Circular 1947-2021

Transcribimos a ustedes un artículo escrito por Fernando Zambrano el 25 de agosto de 2021 en el diario "El Economista" sobre la seguridad en el trabajo desde casa, homeoffice- trabajo a distancia.

Seguridad para el trabajo desde casa

Con un gran número de empleados trabajando desde casa, la seguridad se ha vuelto fundamental, por lo que la adopción de una solución de End User Computing (EUC) es prioritaria para evitar que, a cambio de un aumento percibido en la productividad cuando trabajan de forma remota, lo usuarios finales se conviertan en un objetivo fácil para el robo de información.

End User Computing elimina la necesidad de almacenar datos críticos en dispositivos de punto final, como computadoras portátiles, que pueden ser robadas o estar en peligro de pérdida con facilidad, para que los usuarios accedan a los datos desde un centro de datos centralizado de clase empresarial donde se gestionan, supervisan y realizan copias de seguridad de forma profesional. Pero la centralización de datos por sí sola no es suficiente para proteger a su organización del ransomware, el malware y de una gran cantidad de otras amenazas cibernéticas.

Combatir estos desafíos requiere de un enfoque de varios niveles que incluya tanto la entrega de infraestructura como la solución de intermediación de aplicaciones y escritorios. Requiere la aplicación cuidadosa de las mejores prácticas comúnmente aceptadas, utilizando funciones disponibles dentro de la plataforma elegida en combinación con algunas herramientas especializadas cuando sea necesario.

Seguridad de la infraestructura, los datos y la red para el trabajo desde casa

La plataforma de infraestructura es el lugar obvio para comenzar a proteger su entorno EUC, ya que proporciona la base tanto para el acceso del usuario final como para el almacenamiento de datos. Para proteger la infraestructura física y el software que se ejecuta sobre ella, debe asegurarse de que la plataforma esté reforzada para cumplir con las mejores prácticas de los proveedores, sus pautas de seguridad interna y cualquier estándar de cumplimiento aplicable.

La seguridad de los datos mejorada es uno de los beneficios inherentes con EUC, pero centralizar sus datos por sí solo no es suficiente, se debe de considerar el acceso con privilegios mínimos para garantizar un acceso seguro a la infraestructura y los datos, para ello debe otorgar a los usuarios y administradores la menor cantidad de privilegios necesarios para sus funciones. Además, tomar en cuenta el cifrado de datos en reposo, es decir, asegurarse de que cualquier dispositivo multimedia que se retire del centro de datos, ya sea para reparación o como resultado de un acto ilícito, no pueda leerse.

Zero Trust

Los planes de continuidad del negocio y recuperación ante desastres (BCDR) no son solo para fines naturales. La capacidad de controlar el acceso desde y hacia las sesiones de los usuarios y los servicios de infraestructura es otra parte importante de la seguridad de EUC. La industria de la seguridad llama a esta idea Zero Trust, la cual comienza con la suposición de que no se debe confiar implícitamente en los endpoints ni en los usuarios. Establece límites sobre lo que un grupo de usuarios puede acceder en términos de redes, aplicaciones y datos, lo que reduce el acceso solo al conjunto de recursos requerido.

Con el aumento de las políticas de trabajo desde casa y el aumento resultante en las implementaciones de EUC, es importante aplicar las estrategias adecuadas de continuidad empresarial y recuperación ante desastres para prevenir, detectar y recuperarse de cualquier ataque. Es mucho más seguro identificar una amenaza antes de que pueda causar daño. En una solución EUC, la capa de archivos compartidos es el lugar más lógico para las medidas preventivas.

“Unámonos más que nunca en un Gran Acuerdo Por México”