



Mantener a salvo los secretos empresariales

Con el entorno tecnológico e interactivo en el que trabajamos actualmente, utilizamos sistemas y herramientas informáticas para gestionar todos nuestros procesos e informaciones. Y, al mismo tiempo que invertimos en novedosas aplicaciones en red, también asumimos más riesgos al tener que controlar la difusión de un mayor volumen de datos. Pero ¿de qué riesgos hablamos? Fundamentalmente de seguridad y protección de nuestros archivos y documentos; por eso tenemos que mantener la confidencialidad, integridad y disponibilidad de la información.

Los principales problemas de seguridad en entornos empresariales van más allá del conocido incremento del "malware" (spam, virus, hackers y un largo etcétera). En general, hablamos de un sistema de trabajo digital, interactivo y simultáneo que saca a la luz los puntos débiles de las compañías desde el punto de vista de la seguridad. Cada vez, son más las herramientas de colaboración que utilizamos diariamente en nuestro trabajo, como el correo electrónico, portales de Internet, USB, ordenadores portátiles o móviles, con las que intercambiamos mucha información confidencial sin poder controlarla una vez que la recibe el destinatario.

En cualquier empresa existe riesgo de una fuga de datos pero en entidades públicas, financieras, industriales y sanitarias son especialmente peligrosas. Sin embargo, la mayoría de ellas no tiene integrada en su cultura corporativa la protección de sus datos como elemento central en sus políticas de gestión, administración y comunicación.

¿Qué debemos proteger?

En este contexto, sabemos que existen determinadas aplicaciones que pueden ser más proclives a problemas de pérdidas de información sensible: el correo electrónico (medio más usual de intercambio de información entre usuarios) y portales de contenidos (muy utilizado para almacenar y acceder a la documentación de las empresas). En ambos casos, la probabilidad de fuga de información es alta al ser tan fácil reenviar o guardar información.

Pero tenemos que hablar además de algunas herramientas, en alza sobre todo en las medianas y grandes empresas, que requieren de un mayor control por nuestra parte. Hablamos de aplicaciones que pueden utilizarse por terceros para acceder a datos confidenciales o de acceso restringido sin que el usuario sea consciente. Se trata de "programas espía" que se convierten en una ruta hacia documentos o archivos sensibles de nuestra empresa; una ruta a la que pueden acceder personas ajenas a la compañía. El chat, cada vez más utilizado en entornos profesionales, es una de esas herramientas.

Este tipo de aplicaciones, de uso compartido, son las que revisten un mayor riesgo junto a los programas de captura de pantallas. En sólo unos segundos, una transacción financiera o la imagen de un nuevo producto pueden ser capturadas y dejar de ser confidenciales.

Pero el mayor problema en seguridad empresarial, no son los accesos sino la difusión de información. ¿Nos hemos planteado la posibilidad de que nuestros archivos puedan llegar a manos de la competencia? Pues no es sólo una posibilidad sino un riesgo real. Cuando intercambiamos documentos a través de Internet podemos llegar a perder el control sobre ellos sin saber a quién le podrá llegar y el uso que hará del contenido recibido. Especialmente importantes son los casos en los que trabajamos con datos privados y personales como historiales de pacientes, contactos de clientes o números de cuentas bancarias. Todos no están autorizados para acceder a ellos pero, si no contamos con las medidas de seguridad necesarias, todos podrán hacerlo.

¿Cuáles son las consecuencias?

Si nuestra empresa no cuenta con un sistema de protección que asegure la confidencialidad y la privacidad cuando difunde datos ya sea a través de un PC, un dispositivo móvil o en un USB, las consecuencias no sólo económicas sino en términos de imagen y reputación son importantes. Pensemos simplemente en la confianza que puede transmitirnos una compañía que salta a los titulares porque un empleado ha robado información confidencial.

En el ámbito económico las pérdidas si se produce una fuga de información pueden llegar, en el caso de las grandes empresas, hasta los 1,5 millones de euros al año, según un informe de Datamonitor. A esto hay que sumar la pérdida de clientes, proveedores o inversores que dejen de confiar en una empresa que no ha protegido adecuadamente su información.

Teniendo en cuenta que si se produce una fuga de datos, las empresas están obligadas por ley a informar sobre ello, las repercusiones a nivel de imagen y reputación pueden ser desastrosas. El mismo estudio de Datamonitor recoge que un 70% de las grandes empresas cree que una fuga perjudicaría gravemente su imagen y el 33% considera que podría acabar con su negocio. Y qué podemos decir de las sanciones por incumplir la normativa vigente que regula la seguridad y la protección de datos, especialmente dura en España como podemos comprobar en la ley de Propiedad Intelectual o la Ley Orgánica de Protección de Datos (LOPD).

En definitiva, la mayoría de las empresas desconoce estas consecuencias y la importancia de asegurar cierta información. Llegados a este punto podemos afirmar que tanto las PYMES como las grandes compañías deben plantearse la seguridad como una inversión más que un gasto.

¿Cómo minimizar el riesgo?

Como hemos analizado, tanto dentro como fuera de la empresa es una obligación legal proteger y restringir el acceso a determinadas informaciones para garantizar que no llegue a manos desconocidas y puedan utilizarse contra la propia empresa o sus clientes. Una de las herramientas que nos permitirá auditarlo son las llamadas listas o logs que recogen quién ha hecho qué con un correo o con los datos adjuntos. Con este sistema podremos realizar un seguimiento sobre nuestra información y averiguar cómo está siendo utilizada.

La clave es proteger el contenido; sólo entonces no nos deberá preocupar a quién le pueda llegar porque previamente habremos definido los llamados "permisos de usos". Mi experiencia en GigaTrust corrobora esta premisa; lo esencial es asegurar los contenidos para que independientemente de dónde se encuentre almacenado (USB, ordenador, móvil) y si está siendo utilizado o no, no tengamos riesgo de que pueda usarse de forma malintencionada.

¿Cómo lo hacemos? Con un sencillo software que autoriza si esos contenidos enviados pueden ser copiados, impresos, guardados o reenviados y qué usuarios pueden acceder a ellos. También permite ampliar o extender esta autorización con fechas determinadas, por ejemplo, que sólo se pueda reenviar un balance de cuentas durante un periodo de cuatro días. De esta forma, controlaremos a quién se envía la información y que podrá hacer con ella, por lo que reducimos el riesgo de una fuga de datos ya sea de forma accidental o intencionada.

Estos mismos controles podrán darnos la opción de bloquear determinadas aplicaciones, esas herramientas que –como hemos visto– pueden convertirse en espías. No sólo controlaremos la información cuando se envíe, también mientras la creamos por ejemplo con programas de edición de imagen, para evitar que nos roben nuestra idea.

Este soporte tecnológico, sin embargo, no es suficiente. Para proteger nuestros secretos empresariales necesitamos una verdadera política corporativa de seguridad y un equipo humano formado y concienciado de la importancia de gestionar la información de forma segura. Muchas veces son los propios empleados quienes difunden datos sensibles a personas equivocadas simplemente por error. Por eso, recomendamos que a nivel interno y externo, la seguridad se convierta en un activo más de la empresa y en un valor corporativo esencial en cualquier entidad.

No olvidemos que nuestras ideas son el mejor aval de cualquier empresa, aquello que nos hace diferentes de la competencia; nuestros nuevos proyectos, los lanzamientos de productos o los prototipos exclusivos son el eje del progreso y, por lo tanto, el verdadero motor de la gestión en los negocios. ¿Vamos a arriesgarnos a perder nuestros secretos? ■

