blancco
CERTIFIED DATA ERASURE

Administrar un Proceso de Borrado de Datos dentro de una Organización

UN PROCESO AUTOMATIZADO PARA UNA EFICIENCIA OPTIMA

Blancco White Paper

Publicado 16 Octubre 2012

Introducción

Los directores de información (CIO), directores de seguridad corporativa (CSO) y los directores de tecnología de la información (TI) se enfrentan a una serie de preocupaciones que hacen que su trabajo sea aún más complejo. Encargados de gestionar las operaciones informáticas de la empresa, estos ejecutivos y administradores ayudan a mantener algunos de los elementos más críticos y relevantes de una empresa o entidad gubernamental.

La reducción del personal y los presupuestos más ajustados son sólo algunos de los elementos exigentes con los que se encuentra la administración de TI. Cumplir con los objetivos y benchmarks existentes a la vez que se opera de forma eficiente y rentable con menos recursos y menos dinero ha creado una situación en la que los CIO y sus departamentos de TI deben abordar un nivel de desafíos sin precedentes.

Una parte importante de cualquier política de TI para estos grupos incluye la habilidad de emplear y gestionar una política de seguridad sólida y probada. Un aspecto clave de esta política incluye definir e implementar los procesos de borrado de datos para el equipo de TI que está previsto reutilizar, donar o desechar definitivamente. Esto incluye implementar una solución que detecta una serie de hardware que abarca desde smartphones hasta servidores de alta gama, y aborda la gestión diaria de borrado de datos, así como las necesidades de borrado del ciclo de vida útil de un activo. Este enfoque también debe incluir el seguimiento y la creación de informes de lo que se ha borrado, así como dejar constancia de quién ha realizado el borrado.

Mientras que el borrado de datos es una buena práctica esencial a la hora de mantener una buena seguridad de datos, los directores de TI siguen luchando a diario con presupuestos y recursos reducidos. Para ayudar a implementar el borrado de datos de forma eficiente y efectiva, las soluciones avanzadas de borrado de datos con gestión centralizada ofrecen una forma rápida, automatizada y segura de proteger los datos mientras ayudan a reducir los costes asociados y los recursos necesarios. Las funciones automatizadas agilizan el borrado y permiten personalizar los procesos de borrado y creación de informes para cumplir con las necesidades más perentorias de una organización.

Indicé

Introducción....2

Amenazas por una eliminación incorrecta de los equipos informáticos....4

Pros y contras de las tecnologías de protección de datos 5

Desafíos actuales en la gestión de seguridad de datos....6

Más normativasque las empresas deben cumplir.... 6

Iniciativas en ee. Uu.... 6

Directiva de protección de datos de la ue.... 6

Proceso de borrado completamente auditable.... 7

Byod ha llegado para quedarse 7

La importancia de gestionar el borrado durante toda la vida útil del activo 9

Protección de datos durantela fase de retirada 9

Identificación de datos en sistemas activos 9

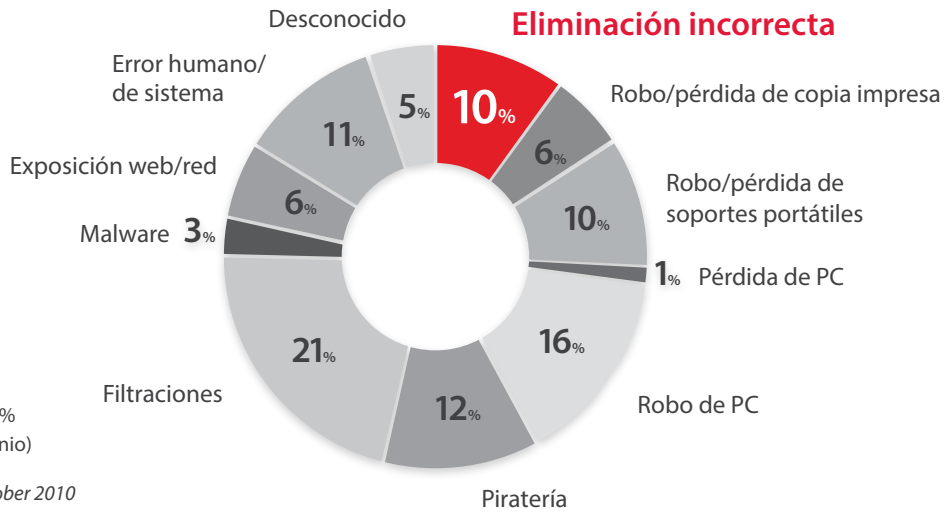
La importancia del borrado in-situ 10

Beneficios de una solución de borrado de datos certificada y orientada a procesos....10

Gestión del proceso 11

Conclusión....12

Referencias....13



Por causa:
número de incidencias como %
del total para 2010 (enero - junio)

Bron: KPMG International, October 2010

Amenazas por una eliminación incorrecta de los equipos informáticos

A menudo, las empresas asocian la amenaza de perder datos con el robo de portátiles u otros soportes portátiles, muchas no son conscientes de que existe un culpable mucho más sutil: una eliminación incorrecta de sus propios activos de TI. De hecho, según un informe de 2010 de KPMG International,[1] en un 10 % de los casos la pérdida de datos se debe a una eliminación insegura de los activos de TI. Esto conlleva graves implicaciones para la reputación de la empresa y costosas multas impuestas por las normativas de protección de datos cada vez más estrictas. Algunos informes indican que alrededor de un 40 por ciento de los discos duros llegan al mercado de segunda mano con información confidencial, incluido un estudio de 2009 de Kessler International.[2]

El borrado de datos ofrece un enfoque basado en software para sobrescribir y eliminar por completo toda la información electrónica, mucha de la cual es sensible o confidencial, almacenada en un disco duro o en otro soporte digital para eliminar o reutilizar. Esta limpieza o eliminación de datos va más allá de los comandos básicos de eliminación de archivos, que sólo eliminan indicadores directos de sectores del disco y permiten la recuperación de datos con herramientas comunes de software. Sin embargo, en el caso del borrado de datos, se elimina toda la información y el disco permanece operativo. Los informes de borrado contienen especificaciones detalladas del hardware y se proporcionan como prueba de la eliminación de datos.

PROS Y CONTRAS DE LAS TECNOLOGÍAS DE PROTECCIÓN DE DATOS

Existen muchas tecnologías de destrucción y protección de datos como la destrucción física de dispositivos, la desmagnetización, la encriptación, el reformateo y otros métodos de software menos completos, pero todos cuentan con desventajas. La destrucción física y la desmagnetización por ejemplo, hacen que el disco quede no operativo y esto impide que se pueda recuperar parte de su valor mediante la reventa o reutilización, además se reduce la capacidad de funcionar de forma sostenible y respetuosa con el medio ambiente. Asimismo, con la destrucción física la recuperación de datos de medios digitales fragmentados sigue siendo posible. Y, dado que se necesitan equipos caros para la destrucción de discos duros, esta actividad normalmente se subcontrata, aumentando así el riesgo de pérdida de datos durante el transporte a las instalaciones de terceros.

Otras estrategias de protección de datos también presentan desventajas. Por ejemplo, la encriptación basada en software puede ser eficaz en algunos casos pero consume mucho tiempo y supone una operación intensiva del procesador y no proporciona un método seguro y verificable para asegurar los datos, especialmente en equipos inactivos. El saneamiento criptográfico al final de la vida útil no ofrece un mecanismo de verificación y esto aumenta los peligros de que se realice una implantación pobre e impide contar con un seguimiento de auditoría visible. A menos que se actualicen continuamente, tanto los sistemas activos como inactivos que emplean encriptación están sometidos a ataques, dejando así datos disponibles para aquellos capaces de descubrir la clave, descifrar la encriptación o aprovechar los puntos débiles de la implementación.

> *La gestión de borrado de datos con tecnología de borrado avanzada es la mejor forma de deshacerse de dispositivos con información confidencial.*

De forma similar, el reformateo de un disco sigue dejando datos intactos, mientras que la tecnología de sobreescritura menos avanzada puede no realizar suficientes pases de sobreescritura o no proporcionar los informes de borrado necesarios para cumplir con las obligaciones normativas. Por ejemplo, la sobreescritura de freeware no proporciona un informe detallado y auditado y la eficacia del software no se verifica de forma independiente.

Por otro lado, la gestión de borrado de datos con tecnología de borrado avanzada es la mejor forma de deshacerse de dispositivos con información confidencial. Al automatizar la eliminación completa de datos con tecnología que ofrece prueba mediante un informe detallado, las empresas se aseguran de que los datos están protegidos, sin afectar a la productividad de los recursos ni a las operaciones globales.

Desafíos actuales en la gestión de seguridad de datos.

Al parecer, las empresas de TI se enfrentan a diario a una lista creciente de desafíos. Mientras se les exige que hagan más con menos, debido al recorte de presupuestos y las limitaciones de personal, sus redes continúan presenciando una cantidad creciente de tráfico procedente de una base de usuarios cada vez más sofisticada.

Según un estudio de 2011 EMC/IDC Digital Universe,[3] de 2005 a 2010, el volumen de datos digitales que pasan por todo tipo de redes ha aumentado casi 10 veces, y no hay signos de que el tráfico vaya a disminuir. Las cifras se duplicaron entre 2010 y 2012 y todo apunta a que volverán a hacerlo en 2015.

> *Los requisitos legislativos y regulatorios existentes sobre protección de datos suponen a las empresas nuevas exigencias que deben cumplirse.*

MÁS NORMATIVASQUE LAS EMPRESAS DEBEN CUMPLIR

En todo el mundo ha aparecido un número de estándares y normativas estrictas específicas de la industria con el fin de reducir el riesgo de exposición de datos confidenciales, incluidas normas relativas a la información sanitaria, financiera y crediticia. Las normativas actuales que exigen específicamente la eliminación de datos son: la Health Insurance Portability and Accountability Act (HIPAA), la Fair and Accurate Credit Transactions Act of 2003 (FACTA), la Payment Card Industry Data Security Standard (PCI DSS), así como la UK Data Protection Act 1998. Asimismo, se están revisando normativas exhaustivas que requieren la eliminación de datos en EE. UU. con la Consumer Privacy Bill of Rights y en Europa con la legislación de la UE sobre la reforma de protección de datos.

INICIATIVAS EN EE. UU.

Los requisitos legislativos y regulatorios existentes sobre protección de datos suponen a las empresas nuevas exigencias que deben cumplirse. En febrero de 2012 el presidente Obama de Estados Unidos publicó un marco para proteger la privacidad y promover la innovación en la economía digital global. Aunque el informe iba destinado a tratar la privacidad de los datos del consumidor, se ponen de manifiesto las tendencias, cuestiones y preocupaciones que afrontan los datos digitales a gran escala.

El informe apunta cómo el marco anterior carecía de una exposición clara de los principios básicos de privacidad que afectan al mundo comercial, así como de un compromiso continuo de todos los interesados para abordar los asuntos de privacidad de datos del consumidor que surgen de los avances en tecnología y modelos de negocio.

Para tratar estos asuntos, la Administración de Obama introdujo la Consumer Privacy Bill of Rights,[4] que abarca un modelo dinámico sobre cómo permitir la innovación actual en las nuevas tecnologías de la información, al mismo tiempo que se ofrece una fuerte protección de la privacidad, incluido el requisito de eliminación de datos. Este nuevo marco fue diseñado para proporcionar una buena definición de los principios básicos de privacidad aplicables al mundo comercial y un compromiso continuo de todos los involucrados para tratar los problemas de la privacidad de datos del consumidor que surgen de los avances en tecnología y modelos de negocio.

DIRECTIVA DE PROTECCIÓN DE DATOS DE LA UE

Mientras tanto, en Europa, los cambios en la protección de datos se han propuesto no sólo para revisar las normas establecidas en 1995, sino para ofrecer más coherencia en la implementación de la legislación actual. Los avances tecnológicos como la introducción de las redes sociales, la computación en nube, los servicios basados en la localización y las tarjetas inteligentes han servido como impulso para actualizar la legislación

de protección de datos de la UE.[5] Existe un borrador con estas actualizaciones que está siendo revisado por los estados miembro de la UE. Dicho borrador contiene los requisitos para la eliminación de datos en línea y el uso de procesos de auditoría para las empresas que tratan datos personales. Además, anima a las empresas a utilizar procesos y herramientas certificados.

Asimismo, se prevé que las sanciones por violación de los nuevos requisitos de la UE alcancen desde 250.000 euros hasta el 0,5 % de la facturación anual total para las infracciones de menor grado y de 1 millón de euros hasta el 2 % de la facturación para infracciones más graves. Las empresas que ofrecen servicios en nube deben cumplir con esta legislación si procesan datos de ciudadanos de la UE, independientemente de dónde se encuentren sus servidores.

Además del rápido aumento en la legislación de protección de datos y en los estándares de la industria, la fragmentación y la gama cada vez mayor de dispositivos y plataformas que se utilizan para almacenar datos hace que los departamentos de TI tengan que gestionar la seguridad en equipos cada vez más diversos. Las estaciones de trabajo y los portátiles, los servidores y dispositivos de almacenamiento, dispositivos móviles como smartphones, máquinas virtuales y equipos con complejos centros de datos son sólo algunos de los muchos tipos de activos de TI que contienen información potencialmente sensible. Con la gran cantidad de información confidencial, las organizaciones deben estar preparadas, desde el punto de vista legal, moral y fiduciario, a borrar datos de diferentes tipos de dispositivos.

PROCESO DE BORRADO COMPLETAMENTE AUDITABLE

A fines de auditoría, un borrado con éxito no es suficiente, es necesario que exista además la prueba de dicho borrado. Es obligatorio que exista una prueba detallada y auditable para cumplir con los requisitos de conformidad, regulación y legalidad. Una auditoría exhaustiva también proporciona documentación importante sobre el ciclo de vida útil de un activo.

Los informes verificables y protegidos contra una manipulación no autorizada son esenciales para cumplir con los requisitos de conformidad, regulación y auditorías legales. Una solución de borrado de datos debe generar informes exhaustivos que proporcionen información crítica para el proceso de auditoría. Esta información debe contener el estado del hardware, los números de serie y las etiquetas de los activos relevantes, los detalles del software para la recolección de licencias, el método de borrado utilizado y el nombre de la persona que realizó el borrado.

Las empresas que ofrecen servicios en nube deben cumplir con esta legislación si procesan datos de ciudadanos de la UE, independientemente de dónde se encuentren sus servidores.

BYOD HA LLEGADO PARA QUEDARSE

Las organizaciones también deben afrontar los desafíos asociados con "Trae tu propio dispositivo" (BYOD). Con más de 150 millones de dispositivos apropiados por empleados y que utilizan en el lugar de trabajo[6], un informe reciente de Juniper Research indica que BYOD ha llegado para quedarse, especialmente cuando el número de smartphones en la empresa podría alcanzar los 350 millones en 2014.[7]

A pesar de su reducido tamaño, los dispositivos móviles contienen una gran cantidad de datos, algunos smartphones y tabletas cuentan con una memoria interna de 64 GB. Estos dispositivos ricos en memoria y cada vez más inteligentes ayudan a la gente a ser más productivos tanto en las tareas personales como profesionales pero pueden contener correos, datos de clientes, contraseñas y otra información sensible que podría ocasionar pérdidas de datos si se desechan sin haber borrado la información antes. Una encuesta de 2009 indica que el 99 % de la gente utiliza sus móviles para algún tipo de uso profesional. El setenta y siete por ciento de los encuestados utilizaban sus móviles para guardar nombres y direc-

ciones de contactos profesionales, el 23 % almacenaba datos de clientes y el 17 % descargaba información corporativa como documentos y hojas de cálculo.[8]

Las amenazas de pérdida de datos de los dispositivos móviles como smartphones y tabletas se asocian a menudo al malware, phishing y a los ataques de spyware, sin embargo, el deshacerse de forma incorrecta de estos dispositivos puede suponer un problema de seguridad aún mayor. Los organismos gubernamentales como por ejemplo la European Network and Information Security Agency (ENISA) consideran que el deshacerse inadecuadamente de smartphones sin haber eliminado por completo toda la información supone uno de los mayores riesgos en seguridad de la información. Además, dichos dispositivos no se someten a muchos de los actuales procesos de borrado para los discos duros usados.[9] Esto es especialmente preocupante si tenemos en cuenta que las predicciones de los analistas son que más de 100 millones de móviles al año no se reciclan.[10]

No basta con restaurar los valores de fábrica para asegurar los datos, ya que pueden recuperarse con herramientas fáciles de conseguir. Para mantener una política de seguridad sólida de dispositivos móviles y proteger la pérdida de datos, las empresas deben implementar una gestión de borrado de datos que cuente con tecnología avanzada y que ofrezca una prueba verificable del borrado de datos, o encontrar un socio reconocido de la industria de eliminación de activos (ITAD) que utilice ese proceso. Respaldados por el conocimiento y la tecnología adecuada o por el proveedor de tecnología, los directores de TI pueden personalizar sus políticas para los dispositivos empresariales y para los móviles en manos de sus empleados.

La importancia de gestionar el borrado durante toda la vida útil del activo

Los clientes y empleados dependen de la seguridad de la información personal y profesional. Si a la hora de eliminar un activo de TI o un dispositivo de almacenamiento la información se borra de forma inadecuada, puede suponer no solo daños a la marca e imagen de la empresa, sino que podría conllevar la disminución de la cotización de las acciones, la pérdida de clientes y socios, así como una prensa negativa. El deshacerse sin cuidado de un disco duro que contenga información confidencial que no haya sido borrada, puede resultar fácilmente en el robo de identidad y puede exponer a una empresa a una publicidad negativa y a costosos litigios. También puede afectar a la rotación del personal, a las operaciones diarias del negocio y a la seguridad interna de la información.

Existen otros ejemplos donde el borrado de datos es importante. Una aplicación o software del sistema que permanece en un disco duro cuando el activo cambia de manos podría violar los términos de licencia del desarrollador del software. Además, la reubicación de un servidor a otro departamento o división puede infringir una licencia de software y puede resultar en costosas multas por parte del proveedor.

PROTECCIÓN DE DATOS DURANTELA FASE DE RETIRADA

Es evidente que la seguridad de la información es una práctica que las organizaciones asumen para proteger la información durante toda la vida útil de un activo. Custodiar esta información confidencial durante la fase de retirada de un activo o cuando un ordenador se reasigna internamente es igualmente importante, pero a menudo se pasa por alto. Dado que encontramos grandes cantidades de información confidencial almacenada en estos activos, los datos deben destruirse por completo antes de que los activos de TI se eliminen, reciclen, reutilicen o se donen.

Utilizando una estrategia de borrado de datos, podrá revender o donar sus activos sin tener que preocuparse por la información sensible almacenada en los dispositivos. La destrucción física también se hace más viable cuando se combina con el borrado de datos, ya que se alcanza un mayor grado de confianza y seguridad. Esto garantiza la protección de datos en caso de que el proceso de destrucción física se realice sin éxito o los avances tecnológicos permitan de alguna manera extraer datos de los fragmentos de los dispositivos.

IDENTIFICACIÓN DE DATOS EN SISTEMAS ACTIVOS

El borrado de datos no es tan solo una actividad de final de vida útil, sino que puede ser necesario en las fases iniciales de la utilización de un activo, por ejemplo, si existe información confidencial temporal que ya no se necesita. Las herramientas avanzadas de borrado de datos pueden identificar el borrado o el saneamiento de archivos y carpetas individuales en sistemas activos. Este proceso de borrado identificado es ideal para eliminar datos temporalmente confidenciales como información de tarjetas de crédito, información de clientes y documentos propiedad de la empresa. Al automatizar la destrucción de datos en un momento o caso determinado, el borrado avanzado asegura la información en servidores activos locales o remotos y en ordenadores, así como en cualquier archivo seleccionado que esté disponible en el sistema, facilitando así la destrucción de datos diaria.

Además, muchas empresas utilizan configuraciones de centros de datos complejas y costosas como las unidades lógicas (LUN) y matrices de almacenamiento. Estos equipos y configuraciones se utilizan, administran y

ejecutan de forma diferente a los ordenadores y portátiles, de forma que el borrado tiene la capacidad de afectar a las funciones esenciales del negocio. Es difícil deshacerse o apagar servidores o matrices de almacenamiento que ejecutan aplicaciones con funciones críticas sin llevar a cabo procesos costosos y largos para volver a activarlos. Por eso, una herramienta avanzada de borrado que pueda identificar datos específicos, LUN o matrices de almacenamiento en sistemas activos es una necesidad.

LA IMPORTANCIA DEL BORRADO IN-SITU

Si la eliminación de activos va a realizarse por un tercero, es importante que la empresa elija un proveedor que utilice procesos de borrado seguros con informes completos. Sin embargo, el borrado de datos in-situ es la opción más segura porque garantiza que los datos confidenciales no salen de la empresa, o incluso que no salen de una oficina en particular. La Asociación Internacional de Directores de Activos de TI (IAITAM)[11] recomienda como mejor práctica un enfoque combinado, utilizando el borrado in-situ antes de transferir la eliminación de activos a terceros y a proveedores de borrado.

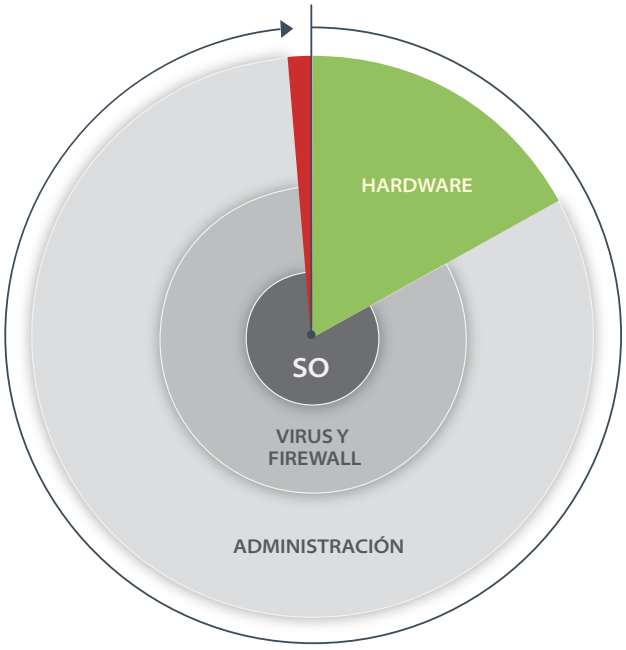
Las estrictas normativas de la industria, los costes monetarios, los posibles daños a la reputación de la empresa por pérdida de datos y el riesgo de fuga de datos destacan la importancia de asegurarse de que se toman los pasos adecuados para garantizar la eliminación completa y segura de información sensible. Si no se toman las medidas oportunas, una organización puede tener que afrontar multas que oscilan desde miles de dólares hasta 1 millón de dólares por infracción,[12] además del riesgo de exponer a los empleados a posibles penas de prisión en ciertas situaciones.

Beneficios de una solución de borrado de datos certificada y orientada a procesos

Aunque el borrado de datos permite a las organizaciones adoptar los pasos necesarios para la eliminación de activos digitales, es esencial trabajar con soluciones que cuenten con aprobaciones nacionales e internacionales, certificaciones y recomendaciones.

Al elegir un software certificado que permita resultados consistentes y fiables y proporcionar una auditoría clara con informes, las empresas, los gobiernos y otras entidades ganan tranquilidad y confianza. Por ejemplo, la certificación internacionalmente reconocida de Common Criteria verifica que el software de borrado de datos ha cumplido con un riguroso e independiente proceso de pruebas que valida su capacidad para borrar datos de forma permanente de discos duros y otros dispositivos de almacenamiento. Asimismo, verifica que el software cumple con los estándares aprobados por la Organización Internacional de Normalización (ISO-IEC 15408).

Además, el utilizar una solución de borrado de datos orientada a procesos, gestionada centralmente y automatizada puede mejorar la productividad y la eficiencia. Un proceso así reduce el error humano mediante seguimiento y auditoría centralizados, entrada de datos manual mínima, entrada automática de datos relativos al hardware y al informe de borrado y, una entrega de informes basada en red que puede agilizar los procesos de auditoría con fines reglamentarios. Además del borrado de datos y la creación de informes, este proceso puede realizar una amplia serie de pruebas de hardware tanto en modo manual como en modo automático, ofreciendo así la información necesaria para reutilizar o recomercia-



Coste del borrado de datos

lizar activos de TI. Con una solución de borrado como esta, también es posible procesar más activos en menos tiempo en comparación con los métodos de eliminación tradicionales o con herramientas de borrados menos robustas y avanzadas. La solución puede personalizarse según las necesidades específicas de una organización y según los entornos de hardware y redes.

GESTIÓN DEL PROCESO

Una gestión en línea completa y centralizada para automatizar el borrado de datos cubre todas las fases del proceso; desde el arranque pasando por el envío del informe a la base de datos hasta terminar el proceso con un certificado de finalización y el apagado del ordenador. Una consola de administración intuitiva ofrece además control de borrado remoto con seguimiento del estado, completa automatización con el mínimo esfuerzo por parte del usuario, así como completos informes y estadísticas del borrado de datos. Estas funciones suponen un aumento en la productividad del 25 al 30 por ciento en comparación con otros métodos. Por ejemplo, con un proceso de borrado avanzado, el personal de TI puede realizar simultáneamente el borrado de hasta 200 discos duros por servidor. Al mismo tiempo, también pueden controlar remotamente el borrado de diferentes tipos de activos de TI.

El rendimiento ganado al centralizar y automatizar el proceso de borrado de datos contribuye a una menor inversión global del software. Teniendo en cuenta los riesgos y las posibles multas por pérdida de datos, el precio de un proceso de borrado de datos bien administrado es mínimo si se compara con el coste total del activo, incluidos los costes de hardware, software, firewall y protección de virus.

Utilizar una solución de borrado de datos orientada a procesos, gestionada centralmente y automatizada puede mejorar la productividad y la eficiencia.

La integración perfecta de una solución de borrado de datos utilizando la infraestructura de TI existente también es crucial desde el punto de vista operativo y económico. Esto incluye la capacidad de trabajar con otros paquetes de gestión de activos de TI y ERP, llevar a cabo la simple importación y exportación de datos y utilizar interfaces de servicios web.

Conclusión

El boom sobre la seguridad de los datos y las normativas de privacidad, el riesgo actual de perder datos y los elevados costes asociados con la pérdida de éstos, no dejan duda de que es necesario tomar medidas para garantizar la eliminación segura y completa de la información sensible. En muchos casos, los fallos de seguridad no se deben a hackers u a otras actividades encubiertas, sino que los estudios demuestran que la eliminación insegura de los activos de TI es en un 10 por ciento de los casos[12] la causa de pérdida de datos.

En el futuro, los activos de TI de una organización seguirán alojando grandes cantidades de información confidencial, por ello, es imperativo proteger los datos mediante un borrado exhaustivo. Los datos deben destruirse por completo antes de que los activos de TI se eliminen, reciclen, reutilicen o se donen. Además, en muchos casos las corporaciones se ven obligadas por los estándares y las normativas gubernamentales y de la industria a garantizar la eliminación segura de información sensible o, de lo contrario, se enfrentan a multas por incumplimiento.

Una solución de borrado de datos avanzada y centralizada ofrece a los usuarios un proceso rápido, automatizado y seguro que ahorra tiempo y dinero a la vez que garantiza la protección de datos confidenciales.

El borrado de datos utiliza un enfoque basado en software para sobrescribir y destruir toda la información electrónica de un disco duro o de otro medio digital a la vez que deja el disco operativo. Las herramientas avanzadas de borrado pueden incluso identificar datos confidenciales en sistemas activos. Por ello, la decisión de adquirir un software de borrado de datos no debe tomarse únicamente al final de la vida útil de un activo, sino que debería tenerse en cuenta al inicio de la utilización del activo.

Por último, mencionar que una solución de borrado de datos avanzada y centralizada ofrece a los usuarios un proceso rápido, automatizado y seguro que ahorra tiempo y dinero mientras garantiza la protección de datos sensible. Con las funciones de borrado automatizado de datos, los departamentos de TI obtienen el enfoque más rápido y personalizado, con un proceso de borrado, creación de informes y auditoría mejorado y agilizado.

Referencias

[1] KPMG International, "Data Loss Barometer –Insights into Lost and Stolen Information in 2010," Issue 3, 2010

[2] Kessler International, "Is Your Confidential Information Being Sold on eBay?", February 2009, http://www.investigation.com/press/press75.htm

[3] IDC, sponsored by EMC Corporation, "Extracting Value from Chaos," June 2011, http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf

[4] Obama Administration, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

[5] European Commission, January 2012, http://ec.europa.eu/justice/data-protection/index_en.htm

[6] MaaSters Blog, "Enterprise Mobility Update: 350 Million BYOD Smartphones by 2014," August 2012, http://www.maas360.com/maasters/blog/businessintelligence/ enterprise-mobility-350-million-byod-smartphones-2014/

[7] Juniper Research, August 2012, http://www.juniperresearch.com/viewpressrelease.php?pr=330

[8] *Government Technology*, "4.2 Million Cell Phone Users Leave Sensitive Data Unprotected," March 2009, http://www.govtech.com/security/42-Million-Cell-Phone.html

[9] ENISA, "Smartphones: Information Security Risks, Opportunities and Recommendations for Users," December 2010, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks/top-ten-smartphone-risks

[10] ABI Research, "Recycled Handset Shipments to Exceed 100 Million Units in 2012," December 2007, http://www.abiresearch.com/press/1015-Recycled+Handset+Shipments+to+Exceed+100+Million+Units+in+2012

[11] http://www.iaitam.org/

[12] *Dark Reading*, "$1.5M Fine Marks A New Era In HITECH Enforcement," March 2012, http://www.darkreading.com/database-security/167901020/security/vulnerabilities/232700031/1-5m-fine-marks-a-new-era-in-hitech-enforcement.html

---

C. Anabel Segura 7, 28108 Alcobendas, Madrid
900 112 012, www.ontrackdatarecovery.es