Espacios de trabajo híbridos: ¿Qué representa para la ciberseguridad?

El trabajo remoto llegó para quedarse y el modelo que parece estar ganando más adeptos es el híbrido, en el cual se le permite a la mayor parte del personal de una organización trabajar desde casa, pero también se le pedirá que concurra a la oficina ciertos días de la semana. Este modelo se entiende como una solución que toma "lo mejor de ambos mundos", tanto para colaboradores como para empleadores. **Según ESET, en el último año se observó que la adopción masiva del trabajo remoto también hizo que se crearan las condiciones perfectas para que prosperen los actores de amenazas.**

El cambio hacia el trabajo híbrido, también conocido en inglés como hybrid workplace, parece inevitable y es poco probable que las cosas vuelvan a ser tal cual eran antes de la pandemia. El modelo de trabajo híbrido contribuye a mejorar el bienestar, la retención y la contratación del personal, impulsar la productividad y revitalizar la fuerza laboral, sin mencionar la reducción de costos que significa.

Sin embargo, todavía hay confusión sobre los detalles. Según McKinsey, **el 90% de las organizaciones a nivel global combinarán el trabajo remoto y el presencial después de la pandemia, aunque el 68% aún no tiene un plan detallado que haya sido comunicado o implementado**. Las amenazas informáticas a menudo prosperan en escenarios donde hay ausencia de preparación y falta de toma de decisiones estratégicas.

Una investigación de ESET realizada a principios de este año encontró que **el 80% de las empresas a nivel global confía en que sus empleados que trabajan de manera remota tienen el conocimiento y la tecnología que se necesita para lidiar con las amenazas informáticas**. Sin embargo, en el mismo estudio, **el 73% de las organizaciones admitió que es probable que se vean afectados por un incidente de ciberseguridad, y la mitad dijo que ya sufrió alguna brecha de seguridad en el pasado.**

Las organizaciones enfrentan múltiples desafíos, muchos de los cuales fueron presenciados de primera mano durante 2020 y la primera parte de 2021. ESET comparte los principales:

-El factor humano: Los trabajadores remotos están más expuestos porque al trabajar desde casa un miembro de la familia o alguien con quien conviven pueden llevarlos a distraerse y, por lo tanto, son más propensos a equivocarse y hacer clic en enlaces maliciosos. Ponerse en contacto con el área de soporte de TI o incluso hacer que un colega revise un correo electrónico sospechoso es mucho más difícil cuando se trabaja de forma remota, mientras que el uso de redes hogareñas y de computadoras personales para el trabajo pueden ofrecer menos protecciones contra el malware.

-Desafíos tecnológicos y específicos de la nube: ESET reportó un **aumento del 140% en los ataques dirigidos al RDP** en el tercer trimestre de 2020. Existe una preocupación por las vulnerabilidades y las malas configuraciones a nivel de software por parte de los usuarios, y por los reportes de credenciales de acceso robadas. El **41% de las organizaciones encuestadas por el**

Cloud Industry Forum cree que la oficina es un entorno más seguro que la nube. Además, un entorno de trabajo híbrido implica una mayor transferencia de datos entre trabajadores remotos, servidores en la nube y empleados de oficina.

Camilo Gutiérrez Amaya, jefe del Laboratorio de Investigación de ESET Latinoamérica, menciona: 'La buena noticia es que, si bien asegurar el trabajo híbrido será un desafío, existen mejores prácticas que pueden guiar a los CISO. El modelo Zero Trust está ganando popularidad como una forma para gestionar trabajadores y sistemas locales y remotos basados en la nube. Requiere múltiples tecnologías para funcionar de manera efectiva, desde la autenticación multifactor (MFA) y el cifrado de un extremo a otro, hasta la detección y respuesta de la red, la microsegmentación y más'.

El modelo Zero Trust se basa en la premisa de que la antigua noción de seguridad perimetral corporativa ha desaparecido, y ya no se puede confiar ciegamente en los dispositivos y usuarios de la red corporativa. En su lugar, deben autenticarse de forma dinámica y continua, con el acceso restringido de acuerdo con los principios de "menor privilegio " y la segmentación de la red para limitar aún más la actividad potencialmente maliciosa.

Gutíerrez Amaya completa: 'Desde ESET compartimos algunas prácticas recomendadas para mejorar la seguridad del trabajo remoto. Antes incluso de pensar en nuevas tecnologías y controles de seguridad, las organizaciones deben reescribir sus políticas para el nuevo modelo de trabajo híbrido. Esto debe incluir permisos de acceso individuales para empleados, procesos de conexión remota, manejo de datos fuera del sitio y responsabilidades de ciberseguridad para los usuarios, entre muchos otros elementos. Por último, si bien las medidas técnicas como la rápida instalación de parches de seguridad obviamente son vitales, también lo son las consideraciones humanas. Brindar capacitaciones de manera regular para mejorar la formación y concientización a través de lecciones breves y dirigidas a todos los empleados es crucial para mejorar la postura de ciberseguridad de cualquier organización. El factor humano puede que sea el eslabón más débil, pero también puede ser la primera línea de defensa'.

En este sentido, ESET acerca la Guía del Empleado Remoto: Ventajas y desafíos del teletrabajo. Para conocer los riesgos, amenazas y políticas empresariales, las herramientas de trabajo remoto, la conectividad de red, sobre soporte técnico y buenas prácticas.