La ciberseguridad, el riesgo del teletrabajo en época del coronavirus

14.10.20 | España

Ya en octubre, con el curso y rutina profesional ya asentados, nos encontramos inmersos en la segunda ola de coronavirus. Mientras unas empresas han adaptado sus instalaciones a la nueva situación para que sus empleados puedan desempeñar sus tareas, otras siguen apostando por el teletrabajo como medida preventiva.

Para permitir que los equipos tengan las mismas facilidades digitales en casa como en la oficina es clave generar diversos puntos de acceso remoto. Para hacerlo, las empresas deben tomar muchas precauciones para impedir que hackers y otras amenazas digitales entren en sus sistemas y los de sus empleados. Proteger los datos internos de las compañías es clave.

Este modelo de trabajo que se impuso durante el confinamiento a contrarreloj, supuso un esfuerzo grande para los equipos de IT de las empresas. Una vez desarrollado, las compañías ahora se enfrentan a otros retos, como la protección de datos y la prevención de ciberataques.

Los datos digitales son moneda de cambio para los criminales. Pueden venderlos, intercambiarlos, utilizarlos para generar ganancia o incluso pedir rescate por ellos. Y las consecuencias oscilan desde molestas hasta peligrosas para la estabilidad de la empresa y la seguridad de sus empleados.

En España, por ejemplo, el 36% de las compañías españolas fueron víctimas de un ciberataque durante los siete primeros meses de 2019, un dato muy superior al porcentaje global (24%), según el estudio de BitDefender, Hacked Off!.

Soluciones eficaces

Afortunadamente, también existen soluciones para minimizar estos peligros. Una de ellas es concienciar a los trabajadores de los riesgos de ciberseguridad, para que la red de su hogar también esté protegida. De este modo, es preferible no usar la cuenta personal para el trabajo, cerrar sesión al terminar los quehaceres o utilizar contraseñas

seguras. También, es aconsejable realizar copias de seguridad a diario para que, en el caso de que se produjera un ataque, fuera posible recuperar los datos fácilmente.

Al mismo tiempo, existen entidades independientes especializadas en ciberseguridad, como TÜV Rheinland, cuyas actividades abarcan este campo en asuntos como la implementación de tecnología, ensayos, servicios administrados o certificaciones. Conscientes de que cualquier intrusión en la red puede tener un impacto letal para una empresa, protege los sistemas de sus clientes de manera integral, proactiva y permanente, con un enfoque único.

De este modo, TÜV Rheinlandayuda a las compañías a comprender cómo, cuándo y dónde están las amenazas en este contexto de transformación digital. El servicio de evaluación de riesgos de la entidad alemana permite a las organizaciones identificar rápidamente los peligros de la ciberseguridad en sus redes industriales. Durante el proceso de acompañamiento, la entidad diseña y opera un programa eficaz de defensa para preservar un posible ataque a la nube que pueda desembocar en terribles consecuencias económicas, sociales y de reputación a la marca.

Otro de los aspectos que se deben tener en cuenta en el mundo digital es la prevención. Los planes de contingencia y contar con profesionales capaces de detectar brechas de seguridad y ataques con antelación es un valor añadido para las compañías cuando se extiende el teletrabajo. TÜV Rheinland ha incorporado recientemente el programa de capacitación en Seguridad Funcional que, a nivel mundial, ofrece entrenamientos para áreas tan sensibles como seguridad de herramientas y maquinaria o análisis de riesgos y peligros de los procesos. Con este programa se obtiene el certificado de ingeniero o técnico “de Seguridad Funcional".

A su vez, TÜV Rheinland apuesta por la formación de profesionales de ciberseguridad, así como auditores en sistemas de gestión de seguridad de la información, bajo la norma ISO 27001:2013. De esta manera, proporciona a profesionales con experiencia en ciberseguridad, una manera de tener su experiencia formalmente reconocida. Este curso incluye, a su vez, el certificado de competencia profesional reconocido a nivel internacional.

Solicitar información sin compromiso

****

TÜV Rheinland is a global leader in independent inspection services, founded nearly 150 years ago. The group maintains a worldwide presence of more than 20,000 people; annual turnover is EUR 2 billion. The independent experts stand for quality and safety for people, technology and the environment in nearly all aspects of life. TÜV Rheinland inspects technical equipment, products and services, oversees projects, and helps to shape processes and information security for companies. Its experts train people in a wide range of careers and industries. To this end, TÜV Rheinland employs a global network of approved labs, testing and education centers. Since 2006, TÜV Rheinland has been a member of the United Nations Global Compact to promote sustainability and combat corruption.

Website: www.tuv.com