Antivirus informático

Antivirus informáticos. Constituyen una herramienta básica de la seguridad informática, que garantiza en principios la protección final de una estación de trabajo contra la infección por programas malignos.

Antivirus informático

Concepto: Un antivirus es una aplicación o programa que identifica y elimina a los virus en las computadoras

Contenido

Surgimiento

Surge en la misma época en que comenzaron a detectarse y difundirse los primeros virus informáticos, también llamados "Virus de PC". El desarrollo y la venta del Software antivirus empezó a principio de la década de 1990 de la pasada centuria, y a lo largo de estos años se han ido consolidando y constituyendo en el producto básico de la Seguridad Informática.

Los antivirus se han convertido en compañeros inseparables del trabajo diario. Hoy en día no se concibe ningún equipo conectado a Internet que carezca de una buena protección contra programas malignos (virus, caballos de troya, gusanos, y otras denominaciones). Las situaciones de riesgo se multiplican cuando un

equipo se conecta a la Red de redes. Sin embargo ningún antivirus es 100% seguro, ya que a medida que avanza la tecnología se perfeccionan los programas malignos que han llegado en muchas ocasiones a deshabilitar antivirus usando vulnerabilidades de los mismos y de los sistemas operativos. Por eso es aconsejable tomar todas las medidas necesarias en los sistemas (deshabilitar reproducciones automáticas, autorun, restauras del sistema, instalar parches de seguridad actualizados, entre otras) y como punto culminante de este proceso tener un software antivirus que se pueda actualizar con frecuencia.

Concepto de Antivirus

Un antivirus es una aplicación o programa que identifica y elimina a los programas malignos en las computadoras; ayudan a eliminar algunas amenazas a la seguridad computacional que no necesariamente clasifican como programas malignos. Pueden realizar varias funciones en dependencia de su configuración, como por ejemplo anti–hacker, anti–spam, defensa proactiva y muchas más.

Antivirus

Los programas antivirus surgen de la necesidad de mantener los sistemas operativos en óptimas condiciones como vigilante seguro, además de proteger los ordenadores de los software mal intencionados. Un programa antivirus analiza información de muy diverso tipo y, en caso de que se encuentre infectada por algún código maligno, según las categorías existentes, procede a su desinfección o eliminación según la configuración que permita cada software. El análisis de la información se produce de muy diferentes maneras dependiendo de dónde provenga.

No es lo mismo que un antivirus se dedique a controlar la actividad de dispositivos extraibles, que la del correo electrónico, o la de la red local. El principio de funcionamiento es similar, pero con matices.El mecanismo de interceptación debe ser específico para cada sistema operativo o componente sobre el que se va a implantar el antivirus. De esta manera, cada vez que se vaya a acceder a la información del disco o de los disquetes, el antivirus interceptará la llamada a la lectura o escritura del disco, analizará la información que se va a leer o grabar y la analizará. Esta misma operación se realiza a través de un driver en modo kernel en Windows NT/2000/XP o un NLM interceptando la actividad de disco en Novell.

A partir de la ploriferación de los programas malignos, se ha desarrollado igualmente una industria dedicada a la creación de programas o antivirus, que tiene como finalidad detectarlos, erradicarlos o prevenir las infecciones virales. Como se ha mencionado, el problema de los programas malignos es que están escritos en códigos de programación muy diferentes que tienen características y funcionamientos muy diversos, lo que hacen que los programas antivirus, solo sean eficaces para combatir el tipo de programas malignos para los cuales fueron diseñados.

Clasificación de los antivirus

- **Preventores:** Los programas que previenen la infección, quedan residentes en la memoria de la computadora todo el tiempo y monitorean algunas funciones del sistema.
- **Identificadores:** Estos productos antivirus identifican programas malignos específicos que infectan al sistema. Los mismos trabajan con las características de un programas malignoss o sus variantes, o exploran el sistema buscando cadenas (secuencias de bytes) de códigos particulares o patrones característicos de los mismos para identificarlos.
- **Descontaminadores:** Sus características son similares a los productos identificadores, con la

diferencia que su principal función es descontaminar a un sistema que ha sido infectado, eliminando el programas malignos y retomando el sistema a su estado original por lo que tiene que ser muy preciso en la identificación de los programas malignos contra los que descontaminan.

Funcionamiento de los antivirus

Cada programa maligno tiene un código de "firma" (como huellas digitales) que lo identifica, por lo cual es detectado por el antivirus. Algunos antivirus tiene la capacidad de detectar programas malignos que no están en su base de datos. Esto se realiza por medio del sondeo del sistema en busca de síntomas clásicos de infección, como por ejemplo fechas extrañas en archivos, programas residentes en la memoria, una configuración extraña del sistema. El problema de esto es que puede dar "falsos positivos" es decir, puede dar por infectado un fichero que en realidad no lo está.

Algunos softwares antivirus

- Segurmática_Antivirus.
- Kaspersky Antivirus.
- Panda_Security.
- Symantec.
- Avira
- Avast!_free_antivirus
- McAfee.
- F–Secure Corporation.
- Nod32.
- AVG.

Programas antivirus

Software antivirus

Orientado a la protección contra el accionar de los programas malignos en sistemas operativos de Microsoft Windows. Incorpora las principales prestaciones de los programas antivirus de uso común, como son:

- Una interfaz amigable con diversas acciones y opciones de configuración.
- Un mecanismo de protección basado en la Protección Permanente y la Búsqueda de códigos.
- Un proceso de actualización de las bases de definiciones de programas malignos.
- El almacenamiento de las estadísticas de funcionamiento, cuarentena, información de códigos.
- La posibilidad de conectarse a un servidor corporativo para la administración remota.

Segurmatica Antivirus

Es la solución de antivirus cubana, desarrollada por la empresa Segurmática radicada en La Habana, cuya misión es garantizar la seguridad de las redes informáticas en Cuba. La versión actual de este producto consiste en software antivirus de ficheros que detecta y descontamina alrededor más de 195 000 programas malignos diferentes. De ellos más de 100 hechos en Cuba o para Cuba. Presenta una versión personal o cliente y una versión corporativa para una red local con dominio la cual permite administrar

centralizadamente los clientes instalados en la red. A sus bases de actualizaciones cada día se le añaden nuevas muestras de programas malignos internacionales que logran introducirse en las redes cubanas. La versión personal de este producto se comercializa para personas naturales en CUP.

SavUnix

Es la solución antivirus cubana para la protección de sistemas de código abierto, es desarrollada por la empresa Segurmática. Funciona para varias distribuciones y en la actualidad se trabaja en el desarrollo de una nueva versión para la protección de sistemas Linux. Es usada fundamentalmente en servidores proxy con filtros de contenido Web y puede utilizarse como para el escaneo a demanda en servidores Linux.

Panda Software

Líder mundial en la prevención de virus e intrusiones, ofrece soluciones de seguridad proactivas de un nivel superior para todo tipo de usuarios, desde grandes corporaciones hasta pequeñas y medianas empresas o usuarios domésticos. Sus productos para empresas permiten una administración automática y centralizada, sin problemas para la protección de toda la red.

Symantec

Le ofrece una de las mejores soluciones, muy fáciles de utilizar, para bloquear virus y piratas informáticos, proteger la información importante, filtrar el correo electrónico no deseado o proteger a su familia contra las amenazas de Internet. Con una colosal experiencia, Symantec es una de las empresas más veteranas en cuestiones de seguridad en Internet.

AVG Technologies

Proporciona completa protección antivirus para PC, redes, servidores de archivos y servidores de correo electrónico. La combinación de métodos de detección proporciona el máximo nivel de protección de los datos sin exigir demasiados recursos del sistema. Ofrece un largo período de licencia que incluye todas las actualizaciones de producto y soporte técnico.

McAfee Security

Ofrece a usuarios domésticos, a pequeñas, medianas y grandes empresas y corporaciones soluciones de seguridad sencillas y muy rentables para proteger los entornos de Microsoft. Protegen los equipos de virus conocidos y no conocidos y desbordamientos del búfer. Con "McAfee Protection–in–Depth Strategy" y su tecnología preventiva de intrusiones, puede detectar y bloquear a los usuarios malintencionados, protegiendo al ordenador antes de que se produzcan los daños.

Kaspersky

Pertenece a la compañia rusa "Kaspersky Lab", con representantes y socios en múltiples paises distribuidos en todos los continentes. Es considerado uno de los antivirus más completos al presentar una serie de opciones que permiten garantizar, además de la seguridad de los ficheros en el sistema, la detección de intrusos, cortafuegos, defensa proactiva, anti–spam, y otras. Este antivirus cuenta con versiones para

estaciones de trabajo y servidores para varios sistemas operativos como windows y linux, también presenta su Kit de administración para redes corporativas y presenta versiones desarrolladas para servidores específicos como "ISAServer".

Antivirus a elegir

Para hacer una buena elección de un antivirus es necesario tener en cuenta algunos requisitos:

- Actualizar patrones o firmas al menos una vez por semana.
- La empresa que lo promueve debe contar con un equipo de soporte técnico con acceso a un laboratorio especializado en códigos maliciosos y un tiempo de respuesta que no excedan de 48 horas, el cual pueda orientarlo en caso de que contenga una infección.
- Se debe contar con distintos métodos de verificación y análisis de posibles códigos maliciosos, incluyendo el heurístico que no se basa en firmas virales, sino en el comportamiento de un archivo, y así se podrá detener amenazas de falsos antivirus o incluso de posibles virus nuevos.
- Se debe poder adaptar a las necesidades de diferentes usuarios.
- Debe permitir la creación de discos de emergencia o de rescate.
- No debe afectar el rendimiento o desempeño normal del equipo.
- El programa residente en memoria debe ser lo mas pequeño posible.
- El número de pasos positivos que se den, tanto en el rastreo normal como en el heurístico, debe ser el mínimo posible.
- Su mecanismo de auto protección debe poder alertar sobre una posible infección por medio de las distintas vías de entrada, Internet, e–mail, red, discos flexibles etc.
- Debe tener posibilidad de chequear el arranque y los posibles cambios en el registro de las aplicaciones.

Fuentes

- Universidad Central "Marta Abreu" de las Villas (http://antivirus.uclv.edu.cu/)
- Segurmática (http://www.segurmatica.co.cu)
- Enciclopedia Informática v1.105. Ing. Osmanys Sánchez Díaz. 2005