Publicado en el 20/12/2016

Las actualizaciones de Windows suponen un problema de seguridad para las PYMES

El incorrecto funcionamiento de algunas de las actualizaciones y la automaticidad de estos procesos representan un riesgo para las pequeñas empresas

Para las pequeñas empresas, las actualizaciones de Windows nunca han estado del todo bien resueltas. Se pasa en determinadas organizaciones de desactivar las actualizaciones a dejarlas de forma automáticas. Pero no siempre es positivo. Con Windows 10 y las actualizaciones obligatorias, al menos en materia de seguridad, la cosa parece haber ido a peor.

Y es que las actualizaciones de Windows se han convertido en un problema para la PYME. O cuanto menos en un engorro. Nadie se encarga de revisar cuándo se actualiza, qué se actualiza o si ha dejado de actualizarse un equipo. Ademas, en la pequeña empresa rara vez se utilizan las actualizaciones centralizadas, distribuidas cuando la empresa decide que es el mejor momento para ella.

Porque si siempre funcionaran bien no habría problemas, pero en ciertas ocasiones provocan un comportamiento errático. En este caso el problema puede afectar a la mayoría de los equipos de una empresa, haciendo que tengan graves problemas en un momento determinado.

Las actualizaciones de Windows tienen un calendario marcado. Se actualizan los segundos martes de cada mes, aunque en España suelen llegar los miércoles. Ese día los equipos descargan e instalan las actualizaciones cuando se apaga el equipo y completan al día siguiente cuando se enciende. Si se reinicia o se apaga el equipo durante la jornada, la interrupción puede durar mucho más de lo deseado por este motivo.

Y esto provoca en muchas ocasiones que los usuarios apaguen de forma abrupta los ordenadores, provocando incluso mal funcionamiento. No es un mal sólo del sistema operativo, también ocurre con otros programas importantes para la empresa, donde en la mayoría de los casos nadie evalúa el impacto de una actualización.

Y en el caso de parar las actualizaciones supone un problema grave de seguridad. Los equipos sin actualizar pueden ser una brecha que aprovechen los atacantes para robar datos o infectar equipos, por lo que al final, el remedio en este caso tampoco resulta efectivo.

Quizás lo ideal sería poder retrasar la actualización una semana, asumiendo un riesgo, pero dejando que se actualice un equipo como piloto. De esta forma sería posible asegurarse que los cambios no van a suponer ningún problema en la organización.

El contenido de este comunicado fue publicado primero en la página web Pymes y Autonomos

Datos de contacto:

Nota de prensa publicada en:

Categorías: E-Commerce Ciberseguridad Recursos humanos