¿Qué es el teletrabajo?

Se llama teletrabajo al método de trabajo donde el trabajador no se encuentra físicamente en las instalaciones de la empresa, sino que se encuentra en una ubicación distinta, pudiendo esta ser su casa o una conferencia, o cualquier ubicación fuera de las instalaciones físicas de la empresa donde está empleado.

El teletrabajo ofrece muchas ventajas, como ahorro de costes para la empresa y para el trabajador, y también de tiempo, al no tener que desplazarse. Se ha demostrado también que el teletrabajo incrementa la productividad de los trabajadores. Sin embargo, el teletrabajo por sí mismo conlleva un gran riesgo de seguridad, ya que las empresas no pueden controlar muchos factores sobre sus trabajadores y los puestos de trabajo que sí podrían controlar si estos estuvieran en las sedes de la empresa. Esto puede acarrear consecuencias como pérdida de información o dispositivos.

Entonces, ¿cómo podemos asegurarnos de que sea seguro?

Para mantener las cinco cualidades de la información (integridad, confidencialidad, trazabilidad, autenticidad y disponibilidad) es necesario que el entorno de teletrabajo cuente con medidas de seguridad equiparables a aquellas que se tendrían en la oficina.

Para explicar un poco más sobre las consecuencias de un entorno de telebrabajo inseguro, explicaremos las posibles situaciones que podrían darse:

Como dijimos, el teletrabajo no se da en las oficinas de la empresa. Esto significa que las medidas de seguridad física de la oficina pueden no estar disponibles. Por ejemplo, los guardias de seguridad, o el acceso mediante un badge o algún identificador, los elevadores con autorización, etc. Al no tener estas medidas disponibles, cualquiera podría entrar a la ubicación de nuestro ordenador. Se entiende que en nuestra casa, estaríamos protegidos por una puerta cerrada con llave, pero si desarrollamos el teletrabajo desde un café, por ejemplo, este no es el caso.

En estos casos, muchos ordenadores vienen con la posibilidad de utilizar un Kensington Lock en ellos para asegurarlos a la mesa, y la empresa debería proveerlos.

Además de esto, uno de los principales motivos por los que el trabajo remoto es peligroso es por el uso de ordenadores personales como estaciones de trabajo, una política conocida como BYOD (Bring Your Own Device). Un ordenador personal no tiene las mismas medidas de seguridad que un ordenador empresarial. No solo eso, sino que las empresas no pueden, por ley, obligarte a instalar ningún software en tu ordenador o dispositivo personal. Y por ende, la empresa tampoco puede asegurarse de que cumplas con políticas de seguridad que aseguren la integridad, confidencialidad, autenticidad, trazabilidad y disponibilidad de los datos.

Para poder sortear estos obstáculos en el teletrabajo, la empresa dispone de varios métodos, que veremos a continuación:

**Escritorio Remoto:** El escritorio remoto es un programa que viene en Windows por defecto, el cual permite manipular la computadora desde otro dispositivo y acceder a ella como si fuésemos el usuario que físicamente se encuentra frente a la máquina. Este programa viene activado en Windows por defecto, lo cual supone una gran vulnerabilidad que puede ser explotada por los atacantes para su propio beneficio. Desde Windows 11, el escritorio remoto ya no está habilitado. El escritorio remoto no viaja cifrado, y permite acceso indiscriminado a la máquina. No es un método recomendado de conectarse a una red de teletrabajo.

**El siguiente método es una VPN.** Una VPN o Virtual Private Network es una red virtual, como su nombre lo indica, que puede ser utilizada para encriptar la información en tránsito y disfrazar el punto de partida y finalización de una conexión. Existen, dentro de las redes VPNs, varias subcategorías, como redes montadas por la empresa misma, VPNs de par a par, o redes montadas por un proveedor externo y contratadas por la empresa.

De cualquier manera, sus beneficios son siempre los mismos. La VPN provee un encapsulamiento de la información, lo que impide que esta información sea vista por alguien que podría potencialmente estar espiando el tráfico de la red, ya que no podrá ver ni el tamaño ni el contenido del paquete.

Para conectarse a una VPN, sin embargo, se requiere a veces de una instalación de un plugin o de un software específico, lo cual nos pondría de vuelta en el planteamiento de que un empleado puede negarse si utiliza su propio dispositivo.

La VPN se puede utilizar para que el empleado se conecte a su escritorio remoto si este está habilitado, ofreciendo una capa extra de protección para volver este entorno más seguro, o se puede utilizar también para que el empleado se conecte directamente a la red de la empresa, como si su ordenador mismo estuviese dentro de la empresa. La desventaja del sistema VPN, sin embargo, es que al final todo el tráfico entra y sale del ordenador del teletrabajador, lo que implica que la información puede ser extraída del ordenador del teletrabajador si este no tiene las medidas de seguridad que debería tener en la empresa.

**El tercer método es un escritorio virtual o Virtual Desktop.** Un escritorio virtual es una solución de virtualización, como indica su nombre, donde la empresa pone a disposición del trabajador básicamente un ordenador virtual de la empresa con todas las configuraciones de seguridad y las aplicaciones que el trabajador necesitaría para realizar su trabajo en la oficina. La diferencia aquí es que este ordenador virtual está contenido en la red de la empresa, es totalmente manejable por la empresa, con lo cual el trabajador no puede negarse a instalar nada, y puede ser accedido desde donde el trabajador esté siempre que tenga una conexión a internet estable. Los datos y toda la información generada por el trabajo permanecerán dentro de los servidores de la empresa con esta solución, lo cual sortea otro de los problemas con los otros métodos de conexión. Un escritorio virtual tampoco es un escritorio remoto, con lo cual no cuenta con las mismas vulnerabilidades, sino que el usuario deberá identificarse antes de usarlo, y tampoco existe riesgo de que alguien se robe el ordenador, puesto que este no existe realmente.

Es una solución costosa, pero es la mejor solución para que un trabajador en remoto pueda conectarse a la empresa, ya que logra solventar todos los problemas que se pueden encontrar en los otros métodos. Aún así, incluso para trabajar en este tipo de escritorios, también se puede emplear una VPN como seguridad adherida.