Riesgos de seguridad de los empleados que trabajan desde casa

Más empleados trabajando desde casa, están causando desafíos de seguridad adicionales.

En una reciente publicación del **Wall Street Journal** - *Silicon Valley Was First to Send Workers Home. It's Been Messy*, el artículo cita información sobre Apple indicando: *"En los últimos días, los desarrolladores de software enviados a casa por el presidente ejecutivo de Apple, Tim Cook, se han quejado de las bajas velocidades de descarga y la creciente confusión sobre las nuevas reglas internas aún en evolución, sobre el trabajo que se les permite realizar. Algunos trabajadores no pueden acceder a sistemas internos cruciales desde su hogar debido a las estrictas políticas de seguridad destinadas a defenderse de los extraños, que ahora incluye a los empleados que se encuentran afuera de las instalaciones"*.

Además, agrega: *"aunque Apple ha alentado al personal a mantenerse alejado de la oficina por razones de salud, muchos ingenieros dicen que continúan llegando a sus puestos de trabajo, debido a la política de la compañía que prohíbe que los productos no liberados sean retirados del campus. La compañía ha aflojado algunas restricciones de seguridad, pero las mantiene firme en cualquier software que pueda revelar la naturaleza de los proyectos restringidos, comentan los empleados "*.

Organizaciones como Apple crearon procesos y herramientas de seguridad en torno a una red segura, es decir, la red corporativa. Genera accesos donde a los buenos se les permite entrar a la red y a los malos se les bloquea e impide ingresar a la red.

Este enfoque funciona bien cuando la organización controla cada aspecto de un proyecto. Sin embargo, hoy en día muchas organizaciones confían en servicios en la nube como JIRA, GITHUB, etc. Para las organizaciones centradas en la nube, la línea entre la red interna y la red externa se desdibuja.

A medida que las organizaciones adoptan un enfoque centrado en la nube, deben utilizar principios de seguridad como **Zero-Trust y Centrado en los Datos**, de esta manera, poner fin a las amenazas sin afectar a los usuarios ni al flujo de trabajo empresarial.

COVID-19 destaca que la seguridad debe estar centrada en los datos. Una postura de seguridad centrada en los datos no depende de la ubicación, el usuario o el dispositivo y se orienta a la Protección Transparente de los Datos.

***DPERP SpA es una empresa partner de SecureCircle**, ofrece la solución DASB (Agente de Seguridad de Acceso a Datos) que elimina las violaciones de datos y mitiga las amenazas internas, sin impacto en la experiencia del usuario final y sin modificaciones en las aplicaciones y flujos de trabajo.*