Toda esta gama de normas, estándares y recomendaciones sirven como **base para la creación de entornos seguros y bien gestionados**, donde se tengan en cuenta los principales peligros, adaptados a cada organización, sea cual fuere su tamaño y sector. Por supuesto que para llevar adelante cualquier proceso de alineación con estándares siempre se debe contar con profesionales idóneos y con experiencia en el tema.

La importancia de las normas en el contexto de la fuga de información radica en que tal como ocurre con muchos otros tópicos de seguridad, no puede ser atacada mediante un único enfoque (técnico, físico o administrativo) sino que debe alinearse cada aspecto para que el producto final sea un entorno confiable.

Por el lado más bien técnico existen distintos mecanismos, software y métodos que permiten evitar la filtración de datos, tanto si se da de manera espontánea (por error u omisión) como si ocurre deliberadamente. Para lo primero es más factible automatizar soluciones y prevenirla, en tanto que para lo segundo es más complicado aunque no imposible. En cualquier caso, queda claro que **hay un punto en el que la organización no puede controlar todo**, y es allí donde las soluciones se complementan con las medidas relacionadas a los aspectos humanos.

En el ámbito personal

A nivel personal el problema tiene otro enfoque, dado que no se habla de estructuras organizacionales, dispositivos de red, servidores, sino mas bien del **manejo que hacen las personas de su propia información**, ya sea guardada en sus computadoras de escritorio, notebooks, teléfonos celulares o *pendrives*, como la que circula en los entornos online como las redes sociales y otros sitios que almacenan datos personales y contienen perfiles de usuarios. Así, el desafío se encuentra en que la información que se considera sensible **solo sea accedida por el usuario** y por quienes este quiera que la conozca.

También aparece un riesgo cuando la información se encuentra almacenada. Si bien la preocupación principal puede ser la pérdida de ciertos archivos, la situación podría mitigarse con la realización de **copias de seguridad** (backups) de lo que se considere importante, de tal modo que si se sufre la pérdida o robo de un equipo portátil o medio extraíble, a la pérdida de confidencialidad no se le sume el inconveniente de perder los datos.

En cuanto a la información *online*, es preciso tener en cuenta que **todo lo que se publica e Internet, podría quedar allí por tiempo indeterminado**, y si bien puede eliminarse, no hay garantía alguna de que esto ocurra realmente, dada su arquitectura implícita y sus reglas tácitas de funcionamiento. Esta

realidad ampliamente aceptada en seguridad de la información implica que se debe tener cuidado y mucha prudencia con lo que se decide publicar en Internet, cualquiera sea el sitio, red social, blog, o plataforma online. Por tal motivo, siempre es recomendable **ajustar lo máximo posible y a plena conciencia las configuraciones de seguridad de las redes sociales**, así como también cuidar de no comprometer la confidencialidad de terceros.

10 Consejos fundamentales

A continuación se brindan algunos consejos a tener en cuenta ante este escenario, de tal modo que sea posible **evitar las principales causas** de fuga de información, principalmente enfocados al ámbito corporativo:

1. **Conocer el valor de la propia información**. Realizar un análisis de riesgos y un estudio de valuación de activos para poder determinar un plan de acción adecuado que permita evitar posibles filtraciones.

2. **Concientizar y disuadir**. Diseñar una estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias laborales y legales.

3. **Utilizar defensa en profundidad**. Considerar la aplicación del modelo de defensa en capas a fin de que las distintas medidas que se toman cubran todos los aspectos del acceso a la información (físico, técnico y administrativo) y así evitar centralizar las soluciones o promover puntos únicos de falla.

4. **Incluir herramientas tecnológicas**. En ámbitos corporativos, contar de ser posible con una solución técnica de protección, por medio de hardware, software, o combinación de ambos, tanto a nivel de redes como de equipos (servidores y estaciones de trabajo). Además, las soluciones contra el malware son particularmente indispensables.

5. **Seguir los estándares**. Alinearse con estándares internacionales de gestión de la seguridad permite disminuir el riego de que puedan ocurrir incidentes, así como también de que el negocio se vea afectado por un determinado evento de filtración.

6. **Mantener políticas y procedimientos claros**. Relacionado con el punto anterior, se debe tener una clara definición y comunicación de las políticas de seguridad y acuerdos de confidencialidad, aceptados y firmados por todos los usuarios. Esto minimiza potenciales fugas de información, al contar con un consentimiento firmado del usuario para no realizar ciertas acciones.

7. **Procedimientos seguros de contratación y desvinculación**. En estos dos momentos se conecta o desconecta una nueva pieza externa con el motor de la organización, por lo que deben tenerse en

cuenta de manera muy particular, controlando especialmente los accesos y registros de los usuarios en sus primeros o últimos momentos de trabajo.

8. **Seguir procesos de eliminación segura de datos**. Es fundamental que los datos que se desean eliminar sean efectivamente eliminados, y los medios de almacenamiento adecuadamente tratados antes de ser reutilizados.

9. **Conocer a la propia gente**. Se recomienda tener presente que en las organizaciones puede haber personas conflictivas o disconformes, que podrían ser foco de cierto tipo de problemas relacionados con la confidencialidad. Si bien puede ser dificultoso detectar estos casos, el hecho de conocer en profundidad al propio personal ayuda a entender la situación general en que se encuentra una empresa y los posibles riesgos.

10. **Aceptar y entender la realidad**. Es necesario hacer lo posible para comprender que se deben tomar medidas concretas y definir un plan realista. No se pueden controlar absolutamente todas las acciones de todas las personas en todo momento, por lo que siempre habrá un margen de error que quedará abierto, y que deberá intentar reducirse al mínimo a medida que pasa el tiempo.

Con esta lista se puede tener una idea general de **los puntos más importantes a tener en cuenta a la hora de combatir la fuga de información**. Como es de esperarse, muchas medidas aplican también a la solución de los más diversos problemas relacionados con la seguridad, y justamente es por esto que conviene contar con una estrategia global, que incluya todos los aspectos de interés para una organización.

Conclusiones

En base a todo lo expuesto, es posible asegurar que el tema quedará planteado de aquí en adelante, y **será cada vez más importante en el futuro**, lo que puede llevar a tomar conciencia sobre la necesidad de planes de acción en todos los contextos, a fin de mantener un entorno seguro tanto en el ámbito personal como corporativo. En las empresas, para mantener sus niveles de confidencialidad esperados, y en el ámbito personal para evitar que los individuos o sus familias queden expuestos.

Además, el hecho de que se requiere un enfoque múltiple para comprender y resolver los problemas relacionados al filtrado de información, tal como se ha descrito, hace que el tema **no pueda ser encarado desde una sola perspectiva** o área de una organización, sino que requiere de una tarea conjunta entre distintas áreas y personas, y un completo apoyo de parte de las autoridades correspondientes. Como corolario, dado que estamos hablando de riesgos, y el riesgo es algo que por definición misma no es posible eliminar (solo reducir) se debe tener en cuenta que un plan especial para combatir la fuga de

información podría incidir en los costos de operación de las empresas dependiendo de las medidas a tomar, y éstos costos deberán ser solventados por el propio negocio. La buena noticia es que teniendo en cuenta una cantidad no muy grande de ítems y consejos tales como los mencionados, **es posible reducir drásticamente los riesgos** y prevenir muchos incidentes, actuando de forma proactiva.(párrafo agregado)

No cabe duda de que **el fenómeno Wikileaks determinó un antes y un después** en cuanto a lo que a fuga de información se refiere, no porque antes no ocurriera, sino porque **en la mayoría de las ocasiones las fugas no se hacen públicas** para salvaguardar la imagen de las empresas e instituciones hacia afuera, y aquí es donde el caso marcó un límite. Sin hacer un juicio de valores sobre el caso, es posible entender que la trama del asunto no es en última instancia la información en sí que se haya filtrado, sino más bien la posibilidad de que tal cosa pueda sucederle a organizaciones tan grandes y preparadas, lo que deja en claro que podría ocurrirle también a empresas y organizaciones más pequeñas.