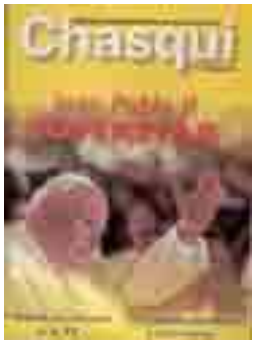


CHASQUI
Centro Internacional de Estudios Superiores de Comunicación para América Latina
chasqui@ciespal.net
ISSN 13901079
ECUADOR

2002

Francis Ficarra

ANTIVIRUS Y SEGURIDAD INFORMÁTICA: EL NUEVO

Chasqui, septiembre, número 79
Centro Internacional de Estudios Superiores de Comunicación para América Latina
Quito, Ecuador
pp. 72-77

Antivirus y seguridad informática:

El nuevo desafío cibernético del SIGLO XXI

Francisco Ficarra

La realidad de los primeros años del nuevo milenio pone de relieve el crecimiento, sin precedentes, de un sector de la sociedad informática, como es la temática del virus, los antivirus y demás mecanismos de seguridad para la información, almacenada principalmente en soportes magnéticos.

Al igual que en la medicina, es mejor prevenir que curar los posible daños que puedan afectar el buen funcionamiento del sistema informático. Obviamente, el factor costos hace que se pueda decidir por una alternativa u otra, dado las opciones existentes. Empero, en la actualidad no existe empresa de informática en el mundo que pueda avalar el 100% de seguridad ante un eventual ataque de los virus, ya que estos evolucionan minuto a minuto.

Francisco V.C. Ficarra, italiano, profesor, periodista y escritor. Residente actualmente entre la costa mediterránea española y los Alpes italianos.
Corre-e: ficarra@ctv.es - f_ficarra@libero.it

Ante tal realidad y siguiendo el camino trazado en la anterior entrega que apareció en Chasqui 78, se presentarán algunas de las alternativas comerciales existentes de distribución internacional, para frenar la expansión de dicha epidemia en los servidores de las grandes instituciones o en las computadoras de los usuarios.

figura - 1

figura - 2

figura - 3

La vulnerabilidad de las redes

Desde hace más de dos décadas, la información, generada por todos nosotros, comenzó un proceso de digitalización, es decir, de transformación al sistema binario. La finalidad era variopinta: agilizar el tiempo de acceso a los datos, disminuir los espacios de almacenamiento del soporte papel, duplicar los contenidos ante catástrofes irreversibles (inundaciones o incendios, por ejemplo), y un largo etcétera. En pocas palabras, poner a disposición de millones de usuarios del todo el planeta los conocimientos adquiridos durante la historia de la humanidad. No obstante, toda esta idea es cada día más frágil.

Ahora, en primer lugar, debemos hacer un breve comentario de cómo está constituida una red telemática. Como es sabido, el diálogo entre computadoras se realiza gracias a la red de telecomunicaciones, o sea, una red telefónica. En dicha red, la comunicación se efectúa por "paquetes" de información. La finalidad última es poner en contacto diversos sujetos, y los mecanismos de trasmisión adoptados permiten controlar la identidad del emisor y del destinatario (mediante un número y/o una serie de letras). Estos controles permiten definir los niveles de autorización para el acceso a la información que se encuentra dentro de la red. Una red que puede ser agrupada en intranet y extranet.

Intranet es una red que, desde la perspectiva técnica, se puede decir que es un componente de Internet (la súper red mundial), es decir, que está incluida en la misma. El objetivo es el acceso de los usuarios o empleados "in situ" pertenecientes a una institución comercial, industrial, etc. Por ende, se sostiene que es la situación típica de las empresas con un determinado nivel de informatización interna. A través de ella circulan todos los documentos relativos a la actividad que desarrolla, desde la oficina de proyectos, hasta la fabricación y pasando por las áreas de administración y técnicas, en el caso de una industria, por ejemplo.

Extranet también está contenida en Internet, pero no es la red interna de la empresa. Está constituida por aquellos colaboradores, proveedores, diseñadores y demás personas que trabajan a distancia, pero que deben acceder a los datos de la empresa o industria para efectuar sus trabajos. La conexión se efectúa mediante un módem.

En todos estos casos hay una computadora que tiene el rol de servidor de los servicios. Dicho servidor es el corazón del sistema informático y consecuentemente el centro de ataque de los virus. Un fallo en el servidor paraliza el trabajo de intranet y de extranet. De allí la importancia de velar por su seguridad.

Seguridad informática

Para solventar los problemas de seguridad, algunas casas comerciales de informática han ideado importantes sistemas denominados "security intelligence" (seguridad inteligente) para salvaguardar la información. Evidentemente, el tema de fondo son los costos. A continuación y al igual que en una pirámide, veremos soluciones de alto nivel, medio y común. Esta última, sería interesante instalarla en cada una de las computadoras personales.

Pirámide de la seguridad informática

Hasta no hace mucho tiempo, el alto nivel o la cúspide de esta pirámide virtual de la seguridad informática estaba reservado a instituciones bancarias u otras análogas (estamos hablando de una media superior de 50.000 dólares estadounidense para la licencia de un software que funciona en el servidor). No obstante, ante la actual coyuntura, se ha producido una nueva demanda de estos sistemas por parte de realidades con un poder adquisitivo inferior, pero que también tienen un servidor, al que hay que proteger. Por ende, hay un nuevo y gran mercado por satisfacer en muchos países del planeta.

Una manera de detectar posibles ataques es la instalación de sistemas que detectan la intrusión al sistema. Al respecto y a modo de ejemplo, la firma IBM, en el último trimestre, ha decidido adaptar un producto comercial para realidades con menor presupuesto llamado "Tivoli Intrusion Manager".

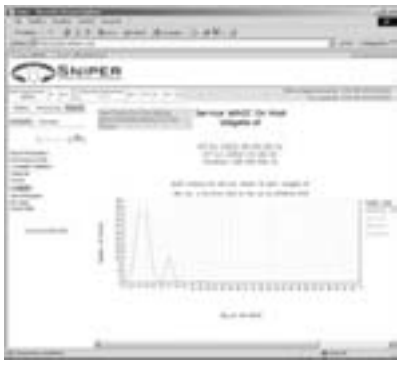


figura - 4

figura - 5

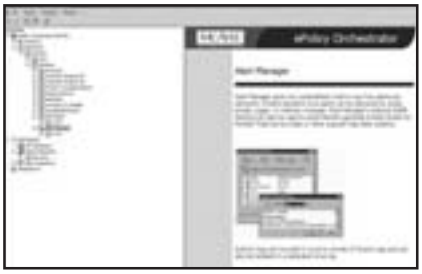


figura - 6

Dicho software es capaz, entre tantas cosas, de: relevar si hay ataques de virus, apagar el servidor, controlar el volumen de información que circula, verificar cada una de las claves de acceso a los documentos, en función del grado de autorización de los usuarios, etc., todo ello en segundos. Cada una de estas acciones se denominan "eventos". La instalación del mismo no es una tarea muy compleja, porque incluye un sistema tutorial, tal como se puede apreciar en la figura 1.

Estos programas se instalan en el servidor y en un par de computadoras para realizar las tareas de control o monitoraje de la evolución de los eventos.Por ejemplo, en automático y dado el ataque del virus, se puede desconectar el firewall y la conexión externa de Internet. Obviamente, para alcanzar tal automatismo es necesario programar el software. He aquí un nuevo problema relacionado o como consecuencias de los virus: la confianza y responsabilidad depositada en el responsable de tal gestión.

Un trabajo de esta naturaleza requiere una preparación previa y una constante disponibilidad -sábados, domingos y feriados inclusive- para resolver los problemas que se puedan presentar. Sin embargo, muchos rechazan esta labor, porque los salarios percibidos como informático en muchos países "industrializados" equivalen al sueldo de un administrativo (todo ello, gracias a la penosa defensa de estos intereses, realizada desde los departamentos de lenguajes y sistemas informáticos). En otras palabras, una gran responsabilidad pero sin reconocimiento alguno en el momento de recibir la paga o nómina.

También ha sonado la alarma en cuanto a los proveedores de servicios de mantenimiento de los sistemas informáticos, porque comúnmente se dice que la agresión es externa a la institución, pero las estadísticas en Europa señalan que muchas veces son debidos a situaciones de "dolo" del personal interno.

Lo cierto es que, por el coste de productos de esta naturaleza, todavía son muchos los que deben optar por otras alternativas. Los centros de cálculos de las universidades europeas tienen otro elemento más que ponderar, a la hora de presentar los presupuestos anuales (muchos recursos económicos de las instituciones educacionales se licuan ante los servicios de mantenimiento existentes y no pueden afrontar nuevas inversiones). Quizás, con el pasar de los meses, estas soluciones magistrales puedan disminuir, aún más el precio.

En este nivel están todas las empresas, fabricas e instituciones que cuentan al menos con un servidor y con un presupuesto de unos 10.000 dólares estadounidenses aproximadamente. Para ellos existe la alternativa de saber en tiempo real cuál es la situación de la red. Al respecto, está el software "Vipe-Kerbero" que pretende dar solución al 99,9% del problema de la seguridad inteligente, mediante el control de los recursos del sistema, haciendo hincapié particular en el firewall y actualizando velozmente las aplicaciones y sistemas operativos.

Para alcanzar todos estos objetivos dispone de las siguientes ventajas: seguimiento de las bases de datos, acepta cualquier tipo de plataforma, en cuanto a sistemas operativos se refiere, permite tener un inventario actualizado de todos los componentes del sistema y sus amenazas (figuras 2 y 3), dispone de un mecanismo de vigilancia y emite un informe con toda la información recogida (figura 4) y gráficas de estadísticas (figura 5).

Otros atributos de cualidad de la aplicación son:

- Policy manager, o sea, cubre el ciclo completo de todas las problemáticas de la vulnerabilidad de las aplicaciones dentro del sistema.
- Interfaz basada en la Web.
- Enciclopedia actualizada de cada uno de los problemas de seguridad.
- Actualización constante.
- Multiplataforma (soporta más de 850 productores de software).
- Alertas en función de los requerimientos del cliente.
- Posibilidad de búsqueda cruzada entre vulnerabilidad / fabricante del software.
- Búsqueda y consulta veloz de los datos críticos.
- Compatibilidad con todos los protocolos IP (son los de mayor difusión en la actualidad).

Desde el punto de vista operatividad/costo cabe señalar, entre otras, las siguientes ventajas:

- Es un producto que se puede administrar desde la Web del cliente, ya sea en modalidad local o remota (vía extranet).
- Control de la red (soporta cada plataforma y componente de la red).
- Monitoreaje en tiempo real.
- Señalización y activación de la alarma en cualquier momento de la intrusión.
- Informes detallados e integrados.
- Simplicidad de uso.

figura - 7

figura - 8

figura - 9

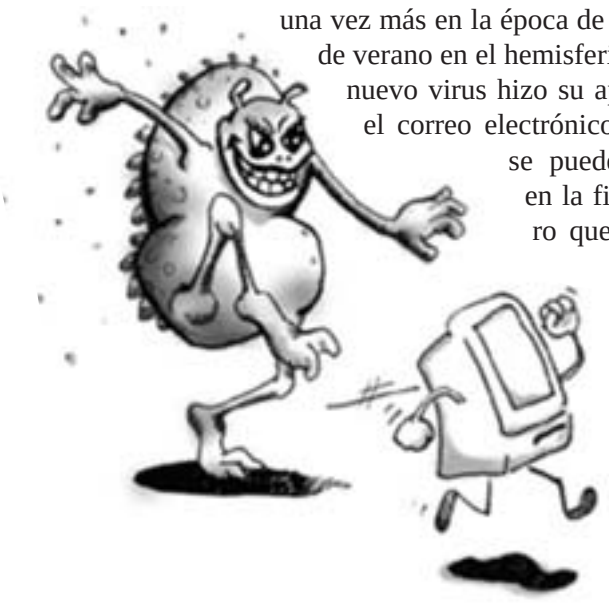
- No requieren licencias del software.
- No es necesario certificaciones o cursos de aprendizaje.

En este nivel están aquellas aplicaciones que acompañan a algunos productos de antivirus, como puede ser McAfee o Norton (en Europa son los dos principales software de antivirus que ocupan los primeros puestos en el listado de ventas). En nuestro caso seguiremos el ejemplo de "McAfee ePolicy Orchetrastor". En las figuras 6, 7 y 8 están algunas de las ventanas del mismo, con sus correspondientes opciones (por ejemplo, en la ventana de la figura 8 se puede ver el ataque de un virus). Su uso es muy simple y permite tener bajo control el correcto funcionamiento de la computadora, ante situaciones anómalas, generadas por los virus.

Se trata pues de una aplicación capaz de brindar el estado actual de la red y cada una de las computadoras que están conectadas. El beneficio de contar con una herramienta de estas características radica en el factor información actualizada. Por ejemplo, se puede saber el total de memoria disponible, el tipo de procesador (Pentium III, IV, etc.), el nombre del usuario, el idioma del sistema operativo, entre tantas otras variables. Esta aplicación se encuentra dentro del software de la firma McAfee.

Por supuesto que existen otras marcas de software antivirus y no es el objetivo final de esta entrega hacer publicidad a determinadas marcas, sino más bien dar información para que el lector tenga un esquema completo de la pirámide en estos temas.

Antivirus en acción



En el momento de escribir estas líneas y una vez más en la época de vacaciones de verano en el hemisferio norte, un nuevo virus hizo su aparición en el correo electrónico, tal como se puede constatar en la figura 9, pero que gracias al correcto funcionamiento del antivirus no generó ningún problema. El mensaje de la figura 10, recibido por un compañero de trabajo da la señal de alerta ante tal situación y aconseja descargar el antídoto del sito Symantec: www.symantec.com

Las aplicaciones antivirus se componen de un motor y un conjunto de vacunas que se actualizan de manera automática en el server (se puede programar varias veces a la semana cuando nadie está trabajando) y el motor una vez al mes, por ejemplo. En el caso del McAfee llevan las letras "Dat Files" (listado o archivo de vacunas) y "Engine Updates" (actualización del motor). Por cierto, hay que tener presente que el idioma del sistema operativo de la computadora es vital para descargar gratuitamente de Internet estos complementos del software antivirus de la firma McAfee. Cada uno de ellos tiene un número asociado que señala la versión de los mismos. Para mayor información al respecto se puede consultar la siguiente dirección de Internet: www.mcafeeb2b-.com/naicommon/download/dats/find.asp

Si consultamos la página Web de varios productores de software, el coste de estos programas no es muy elevado para los usuarios domésticos. Ciertamente que la mayor inversión recae en el servidor y cada una de las computadoras que componen la red interna (client). Pero que a nadie sorprenda que en muchos sitios de Europa, todavía se pueden encontrar servidores instalados sin antivirus. No es una cuestión de medios económicos, más bien se debe al analfabetismo en materia de cultura informática.

La instalación de estos programas comerciales no requiere de grandes conocimientos de informática, puesto que todos ellos disponen de un mecanismo tutorial. Lo que sí es vital es la práctica semanal de actualizar el antivirus y de vez en cuando el motor que lo hace funcionar.

A modo de cierre ...

Lo que se ha pretendido es tener una visión más global de las soluciones existentes en el mercado internacional en materia de seguridad y antivirus. Además, se ha confirmado una vez más, en estas líneas, que con el tema de los antivirus muchos

"hacen su agosto" (expresión coloquial que significa ganar dinero de manera fácil), en el mes de agosto o vacaciones de verano en la parte norte de nuestro planeta.

Los virus son el fruto de los algoritmos matemáticos en manos destructivas. Que a nadie sorprenda que muchos departamentos de matemáticas en el Viejo Continente sean un auténtico tumor maligno del buen funcionamiento de la informática y todas sus derivaciones. Basta ver los personajes burlones, indignos, incompetentes e ignorantes funcionarios que pululan como catedráticos o titulares en determinados centros de formación universitaria de la península Ibérica, por ejemplo. Lamentablemente y ante tal panorámica, tenemos virus para rato, porque nadie hace nada para erradicar tan penosa situación.

La cúspide de la pirámide de la seguridad informática tiende a acercarse más hacia todos los constituyentes de Internet, mediante políticas de reducción de precios en aplicaciones de elevada calidad y que antes eran destinadas a un sector muy selecto de la informática. Este es un paso importante y decisivo para eliminar la plaga que aflige a millones de usuarios de computadoras.

figura - 10

Hay que recordar siempre que el elemento clave, en todo este proceso, sigue siendo el ser humano. De nada vale tener el último software de avanzada tecnología y que cuesta muchos billetes, cuando a la persona que realiza tales labores no se le reconoce su tesón y responsabilidad para el buen funcionamiento de cada uno de los componentes de la red intranet, extranet e Internet.

Por último, hay que establecer un conjunto de políticas y su cumplimiento periódico para prevenir catástrofes mayores, como puede ser la pérdida completa de la información almacenada en un disco duro. Al igual que en la medicina, "más vale prevenir que curar".

LOS VIRUS EN LA RED

Los siguientes son algunos sitios de la red con información actualizada sobre los virus

- Estudio sobre virus informáticos http://www.monografias.com/
- Campaña que organizan conjuntamente el Gobierno español y la empresa Panda Software, con el fin de informar sobre el tema y dar soluciones a los afectados http://www.sinvirus.com/
- Centro de Alerta Temprana del Gobierno español sobre virus informáticos http://www.alerta-antivirus.es/

- Empresas desarrolladoras de software antivirus:
  http://www.mcafeeb2b.com/
  ttp://www.pandasoftware.es/
  http://www.vsantivirus.com/
  http://www.symantec.com/

- Antivirus gratis:
  http://www27.brinkster.com/
  http://www.ciberganancias.com/
  http://www.logratis.com/
  http://recursosgratis.com/
  http://www.ciudadfutura.com/
  http://www.123.cl/

- Portales informativos sobre seguridad informática, virus, criptología y antivirus:
  http://seguridad.internautas.org/
  http://www.kriptopolis.com/
  http://www.hispasec.com/
  http://www.antivirus.com.co/