Publicado en Madrid el 18/03/2020

El teletrabajo puede poner en peligro la ciberseguridad de buena parte de las empresas españolas

Desde S2 Grupo se ha señalado que la falta de seguridad de los sistemas de comunicación entre los hogares de los empleados y la empresa es una de las principales puertas de acceso a los ciberdelincuentes. La empresa de cibserguridad recomienda la incorporación de sistemas de comunicación cifrados, como las VPN, que ciberprotejan la información que se maneja mediante el teletrabajo

Ante el decreto del Gobierno del estado de alarma, muchas empresas han optado por el teletrabajo para poder seguir funcionando. Desde S2 Grupo se ha advertido que la mayor parte de las empresas y organizaciones españolas, aunque cuenten con múltiples mecanismos de ciberseguridad, no están preparadas para estar ciberprotegidas a través del teletrabajo y esto podría poner en jaque la seguridad de las mismas.

“El teletrabajo es una alternativa para evitar los contagios y mantener la actividad económica. Ahora bien, en España hay muchas pymes y empresas u organizaciones de cualquier tamaño, que nunca se lo habían planteado. En la situación actual, prácticamente se han visto forzadas a implantarlo y muchas no están preparadas para ello, principalmente, desde el punto de vista de la ciberseguridad”, ha declarado José Rosell, socio-director de S2 Grupo.

“En el momento en el que se establece el trabajo a distancia hay comunicación entre la vivienda de una persona y la oficina donde están los ordenadores o los datos con los que se tiene que trabajar. Esto supone que habrá un tráfico de datos entre ambos lugares y ello requiere hacerlo con unas garantías para que no puedan ser captados por terceros, como pueden ser los ciberdelincuentes”, ha explicado Miguel A. Juan, socio-director de S2 Grupo.

Desde la compañía se ha señalado que para ciberproteger a las empresas u organizaciones es fundamental, que se establezca una línea de comunicación segura entre el lugar en el que se encuentra el trabajador y la empresa donde están los datos, ya que pueden estar muy bien blindadas en su ciberseguridad pero que haya fugas a través del canal de comunicación con el profesional que trabaja desde fuera de la empresa trabajando a distancia. Esto se consigue mediante VPNs o redes privadas virtuales, que son como túneles a través de los cuales pasan los datos protegidos porque han sido cifrados.

“Las empresas ahora son responsables de la custodia de muchos datos. Datos de carácter personal, económicos, etc. Al establecerse esta comunicación se corre el riesgo de que un ciberdelincuente intercepte esas comunicaciones y obtengan credenciales que luego le permitaentrar en la empresa y acceder a la información. Este riesgos se minimiza si se usan VPNs”, ha aclarado Miguel A. Juan.

Por otro lado, desde S2 Grupo se ha destacado que otro peligro adicional es que el entorno del domicilio del trabajador no forma parte de la red TIC de la empresa y no sigue los mismos criterios de ciberseguridad que ésta.

“Una empresa puede tener todos los sistemas de seguridad que quiera pero si esta persona en su casa el ordenador lo tiene conectado a otro ordenador que tiene un virus o un malware, o que está abierto o lo usan también los niños para descargarse juegos o cualquier aplicación, el problema está en que a través de esa casa, se puede abrir la puerta de entrada de los ciberdelincuentes a la empresa”, ha afirmado José Rosell.

Según han informado, que ésta es la vía más común por la que a diario se suceden problemas de ciberseguridad como ransomware o petición de rescates a las empresas, entre otros.

“Podemos tomar las precauciones para no ser contaminados por un malware, pero si un empleado tiene un comportamiento poco ciberseguro, puede contaminarse la empresa por un malware o un ciberataque”, ha concluido Miguel A. Juan.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Telecomunicaciones E-Commerce Ciberseguridad Recursos humanos