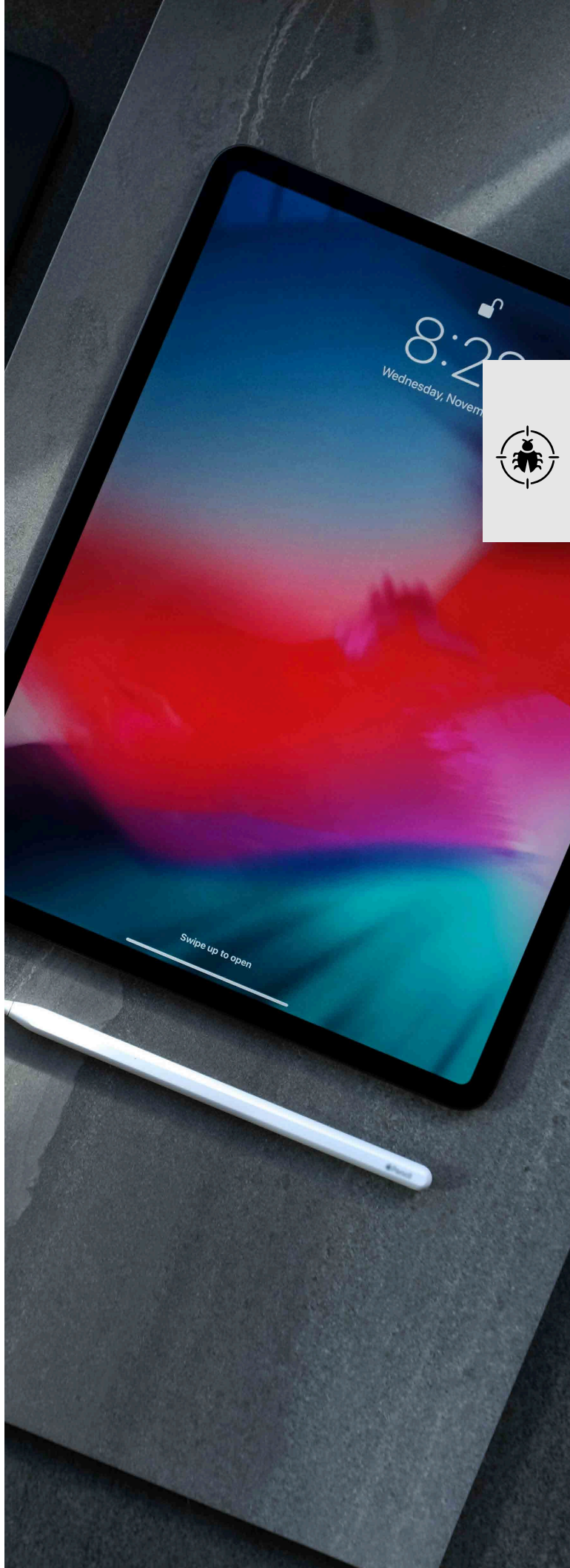
Trabajo remoto y ciberataques, los grandes desafíos para este año

El modelo de trabajo híbrido, incorporado masivamente en el mundo corporativo, continuará modificando el escenario de los equipos de TI de las diferentes organizaciones.

Con motivo de este cambio paradigmático, un equipo de especialistas, realizó un estudio para anticipar lo que sucederá en 2022.

Los expertos anticipan que **muchos equipos todavía no tomaron las medidas necesarias para la adopción del trabajo remoto.** Los trabajadores están solos y se conectan entre ellos a través de redes personales menos seguras que las corporativas. Estas vías de contacto privadas son un punto de entrada sencilla a la red corporativa: los piratas informáticos saben que esto es y utilizan estos nodos para atacar la organización.

Además de concentrarse en las redes de usuarios domésticos, **los hackers apuntan a dispositivos como computadoras portátiles y tabletas personales que carecen de seguridad de nivel corporativo,** como firewalls, anti-malware y actualizaciones de parches y software.

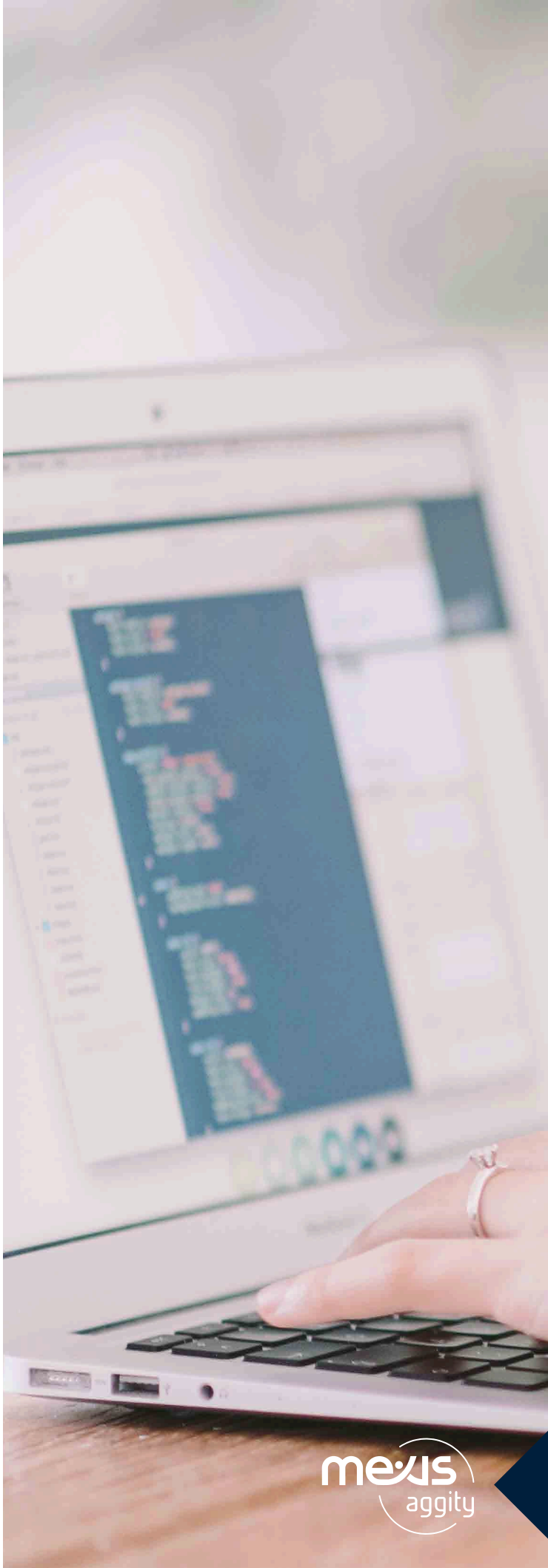


El contexto no es positivo. Ya el Foro Económico Mundial advirtió que los ciberdelitos figuran entre los 10 problemas más importantes en términos de proyección futura y, según el Banco Interamericano de Desarrollo, los delitos digitales pueden superar el 1% del PBI de algunos países.

Además, dado que la TI en sí es en gran parte remota –ya no están en los pasillos para hacerles una pregunta–, es más fácil para los ciberdelincuentes usen la ingeniería social –hacerse pasar por un empleado del equipo de sistemas, por ejemplo– para obtener credenciales de empleados remotos desprevenidos.

El proceso de transferencia de archivos es otro punto especialmente vulnerable.

Para lograr sus objetivos como organización, las empresas necesitan mover archivos sensibles entre socios, clientes áreas y sistemas, y mientras circulan, están potencialmente expuestos a ataques. Por eso, durante 2021, muchas compañías reemplazaron métodos tradicionales de transferencia de archivos, como soluciones de Managed File Transfer (MFT)."



Las soluciones MFT brindan colaboración segura y transferencias de archivos de datos confidenciales, además de aportar capacidades avanzadas de automatización del flujo de trabajo sin la necesidad de secuencias de comandos. El cifrado y el seguimiento de la actividad también permiten el cumplimiento de normativas internacionales de protección de datos, fundamental especialmente para empresas multinacionales que deben cumplir reglas de compliance.

Mientras tanto, para este año **se espera un incremento de los ciberataques en infraestructura crítica: el valor de la información tendrá mayor preponderancia que la magnitud de los datos.**

Y esto es crítico en organizaciones que se expanden con recursos en la nube. En ese sentido, la elaboración de políticas concretas es fundamental para desarrollar mejores prácticas de cara a este 2022. “Los problemas de seguridad y cumplimiento surgen cuando las políticas son ambiguas y no están claramente definidas; no deben estar abiertas a interpretaciones ni ser inequívocas. Hacer cumplir las políticas que sean probables, ejecutables, compartibles, confiables y procesables será la máxima prioridad durante el próximo año”, indica el informe.

A medida que las organizaciones mueven más carga de trabajo a la nube, se acelera la necesidad de automatizar la seguridad y el cumplimiento de los protocolos. Los equipos de TI deben afrontar cambios continuos en sus entornos tecnológicos para atender las necesidades que imponen los objetivos comerciales y el cumplimiento de las regulaciones y las mejores prácticas de seguridad.

A pesar del cambio al trabajo híbrido y el aumento de las vulnerabilidades, muchas organizaciones no han implementado completamente las medidas que respalden el papel de la automatización en la mejora de la seguridad.

La clave estará en poner el foco en integrar los distintivos activos de data al mismo tiempo que se desarrolla una experiencia humana, más robusta y a la altura de los diferentes desafíos, indican los expertos de Progress. Las organizaciones deberán así enfrentar al desafío de mantener un equilibrio entre el establecimiento de una postura de seguridad sólida y la maximización del tiempo de actividad de los usuarios.

"El mundo nos obliga a estar más conectados y, al mismo tiempo, a estar más precavidos en términos de seguridad. **Necesitamos garantizar nuestra seguridad y también la de nuestros clientes.** No es posible esperar reactivamente: hay que estar en evolución y alerta. Que los equipos de negocio y de seguridad caminen de la mano se ha vuelto una necesidad imperiosa", explicó Francisco Larez, VP de Progress Latinoamérica.

"La transformación digital ya es historia y quedará como el gran tema de 2021. Hacia adelante hay un mayor entendimiento del ecosistema tecnológico, desafíos más complejos y herramientas innovadoras y eficaces que permiten estar un paso adelante. Las organizaciones deben entender que la actualización es permanente y que su negocio puede depender de eso", concluyó.

Fuente de información:
https://cio.com.mx