

¿Cómo se puede evitar la fuga de información en las empresas?

Los casos de WikiLeaks y de Sony, donde se filtraron registros privados de millones de usuarios, demostraron la capacidad de las redes informáticas para robar, traficar y publicar datos importantes. Cristian Borghello, de ZMA, explica en esta nota los mecanismos disponibles para tapar esas brechas

Por Cristian Borghello, External Security Consultant de ZMA

iProfesional.com

Jack Ryan, el legendario personaje de **Tom Clancy** en "[Juegos de patriotas](#)", describió en una ocasión una trampa para descubrir filtraciones de documentos dentro de la **CIA**. Pero, lamentablemente, este tipo de técnicas parece no funcionar en el mundo actual y digital, como lo demuestran cientos de casos diarios de fuga de información confidencial de organismos públicos y empresas privadas.

Hace exactamente 40 años, **EE.UU.** sufría su primera gran fuga de información clasificada, conocida como "los papeles del Pentágono" ([recientemente desclasificados](#)) donde el diario **The New York Times** publicó 7.000 páginas de documentos del **Departamento de Defensa** sobre su invasión militar y política a **Vietnam** entre 1945 y 1967.

En ese momento, la persona responsable de dicha filtración, **Daniel Ellsberg**, sufrió un acoso similar al que hoy sufren el soldado **Bradley Manning** y **Julian Assange**, responsables de la publicación de miles de documentos a través de **WikiLeaks**.

Más allá de las filtraciones, WikiLeaks representó el mayor golpe mediático del cual se tenga conocimiento sobre este tema, cambió la forma de ver y analizar las noticias así como demostró la capacidad de las redes informáticas para robar, traficar y publicar información.

Este hecho también quedó confirmado con el robo de más de 7 millones de registros de las bases de datos de la empresa **Sony**, donde no sólo se encontraban los datos de sus jugadores sino también sus tarjetas de crédito.

Medidas

Pero, ¿cuáles son las medidas que debe tomar una organización pública o privada para evitar esta fuga de datos sensible?

Inicialmente toda organización debe pasar por un proceso ineludible de **clasificación de su información**, en términos de su valor, requerimientos legales, sensibilidad y criticidad para la organización.

Si no se realiza dicho proceso, no se conocerá el valor de la base que se tiene y, por lo tanto, no se podrá realizar un análisis costo-beneficio ni tampoco se podrá decidir qué conviene proteger o la forma de hacerlo en términos económicos y de riesgos para la organización.

Debido a que el valor de la información es difícil de determinar (por ejemplo, **¿cuánto cuesta una base de clientes?**) y puede ser diverso de acuerdo a las variables consideradas, es necesario clasificar la información para categorizar los datos de acuerdo a su relevancia en cuanto a Confidencialidad, Integridad y Disponibilidad (CIA).

Controles

Una vez realizado este proceso, la organización estará en condiciones de saber cuánto invertir en la protección de la información y comenzar a implementar controles a los distintos tipos de datos clasificados:

- **Controles administrativos:** políticas y procedimientos definidos por la organización.
- **Controles físicos:** barreras físicas para evitar el contacto con los sistemas. Incluye guardias, seguridad física del edificio en general, etc.
- **Controles lógicos y técnicos:** requieren mecanismos de soft y hard. Implican la restricción lógica de acceso a los sistemas y la protección de la información.

Cada organización es un conjunto único de elementos interrelacionados y, por lo tanto, tampoco aquí existe un manual o guía maestra para implementar los controles, pero algunos de los que se deberían considerar son los siguientes:

1. Marcas de agua

Son textos, imágenes o audio que aparecen detrás o encima de un documento impreso o digital, perceptible o no. Estas marcas causan sombras, luces, variaciones o reflejos que facilitan la identificación y autenticación mientras dificultan la copia o duplicación.

Pueden ser ubicadas en documentos físicos (por ejemplo un billete) o en documentos electrónicos a través de aplicaciones que permiten agregar marcas (serie de bits) que identifican un documento en forma unívoca.

2. Firmado digital de documentos

Es el proceso que mediante el uso de la criptografía permite identificar y autenticar mensajes o documentos.

En este caso los procesos de firma digital (y el uso de dispositivos relacionados) permiten determinar con un alto grado de precisión quién tiene acceso a un documento, quién lo ha generado, quién lo ha enviado, cuándo lo ha hecho y, además, estas personas no podrán negar ninguna de estas acciones (proceso de "no-repudio").

3. Registro (logs)

Es un proceso de autorización y asignación de permisos, que tiene como objetivo que cada usuario, tarea y fecha sea identificable y rastreable (pistas de auditoría) para permitir que cualquier acción de apertura, lectura, escritura, modificación o borrado de un documento quede registrada, así como su autor.

4. Data Loss Prevention (DLP)

Son aplicaciones que permiten registrar, monitorear y controlar los datos digitales en una infraestructura tecnológica de forma tal que cualquier tipo de acción realizada sobre la información quede registrada.

Estos softwares controlan si un archivo o documento puede ser accedido, así como las acciones que se pueden realizar sobre el mismo (abrir, copiar, enviar, etc.).

Los DLP pueden aplicarse sobre datos en reposo (dónde y cómo se almacenan), datos en movimiento (dónde y cómo se envían) y datos en uso (en el puesto de trabajo) pero estas aplicaciones no se podrán instalar ni administrar si no se conoce la información de la organización, para lo cual es necesario el proceso inicial de clasificación.

5. Antivirus, firewall e IDS

Herramientas capaces de detectar y bloquear en forma proactiva cualquier tipo de código dañino o tráfico anómalo dentro de una red.

6. Backup

Las copias de seguridad son la única solución cuando todos los demás controles han fallado y se han perdido o eliminado los documentos. Lamentablemente ni siquiera los backup pueden solucionar el hecho de que información confidencial sea hecha pública, caso en el cual, sólo habrá medidas de mitigación de daños e incidentes.

Quizás la protección de la información no es tan trivial como lo describe Jack Ryan pero sin dudas el proceso inicial no cambia: **la organización no debe pecar de negligencia** y para ello debe ser consciente del grado de criticidad de la información, porque si no nunca será capaz de protegerla e implementar controles adecuados para cada tipo de datos que maneja.