Publicado en Barcelona el 18/03/2021

Gran Via BC asegura que el teletrabajo ha venido para quedarse en combinación con el trabajo presencial

Una rápida transición al trabajo remoto ha hecho que los técnicos informáticos tengan que estar mucho más vigilantes que con el trabajo habitual en las oficinas

Muchas empresas, preocupadas todavía por la situación sanitaria actual alterada por la pandemia de la Covid-19, continúan organizando a sus trabajadores entre aquellos que trabajan desde casa y los que se sitúan en los espacios de trabajo de forma más habitual. Este cambio respecto al modelo más tradicional de trabajo también puede exponer estas organizaciones a los ciberataques si no se toman precauciones.

Empresas que van desde gigantes tecnológicos hasta startups y pymes continúan apostando por una fórmula de trabajo híbrido. Sin ir muy lejos, se ve como en en España el teletrabajo es una tendencia que actualmente marca un 34% de la actividad en combinación con la jornada en el centro de trabajo. Pero si se mira más allá, Microsoft, Alphabet, Facebook y Apple siguen instando a los empleados a trabajar desde casa, si sus tareas diarias lo permiten. Varias empresas tecnológicas, incluidas Google y Cisco, mantienen su oferta de herramientas de colaboración de forma gratuita, puesto que empresas de todo el mundo han implementado políticas de trabajo desde casa y se mantienen canceladas las conferencias físicas.

"Hemos notado cómo el trabajo a distancia no solo respondía a una necesidad del momento sino que ha venido para quedarse en combinación con el trabajo más presencial", afirman desde Gran Via Business & Meeting Center, centro de negocios ubicado en Barcelona, en referencia a cómo este nuevo nivel de flexibilidad del puesto de trabajo pone a prueba la estrategia en ciberseguridad de las empresas.

La experiencia y el trabajo diario en este workspace va alineada a las últimas noticias de ataques informáticos y opina que estas prácticas están mejor defendidas en un centro de espacios de trabajo. “Cuando los trabajadores empiezan a conectarse desde cafeterías o espacios públicos, pueden poner en riesgo información sensible sin saberlo; aquellos que visitan otros espacios de trabajo para cambiar el paisaje pueden dejar sus dispositivos desatendidos”, argumenta en referencia a cómo los sistemas informáticos de los workspaces suponen una doble barrera de seguridad contra posibles ataques desde la red.

Aspectos a tener en cuenta con el teletrabajo

"En casa hay una tendencia a bajar la guardia puesto que la gente se siente más segura, de forma que cualquier mal hábito de seguridad informática desde casa se puede traducir en posibles vías de entrada para los ciberdelincuentes", explican desde el equipo de Gran Via BC al tratar como el reto más grande es recordar y reforzar positivamente unos buenos hábitos de seguridad, algo que se encuentra fortalecido con los sistemas informáticos y profesionales a disposición de los usuarios de

workspaces profesionales con una buena infraestructura de servicios.

“Es posible que los empleados que trabajen desde casa no tengan las mismas herramientas de protección que en el trabajo. Por eso es clave tener una buena estrategia en seguridad y unos protocolos muy definidos”, añaden en Gran Via BC.

Los empleados también pueden perder sus credenciales o compartirlas accidentalmente a través de una Wi-Fi pública. Si un atacante los captura e inicia sesión en una aplicación empresarial, será difícil para los equipos de seguridad determinar cuál ha sido el acceso inadecuado. Por eso, una vez más es importante poder acceder a redes seguras y con cortafuegos o filtros que impidan este tipo de accesos.

Qué medidas se tienen que tomar para proteger a los empleados en situación de teletrabajo?
"Se tiene que ser más proactivo en materia de prevención. Por eso es muy importante que todos los equipos y dispositivos estén actualizados con las últimas versiones disponibles", señalan en el workspace barcelonés, donde aconsejan a los departamentos TIC que generen materiales de formación diseñados para que los trabajadores sepan qué hacer y que pueden esperar si experimenten un incidente de seguridad. Si lo hacen, los empleados tendrían que saber informar inmediatamente sobre cualquier amenaza y preocupación que puedan tener para la seguridad.

Otro aspecto que menciona es la autenticación multifactor, basada en una confirmación del código de seguridad del usuario con el teléfono u otros dispositivos, para los usuarios que accedan a servicios empresariales sensibles a través de la red, como soluciones de acceso remoto.

Desde Gran Via BC resaltan que las empresas que se estén adaptando al trabajo remoto tendrían que seguir de estrategias de comunicación interna para poder estar sobre aviso de cualquier incidencia de manera rápida y efectiva. En esta línea es imprescindible poder ofrecer un buen ritmo de formaciones a los trabajadores para que puedan reconocer las amenazas que pueden tener a sus correos o teléfonos móviles. "Además de la tecnología, las personas son realmente importantes y son la primera línea de defensa que más se tiene que cuidar", puntualizan.

Datos de contacto:
EDEON MARKETING SL
Comunicación · Diseño · Marketing
931929647

Nota de prensa publicada en: Barcelona

Categorías: Inmobiliaria Marketing Cataluña Emprendedores Logística E-Commerce Recursos humanos Oficinas