

Cómo disminuir los delitos cibernéticos y su impacto económico

by Revista Vinculando - miércoles, enero 13, 2010

https://vinculando.org/articulos/software_antivirus_y_delitos_ciberneticos_impacto_economicos.html

Si nos detenemos a analizar, veremos que una gran variedad de las actividades cotidianas tanto en ámbito laboral como en el hogar, están vinculadas con el uso de una computadora personal y la red de redes Internet.

Dichas actividades van desde las académicas (investigación), laborales (empresas públicas o privadas), las que son simplemente redes sociales de comunicación (Facebook, Chat, Twitter, Messenger), etc.

Es importante considerar que existe un alto grado de riesgo de infección de nuestra información si no se cuenta con un software antivirus con firmas actualizadas, pero aún contando con éste, el riesgo persiste ya que cada día se crean más de 300 virus informáticos y 200 spyware en promedio en el mundo, por lo que la pregunta inmediata que surge es:

¿Cuál es la mejor protección Software Antivirus?

Basado en experiencias y pruebas de laboratorio realizadas a diferentes marcas de antivirus líderes en el mercado, podemos afirmar que no hay ningún software antivirus que ofrezca el 100% de certeza, y si alguno asegura que si, no está siendo honesto.

Lo anterior se sustenta en dos puntos principales:

El primero es el creciente desarrollo de malware y proliferación de los mismos en todo el mundo a través de Internet. En el evento “Symantec LeadershipForum 2009”, celebrado en México el pasado mes de octubre, se mencionó que estamos próximos a la preocupante cifra de 1,500,000 virus, de los cuáles solo es posible detectar un 80% de esta cantidad de firmas. Este aumento de virus informáticos va de la mano con el delito cibernético, por las ganancias que reditúa. Se estima que por cada 7,000 dólares invertidos, se obtienen ganancias alrededor de los 200,000 dólares. Adicionalmente a esto existe una falta de legislación para tipificar dichos delitos englobados en el termino de *cybercrime*.

El segundo es lo que llamamos “Día?Cero” (Zero?Day), que no es más que el tiempo que tarda en actualizar la lista de firmas nuestro software antivirus, desde que lo compramos hasta instalarlo y conectarse a Internet. Ya que durante este lapso de tiempo podemos tener el riesgo de ataques y pérdida de información. Varias firmas de virus cuentan con la protección proactiva para este caso, minimizando el riesgo hasta un 90%.

Para los expertos en Tecnologías de la Información, el impacto de los virus informáticos ha llevado a considerar a la información que poseen como un activo, por los costos que generan la paralización de productividad de sistemas comprometidos por ataques cibernéticos. Aún así las empresas no han hecho conciencia de lo grave de esta problemática y el impacto laboral, pues sólo asignan en promedio un 7% del presupuesto de informática para el rubro de seguridad. La crisis económica ha obligado a una tendencia a la baja del gasto mundial en tecnología de la información. La consultora Gartner previó un retroceso del 3.8% para 2009, es decir de los 3,400 millones registrados en 2008, se invertirían 3,200 millones de dólares el año siguiente. Como vemos es algo preocupante para la creciente oleada de ataques cibernéticos.

La siguiente tabla muestra solo algunos de los más de 10 análisis realizados para evaluar software antivirus cada año. Podemos ponderar cada punto de acuerdo a nuestras necesidades particulares de seguridad y presupuesto

Consideraciones

Soporte Técnico

Es importante contar con soporte técnico local para dar solución inmediata a problemáticas que se presenten con el software (24X7).

Precio

No menos importante considerar el costo por licencia del software, esto dependiendo de la suite o paquete que elijamos.

Intuitiva y Fácil

Debe contar con una interfaz amigable al usuario final, tanto para su instalación, como para su operación en el análisis de virus.

Efectividad

No es fácil comprobar la efectividad del software antivirus sin realizar pruebas específicas. Las estadísticas No siempre reflejan la realidad.

Actualizaciones

Revisar el tiempo programado del software para realizar la actualización de FIRMAS de VIRUS en línea, por lo general debe ser de horas o diario. Dependiendo de su laboratorio de investigación de análisis de virus emergentes.

Suite o Paquetes

Seleccionar un paquete implica un dilema, ya que existe una variedad de software antivirus: con Anti?Spyware, Anti?spam, Firewall, protección WiFi, protección Phishing, Control Parental, Optimizador de PC, Función Backup, Protección Robo de Identidad, etc., que incrementan el costo dependiendo de la solución mas completa. Por lo cual debemos generar un perfil de nuestros hábitos y servicios usados en Internet, para tomar el paquete mas ad hoc a nuestras necesidades.

Porcentaje de Falsos Positivos