

## **Un 60% de las redes WiFi carecen de protección, según un estudio de PandaLabs**

- **El informe Seguridad en Redes Inalámbricas pone de manifiesto la debilidad de los sistemas de protección WEP, así como la validez de las alternativas WPA y WPA-PSK**
- **Las pruebas de wardriving (exploración de las redes inalámbricas al alcance en un recorrido concreto) llevadas a cabo a nivel internacional arrojan resultados preocupantes: casi un 60% de las redes carecen de protección alguna**
- **Las redes WiFi se perfilan como una vía para llevar a cabo ataques dirigidos, ya que permite la intrusión en sistemas sin necesidad de intermediarios**

Panda Software publica el informe Seguridad en Redes Inalámbricas, un estudio llevado a cabo por PandaLabs en el que se pone de manifiesto las deficiencias de seguridad que presenta el protocolo WEP, el más usado habitualmente en entornos Wi-Fi, así como la razonable fiabilidad de otros sistemas más actuales, como WPA ó WPA-PSK. De hecho, casi un 60% de las redes, según el estudio, no implementan ningún sistema de seguridad.

El estudio comprende una introducción sobre las redes inalámbricas y una serie de conceptos básicos, para describir a continuación los principales protocolos de seguridad, como WEP y WPA, y sus principales debilidades. Del mismo modo, el documento aborda la seguridad en los sistemas de Portales Cautivos, aquellos utilizados para regular conexiones en redes abiertas, como las de aeropuertos, hoteles, o establecimientos públicos, entre otros. El estudio se puede descargar desde: <http://www.pandasoftware.es/wifi/>

El estudio pretende mostrar el nivel de seguridad de las redes inalámbricas desde un punto de vista didáctico, planteando métodos de seguridad y cómo estos pueden ser vulnerables por sus limitaciones de diseño, o si simplemente no están correctamente configurados, afirma Luis Corrons, director de PandaLabs. De este modo un usuario puede conocer los peligros que acechan desde el momento en que se despliega una red WiFi si no se toman las medidas pertinentes.

Las conclusiones del estudio son claras: la seguridad aplicada a las redes WiFi es, en general, insuficiente. Mientras que el protocolo más utilizado para la seguridad de la red, WEP, contiene múltiples vulnerabilidades, los protocolos más eficaces, como WPA ó WPA-PSK, apenas son implantados por los usuarios. PandaLabs pudo comprobar este extremo en diversas prácticas de wardriving realizadas a nivel internacional, en países como Suecia, Eslovenia, Canadá o Argentina, en las que casi un 60% de las redes carecen de protección. Las pruebas de wardriving consisten en el estudio de las redes inalámbricas detectadas a lo largo de un recorrido en concreto, por medio de un dispositivo WiFi móvil y un software de exploración de redes.

Las redes inalámbricas se perfilan como una vía de entrada para los códigos maliciosos silenciosos, así como para la realización de ataques dirigidos, ya que constituyen una puerta de acceso a las redes corporativas. No solamente permiten la introducción de hackers, sino de códigos maliciosos de todo tipo: desde aquellos que pueden estar diseñados para atacar a un usuario en concreto, hasta formas de spyware usadas solamente en cierto tipo de empresas seleccionadas por su tamaño, sector. etc.

Si bien es cierto que aún no se han explotado las redes inalámbricas de forma intensiva para fines maliciosos, parece claro que los usuarios no son plenamente conscientes de la amenaza que podría suponer para su seguridad comenta Luis Corrons. El caso de las empresas es más delicado: si hay redes corporativas con despliegue WiFi que no están correctamente protegidas, el alcance de un potencial ataque ya es más preocupante, ya que podría comprometer la seguridad de toda la empresa, y ser un punto de entrada a la misma para malware o ataques dirigidos, por medio de cualquiera de las técnicas explicadas en este informe

El documento finaliza con una serie de recomendaciones básicas para proteger redes WiFi, de acuerdo al análisis de seguridad realizado previamente, así como un análisis de las perspectivas de futuro.

Junto a este mensaje adjuntamos el propio estudio, aunque también está disponible en:  
<http://www.pandasoftware.es/wifi/>

Fuente;  
[PandaLabs](#)

**Fecha artículo: 2006-03-15 21:30:20 - url artículo: <http://www.internautas.org/html/696.html>**

**Logos y marcas propiedad de sus respectivos autores.**

**Los comentarios son propiedad y responsabilidad de cada autor.**

**© 1998-2009 Asociación de Internautas - <http://www.internautas.org>**

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)