Fernando de la Cuadra
Editor Técnico Internacional
Panda Software (www.pandasoftware.es)
E-mail: Fdelacuadra@pandasoftware.es

Seguridad en conexiones VPN

Cada vez más, los empleados de las empresas pasan muchas horas de su tiempo fuera de la oficina. Sin embargo, en aras de una mayor rapidez en las operaciones y una mejor relación con clientes y proveedores, es absolutamente necesario que estén conectados con la oficina. Esas conexiones se llevan a cabo a través de muchos tipos distintos de dispositivos, pero fundamentalmente a través de ordenadores portátiles y redes inalámbricas, ADSL o módem.

Sea cual fuere el sistema de conexión, no podemos olvidar que en esos ordenadores puede haber muchos elementos que no están controlados por los administradores de red y pueden no cumplir las políticas de seguridad establecidas en la empresa. Y, lo que es peor, en muchos casos (y la experiencia de los centros de Soporte Técnico de Panda Software así lo corrobora), los usuarios de estos ordenadores desactivan las medidas de seguridad (antivirus, firewall, etc.) para obtener un mejor rendimiento. En poco tiempo, los códigos maliciosos se apoderan del sistema.

Cuando el ordenador infectado se conecta de nuevo a la red empresarial, bien sea a través de una conexión remota o directamente en la red de la oficina, el peligro de propagación de esos códigos maliciosos instalados en el ordenador es muy alto.

Al igual que los empleados que se desplazan, los tele-trabajadores también pueden ser un peligro. El tele-trabajo es una forma flexible de organización del trabajo que consiste en el desempeño de la actividad profesional en el domicilio del trabajador. Engloba una amplia gama de actividades, e implica el uso de ordenadores y la conexión permanente entre el trabajador y la empresa.

Esta nueva visión del trabajo trae consigo que el ordenador con el que el empleado lleva a cabo sus funciones sea también, en la práctica totalidad de los casos, el mismo ordenador de uso familiar. No olvidemos que el tele-trabajo es una de las mejores opciones para compatibilizar el trabajo con la vida familiar, por lo que es probable que personas no formadas en materias de seguridad (o incluso el propietario del equipo, disfrutando de su ocio) permitan involuntariamente el acceso de códigos maliciosos al ordenador.

Otro peligro que suele plantearse es el problema de la posible intercepción de la comunicación entre la oficina y el tele-trabajador, o el empleado desplazado. La sola posibilidad de que un hacker pudiera hacerse con, por ejemplo, un plan estratégico, haría temblar a los directivos de cualquier empresa.

No hay manera de evitar al 100% que una conexión sea interceptada, cualquier usuario de una comunicación (sea postal, telegráfica, e-mail, etc.) lo sabe. Por ello se establecen sistemas de cifrado que hagan incomprensible la información a aquellos que no están implicados. Gracias a estos sistemas, puede asegurarse que aunque alguien pueda llegar a acceder a los datos transmitidos, éstos van a ser ininteligibles.

Uno de los sistemas más utilizados por las empresas para garantizar el secreto de las comunicaciones con empleados remotos son las Virtual Private Networks o VPN (Redes privadas virtuales). Estos sistemas consisten en la instalación de sistemas de cifrado de la información en el ordenador del tele-trabajador y en la "puerta" de las comunicaciones en la empresa. De esta manera, Internet, que es una red pública, se convierte de manera virtual en una red privada, ya que aunque el acceso a las trasmisiones sea posible, no lo es la interpretación de los datos transmitidos, lo que equivale a tener una red privada.

Ahora bien, si mezclamos el concepto de cifrado de la información de los tele-trabajadores con el de la protección contra código malicioso, nos encontramos con el problema de que si un usuario no cumple con los requisitos de seguridad de la compañía, puede estar infectado o

sufriendo el ataque de un hacker. En este caso, y gracias a la VPN, el virus o el atacante puede tener acceso directo a los recursos corporativos con el mismo nivel de privilegios que el usuario de la VPN. El riesgo es muy, muy alto.

Los usuarios de una red corporativa con un ordenador fijo y suficientemente protegido tienen el apoyo de los administradores de sistemas o de los técnicos de la red, de manera que las políticas pueden implementarse de una manera muy rápida simplemente por la proximidad física. Sin embargo, al estar el trabajador en otra ubicación, el "paraguas" no existe y puede producirse el desastre.

Para evitar estos problemas, la solución suele ser la instalación de mecanismos de seguridad en los ordenadores remotos, que impidan la entrada de códigos maliciosos o ataques de hackers, y no puedan ser desactivados por los usuarios. Esta solución es fácil de implementar, pero puede topar con la incomprensión de los usuarios, al sentir que tienen sistemas vigilados y cerrados. O, incluso, la negativa del usuario al ser el sistema propiedad del trabajador y no de la empresa.

Ante esto, la mejor opción es establecer, antes de que se establezca la conexión cifrada con la oficina, unos niveles de seguridad que deben cumplirse. Así, comprobando si existe, por ejemplo, un firewall activado, podremos tener la tranquilidad de que el usuario no está siendo espiado por un hacker.

La comprobación de los niveles de seguridad que debe cumplir el equipo remoto que desea conectarse a la red corporativa debe ser lo más amplia posible. Puede ocurrir que la política de seguridad en la empresa exija que el usuario tenga instalado el antivirus "X", y con una actualización "Y". Pero si el usuario remoto está estableciendo la conexión con su sistema particular, es posible que el antivirus sea completamente distinto y con requisitos de actualización distintos (los que establezca el propio usuario según sus necesidades o deseos). Aunque el sistema sea seguro desde un punto de vista objetivo, no estará cumpliendo con la política de seguridad de la empresa.

La solución para estos casos necesita de un sistema de chequeo de la seguridad remota de una manera amplia, admitiendo que hay sistemas de seguridad distintos y que cualquiera de ellos puede ser utilizado por un usuario remoto. Si la comprobación de la seguridad se lleva a cabo con miras amplias -eso sí, sin disminuir los niveles exigibles-, se flexibilizará la libertad de los trabajadores sin mermar las exigencias de seguridad.

Sin duda, es necesario establecer un sistema de chequeo del status de seguridad de los equipos remotos conectados mediante VPN a la red corporativa. Y el chequeo debe ser percibido por el usuario remoto como una ayuda a la seguridad general, no como una imposición corporativa y además, debe hacerse con suficiente amplitud como para abarcar productos y sistemas de seguridad no corporativos, sino elegidos por el tele-trabajador en su ámbito doméstico.

De esta manera, todos los implicados en la conexión a través de una VPN aumentarán su seguridad de una manera realmente efectiva.

Fernando de la Cuadra
Editor Técnico Internacional
Panda Software (http://www.pandasoftware.com)
E-mail: Fdelacuadra@pandasoftware.com