CONTENIDO PATROCINADO | DOCUMENTO TÉCNICO

Protegiendo la seguridad en entornos de trabajo remoto e híbrido

Las empresas con personal remoto e híbrido enfrentan cada vez más riesgos de seguridad. Sin embargo, con un enfoque adecuado y las soluciones correctas, estas organizaciones se pueden proteger de forma efectiva.

CIO

PATROCINADO POR

TeamViewer

MÁS DE LA MITAD DE LOS EMPLEADOS A TIEMPO COMPLETO DE LOS ESTADOS UNIDOS DE AMÉRICA pueden trabajar de forma remota y la mitad de ellos son trabajadores híbridos, **según un estudio de Gallup**. Con la cantidad creciente de trabajadores remotos e híbridos, las empresas a menudo se enfrentan a riesgos de seguridad conocidos y desconocidos.

Las empresas han cambiado sus estructuras para que el trabajo se adapte a los nuevos formatos, más allá del perímetro corporativo tradicional para abordar nuevos requisitos como la nube, los usuarios remotos, las aplicaciones, la tecnología del Internet de las Cosas y la tecnología operativa (IoT/TO). Esta realidad, además, aumenta la superficie general de ataque, que ahora se extiende a los dispositivos utilizados en casa y las redes wifi.

Estos tipos de riesgos de seguridad representan un problema crítico a la luz del número creciente de ataques de ciberseguridad en los últimos años. Un estudio reveló **que las violaciones materiales sufridas por las empresas de todas las industrias aumentó hasta en un 20,5 % entre el 2020 y el 2021**. Otro estudio demostró que **el trabajo desde casa aumenta la frecuencia de los ciberataques en un 23,8 %.**

Las violaciones de datos pueden ser costosas tanto en términos financieros como desde el punto de vista de la confianza del cliente. El costo de la violación de datos promedio aumentó en el 2022 a $4,35 millones, de $4,24 millones en 2021 y $3,86 millones en el 2020. Con la tasa actual de crecimiento, **se estima que el daño de los ciberataques alcance $10,5 millones anuales para el 2025**.

El departamento de TI, por su parte, termina desbordado por la creciente necesidad de asistencia, administración y mantenimiento de la visibilidad de todos los dispositivos remotos y de red conectados. Sin medidas de seguridad sólidas, los dispositivos remotos están en riesgo, ya sean de la empresa o de los empleados.

"Los departamentos de TI hoy se enfrentan a entornos de TI heterogéneos y distribuidos que son la contracara de un lugar de trabajo estandarizado en un entorno corporativo fortificado y con control de accesos", afirma Frank Ziarno, Vicepresidente de Gestión de Producto en TeamViewer. "El uso de redes de wifi desprotegidas o dejar las computadoras portátiles sin supervisión por un momento podría parecer inofensivo pero, de hecho, es fatal para una empresa. Para mantener una sólida postura de seguridad, los departamentos de TI necesitan expandir el mismo nivel de protección hacia los dispositivos remotos como si estuvieran en la sede central, a través de capacitación y soluciones de seguridad adecuadas."

Los principales desafíos de seguridad

A menudo, los riesgos menores pueden escalar (y de hecho lo hacen), con serias consecuencias si no se tratan rápidamente. Estos son los principales riesgos de seguridad que las empresas enfrentan al incorporar el trabajo híbrido:

1. Vulnerabilidades de los dispositivos remotos y de red

Un programa antimalware obsoleto es una de las amenazas de seguridad más importantes en lo que se refiere a dispositivos remotos y de red. Otros problemas potenciales incluyen sistemas operativos obsoletos, comportamiento anormal de la memoria y cortafuegos deshabilitados.

Los programas antivirus obsoletos o incompatibles pueden exponer a las empresas a riesgos serios, ya que propician que los jáquers controlen fácilmente los sistemas y los datos. Si bien los programas antivirus obsoletos pueden seguir funcionando hasta cierto grado, a menudo no pueden manejar y neutralizar los programas maliciosos o las amenazas de seguridad de forma efectiva.

2. Ciberataques

Los puntos finales como las computadoras y los dispositivos móviles simplemente no están protegidos de la misma manera que los servidores.

Los ciberdelincuentes reconocen los dispositivos como lugares vulnerables para ejecutar ataques con técnicas como el phishing, el secuestro de datos y los ataques de día cero, tres de los tipos de ataque más comunes y costosos.

3. Pérdida de datos

La pérdida de datos puede suceder de varias formas, como a través de la pérdida de dispositivos u el olvido de ellos en algún sitio. Por lo general, las empresas no realizan copias de seguridad de sus dispositivos, ya que piensan que sus programas antimalware ofrecen protección suficiente. Sin embargo, la pérdida de datos puede incluir lo siguiente:

- Los ciberdelincuentes que roban dispositivos de casas, oficinas, automóviles y cafeterías.
- Los empleados que accidentalmente borran archivos de los discos duros.
- Desastres naturales, como inundaciones e incendios.

Algunas empresas dependen de sus empleados para realizar la copia de seguridad de sus puntos finales. Pero es un error. Los empleados podrían no estar debidamente capacitados o motivados para realizar esa tarea. Depender de los empleados para ese fin también significa que el departamento de TI no podrá visualizar las copias de seguridad que se deben hacer supuestamente en discos duros externos. No hay forma de garantizar que las copias de seguridad se hayan realizado.

4. Monitoreo de TI insuficiente

Con frecuencia, los departamentos de TI no pueden visualizar por completo los dispositivos de los usuarios finales. El personal de TI no puede identificar si todos los dispositivos remotos e híbridos están funcionando correctamente y cuántos de ellos están conectados a la red corporativa en determinados momentos.

Sin un monitoreo eficiente, no se parchan los dispositivos que son vulnerables frente a los ciberataques ni se actualizan los sistemas operativos y los programas de terceros. El departamento de TI no puede realizar auditorías espontáneas de forma eficiente para encontrar programas prohibidos o potencialmente dañinos en la red de la empresa, identificar dispositivos no autorizados, ver el estado de las copias de seguridad o recopilar información crítica sobre los dispositivos sin depender de las acciones del usuario final. El riesgo no solo es para el punto final individual sino para la red entera.

Soluciones que funcionan

¿Cuál es la respuesta? Es fundamental comenzar con un panorama integral y completo de todos los dispositivos (sin importar el tipo de dispositivo, el fabricante o el sistema operativo), incluido cualquier dispositivo que sea propiedad de los empleados. Las aplicaciones y las herramientas que le permite al departamento de TI monitorear y gestionar todos los dispositivos de red pueden mejorar la eficiencia y la efectividad de la TI de manera dramática.

"La protección cibernética siempre será una batalla", afirma Robert Haist, Jefe de Seguridad de la Información en TeamViewer. "Los ciberdelincuentes siempre están al acecho y las empresas siempre deben estar un paso más adelante que ellos. La estrategia de seguridad de una empresa requiere atención, supervisión y reevaluación continuas de herramientas, estructuras y enfoques. Obtener y mantener datos profundos de todo el entorno de TI distribuido es el primer paso fundamental para lograr una postura de seguridad sólida y sostenible. Solo puedes proteger aquello que sabes que existe."

Aquí te presentamos cuatro tácticas para ayudarte a evitar los riesgos de seguridad asociados al trabajo remoto e híbrido:

1. Realiza un monitoreo web de forma proactiva.

Sin un monitoreo web proactivo, los empleados que navegan por la web pueden realizar descargas infectadas o acceder a sitios web maliciosos, ya sea de forma intencional o accidental.

Una solución de monitoreo web eficiente utiliza los servidores alrededor del mundo para probar tu sitio web periódicamente. Si el sitio web demora demasiado en responder o ya de plano no responde, se envía un alerta. Con un monitoreo web proactivo, el departamento de TI puede recibir información sobre una amenaza o un apagón. Una buena herramienta de monitoreo web debe tener lo siguiente:

- Scripts automatizados para que los procesos críticos se ejecuten en todo momento de manera correcta.
- Un tiempo de respuesta rápido con notificaciones para una rápida resolución de problemas.
- Un sistema de informes para obtener una analítica completa del rendimiento para fines de optimización.

2. Elimina tu VPN.

Si bien una red privada virtual (VPN) es la solución estándar para que los empleados accedan a los sistemas corporativos, esta presenta varias desventajas. Las VPN son complejas y su instalación y configuración conllevan mucho trabajo. Además, presenta problemas en términos de escalabilidad y seguridad.

Con una VPN, pueden surgir inconvenientes cuando los usuarios descargan archivos desde el servidor en su propia computadora y realizan cambios en el documento de manera local antes de guardarlos en el servidor.

En lo que la seguridad concierne, nada evita que los trabajadores remotos guarden documentos en sus dispositivos personales. Incluso, las VPN pueden dejar de funcionar sin motivo aparente y, como consecuencia, la conexión entre el servidor y el dispositivo queda desprotegida.

3. Utiliza una plataforma de monitoreo y gestión remota.

Con el acceso remoto, los trabajadores pueden acceder directamente a sus computadoras de escritorio del trabajo, ver una imagen en espejo de lo que está pasando en el dispositivo remoto y manejar el equipo desde cualquier lugar del mundo.

Todas las sesiones y los archivos transferidos cuentan con protección por cifrado de extremo a extremo. Los trabajadores remotos pueden trabajar de forma eficiente sin latencia o retrasos en las acciones como la transferencia o la descarga de archivos.

A diferencia de una VPN, que requiere de largas instalaciones y configuraciones y que debe ser compatible con tu rúter, las soluciones de acceso remoto basadas en la nube se pueden implementar y escalar en minutos sin tener que realizar un amplio mantenimiento.

Las plataformas de monitoreo y gestión remotos (RMM) mantienen los dispositivos seguros de tres formas, en un solo panel de control que es muy fácil de utilizar:

- Los programas antimalware evitan y corrigen los ciberataques.
- Las herramientas de gestión de parches eliminan las vulnerabilidades de los programas informáticos.
- Las copias de seguridad programadas periódicamente garantizan que los datos de los dispositivos estén respaldados en la nube y que estén disponibles para poder restaurarlos y recuperarlos si sucede un ciberataque.

Gracias a las plataformas de monitoreo y gestión remotos, el departamento de TI puede realizar auditorías espontáneas para detectar programas maliciosos en la red de la empresa, recolectar datos críticos sobre los dispositivos y visualizar fácilmente el estado de las copias de seguridad, las actualizaciones de los programas y los parches.

Conclusiones

Los riesgos de seguridad asociados al trabajo remoto e híbrido son reales. Pero con el enfoque adecuado y las soluciones correctas, las empresas pueden protegerse efectivamente para evitar futuros ataques e interrupciones en el negocio.

¿Estás en riesgo? Responde este pequeño cuestionario para saber a qué riesgos de seguridad del trabajo remoto e híbrido podría estar enfrentando tu empresa.

Sí	No		Sí	No	
○	○	¿Puedes asegurar que tus conexiones se realizan según los controles de acceso?	○	○	¿Puedes aprovechar los roles preexistentes en tus herramientas?
○	○	¿Sabes en qué momento determinado se utilizan tus herramientas?	○	○	¿Puedes utilizar funciones de compra centralizada y de delegación de gestión?
○	○	¿Cuentas con acceso a sistemas sensibles gestionados únicamente con permisos?	○	○	¿Puedes garantizar que tus usuarios son realmente de tu empresa?

Si respondiste "no" a cualquiera de estas preguntas, tu empresa está en riesgo. **Contacta a un experto** hoy mismo para hablar sobre las vulnerabilidades de tu empresa.

CIO

PATROCINADO POR TeamViewer