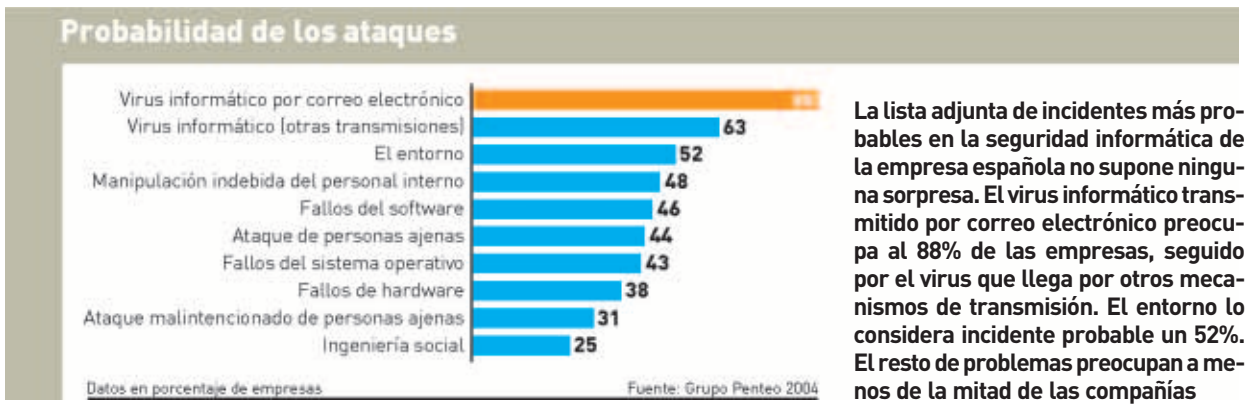
GESTIÓN



La lista adjunta de incidentes más probables en la seguridad informática de la empresa española no supone ninguna sorpresa. El virus informático transmitido por correo electrónico preocupa al 88% de las empresas, seguido por el virus que llega por otros mecanismos de transmisión. El entorno lo considera incidente probable un 52%. El resto de problemas preocupan a menos de la mitad de las compañías

KATJA ENSELING

LA EMPRESA ESPAÑOLA Y LAS TECNOLOGÍAS DE LA INFORMACIÓN

¿Falta cultura de seguridad?

Los incidentes informáticos se resuelven de forma puntual pero en muchas compañías aún no se enfocan con un planteamiento estratégico

Jordi Goula

Quien sea usuario habitual de ordenador habrá observado cómo en las últimas semanas está siendo literalmente bombardeado por virus que tratan de entrar a través de los canales de mensajería del aparato. La mayor vulnerabilidad de los sistemas tiene su afortunada y necesaria contrapartida en unas mayores barreras de seguridad. De no ser así, dada la total dependencia de los sistemas informáticos que ya tiene nuestra vida cotidiana –desde tomar el avión, hasta sacar dinero o simplemente enviar un e.mail– ya nos habríamos paralizado.

Si los particulares estamos en esta tesitura, qué no será el mundo empresarial. Los atentados del 11–S pusieron de relieve –en el apartado menos dramático a nivel personal, pero muy preocupante en el aspecto económico– la necesidad de desarrollar hasta límites insospechados hasta entonces la seguridad de los sistemas, sencillamente, para que puedan seguir trabajando las empresas. Tanto es así, que esta fecha supuso una inflexión al alza en los gastos de seguridad informática en todo el mundo. Hoy, como promedio, se estima que las empresas de los países desarrollados destinan el 11% del presupuesto del departamento de Tecnologías de Información y Comunicación (TIC) a seguridad.

¿Y en España? Pues parece que algo menos. La media estaría en el 8,9% y la moda alrededor del 8%, lo que supone un aumento no desdeñable sobre la media del año anterior que fue del 7,8%, según pone de relieve el informe "La Seguridad Informática en la empresa española en 2004", realizado por Aniel y Grupo Penteo. "Este incremento en el gasto es consecuencia del aumento de las incidencias. En 2003 un 83% de las empresas tuvieron algún problema –en su gran mayoría no graves– mientras que en 2002 habían sido sólo un 62%", afirma Antoni Maciá, director general de Penteo, para quien, en un tema tan crítico como la seguridad, "las empresas españolas dan muestra todavía de falta de proactividad".

De la misma opinión es Juan Gascón, director de telecomunicaciones de Aniel, para quien, "cabe destacar la escasez de medidas preventivas aplicadas por las empresas, así como el elevado porcentaje de empresas que declaran incumplir las políticas de seguridad establecidas. En este sentido, es necesario reforzar tanto las políticas de seguridad como la formación".

¿Qué tiene que ver la formación en este asunto? Muchísimo, no en

El eslabón más débil de la cadena de seguridad en los sistemas informáticos es el usuario final

vano el eslabón más débil de la cadena de seguridad en las TIC acaba siendo el usuario final. Desde dejar abierto el PC, hasta prestar el password o incurrir en riesgos claros en la mensajería, se cae habitualmente en un rosario de riesgos. Por ello, la formación sobre seguridad informática ha aumentado en la empresa, pero no lo suficiente. En 2002 eran un 52% las empresas que impartían cursos a todos o algunos de los empleados y en 2003 fueron el 63% .

El ejemplo del Port de Barcelona

"Este año parece que todas las empresas se preocupan más de la seguridad de los sistemas", asegura Rafael Gomis, director de organización y sistemas de información de la Autoridad Portuaria de Barcelona. "Nuestras medidas de seguridad se centran en los tres grandes apartados a considerar: la confidencialidad de la información, la integridad de la misma y la continuidad del sistema". comenta. Con respecto a la confidencialidad, explica que la resuelven con tres actuaciones: control de accesos, asegurar barreras de entrada con cortafuegos y máxima seguridad en las comunicaciones (intercambio de datos). Para asegurar la integridad de la información, se utilizan antivirus y copias de seguridad, que se las lleva una empresa externa a sus cajas fuertes. "A veces recuperar toda la información resulta muy difícil. No puedes perderla. Y hay otro aspecto importante que añadir: ver que las aplicaciones se hagan bien. Esto te obliga a hacer controles muy exhaustivos". Con respecto a garantizar la continuidad de los sistemas se replican los ordenadores principales. "Tenemos duplicados los equipos críticos y también los datos, en lugares diferentes los que consideramos más importantes. Priorizamos la seguridad de los procesos de negocio críticos, los que permiten desarrollar la actividad en el puerto, así como los que pueden afectar la seguridad personal (mercancías peligrosas...). También tenemos planes de contingencia en aspectos críticos".

Para Maciá, la clave está en nombrar un responsable de seguridad en la empresa, que en las pymes puede ser a tiempo parcial. "Ha de ser una persona que piense constantemente en estos temas, cómo mejorarlos. No es una tarea fácil, porque debe luchar contra la incomprensión de los empleados y a veces hasta de los directivos. Mire, aunque se tenga un óptimo plan de contingencias, si no hay una concienciación generalizada en la empresa sobre la gravedad del asunto, no haremos nada". Por cierto, en el informe se pone de relieve que todavía un 42% de las empresas españolas aseguran no tener planes de contingencia y que la gran mayoría no realiza auditorías de seguridad, a pesar de que todas –eso sí– consideran necesaria su realización para garantizar la seguridad de los sistemas.

Para Maciá, las debilidades de la seguridad de las TIC en nuestras empresas pasan por dos ejes. En el primero apunta que "no se enfoca la seguridad desde un planteamiento estratégico, sino que se basa en buscar soluciones puntuales". En cuanto al segundo, cree que nos "falta cultura de la seguridad en muchos pequeños detalles. Este aspecto es importante porque va más allá de la inversión. Hay pymes, por ejemplo, que se juejan el negocio en ello y no son conscientes".

A la vista del entorno, pues, la tendencia parece evidente. Para Juan Gascón, "la seguridad se ha convertido en un requisito imprescindible para el buen funcionamiento de las empresas. Por ello, veremos una tendencia creciente en los próximos años a aumentar las medidas que permitan garantizar la seguridad de los sistemas de información. Esta situación involucrará tanto a empresas como a administraciones".

Los pasos que dar

En el estudio se detalla el procedimiento para una adecuada gestión del riesgo de una compañía, que permite un acercamiento a la seguridad de los sistemas con una visión más realista del entorno actual. Además, realiza especial énfasis en implicar a toda la empresa en la aplicación de las medidas de seguridad.

Identificar los activos críticos

La empresa debe valorar los diferentes elementos que posee, tanto físicos (ordenadores...), como de conocimiento (información...) y ser capaz de organizarlos según su importancia. Los bienes más críticos merecerán mayor protección.

Riesgos y vulnerabilidades

La compañía debe analizar qué amenazas tiene a su alrededor, ver cuales son sus riesgos y cuáles de éstos pueden afectar a sus activos críticos. Por otro lado, debe tomar una actitud activa en la detección de vulnerabilidades en sus sistemas

Ponderar los efectos

Para poder determinar las necesidades de inversión es importante analizar cuidadosamente qué efectos podría tener una materialización de las amenazas sobre los activos críticos de la compañía. Así, es más fácil priorizar la protección, según la gravedad que tendría un fallo en la seguridad

Minimizar los riesgos

El siguiente paso es estudiar cómo se puede reducir el riesgo y el número de aspectos vulnerables, como por ejemplo, implementando un programa (antivirus, cortafuegos, IDS, etc.). El objetivo no es eliminar el riesgo, sino lograr que se sitúe en un nivel aceptable.

Aplicar políticas adecuadas

Revisadas las posibilidades de minimizar el riesgo, se deben aplicar aquellas políticas y técnicas que se consideren más adecuadas teniendo en cuenta la situación específica de cada compañía. Esto implica considerar los activos críticos y las amenazas, pero también otros aspectos, como el coste, la velocidad de recuperación...

Probar los mecanismos

Periódicamente deben realizarse pruebas que permitan asegurar la efectividad de los mecanismos y políticas utilizados. Así, se asegura que si se produce un evento no deseado, los elementos estarán operativos, los programas en funcionamiento, el personal del departamento TIC preparado...

Control preventivo

Es preciso también que la compañía sea capaz de percibir cuando ocurre un evento no deseado. Para ello, debe establecer los requisitos necesarios para poder controlar sus sistemas y poder actuar en caso de necesidad, prestando especial atención a los puntos vulnerables.

Revisión permanente

Además de vigilar posibles ataques y probar los sistemas implementados periódicamente, es importante también que todos los elementos establecidos en la política de seguridad estén en constante revisión. Tanto los activos de la compañía, como las posibles amenazas y los métodos de mitigación del riesgo están en evolución permanente. Esto significa que las políticas establecidas también deben ser revisadas, para garantizar su adecuación a la realidad de la compañía y a las amenazas y técnicas existentes.