



Sobre el almacenamiento seguro y la confidencialidad en el tiempo

Desde el mes de octubre de 1992 en el que se promulgó la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, ya se establecía la obligación de proteger, mediante cifrado, los datos calificados como de nivel alto (salud, sexualidad, religión, etc.). A pesar de ello, son muy pocas las empresas e instituciones que, en todo este tiempo, han tomado alguna medida realmente eficaz para cifrar esos datos. Por otra parte, el sostenido incremento en el número de incidentes acaecidos en sistemas de información durante estos últimos quince años parece que está revitalizando, junto con las exigencias normativas, el tema de la protección eficaz y real de los datos que se almacenan y sobre los que se construyen todos los negocios e instituciones de la denominada Sociedad de la Información.

En la última década, la capacidad de almacenamiento y la demanda de éste han aumentado de forma espectacular. No sólo se han seguido leyes exponenciales en la capacidad de los discos duros y de los sistemas ópticos de almacenamiento, sino que además ha ido cambiando la misma forma de organizar éste. De los sistemas descentralizados basados en PCs más o menos interconectados en red, se han pasado a los sistemas esencialmente reticulares y cooperativos en los que los datos no pueden estar en cada PC sino en servidores generales de datos (SAN¹ y NAS²).

A estos cambios habría que unir la proliferación de sistemas de almacenamiento de datos (sistemas de salvaguarda y de respaldo) que no sólo no se encuentran dentro del perímetro físico de un ordenador, o de la habitación que lo contiene, o incluso del edificio que alberga a ésta, sino que están más allá de cualquier perímetro físico clásicamente definido. El reblandecimiento, el difuminado o incluso desaparición de los perímetros de seguridad hace que la protección de los datos ya no pueda ser física, sino que tenga que pasar a ser una protección lógica. Por si este hecho no fuese suficiente, también tenemos que re-

Las exigencias normativas y el creciente número de incidentes contra la confidencialidad e integridad de los datos revive el arte del cifrado como mecanismo de protección. Sin embargo, las diferentes ofertas del mercado no parecen ser suficientes, y se plantea la necesidad de nuevos y mucho más avanzados sistemas de Gestión de Claves para reconocer en su protección los diferentes matices que tienen las distintas informaciones.

cordar que más de dos terceras partes de los ataques los cometen agentes internos a la organización por lo que huelga hablar de perímetros. Está llegando el día en el que la única protección que se le podrá dar a los datos, a la información, al poder, será a través de su cifrado mediante sistemas criptográficos robustos.

Para poder entender lo que realmente está pasando es necesario darse cuenta

o el SFS o *Secure File System*⁵ de Peter Gutmann. Por ser el más reciente y por su impacto, quizás convenga mencionar el sistema *BitLocker Drive Encryption* que es el sistema por el que apuesta Microsoft en su Windows Vista y Windows 2008 Server, y que proporciona el cifrado de volúmenes completos. Por defecto, este sistema utiliza el AES en modo CBC con una clave de 128 bits combinada con un

el crecimiento de las capacidades de los equipos. Entonces, quizás la explicación del escaso avance del cifrado de los datos en su almacenamiento esté en que muchas de las soluciones anteriores son cifradores de volúmenes lógicos, de "unidades virtuales de disco" para entendernos; ésta es una solución óptima para proteger los equipos portátiles (PDAs, *smartphones*, PCs, memorias USB, portátiles, etc.) cuando los roban, ya que los datos que sustraen son inútiles sin la clave; pero, realmente, estas soluciones no protegen la información del ataque de "los de dentro", de los que tienen acceso autorizado a esos equipos.

Gestión de claves

El uso de técnicas de cifrado lleva indisolublemente asociado el problema de la Gestión de Claves. Cifrar la información equivale a concentrar toda la disponibilidad de ésta en la de la clave con la que se cifra, por lo que el cifrado sólo traslada la protección de toda la información a la protección de la clave que la cifra (mucho más pequeña y manejable). Además de esto, también hay que resolver cómo, cuándo y quién utiliza esa clave para descifrar los datos siempre que éstos son necesarios. El incorrecto uso de la clave y/o su custodia pone en riesgo la confidencialidad de todos los datos, y su pérdida acarrea que la información se pierda irremisiblemente. Quizás sea este último motivo, el miedo a perder la clave y perderlo todo, lo que frena la adopción de sistemas criptográficos para proteger la confidencialidad de los datos.

Los sistemas actuales y los productos que los implementan no resuelven el problema de dar a los datos la confidencialidad que necesitan cuando están almacenados dentro de los actuales sistemas de información, y ello se debe a que utilizan una Gestión de Claves primitiva o inexistente. Si el sistema a emplear no permite plasmar, de forma segura, los matices más sutiles de la confidencialidad de los datos, eso es que queda aún mucho por hacer. El problema tiene solución; lo que hace falta es conocer el problema y querer realmente encontrarla. ■

Los sistemas actuales y los productos que los implementan no resuelven el problema de dar a los datos la confidencialidad que necesitan cuando están almacenados dentro de los actuales sistemas de información, y ello se debe a que usan una Gestión de Claves primitiva o inexistente.

de que las tecnologías de cifrado de sistemas de almacenamiento no son nada nuevo; los hay que cifran la información antes de que sea almacenada en forma de fichero, mientras que otros están pensados más como *drivers* de dispositivo que se encargan de cifrar la información por debajo del sistema de ficheros y por encima del dispositivo físico.

Ya en 1993 se hablaba del *Cryptographic File System* (CFS³) de Mat Blaze, pero son varios los que han aparecido desde entonces. Algunos ejemplos son el *File Vault* de Apple que aparece en su MacOS 10.3. Este sistema trabaja sobre volúmenes lógicos que se montan y desmontan según esté o no conectado el usuario; la clave maestra de estos volúmenes es, a su vez, cifrada con la contraseña del usuario. Otro ejemplo es el EFS o *Encrypted File System* que ha venido formando parte de diferentes versiones de los Microsoft Windows (desde Win2000), el Ncryptfs, A Secure and Convenient Cryptographic File System⁴ de Charles P. Wright et al.,

"*Elephant diffuser*" diseñado por Microsoft "para mayor seguridad". Conviene resaltar que BitLocker no es una tecnología solo-software, sino que hace uso de los *chips* de seguridad TPM que serán incorporados en la mayoría de los PCs con el paso del tiempo. Los TPM⁶ son *chips* resistentes a manipulaciones que van montados sobre las placas madre de los equipos.

Con estos ejemplos vemos que en estos últimos quince años no han faltado soluciones para cifrar los datos a la hora de almacenarlos; sin embargo, la adopción de estas tecnologías parece haber sido tímida y quizás la explicación de ello sea que no son las adecuadas. Es cierto que cualquier proceso (criptográfico) suplementario supone extraer capacidades computacionales para emplearlas en cifrar y descifrar los datos, pero eligiendo bien la implementación y el cómo hacerlo, este "canon" no supera el 7-10%, por lo que el coste efectivo de la protección lógica de los datos es perfectamente asumible, visto

¹ Una Storage Area Network (SAN) es una arquitectura que enlaza a los ordenadores sistemas de almacenamiento como las granjas de discos, las librerías de cintas, y las gramolas de discos ópticos a servidores de tal manera que para los sistemas operativos de los terminales esos sistemas de almacenamiento aparecen como sistemas locales.

² Network-Attached Storage (NAS) es el nombre dado a una tecnología específica dedicada al almacenamiento que se conecta directamente a la red para proporcionar acceso centralizado a los datos por parte de terminales heterogéneos. Estos sistemas usan protocolos basados en ficheros tales como NSF o SMB/CIFS (p. e. Samba 1992) donde está claro que el almacenamiento es remoto y los usuarios solicitan trozos de ficheros y no bloques de disco.

³ Ver Matt Blaze: *A Cryptographic File System for Unix*. First ACM Conference on Communications and Computing Security, Fairfax, VA, November 3-5, 1993.

⁴ Ver <http://citeseer.ist.psu.edu/wright03ncryptfs.html>

⁵ Ver <http://www.cs.auckland.ac.nz/~pgut001/sfs/index.html>

⁶ Ver <https://www.trustedcomputinggroup.org/specs/TPM/>

JORGE DÁVILA MUÑOZ
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad
de Informática – UPM
jdavila@fi.upm.es