CySec News

2019 NOVIEMBRE

BORRADO SEGURO

INTRODUCCIÓN

Es importante definir ¿qué entendemos por borrado seguro de un archivo? el pensamiento de muchos es que con tan solo enviar a la papelera de reciclaje sus archivos éstos no se podrán recuperar, nada más alejado de la realidad, lo que sucede es que al eliminar un archivo de la forma habitual se elimina el acceso directo en el disco duro pero el archivo seguirá existiendo. Es fundamental que los datos que se desean eliminar sean efectivamente eliminados, y los medios de almacenamiento adecuadamente tratados antes de ser reutilizados.

Para hacer más difícil la tarea de recuperación debemos sobrescribir el espacio físico que utiliza el archivo en la unidad que lo almacena, la efectividad de este método dependerá de la cantidad de veces que se realice el proceso y los algoritmos utilizados, existen numerosas herramientas para realizarlo.

DESARROLLO

Borrado seguro o sanitización de datos, de acuerdo con el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), se refiere a un proceso que impide el acceso a la información sobre los medios para un determinado nivel de esfuerzo, es decir, que los datos no se recuperen fácilmente.

Riesgos de no realizar el borrado seguro de los datos Cuando la información no es eliminada de forma segura, sobre todo la información crítica para el negocio, ésta podría aparecer de fuera del alcance de la organización e inapropiadamente, impactando sobre:

Activo de información	Riesgo
Datos personales de los clientes o colaboradores de la organización.	• Fuga de datos personales • Ser sujeto de infracciones por no incumplimiento de la Ley de protección de datos personales (Ley 29733) • Pueden ser utilizados para cometer fraude o suplantar la identidad.
Datos críticos de la organización	• Podrían ser recuperados y usados por adversarios o la competencia.
Obra intelectual (obras literarias, películas, música, obras artísticas, entre otros)	• Puede ser afectada, derivando en pérdida de reputación y/o ingresos. • Daño de la imagen corporativa.

ESTÁNDARES DE BORRADO

- **Reino Unido**: Her Majesty's Government (HMG) Infosec Stardard 5 (IS5)
- **Europa**: EN15713.
- **Alemania**: DIN-66399.
- **USA**: NIST-800-88

ALGORITMOS Y MÉTODOS DE BORRADO SEGURO

Algunos algoritmos de borrado seguro son:

- **Grado 1. Super Fast Zero Write:** sobreescritura del soporte con un valor fijo (0x00) en cada tercer sector. Nivel de seguridad bajo.
- **Grado 4. Random Write:** Sobreescritura del soporte con valores aleatorios. Su fiabilidad aumenta con el número de pasadas. Nivel de seguridad medio.
- **Grado 12. North Atlantic Treaty Organization:** Estándar de borrado de la OTAN (North Atlantic Treaty Organization). Sobrescribe el soporte siete veces. Las primeras seis pasadas son de sobreescritura con valores fijos alternativos entre cada pasada (0x00) y (0xff). La séptima pasada sobrescribe con un valor aleatorio. Nivel de seguridad alto.

- **Grado 14. US Department of Defense (DoD 5220.22-M) + Gutmann Method:** Método de alta seguridad consistente en 35 pasadas, complementable con iteraciones de Mersenne, para agilizar los procesos de borrado seguro mediante la generación de números pseudoaleatorios. Combina el Grado 13 y el 10. Nivel de seguridad muy alto.
- **Secure Erase:** Secure Erase es el nombre dado a un conjunto de comandos disponibles desde el firmware en discos duros basados en PATA y SATA.

Existen **métodos** más sofisticados para recuperación de información, al grado de que ya no es recomendable únicamente la sobreescritura en los discos magnéticos (aunque en la práctica es mejor siempre hacerlo).

- **Desmagnetizadoras:** Durante el proceso de desmagnetizado, los medios de almacenaje son irradiados con un potente campo magnético que supera su resistencia magnética, la coercitividad del disco duro. Las pulsaciones cortas e intensas borran para siempre los datos del disco duro.
- **Destructoras de discos:** Rompen los discos en piezas diminutas en poco tiempo algunas utilizan el nivel de seguridad H5 conforme a DIN 66399. La destrucción del disco se lleva a cabo de manera segura y económica, con posibilidad de inspeccionar visualmente el proceso de manera muy sencilla para asegurarse que se ha completado con éxito.

CONCLUSIONES

- Toda información sensible tiene que ser borrada de forma segura.
- Evita desechar un medio de almacenamiento sin antes borrar de forma segura su contenido.
- Todo archivo borrado siempre estará almacenado en el medio de almacenamiento físico, algunos algoritmos hacen casi irrecuperables los archivos, pero nunca se puede asegurar al 100%.
- El único método seguro al 100% para eliminar datos es destruir el medio de almacenamiento

FUENTE DE REFERENCIA

- https://www.semshred.com/resources/din-standards/din-standard-66399-hard-drives/#H-2
- https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/
- https://underc0de.org/foro/seguridad/t29314/
- http://joaquin.medina.name/web2008/documentos/informatica/herramientas/BorradoSeguro/BorradoSeguro.html
- https://www.lifewire.com/dod-5220-22-m-2625856
- https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media
- http://inicio.ifai.org.mx/DocumentosdeInteres/Guia_Borrado_Seguro_DP.pdf
- https://www.bsia.co.uk/Portals/4/Publications/204-id-en15713-guide.pdf

Contribuidora

Patricia Núñez Luque, Ing. de sistemas de la Universidad Nacional de San Agustín, con más de 10 años de experiencia en TI, actualmente labora como especialista en seguridad de la Información en el sector estatal.

LinkedIn: https://www.linkedin.com/in/patricia-nu%C3%B1ez-luque/

Recursos LCW

LinkedIn	https://www.linkedin.com/company/cysecbywomen/
Facebook	https://www.facebook.com/CySecByWomen/
Twitter	@cysecbywomen