Publicado en España el 25/02/2021

S2 Grupo aumentó su volumen de negocio un 12% en 2020

La compañía española especializada en ciberseguridad y gestión de sistemas críticos S2 Grupo ha cerrado 2020 un crecimiento de su volumen de negocio del 12%. Su facturación consolidada en el último ejercicio ha sido de 19,5 millones de euros, frente a los 18,2 millones de euros de 2019

Según ha informado la compañía en un comunicado, el ejercicio 2020 cerró con un aumento en su volumen de negocio del 12%, con una facturación consolidada de 19,5 millones de euros, frente a los 18,2 millones de euros de 2019. En este contexto, la inversión en I+D ha sido "uno de los ejes esenciales de la empresa de ciberseguridad" y, por ello, en 2020 ha continuado manteniendo su apuesta por este ámbito con una inversión en 1,5 millones de euros. De este modo, se ha "consolidado la estrategia establecida en su plan de negocio para el último ejercicio", según el comunicado de S2 Grupo.

En relación a su equipo, S2 Grupo ha cerrado 2020 con una plantilla estable de 414 profesionales, un 19% más que en 2019.

“Si algo ha caracterizado a 2020 ha sido la presencia de una pandemia que, por supuesto no estaba prevista, y que nos ha hecho dar un salto enorme en la digitalización de nuestras compañías. Un salto que, además se ha tenido que dar de forma inmediata, de un día para otro. Lógicamente estoy ha traído consigo la creciente necesidad de ciberseguridad en todo tipo de entidades públicas y privadas”, ha explicado José Rosell, socio-director de S2 Grupo.

“Nuestra previsión tanto para 2021 como para los próximo años, es que este salto se acelere todavía más. De hecho, el impulso con los planes de recuperación europeos y nacionales se fundamenta en la transformación digital y en la economía verde, dándole una relevancia troncal a la ciberseguridad en todos los ámbitos”, ha declarado Miguel A. Juan, socio-director de S2 Grupo.

Tendencias de la ciberdelincuencia y retos de la ciberseguridad en 2021

S2 Grupo ha destacado que la pandemia ha hecho que en 2020 todas predicciones de ciberseguridad que se hicieron para ese año quedaran alejadas de la realidad, debido a todos los cambios que surgieron, principalmente en entornos laborales, a raíz de este hecho.

Por lo que se refiere a las tendencias de la ciberdelincuencia y principales retos de la ciberseguridad en 2021, expertos de S2 Grupo han destacado que hay que tener en cuenta:

1.- En primer lugar, que se mantendrá el teletrabajo.- Esto hace que se tenga que reforzar la ciberseguridad tanto de las empresas, de los dispositivos personales y de los propios hogares, porque ahora aprovechar las brechas en este campo es uno de los grandes objetivos de la ciberdelincuencia

para ciberatacar a las organizaciones. Desde S2 Grupo se ha resaltado que las infraestructuras críticas son todavía más críticas en situaciones de crisis debido, entre otros factores, a que se degrada la capacidad de respuesta al no estar físicamente, al estar limitados los desplazamientos físicos, etc. Por tanto, es muy importante la inversión en ciberseguridad porque cualquier sistema expuesto a Internet es objetivo claro para los ciberatacantes.

2.- En segundo lugar, otro de los objetivos directos de los ciberdelincuentes serán los sistemas de videoconferencias, dropbox, mensajería, etc. .- Expertos de S2 Grupo han asegurado que al tratarse de herramientas básicas, se incrementa su exposición en todos los sentidos y puede, incluso, encontrarse venta de credenciales de Zoom en los mercados negros.

3.- En tercer lugar, la presencia de malware, phishing, scam y dominios “covid” registrados.- El término “covid” está siendo utilizado como un cebo para que los usuarios se descarguen código dañino, robar credenciales, datos personales, etc. De hecho, se están detectando al día más de 1.500 dominios “covid” maliciosos. En abril de 2020, Google bloqueó al día 18 millones de correos maliciosos relacionados con el término “covid”.

4.- En cuarto lugar, también será relevante el ciberespionaje, sobre todo, relacionado con las vacunas e investigaciones sanitarias. Y otro de los aspectos relacionados con esto, será la desinformación como forma de ciberataque a través de la creación de artículos falsos, posicionamiento ante la ciudadanía, etc.

5.- En quinto lugar, cada vez se están dando más ciberataques muy sofisticados contra la cadena de suministro, como fue el conocido caso de Solarwinds, y esto puede poner en jaque a organizaciones muy potentes desde el punto de vista de ciberseguridad.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: España

Categorías: Finanzas E-Commerce Ciberseguridad