

Rincón Legal

La securización de las redes wi-fi



“La tentación ya no vive arriba”, vive abajo, enfrente, al lado y en cualquier espacio alrededor de unos pocos metros. Es la red más buscada y más vulnerable. La información viaja por las redes inalámbricas a través de habitaciones de hotel, oficinas, viviendas, cibercafés y aeropuertos, traspasando paredes y recorriendo calles, sorteando la seguridad y no con muchas garantías.

Ana Marzo Portera



Sin cables y sin protecciones físicas, estas redes abiertas no son capaces de garantizar los accesos no autorizados a las carpetas y archivos o la recuperación indebida de información que viaja a través de las mismas, bien sean datos, claves, contraseñas, cuentas de correo, conversaciones u otras informaciones.

Básicamente, las posibilidades de uso de las redes podemos resumirlas en dos: usos domésticos y usos empresariales. Es obvio que es aquí donde encontramos por tanto los mayores problemas, en la seguridad de las empresas y de los negocios, puesto que, en definitiva, la utilización de estas redes implica dejar una puerta abierta a todos los activos intangibles de una entidad, desde el capital humano y los conocimientos

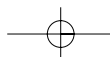
hasta las ideas, estrategias comerciales, listados de clientes, etc.

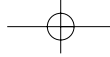
Aunque tradicionalmente los activos físicos han constituido la parte más importante del valor de cualquier entidad y se les ha considerado como el factor principal a la hora de determinar la competitividad de aquella en el mercado, en los últimos años es evidente que la situación ha variado de manera significativa. Así ha sucedido que principalmente, y como consecuencia de la revolución que se ha producido en las tecnologías de la información y el crecimiento de la economía del sector servicios, a menudo los activos intangibles han pasado a ser más valiosos que los activos físicos.

A diferencia de los activos tangibles, los

intangibles no tienen existencia material; están incorporados en procesos, prácticas, “saberes”, competencias y destrezas de los individuos, en culturas organizacionales y filosofías de gestión, en infraestructura organizacional y en elementos de propiedad intelectual. Es difícil valorarlos con precisión -sobre todo en el caso de las entidades privadas- hasta que la empresa sale a la venta, y su valor depende del comportamiento total de la organización en el mediano y largo plazo.

Y todo ello quizás a la vista y alcance de cualquiera que con un poco de destreza, habilidad e intuición, ciertos conocimientos básicos, un equipo adecuado y una tarjeta Wi-Fi puede entrar, ver, copiar y llevarse toda la información, o peor aún, la puede borrar y modificar.





Es bien sabido que, un modo fundamental de protección de todos estos activos intangibles es el jurídico, esto es, mediante su protección a través de los instrumentos que nos proporciona en la actualidad tanto la normativa sobre propiedad intelectual y/o propiedad industrial, como otras vinculadas. Ahora bien, por supuesto no hace falta decir que securizar los elementos donde se almacena la información es algo previo, fundamental y básico, dado que la protección jurídica no podrá evitar los daños emergentes, lucro cesante y perjuicios que a la empresa le cause una acción ilegítima derivada de la comisión de un delito informático o como algunos lo denominan "ciberdelito".

El mundo virtual basado en las nuevas tecnologías se ha convertido en un reto intelectual para unos y una barrera para otros. La complejidad técnica de los sistemas informáticos y del diseño de las redes y de los protocolos de comunicaciones que se utilizan genera indudablemente diferencias de conocimiento entre los usuarios de la Red. Éstas son utilizadas por unos pocos para hacer prevalecer sus intereses particulares o de sus organizaciones delictivas.

En este sentido, las redes Wi-Fi son objetivo de los apasionados del mundo de la informática, tanto de los "hackers" (con el solo fin de curiosar, sin intención de causar un desastre o daño alguno), o los "crackers" (con el objetivo de romper y producir el mayor daño posible).

Una cuestión importante para las empresas es

el hecho de que la inseguridad de las redes Wi-Fi está sancionada por nuestra legislación, cuando a través de las mismas un tercero, bien con el ánimo de curiosar, bien con el ánimo de causar un daño, accede a datos de carácter personal a los que en principio no está autorizado a hacerlo.

En estos casos, nuestros órganos de control (Agencia Española de Protección de Datos) y nuestros juzgados y tribunales han sido contundentes: la entidad que por el motivo que sea -responsable y/o encargado del tratamiento- legítimamente almacena información que contiene datos de carácter personal relativos a individuos (clientes, empleados, proveedores, candidatos a puestos de trabajo, personas de contacto y otros) está obligada a adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural, quedando prohibido a estas entidades el registro y tratamiento de datos en ficheros y sistemas que no reúnan las condiciones determinadas por la legislación vigente respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

En palabras de nuestras instituciones "no basta, entonces, con la adopción de cualquier medida, pues deben ser las necesarias para garan-

tizar aquellos objetivos que marca el precepto. Y, por supuesto, no basta con la aprobación formal de las medidas de seguridad, pues resulta exigible que aquéllas se instauren y pongan en práctica de manera efectiva..... considerándose infracción grave el mantenimiento de los ficheros sin las debidas garantías de seguridad...." Aún más, "...la entidad no observó una conducta diligente tendente a salvaguardar la información, y esta conducta basta para consumir la infracción. ... En consecuencia, esa falta de diligencia configura el elemento culpabilístico de la infracción administrativa.....".

En definitiva, en nuestra opinión y antes de adoptar la decisión empresarial de utilizar las redes Wi-Fi, cualquier entidad debería valorar una serie de cuestiones como son, su necesidad, oportunidad, funcionalidad, la determinación de sus usuarios, la política de seguridad a establecer tal como, cambio regular de contraseñas y claves, sistemas de encriptación, número de dispositivos de conexión, etc., riesgos económicos (daños, pérdidas, robos de información) y riesgos jurídicos (infracción y coste de la sanción). Quizás no en todos y para todos los casos el coste de oportunidad de uso de una red Wi-Fi sea lo más conveniente. ■

Ana Marzo Portera - Abogado
ana@equipomarzo.com

Marzo & Abogados

DERECHO Y NUEVAS TECNOLOGÍAS

Suscríbete gratis

¡Suscríbete gratis a nuestra revista AUSAPE!

La revista AUSAPE es el medio de comunicación directo de esta Asociación con sus empresas asociadas. En ella se informa de todas las actividades llevadas a cabo por AUSAPE, además de incluir información de primera mano sobre las últimas novedades tecnológicas que afectan al sector de las TIC.

Si todavía no estás suscrito y quieres recibir esta revista, totalmente gratis, rellena el siguiente cupón y envíalo por fax al número: **91 510 03 25**. También puedes mandarnos un e-mail a secretaria@ausape.es incluyendo en él los datos que se solicitan.

Empresa:

Asociado de AUSAPE (SÍ NO):

Nombre:

Cargo:

Dirección:

CP:

Población:

Provincia:

Teléfono:

E-mail:

Asociación de Usuarios de SAP en España
C/ Torrelaguna, 77
28043 Madrid
Teléfono: 91 456 72 11 / Fax: 91 510 03 25
e-mail: secretaria@ausape.es
Web: www.ausape.es

