Publicado en Madrid el 11/02/2020

La falta de inversión en cibereducación es la principal amenaza para las empresas según S2 Grupo

Desde S2 Grupo aseguran que este problema hace que las llamadas técnicas de "ingeniería social" sean tan efectivas a la hora de "engañar" a los empleados e introducir malware en las compañías. Con motivo de la celebración del Día de la Internet Segura, el equipo de expertos de S2 Grupo ha establecido 7 puntos clave para la ciberseguridad de las empresas, que abarcan desde la importancia de disponer de herramientas de monitorización hasta controlar los sistemas IoT incorporados a los procesos

Cada 11 de febrero se celebra el Día de la Internet Segura y desde S2 Grupo se ha advertido de que una de las principales brechas en la ciberseguridad en las empresas reside en la falta de educación de los empleados en cómo utilizar de forma segura las Nuevas Tecnologías.

En este sentido, las malas prácticas, la falta de inversión, la falta de generación de una cultura adecuada de ciberseguridad, etc., son acciones que “facilitan” mucho el trabajo de los ciberdelincuentes.

“El enorme grado de falta de cultura en ciberseguridad hace que sea relativamente fácil, mediante técnicas de ingeniería social "engañar" a los empleados que confian que lo que se les remite al correo o los archivos que hay en USB son legítimos. Normalmente, es más fácil atacar que defender, ya que sólo requiere encontrar un hueco para acceder. Por eso, se debe evitar que existan esos huecos”, ha afirmado José Rosell, socio-director de S2 Grupo.

“Otro error grave es la costumbre de tener redes sociales cada vez más nutridas con miles de contactos no conocidos, que hace proliferar los perfiles falsos que encuentran fácil tener un gran número de seguidores que "validan" su identidad y, por tanto, lo hacen más confiable. En definitiva, el error es dar por buenas cosas que en el mundo físico hemos aprendido, durante años, a distinguir que no lo son y que en el ámbito digital no somos capaces de hacerlo de la misma forma”, ha asegurado Miguel A. Juan, socio-director de S2 Grupo.

Expertos de la compañía han explicado que este tipo de acciones son las que facilitan la propagación de ciberdelitos como el phising o el llamado “fraude al CEO”, por ejemplo.

Junto a esto, desde S2 Grupo se ha insistido en que es necesario que las empresas inviertan en formación que permita a los empleados conocer cómo es un uso ciberseguro de las herramientas TIC.

“Éste es uno de los puntos flojos de las estrategias defensivas en ciberseguridad. Hay que hacer que la cultura de ciberseguridad de las compañías sea lo suficientemente robusta como para que no haya eslabones muy débiles”, ha declarado Miguel A. Juan.

“En este sentido, hay que concienciar de forma continua a todo el personal y darle los elementos oportunos para la gestión efectiva del riesgo para que sepa cómo actuar cuando este se materialice. Además, no se puede reducir a dar cursos sin más, hay que asegurarse que son efectivos y que la cultura de la compañía en ciberseguridad mejora, es decir, madura”, ha enfatizado José Rosell.

7 recomendaciones de ciberseguridad para mejorar la protección de las empresas (independientemente de su tamaño):

Disponer de los medios defensivos y de monitorización adecuados.

Disponer de las capacidades de inteligencia precisas para saber qué y cómo debe buscar para evitar la intrusión de ciberdelincuentes.

Implementar procesos de vigilancia que les ayude a anticipar posibles ataques o fugas de información.

Disponer de planes de concienciación y formación en ciberseguridad de todo el personal.

Contar con los medios técnicos/lógicos adecuados.

No descuidar los sistemas OT ni los sistemas IoT incorporados en sus procesos.

En definitiva, seguir esquemas como ISO 27001 y 27002 o el Esquema Nacional de Seguridad, que establecen de forma sistemática y robusta que es lo que hay que hacer para mejorar en la gestión de la ciberseguridad.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Educación E-Commerce Ciberseguridad Recursos humanos Otros Servicios