Prevenir virus informáticos: primordial

Jan Hruska, Sophos Plc, Oxford, Inglaterra
Primera publicación: Agosto 2000

RESUMEN

En este monográfico se describe la actual situación de los virus informáticos, las vías de entrada más utilizadas, procedimientos de prevención, tipos de programas antivirus, instalación y administración de programas antivirus y medidas para contrarrestar los efectos de un virus.

Virus en la actualidad

La cifra de virus conocidos pasó de 50.000 en agosto de 2000.

La cifra de virus conocidos sobrepasó los 50.000 en agosto de 2000. La mayoría de ellos (74%) son virus parásitos (los que atacan a archivos ejecutables), a continuación están los virus de macro (19%) y el 7% son virus de sector de arranque. En mayo de 2000, el 88% de los virus notificados por clientes de Sophos fueron virus de macro, el 9% virus parásitos y tan sólo el 3% fueron virus de sector de arranque. Nótese que sólo se contabiliza cada virus notificado, y no el número de ordenadores al que afecta, por ejemplo, en una compañía; estas estadísticas no son infalibles pero sí reflejan lo que sucede ahí afuera.

El número de nuevos virus descubiertos cada mes no para de crecer. En el segundo trimestre del año 2000, en el laboratorio de virus de Sophos se trataron unos 800 virus nuevos cada mes.

Es imposible predecir cuál será el próximo virus en extenderse y causar daños por todo el mundo. Tendrá que analizarse cada uno de ellos e incluir su detección y desinfección en los programas antivirus.

Ante la avalancha de virus que llega a los laboratorios de las compañías antivirus, se presenta el dilema de cuáles tienen prioridad. Es imposible predecir cuál será el próximo virus en extenderse y causar daños por todo el mundo: tendrá que analizarse cada uno de ellos e incluir su detección y desinfección en los programas antivirus. De cualquier manera, existe un grupo de virus con un mayor **potencial** de expansión. Los virus que se autoduplican a través de Internet y los que emplean cierta psicología para facilitar su expansión (como el virus Carta de amor, Love Letter) están claramente dentro de esta categoría.

Medidas antivirus

Utilizar un programa antivirus no debería ser el único medio de defensa. ¿Qué otras medidas se pueden tomar?

No utilice .DOC

No utilice los formatos de archivo DOC o XLS. Es más seguro el formato RTF o CSV.

Es más seguro utilizar RTF. La apariencia del documento será la misma que en Word, pero el formato RTF no admite macros, por lo que no puede contener virus.

Aunque tenga cuidado: un archivo de Word con extensión RTF no es necesariamente inofensivo. Word puede guardar archivos en formato de Word (y con macros) bajo cualquier extensión.

No utilice .XLS

Es más seguro utilizar el formato CSV. Sucede igual que con los archivos RTF.

Utilice PowerPoint 7 o anterior

PowerPoint 7 y anteriores versiones no admitían macros, por lo que no había peligro de virus. De cualquier manera, las nuevas posibilidades que ofrece PowerPoint 8 respecto a versiones anteriores invitan al usuario a actualizarse, aunque pierda así una herramienta a prueba de virus.

Utilice visualizadores, no aplicaciones

Al hacer doble clic sobre un archivo, por ejemplo un adjunto de correo, la mayoría de los sistemas están configurados para ejecutar la aplicación asociada al tipo de archivo (archivos DOC abrirán Word, archivos XLS abrirán Excel, etc). El problema es que esas aplicaciones también ejecutan las macros de los archivos, y con ello los posibles virus.

La mayoría de los programas de email se pueden configurar para utilizar visualizadores de archivos. Estos programas no pueden, normalmente, ejecutar macros. Así, al visualizar el contenido de archivos de esta manera, no hay posibilidad de infección. En muchas ocasiones no necesitará trabajar sobre el documento, por lo que el sistema de visualizadores dentro de una compañía es un efectivo método antivirus.

No intercambie archivos ejecutables

En general, es completamente innecesario enviar archivos ejecutables. Si necesita enviar archivos comprimidos, es más seguro utilizar el formato normal (lo que requerirá que el receptor disponga del programa descompresor).

En la gran mayoría de los casos es completamente innecesario intercambiar código ejecutable; incluso, a veces, ilegal ya que viola los derechos de autor. Existe cierta tendencia a intercambiar archivos en formato autodescomprimible: por razones de seguridad es mucho mejor comprimir los archivos de forma simple (lo que requerirá que el receptor disponga del programa descompresor).

Es posible bloquear el paso de archivos ejecutables en la puerta de acceso a Internet. Por desgracia, es imposible detectar el código ejecutable con precisión total, ya sea comprobando la extensión del archivo o su contenido. De cualquier manera, bloquear archivos ejecutables con extensiones como EXE, VBS, SHS etc. resulta ser una excelente medida antivirus.

Concienciar al usuario es también una parte fundamental para prevenir infecciones a través de archivos recibidos por email: la tentación de instalar el último salvapantallas puede ser muy alta para alguien que no ha sido informado sobre los posibles riesgos.

Cambie la secuencia de arranque en la CMOS

La mayoría de los equipos vienen configurados para arrancar desde la unidad A: y, si no hay ningún disco en la disquetera, desde la unidad C:. Si el usuario deja un disco infectado en la disquetera, el equipo quedará infectado en el arranque.

Hacer que el equipo se arranque desde la unidad C: eliminará por completo el riesgo de virus de sector de arranque puros.

En los ordenadores actuales es muy fácil cambiar la secuencia de arranque de la CMOS. Hacer que el equipo se arranque desde la unidad C: eliminará por completo el riesgo de virus de sector de arranque puros. Si necesita iniciar el equipo desde la disquetera en un momento dado, podrá cambiar la secuencia de nuevo para esa ocasión.

La mayoría de organizaciones, sin embargo, no utilizan esta simple técnica.

Desactive Windows Scripting Host

Windows Scripting Host debería desactivarse.

Si no utiliza Windows Scripting Host (WSH), debería desactivarlo. Encontrará cómo hacerlo en http://www.sophos.com/support/faqs/wsh.html.

Manténgase informado con boletines de seguridad

Hasta noviembre de 1999, expertos antivirus podían afirmar con autoridad que un ordenador no podía quedar infectado con tan sólo leer un email. Por supuesto, habían analizado las especificaciones de los programas disponibles en ese momento y no existía ninguna forma aparente por la que eso pudiera suceder. Desafortunadamente, existían ciertas discrepancias entre las especificaciones de Microsoft Outlook y lo que el programa realmente hacía (también conocido como 'bug'), lo que permitió a virus como BubbleBoy infectar equipos con tan sólo leer un mensaje de correo. Microsoft publicó un parche para solucionar el problema (lea el boletín de seguridad de Microsoft MS99-032), aunque muy pocos lo aplican. Kakworm, que utiliza ese mismo agujero, es uno de los virus más extendidos hoy en día.

Kakworm, que utiliza un agujero de seguridad, es uno de los virus más extendidos hoy día.

La cada vez mayor complejidad de los programas actuales para conseguir más prestaciones, un aspecto más atractivo y otras sofisticaciones obliga a tener más gente trabajando en el programa para finalizarlo más rápidamente (lo que lleva de forma invariable a reducir el nivel de competencia del programador y la calidad de los programas). No tiene mucho sentido en quejarse de que Windows y los programas para este sistema operativo son inestables: la demanda insaciable del mercado es la principal culpable indirecta de los continuos fallos.

Esta situación no tiene visos de mejorar. Lo mejor que puede hacer una organización es mantenerse informada con boletines de seguridad para poder tapar agujeros.

Realice copias de seguridad

Pérdida de datos es sólo uno de los efectos de los virus. No es nuevo ni tampoco el peor de ellos. Las copias de seguridad son parte de la seguridad informática desde sus primeros días, evitando perdidas irreversibles de datos.

Corrupción de datos es mucho peor que su destrucción. Suele ser difícil de detectar, por lo que puede continuar durante meses.

Corrupción de datos es mucho peor que su destrucción. A menudo es difícil de detectar, por lo que puede continuar durante meses. Restaurar los datos desde copias de seguridad puede no ser solución, porque los documentos estén modificados o por obsoletos.

De cualquier manera, las copias de seguridad son una efectiva defensa contra los virus.

Tipos de programas antivirus

Escáner

Los escáneres son el tipo de antivirus más utilizados hoy día. Disponen de detección e información sobre la desinfección de todos los virus conocidos. Son fáciles de utilizar y capaces de identificar el virus (ARCHIVO.DOC está infectado con el virus 'Blah').

La principal desventaja es que deben mantenerse actualizados constantemente con información sobre nuevos virus para que sigan siendo efectivos.

De sumas de verificación

Se basan en la detección de cambios. Cuando un virus infecta un elemento, éste cambiará, lo que permite su detección. De esta manera se detectarán virus conocidos y nuevos, siempre que comprueben los elementos adecuados.

La principal dificultad es que este tipo de antivirus no puede detectar si el cambio en un archivo es legítimo o debido a un virus. En otras palabras, los resultados de un antivirus de sumas de verificación deben ser interpretados por alguien con experiencia. Otro problema es que estos antivirus detectan el virus una vez que se ha producido la infección; no sirven como medida preventiva. Sólo detección no es de gran ayuda.

Heurísticos

Los programas heurísticos usan reglas para distinguir lo que es un virus de lo que no. Por desgracia, no es todo tan sencillo.

Heurística (del griego ευρισκω, hallar, inventar) es la estrategia, método o truco utilizado para mejorar la eficiencia de sistemas que intentan dar solución a problemas complejos. En el contexto de programas antivirus, se utiliza para describir al programa que aplica reglas para distinguir lo que es un virus de lo que no. Estos antivirus heurísticos tienen el atractivo de que aparentemente no necesitan actualizarse.

Por desgracia, no es todo tan sencillo. El mayor problema es que los que crean los virus aprenden las reglas de detección y crean nuevos virus que las evitan. Las compañías antivirus tendrán entonces que modificar sus programas, por lo que los usuarios deberán actualizarse inevitablemente. Además, los antivirus heurísticos son proclives a generar falsas alarmas, es decir, encontrar virus donde no los hay. Este problema hace que no sean adecuados para el uso corporativo.

Puntos de entrada de virus

Para conocer dónde debemos colocar los controles antivirus en una organización, es importante establecer cuáles son los puntos de entrada más comunes.

Email

Actualmente, la inmensa mayoría de las infecciones están causadas por adjuntos infectados.

Actualmente, la inmensa mayoría de las infecciones están provocadas por adjuntos de correo electrónico infectados. La facilidad con la que el usuario puede ejecutar un archivo adjunto es uno de los factores que permiten la rápida expansión de estos virus. Si el mensaje es sugerente (algo como "lee con cariño la Carta de Amor que te envío") y la extensión del archivo adjunto parece inofensiva (LOVE-LETTER.TXT.vbs, un archivo de texto no puede tener virus, ¿no?), la tentación puede ser irresistible.

El peligro de infección por archivo adjunto, por supuesto, no es exclusivo del email. A través de grupos de noticias también es posible intercambiar archivos y cada día se bloquean más archivos infectados en estos servidores.

World Wide Web

La Web está plagada de páginas con material infectado. El acceso a Internet desde cada puesto en la oficina no es tan sólo posible, sino dado por hecho en muchos casos. Descargar archivos potencialmente infectados es muy sencillo.

En muchas organizaciones se han dado cuenta de que es mejor dar acceso a Internet desde equipos físicamente separados.

En muchas organizaciones se han dado cuenta de que es mucho más seguro ofrecer el acceso a Internet desde equipos físicamente separados. No sólo se separa así estos equipos de la red principal, sino que además los empleados tienden a pasar menos tiempo 'surfeando la Web' para temas no relacionados con el trabajo, ya que resulta obvio cuando no están en su mesa.

Disquetes y CD-ROM

El uso de disquetes ha descendido radicalmente con la implantación de redes, pero la mayoría de equipos aún vienen equipadas con una unidad para disquetes. El 3% de todas las infecciones se deben a virus de sectores de arranque, lo que demuestra que el disquete no ha muerto (todavía). El CD-ROM (a menudo el que acompaña a revistas), también ha demostrado ser un frecuente portador de virus.

Puntos de control antivirus

Instale un programa antivirus en la puerta de acceso a Internet, en el servidor y en las estaciones.

Existen tres puntos principales en los que debe instalar un programa antivirus: en puertas de acceso a Internet, en servidores y en cada estación de trabajo.

Puerta de acceso a Internet

La puerta de acceso es el punto que conecta la red interna de la compañía con Internet. Es sin duda un buen lugar para instalar un programa antivirus que compruebe cada correo, entrante o saliente, con archivos adjuntos.

La gran ventaja de disponer de un programa antivirus en la puerta de acceso a Internet es que un email con un archivo infectado que va dirigido a diferentes direcciones dentro de la empresa se bloqueará de una sola vez, sin que llegue a generar alertas en cada una de las estaciones de trabajo.

La principal desventaja de utilizar un programa antivirus en este punto es que puede actuar como un cuello de botella, ralentizando la entrada y salida de correo electrónico.

Hoy día pocos email se encriptan y la efectividad del escaneado en la puerta de acceso es bastante alta, aunque bajará en el futuro.

Un problema a considerar es el uso creciente de sistemas de encriptación de datos. No tiene sentido escanear adjuntos encriptados ya que los posibles virus quedarán ocultos. De momento no es una práctica muy habitual y la efectividad del escaneado en la puerta de acceso es bastante alta, aunque irá cambiando en el futuro.

Servidores

Utilizar un programa antivirus en el servidor para escanear los archivos almacenados es más eficiente que escanearlos desde una estación. En primer lugar, se minimiza el tráfico en la red ya que el escaneado se realiza de forma local en el servidor. Segundo, mecanismos de camuflaje que utilizan algunos virus no son efectivos ya que el virus nunca llega a 'activarse' en el servidor.

La mayoría de organizaciones instalan un programa antivirus para escanear los servidores en intervalos regulares, normalmente en períodos de baja actividad.

Estaciones de trabajo

El control antivirus en la estación de trabajo es probablemente la parte más importante en esta estrategia.

El control antivirus en la estación de trabajo es probablemente la parte más importante en esta estrategia. Incluso si un virus encriptado burla el escáner de la puerta de acceso de Internet, o si el escáner del servidor no lo detecta (ya que no escanea el email), el virus será detenido en la estación de trabajo antes de que pueda infectar el equipo y extenderse.

Mantener al día el programa antivirus de todas las estaciones de trabajo es a menudo uno de los principales problemas con los que se encuentra un administrador de sistemas; especialmente si no todos los equipos se encuentran permanentemente en red (como portátiles que se conectan sólo durante ciertos intervalos de tiempo).

Administración de programas antivirus

Ya que hoy día la efectividad de un programa antivirus depende de la frecuencia con la que se actualiza, es muy importante que el programa cuente con las herramientas más efectivas a la hora de instalar, actualizar y administrar el sistema antivirus.

Actualización a través de Internet

Actualización automática de un antivirus a través de Internet es una idea muy atractiva para administradores de sistemas. Sin embargo, esto implica dar control a la empresa antivirus sobre la red interna.

Actualización automática de programas antivirus a través de Internet es una idea muy atractiva para administradores de sistemas. Sin embargo, esto tiene serias implicaciones para todo el sistema de seguridad de una organización ya que se está dando a la empresa del programa antivirus el control y el poder de decisión sobre lo que se instala en su red interna. Pocas empresas ofrecerían dicha libertad, se prefiere la intervención de un especialista para controlar el proceso. Esa persona podrá decidir cuándo y cómo realizar ciertas actualizaciones, y cualquier programa nuevo se probará antes de instalarlo en toda la red.

Administración

El administrador que se enfrente a la instalación a gran escala de un programa antivirus deberá disponer de una herramienta eficaz con la que comunicarse con el programa (admin->programa->admin). El programa necesita mantenerse actualizado (admin->programa) mientras que el administrador necesita conocer la situación en cada momento, en relación con virus y otras partes del programa (programa->admin).

Para la realización de actualizaciones se utilizan principalmente tres técnicas diferentes: 'push' (el servidor lleva a cabo el proceso), 'pull' (cada estación se encarga de su propia actualización) y una combinación push/pull. Todas tienen sus ventajas e inconvenientes y la utilización de una u otra técnica dependerá de la estructura de la red, la velocidad de las conexiones, el modelo de utilización, etc.

Contrarrestar los efectos de los virus

Si pasara lo impensable y un virus lograse penetrar todas las defensas, la organización debería disponer de un sistema de contención para minimizar el número de equipos infectados.

Si pasara lo impensable y un virus lograse penetrar todas las defensas, la organización debería disponer de un sistema de contención adecuado para minimizar el número de equipos infectados, además de poder restaurar el estado anterior de estos. Se trata de un tema relativamente complejo y las soluciones no son sencillas.

Una incursión vírica normalmente ocurre cuando el programa antivirus no es capaz de reconocer un determinado virus. Mantener una buena relación con la empresa antivirus y saber que actuarán de forma inmediata ante cualquier emergencia forma parte de una buena estrategia antivirus.

Tratar la infección de virus que se dejan entrar en la organización será bastante más caro que el coste de mantener un programa antivirus. El mayor gasto irá en horas de trabajo, ya que probablemente será necesario desinfectar cada estación de trabajo (inutilizada mientras tanto) por separado y dejarla en su estado anterior.

Disponer de reglas de estandarización para la instalación de los programas que se utilizan en la organización, incluso la utilización de imágenes de disco, será de gran utilidad a la hora de restaurar estaciones infectadas.

S|O|P|H|O|S

Sophos Plc • The Pentagon • Abingdon • Oxfordshire • OX14 3YP • Reino Unido
Tel +44 01235 559933 • Fax +44 01235 559935

www.sophos.com