HOME OFFICE: ¿CÓMO PROTEGER LOS DATOS DE TU EMPLEADOS Y DE TU EMPRESA?

El Home Office es una forma de trabajo cada vez más buscada por las empresas. Permite una mayor flexibilidad tanto para los empleados como para los líderes empresariales, sin embargo, esta práctica no está exenta de riesgos desde el punto de vista de la seguridad informática y la protección de datos. Entonces, ¿cómo puedes proteger los datos de tu empresa así como los de tus empleados desde casa?

1. Identificación de los riesgos vinculado por el Home Office

El desafío de la seguridad informática en el Home Office, es de garantizar la protección de datos confidenciales de las empresas que manejen esquemas vía remota. Para esto, es esencial revisar la seguridad de TI, pero también crear conciencia a tus empleados sobre las mejores prácticas para evitar ataques cibernéticos.

Hay 3 riesgos principales vinculados con el Home Office para tus empleados y empresa:

- *La imposibilidad para tus empleados de tener acceso a los recursos necesarios* para sus trabajos (archivos, documentos) y, por lo tanto, la incapacidad para trabajar eficientemente.
- *La contaminación del sistema de tu empresa* vinculado a una violación de seguridad en el dispositivo personal de uno de tus empleados.
- *Eliminación o fuga de los datos confidenciales de tu empresa*.

2. Sensibilizar a tus empleados sobre los riesgos en términos de ciberataques

Tus empleados en su lugar de residencia son mucho más vulnerables que en su lugar de trabajo. ¿Por qué? Porque cuando están en Home Office, están menos concentrados porque no están en sus ambientes profesionales de trabajo, por lo tanto, se convierten en presas fáciles. Los “hackers” aprovechan de la relajación y la falta de atención de tus empleados. Muchas personas usan las mismas contraseñas, para su vida profesional y personal, por lo tanto, es esencial tener contraseñas separadas para garantizar un mínimo de seguridad en línea. Este punto parecerá básico, pero muchos colaboradores incurren en esta práctica.

Para evitar este tipo de inconvenientes, es esencial informar a tus empleados sobre los desafíos de la seguridad informática y recordar los conceptos básicos de seguridad cibernética, tales como:

- Realizar una actualización periódica del antivirus.
- Separar los correos electrónicos profesionales de los personales.
- Limitar el uso de periféricos (USB, unidad externa), de un computador a otro para transferir datos.
- Desasociar las contraseñas personales y profesionales.

3. Establecer un plan de prevención de riesgos

Para limitar los riesgos informáticos por el Home Office. Debes adoptar medidas concretas al nivel de tu empresa para protegerte a ti mismo y a tus empleados.

Asegurar tu sistema de información

Para evitar ciberataques, algunas medidas son necesarias para la protección de datos, tales como:

- Con un ERP o sistemas de gestión: **definir un perfil para tus empleados con acceso diferente según sus puestos**.
- Equipar todas las estaciones de trabajo, computadoras de tus empleados como mínimo **un firewall, antivirus y herramienta de bloqueo de acceso a sitios maliciosos**.
- **Desagrupar y proteger los dispositivos**. Más allá del antivirus, el sistema más efectivo para limitar la contaminación entre equipos profesionales y personales, es reducir los derechos administrativos tanto como sea posible en una computadora. Y, por lo tanto, asignar una computadora de trabajo para un empleado en Home Office que se actualizará periódicamente para seguridad.

Proteger tu empresa con la nube

Con la nube, el principal desafío es asegurar los datos almacenados que pasarán. Hay algunas reglas de seguridad cibernética que puedes establecer:

- **Definir una identificación única por usuario y prohibir cuentas compartidas**. Para las contraseñas, las reglas de seguridad son: al menos 8 caracteres que comprenden 3 de 4 tipos de caracteres (mayúsculas, minúsculas, números, caracteres especiales).
- **Utilizar protocolos que garanticen la confidencialidad y autenticación del servidor** receptor, por ejemplo HTTPS para sitios web y SFTP para transferencia de archivos, utilizando las versiones más recientes de estos protocolos.
- **Aplicar los últimos parches de seguridad al equipo y software utilizado** (VPN, solución de oficina remota, mensajería, videoconferencia, etc.)

- **Implementar mecanismos de autenticación de dos factores** en servicios accesibles de forma remota para limitar los riesgos de intrusiones
- **No permitir que las interfaces de servidor no seguras sean directamente accesibles**. En general, limite el número de actividades al mínimo estricto para reducir el riesgo de ataques.

Publicado el, 16/04/2020