Abaco
INSTITUTO SUPERIOR TECNOLOGICO PRIVADO

Mitos Acerca del Seguridad del Código Abierto

por Fernando P. García

1. El Software Libre es Riesgoso para la Seguridad de TI

- **Sólo lo usan fanáticos de "Hágalo Usted Mismo"**
  - La mayoría de grandes empresas de Europa y Norte-américa utilizan el sotfware libre para aplicaciones de misión crítica.
- **Es muy cambiante y evoluciona constantemente**
  - El Software Libre para seguridad de redes se encuentra en un proceso continuo de evolución debido a las constantes investigaciones y desarrollo de la comunidad de programación de código abierto.
- **Requiere constantemente de parches de seguridad: "Agujeros por todos lados"**
  - Debido a la gran cantidad de personas y compañias que trabajan buscando posibles errores y fallas de diseño, estos se descubren con mucha mayor rapidez que en el software cerrado e igualmente se corrijen con diligencia.

2. El Software Libre es Gratis

- **No tengo que pagar por algo que puedo bajar grátis de la Internet**
  - Aunque uno pueda bajar el software libre de forma "gratuita", la administración adecuada de este requiere de conocimiento y, por consiguiente; de una correcta inversión en soporte.

3. Los Proveedores de Código Abierto Añaden Poco Valor a los Proyectos de OSS

- **Pagar por soporte para Software Libre es un desperdicio porque los proveedores no añaden ningún valor**
  - Los proveedores de Software Libre dan soporte a la comunidad y no solo añaden valor a las aplicaciones, sino también documentación, mejoras de desempeño, respaldo financiero y más.
- **No es legal cobrar por algo que uno no ha desarrollado**
  - El desconocmiento de las licencias de código abierto, tales como: GPL ó BSD, lleva a pensar lo anterior, pero éstas definen claramente las reglas del juego y sobretodo la posiblidad de cobrar por añadir valor a las aplicaciones.

4. Las Soluciones Propietarias son Mucho Más Confiables que las de Código Abierto

- **El secreto del código cerrado lo hace más difícil de vulnerar**
  - La ley de Linuz nos enseña que la visiblidad de un error es directamente proporcional a la cantidad de ojos que revisan el software.
  - Los proveedores de código cerrado tienden a ocultar los errores de su software.
  - El software libre se auto-monitorea constamente y tiene políticas estrictas de revisión antes de lanzar versiones "estables".

5. La Seguridad del Software Libre es Demasiado Compleja para las Pequeñas Empresas

- **El software cerrado es más fácil de usar**
  - Los proveedores de código cerrado tienden a atrapar al cliente para mantenerlo comprando sólo sus productos y evitando que se acerquen a la competencia.
  - La integración entre herramientas de código cerrado es muy limitada y compleja, esto encarece el soporte.
  - El software libre busca la integración y ahorro de esfuerzos (ó calorías), reduciendo el costo de soporte.

Bibliografía

- **Astaro OrangePaper:** Descubriendo la Verdad Detrás de los Mitos de la Seguridad del Código Abierto. 2007-11-01. Angelo Comazzetto