

S2 Grupo: "si se es víctima de un ciberataque hay que saber reaccionar para minimizar su impacto"

Con motivo de la celebración este martes, 9 de febrero, del Día Internacional de la Internet segura, la empresa de ciberseguridad S2 Grupo destaca la importancia de saber reaccionar si es víctima de un ciberataque como elemento esencial para minimizar, en lo posible, su impacto

Con motivo de la celebración este martes, 9 de febrero, del Día Internacional de la Internet segura, la empresa de ciberseguridad S2 Grupo destaca la importancia de saber "reaccionar" si es víctima de un ciberataque como elemento esencial para minimizar, en lo posible, su impacto.

Actualmente, todas las personas que tienen acceso a Internet tienen que lidiar con dos escenarios: los hogares y las empresas. Pero la problemática de la situación actual es que, a su vez, éstos pueden estar muy relacionados a raíz del teletrabajo.

En un comunicado remitido por S2 Grupo se pone de manifiesto que "para proteger la información de una organización debemos ser capaces de gestionar su seguridad de forma correcta y esto conlleva, entre otras cosas, el establecimiento de una capacidad de gestión de incidentes de seguridad, ya que esta capacidad permitirá a la empresa u organismo responder de forma correcta al ciberataque y ser más eficaces en su resolución".

"Es imposible que la ciberdelincuencia desaparezca, por eso es tan importante una buena gestión de la ciberseguridad en las organizaciones y también en nuestros hogares", ha añadido Miguel A. Juan, socio-director de S2 Grupo.

En caso de recibir un ciberataque cuando se está en casa, lo primero es tener en cuenta que cualquier ataque en el hogar puede afectar a la compañía donde trabajen sus miembros. Por tanto, hay que comunicárselo. "Esto es aún más importante en el caso de personas que ocupen puestos directivos o que manejen información sensible", ha afirmado José Rosell, socio-director de S2 Grupo.

La compañía recuerda que, en otro tipo de ciberdelitos, "hay que ponerlo en manos de la Policía", pues las unidades de Delitos Telemáticos están preparadas para ello, muy especialmente en el caso de cuestiones que afecten a los niños", ha continuado Rosell.

¿Cómo actuar si el ciberataque es en la empresa propia?

La nota de S2 Grupo incide en que una vez ha sucedido el ciberataque "lo más importante es avisar inmediatamente a los expertos en gestión de incidentes, que se encargarán de todos los aspectos legales, técnicos y de resolución".

El segundo paso, es "no realizar ninguna acción sobre la red hasta que ellos acudan". Aunque esto suele costar por el estrés que se crea, es muy importante para no complicar aún más la situación.

Después de informar al equipo que se encargue de la gestión de ciberincidentes, éstos realizarán un análisis de la situación y recopilarán todos los datos que ayuden a averiguar cómo ha sucedido, por dónde han "entrado" los ciberdelincuentes, cuántas personas se han visto afectadas, cuál es el alcance de la acción, etc.

Posteriormente, aplicarán su trabajo para detener la intromisión en los sistemas de la empresa y, de esta forma, que la acción de los ciberdelincuentes genere el menor impacto posible en la organización.

Desde S2 Grupo se ha incidido en que, como "es imposible evitar con total garantía la materialización de ciberataques", es clave aprender de ellos para mejorar los mecanismos de seguridad desplegados e incrementar así la seguridad global de los hogares y de las organizaciones.

Datos de contacto:

Luis Núñez
667574131

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional E-Commerce Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>