SEGURIDAD APLICADA

Seguridad en Redes Wireless (Wi-Fi)

Las redes Wi-Fi poseen una serie de ventajas, entre las cuales podemos destacar:

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.

Pero como red inalámbrica, la tecnología Wi-Fi presenta los problemas intrínsecos de cualquier tecnología inalámbrica. Algunos de ellos son:

- Una de las desventajas que tiene el sistema Wi-Fi es la pérdida de velocidad en comparación a una conexión con cables, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- La desventaja fundamental de estas redes existe en el campo de la seguridad.
- Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son:

- Utilización de protocolos de cifrado de datos para los estándares Wi-Fi como el WEP y el WPA, que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos
- WEP, cifra los datos en su red de forma que sólo el destinatario deseado pueda acceder a ellos. Los cifrados de 64 y 128 bits son dos niveles de seguridad WEP. WEP codifica los datos mediante una “clave” de cifrado antes de enviarlo al aire.
- WPA: presenta mejoras como generación dinámica de la clave de acceso. Las claves se insertan como de dígitos alfanuméricos, sin restricción de longitud
- IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios.
- Filtrado de MAC, de manera que sólo se permite acceso a la red a aquellos dispositivos autorizados.

Dispositivos Fijos y Móviles

Máquinas y Dispositivos de Escritorio

Los ordenadores y dispositivos de escritorio (Impresoras, faxes, pequeños concentradores, concentradores usb, etc) son uno de los puntos más difíciles de controlar, pues dependen totalmente del uso o mal uso que el usuario mal pueda realizar de ellos o sobre ellos. La única solución en este caso es la implantación de una política clara y comprensible para el usuario mal de uso de los dispositivos que están a su cargo.

Es importante responsabilizar de alguna forma al usuario mal del hardware que está a su cargo, sin que esto suponga una carga añadida a su trabajo normal.

Ordenadores Portátiles

Debemos tener en cuenta la portabilidad de estos dispositivos, lo que los hace susceptibles de ser robados con facilidad, sobre todo cuando se encuentran fuera de la empresa.

Por eso debe responsabilizarse seriamente a los usuarios de los portátiles que sacan de la empresa, manteniendo un control de entrada/salida de estos dispositivos y de la integridad física de los mismos. En caso de robo el usuario debe comunicar con absoluta inmediatez a la empresa el evento que se ha producido, para que esta pueda minimizar los riesgos que implica el robo de los datos que ese portátil pueda contener.

Dispositivos de mano (Teléfonos Móviles, etc...)

Para los dispositivos de mano solo debemos decir que deben tomarse exactamente las mismas medidas que para los portátiles, aunque teniendo en cuenta que normalmente no contienen datos tan críticos para la empresa como los portátiles, aunque son mucho más fáciles de robar. Es bastante común este caso, el robo de un dispositivo de mano con todos los datos de un empleado, que luego pueden ser usados, pues suelen contener números de teléfono internos de la empresa, datos sobre la empresa y en los casos más aterradores incluso passwords de acceso a los sistemas.

Lo mejor que se puede hacer es no mantener nunca datos importantes en este tipo de dispositivos, sobre todo passwords de acceso, y el aconsejar también que si uno de estos dispositivos es robado o perdido se realice un informe donde se indique que datos susceptibles de ser usados para hacking social o informático pudiera contener el dispositivo.