Cómo evitar la fuga de información en las organizaciones

26 de junio
2011

"¿Qué diablos es esa trampa para canarios?

Bueno, usted conoce el problema que tiene la CIA con las filtraciones de informaciones. Cuando estaba terminando el primer borrador del informe, se me ocurrió una idea para que cada informe fuese único. Cada sección tiene un sumario. Y cada sumario está redactado de una manera bastante dramática. Cada frase del sumario o acápite tiene seis versiones distintas, y la mezcla de esos párrafos es única en cada copia numerada del documento. Existen más de mil posibles versiones distintas, pero sólo noventa y seis ejemplares numerados del documento en sí. El motivo por el que los párrafos del sumario son sensacionalistas, es para permitir que un reportero los cite al pie de la letra en medios periodísticos. Si llegara a citar partes de dos o tres de esos párrafos, sabemos de inmediato cuál fue la copia que vio y, por lo tanto, dónde se produjo la filtración."

Autor: Lic. Cristian Borghello CISSP-MVP
Versión: 1.0 (20110626)
Descarga: www.segu-info.com.ar

Introducción

Así describe Jack Ryan, el legendario personaje de Tom Clancy en "Juegos de patriotas" [1], una trampa para descubrir filtraciones de documentos dentro de la CIA. Lamentablemente este tipo de trampa 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 cuarenta años, EE.UU. sufre su primera gran fuga de información clasificada, conocida como "los papeles del pentágono" (recientemente desclasificados) [2] en 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 [3], 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 solo se encontraban los datos de sus jugadores sino también sus tarjetas de crédito.

¿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 dicha clasificación, no se conocerá el valor de la información y, por lo tanto, no se podrá realizar un análisis costo beneficio y tampoco se podrá decidir que 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 (¿cuánto cuesta una base de datos de clientes?) y puede variar 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). Excepto para el ambiente militar, no hay un único método ni un manual maestro para llevar a cabo la clasificación de la información, ya que cada industria y negocio es único y particular.

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.

Tipos de controles

- **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:** controles que requieren mecanismos de *soft* y *hard*. Implican la restricción lógica de acceso a los sistemas y la protección de la información

Cada sistema y 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:

Marcas de agua: texto, 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 y dificultan la copia o duplicación. Estas marcas 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 identifica un documento en forma unívoca.

Firmado digital de documentos: 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, quien lo ha generado, quien lo ha enviado, cuando lo ha hecho y, además, estas personas no podrán negar ninguna de estas acciones (proceso de "no-repudio").

Registro (*logs)*: un proceso de autorización y asignación de permisos tiene como objetivo que cada usuario, tarea y fecha sea identificable y rastreable (pistas de auditoria) para permitir que cualquier acción de apertura, lectura, escritura, modificación o borrado de un documento quede registrado así como el autor de dicha acción.

Data Loss Prevention (DLP): 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 queda registrada. Estos software 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.

***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.

Referencias

[1] Juegos de patriotas - Tom Clancy -1987
http://es.wikipedia.org/wiki/Juegos_de_patriotas
[2] EE.UU. publica los Papeles del Pentágono sobre la guerra de Vietnam
http://bit.ly/lFwqZB
http://www.nytimes.com/2011/06/08/us/08pentagon.html
http://blogs.archives.gov/ndc/?p=138
[3] Entrevista a Daniel Ellsberg
http://bit.ly/j3rRYI