Publicado en Madrid el 06/10/2021

Las pymes son las entidades que presentan el mayor número de ciber-riesgos

Según un estudio y ciberseguridad realizado por S2 grupo, las pymes son las entidades que presentan el mayor número de riesgos en el ámbito de la seguridad de la información. Tanto es así que el 74% de las pequeñas y medianas empresas ha sufrido algún problema de ciberseguridad a lo largo de su historia

La compañía especializada en ciberseguridad y gestión de sistemas críticos S2 Grupo ralizado un estudio sobre pymes y ciberseguridad, en el que se pone de manifiesto que actualmente estas organizaciones se enfrentan principalmente a siete barreras que necesitan superar para proteger su ciberseguridad y la continuidad de sus negocios.

“Hoy en día, no sólo las grandes compañías tienen una gran dependencia de las TIC. Las pymes, que constituyen más del 99% del tejido empresarial europeo, presentan riesgos más que significativos en este ámbito y éstos constituyen una gran amenaza para su negocio. De hecho, hay estudios recientes que afirman que el 90% de las grandes corporaciones han sufrido una brecha de seguridad y que este porcentaje se traduce en un 74% en el caso de las pymes.”, ha declarado José Rosell, socio-director de S2 Grupo.

“Las pymes tienen una fuerte dependencia de las TIC a la hora de desarrollar sus servicios y, sin embargo, en su mayoría no disponen de medidas de ciberseguridad", ha afirmado Miguel A. Juan, socio-director de S2 Grupo. Por tanto, "éste es uno de los grandes retos a los que nos enfrentamos en los próximos años”, ha añadido el directivo de la compañía.

Barreras para la ciberseguridad de las pymes

En este sentido, S2 Grupo ha destacado las siete principales barreras que dificultan la implementación de los estándares de seguridad de las empresas. En concreto:

Su desconocimiento sobre los estándares de seguridad de la información aplicables.- En muchos casos, sobre todo entre aquellas pymes que no pertenecen al sector de las TIC, existe desconocimiento acerca de los estándares existentes. A menudo echan en falta un punto de referencia o consulta único, de modo que puedan pedir consejo acerca de que estándar es el más adecuado para ellos por ser el que mejor se adapta a sus necesidades, requerimientos por parte de terceros, etc.

Falta de compromiso de la dirección.- Debido a que los recursos de las pymes suelen estar más limitados y que sus esfuerzos están centrados en ser competitivos en su ámbito de negocio, es difícil para la dirección percibir de una manera clara cómo implementar unos estándares de seguridad de la información añade valor a su negocio y les puede proporcionar ventaja competitiva frente a la competencia.

Percepción equivocada acerca de los objetivos de los ciberataques.- Entre la mayoría de dirigentes y empleados de pymes, existe la extendida creencia de que los ciberataques afectan principalmente a grandes organizaciones, y no a empresas de su envergadura, ya que ellos no almacenan y/o tratan

información tan crítica.

Falta de contribución en el proceso de desarrollo de los estándares.- El diseño de los estándares de seguridad de la información está impulsado, principalmente, por grandes organizaciones, y éstos están destinados a cubrir sus múltiples procesos de negocio. Como consecuencia, los estándares asumen que todas las organizaciones tienen los recursos suficientes para implementarlos, y que tienen el entendimiento necesario acerca de los requisitos técnicos y no técnicos que se incluyen en los mismos.

Falta de capacidades en ciberseguridad.- Una de las principales acciones requeridas a la hora de implantar un estándar es asignar roles y responsabilidades de seguridad de la información a algunos empleados. Los roles de seguridad que son requeridos para gestionar estos estándares son varios y con distintos perfiles, y esto excede la capacidad de recursos humanos de la mayoría de pymes.

Presupuesto y recursos limitados.- El poco presupuesto destinado a seguridad de la información parece ser uno de los grandes impedimentos para las pymes a la hora de implantar un estándar. Hay que tener en cuenta que la implementación de éstos requiere inversión en consultores especializados que les guíen, para cumplir con los requerimientos técnicos de los estándares, para adquirir soluciones software, nueva infraestructura TIC, etc.

Gestión de riesgos.- Para la mayoría de pymes, la seguridad de la información es todavía un campo emergente y éstas no aplican el mismo grado de rigurosidad a la hora de evaluar los riesgos de seguridad de la información que a la hora de evaluar riesgos financieros, legales, operacionales, etc.

Pese a todo, las pymes "son poco a poco más conscientes del potencial impacto que puede tener hoy en día la interrupción de sus procesos de negocio debido a un incidente de seguridad y de cómo una adecuada gestión de los riesgos puede protegerlos frente a las amenazas y vulnerabilidades asociadas a sus activos de información", concluye el comunicado de la compañía.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Emprendedores Ciberseguridad Recursos humanos