El difícil equilibrio entre el trabajo en red y el filtrado de datos; la visión de Easynet

Easynet Global Services ofrece recomendaciones a las empresas para que permitan el acceso a los datos sin que ello los ponga en riesgo

La “consumerización de TI” ha traído consigo que gran parte de los empleados utilice su propio hardware en el trabajo. De hecho, una encuesta de IDC muestra que el 95% de los trabajadores de la información utiliza algún tipo de tecnología adquirida por ellos mismos. Más allá de esto, muchas empresas están aprovechando las redes sociales para mejorar la colaboración y potenciar la creatividad en la organización. Las compañías se están transformando en empresas “más porosas”; lo que implica más facilidad para mover y acceder a los datos.

Javier Morgado, country manager de Easynet Global Services afirma que “La apertura de datos para los empleados tiene sus beneficios, como la agilidad y la creatividad, pero también tiene una contrapartida: los datos tienen más posibilidades de ser filtrados. Por ejemplo, cada vez que un empleado deja o es despedido de la compañía, existe un riesgo”.

Tomar medidas drásticas contra usuarios finales y ajustar las políticas de la empresa no es una opción porque podría desmoralizar a los empleados y llevar a la empresa a perder los beneficios que le reporta el hecho de animarles a colaborar. Easynet recomienda a las empresas que utilicen marcos de seguridad establecidos y que dediquen tiempo a formar a sus empleados en el papel vital que deben jugar para mantener segura la información. Los CIOs tienen que asegurarse de que sus sistemas de gestión de la seguridad de la información son lo más robustos posible. Sin embargo, muchas compañías tienen en marcha procesos de seguridad y políticas que han quedado obsoletos desde hace más de 10 años.

“Es totalmente necesaria la involucración de todos los empleados y en muchas circunstancias, esta es la parte más difícil. Se trata de establecer políticas, formar a los empleados y crear una atmósfera de vigilancia – desde el uso de contraseñas complejas hasta alentar a las personas a denunciar irregularidades. Así evitarán la filtración de la información sensible hacia el exterior de la empresa” afirma Javier Morgado, country Manager de Easynet Global Services.

Los CIOs que quieran aumentar su seguridad, pero no estén dispuestos a dedicar los recursos para ello, tienen la opción de dejar partes clave de su infraestructura a proveedores que sí reúnan estos requisitos. De este modo, dichas partes de la infraestructura empresarial lo cumplirán por defecto, ayudando al cumplimiento total del objetivo.

La seguridad seguirá siendo un asunto a considerar por las organizaciones, pero hay medidas que se pueden tomar para garantizar que sus procesos sean efectivos. Esto implica una inversión específica y la actitud de seguir lo que puede ser un cambio cultural dramático. Aunque los CIOs estarán tentados de tomar el camino rápido y fácil de cortar el acceso a los empleados a las redes sociales, no beneficiará a las empresas a largo plazo. Los empleados necesitan seguir un enfoque basado en políticas, educación y fuentes de inteligencia. Los CIOs no solo deben proteger su empresa y animar a un uso más ambicioso de la tecnología, sino que deben utilizar sus posturas de seguridad como una estrategia para competir y ganar negocio.
