

La actualización de programas como medida de seguridad



No es una solución universal, pero definitivamente un elemento importante

Prefacio

Todos conocemos la necesidad de realizar actualizaciones e instalaciones de parches de manera oportuna, pero ¿cómo podemos asegurarnos que nuestros sistemas realmente están más protegidos?

¿Qué pasaría si no instalamos uno o más parches?

¿Vale el tiempo y esfuerzo invertidos?

¿Será su sistema más vulnerable, a los ataques de piratas, si no los instala?

Algunas respuestas a estos interrogantes:

El objetivo de la actualización:

Al actualizar e instalar parches en programas de su ordenador, logra dos objetivos:

1. Sus aplicaciones se encuentran más actualizadas, lo que debería mejorar tanto el rendimiento como la estabilidad.
2. Sus programas son menos vulnerables a los ataques y, por lo tanto, más seguros.

El primer objetivo es bastante simple: obtener actualizaciones que están diseñadas para las configuraciones actuales de su equipamiento físico y de las aplicaciones instaladas en su ordenador.

Por consiguiente, los programas actualizados deberían ejecutarse de manera más efectiva y sin problemas en su equipo. Este enfoque garantiza menos errores y mal funcionamiento y, a la vez, disminuye el tiempo para ejecutar una tarea específica, por ejemplo, una actualización de un juego que ha sido diseñado para incrementar el índice de actualización de marcos.

El segundo objetivo es fácil de entender pero difícil de medir. La teoría indica que la actualización cierra los agujeros existentes en sus programas y elimina las vulnerabilidades inherentes, de forma tal que las aplicaciones se tornen más seguras y más resistentes a las intrusiones y secuestros.

Pero, a menos que usted sea un profesional de la seguridad, es difícil calcular la efectividad y confianza de estas actualizaciones. Por lo que muchos usuarios se preguntan: ¿Realmente me beneficio al instalar estas actualizaciones de seguridad?

A continuación trataremos de responder esta pregunta razonable, concentrándonos en las actualizaciones de seguridad, pero siempre recordando que las mejoras de rendimiento y estabilidad, son casi tan importantes para la salud y confiabilidad general de su sistema como las anteriores.

Tipos de actualizaciones de seguridad

Las actualizaciones de seguridad pueden dividirse en cuatro tipos principales:

1. Filtrado de paquetes (tráfico global y datos por proceso)
2. Vigilancia de puertos
3. Defensa contra ataques de piratas
4. Protección de la privacidad del usuario

1. Actualizaciones sobre el sistema operativo

El sistema operativo más utilizado en la actualidad es Windows en su versión XP. Todos los meses, múltiples actualizaciones a sus servicios internos, diseño de motor, componentes integrados, controladores propietarios y pequeños programas utilitarios, se publican en el llamado martes de parches (*Patch Tuesday*).

Estas actualizaciones solucionan problemas con protocolos de conexión, reparan el Kernel para que refleje los últimos estándares de seguridad y, además, aplican ajustes a la configuración actual de seguridad y a la del entorno. Todo esto con el objetivo de incrementar la seguridad del programa principal: el sistema operativo del ordenador.

Muy a menudo, hemos visto un pico en la cantidad de epidemias de virus y gusanos que pueden vincularse, directamente, con la autocomplacencia e indiferencia de las personas, a las actualizaciones del sistema operativo. Estas actitudes son el desencadenante para comprometer a gran cantidad de ordenadores en todo el mundo. Los ejemplos son variados, y los resultados, desafortunadamente, pueden ser muy graves. Probablemente recuerde el episodio de los archivos *Windows Metafile* (WMF) a finales del año pasado: se descubrió una falla en la forma en que Windows procesaba algunos formatos de archivos gráficos, lo que permitió a los agresores crear gráficos especiales y explotables que ejecutaban, de manera remota, código arbitrario en sistemas sin parches.

La vulnerabilidad afectó no solamente a los productos de Microsoft (por ejemplo, Outlook e Internet Explorer), sino también a aplicaciones de terceros, que confiaban en los motores compartidos de creación de gráficos *Windows Metafile* (WMF) y *Enhanced Metafile* (EMF) para mostrar imágenes. El resultado final fue que cualquier imagen infectada que se abriera en un ordenador (ya sea al visitar, sin darse cuenta, un sitio de Internet con gráficos dañinos o, al visualizar un correo electrónico con este tipo de archivos) causaba automáticamente una descarga de código malicioso.

Si bien Microsoft demostró rapidez para solucionar este problema, los usuarios no mostraron lo mismo para actualizar sus sistemas y corregir esta vulnerabilidad. Por lo tanto, una gran cantidad de virus y otros programas con código malicioso explotaron la falla, e infectaron cientos de miles de equipos. Sólo en ese momento, los usuarios se dieron cuenta que aplicar los parches de seguridad, podría ser una buena idea.

Windows es un programa tan complejo y con tantas piezas, que cuenta con varios servicios (programas pequeños complementarios) que se ejecutan, deliberada y predeterminadamente, en segundo plano. Estos subprogramas satisfacen los requerimientos de las personas que utilizan configuraciones sofisticadas en las aplicaciones de su trabajo (más comúnmente en entornos con múltiples usuarios y controladores de dominio). La mayoría de los usuarios hogareños nunca utilizan estos servicios, por lo tanto, desactivarlos es una opción segura.

Puede obtenerse información valiosa acerca de la ejecución de servicios, y de algunos a menudo innecesarios, de estas fuentes reconocidas de Internet:

[PC Flank](#)

[Black Viper](#)

Algunos de estos servicios utilizan la red para comunicarse, y por consiguiente, abren sus propios puertos de conexión y escuchan los comandos desde un equipo remoto. A continuación, comunican los datos sobre estos canales cuando se establece un enlace legítimo.

Cuando estos servicios presentan fallas o vulnerabilidades (ya sea a través de una investigación interna o como resultado del trabajo de un investigador en seguridad independiente) todos esos canales de comunicación, se convierten en un objetivo muy tentador para que los piratas se apoderen de equipos vulnerables, e invadan las redes. Con frecuencia, este camino ha sido utilizado para explotaciones y sin duda continuará siendo utilizado, hasta que Microsoft tome cartas en el asunto para evitarlo.

Dado que Windows es tan complejo, es casi imposible que publique parches rápidamente y de manera consistente, porque se debe realizar una gran cantidad de pruebas e investigaciones para garantizar que los parches no inutilizan otros programas. Por lo tanto, los usuarios nunca pueden estar seguros sobre cuántas vulnerabilidades de seguridad han dejado de ser tratadas en alguna publicación en particular de parches (y, por lo tanto, están abiertas para ser explotadas por la comunidad de piratas).

Más allá de esto, existe también un mercado negro de vulnerabilidades de Microsoft, dónde personas sin escrúpulos venden sus descubrimientos a bandas de delincuentes cibernéticos, por supuesto, sin el conocimiento de Microsoft.

Para acceder a la configuración de la herramienta de actualizaciones automáticas de Windows XP (Windows Update):

1. Localice el vínculo **Mi PC**.
Puede acceder a través del Explorador de Windows y el menú Inicio, entre otras posibilidades.
2. Pulse con el botón secundario del ratón sobre el mismo y posteriormente en **Propiedades**.
3. Seleccione la pestaña **Actualizaciones automáticas**.
4. De acuerdo a sus preferencias y entorno de trabajo, establezca la configuración deseada.
5. Pulse en el botón **Aceptar**.

Las actualizaciones de MacOS y Linux también pueden recuperarse y aplicarse automáticamente. Para obtener instrucciones acerca de la actualización de estos sistemas operativos, diríjase al correspondiente archivo de **Ayuda** en su ordenador.

2. Actualizaciones a programas integrados en el sistema operativo

Los programas embebidos en el sistema operativo, incluyen aplicaciones integradas en el paquete de instalación, junto con el sistema operativo mismo.

La mayoría de estos programas fueron diseñados por Microsoft y para Windows, por consiguiente es su responsabilidad mantenerlos seguros y actualizarlos cuando sea necesario.

Microsoft ha avanzado en este sentido, pero nada es 100% seguro en el negocio de las aplicaciones. Los programas de Microsoft no son la excepción (sino más bien la regla) y, por lo tanto, a menudo tienen defectos en la seguridad.

Casi todos los meses, aparecen en las noticias, nuevas historias de vulnerabilidades en el programa navegador (Internet Explorer), en el cliente de correo electrónico (Outlook Express) y en el reproductor multimedia (Windows Media Player).

Por lo tanto, es importante actualizar todas estas aplicaciones de Microsoft preparadas para Internet, a través de los procedimientos de **Actualizaciones automáticas** mencionado anteriormente.

3. Actualizaciones a controladores de dispositivos

Los controladores de dispositivos son pequeños programas que manejan el funcionamiento del equipamiento físico instalado (adaptadores de red, tarjetas gráficas y de sonido, entre otros).

Al instalar los controladores más recientes, no solamente mejora el rendimiento y elimina los problemas de estabilidad, sino que también tiene la oportunidad de cerrar cualquier agujero de seguridad.

No hace mucho tiempo, se informó de un **caso** en el que los controladores de la plataforma de Intel Centrino tenían una falla que abría el acceso a la red inalámbrica del ordenador infectado.

Esto permitía, a los agresores, ejecutar código de manera remota en los ordenadores portátiles basados en Centrino.

Los usuarios de este tipo de equipo fueron notificados para que aplicaran rápidamente el parche corrector.

Estos tipos de fallas aparecen cada vez más a menudo. A medida que la conectividad inalámbrica y el acceso a Internet de alta velocidad continúan ampliándose, los usuarios de dispositivos de telecomunicaciones, como por ejemplo, módems, adaptadores inalámbricos y enrutadores deben estar alerta y consultar los sitios de los fabricantes, de vez en cuando, para asegurarse que cuentan con los últimos controladores instalados.

4. Actualizaciones a programas de terceros

Las aplicaciones de terceros son aquellas cuyos desarrolladores difieren del desarrollador del sistema operativo donde se encuentran instaladas.

Si bien la mayoría de los usuarios utilizan un núcleo central de aplicaciones de Windows, programas como Adobe Acrobat Reader, el navegador Firefox, Skype VoIP o la barra de herramientas de Google, pueden encontrarse en diversos ordenadores hogareños con acceso a Internet.

Estos y otros programas, dado que son populares y ampliamente utilizados, han experimentado problemas de vulnerabilidad de la misma forma que Microsoft, lo que llevó a los desarrolladores a publicar parches.

Ya que la mayoría de estos programas utilizan Internet para funcionar, la regla general es dejar la actualización automática activada y ejecutar estos programas solamente cuando sea necesario.

La desventaja de las actualizaciones de seguridad

Junto con los efectos positivos de la actualización, también existen algunas desventajas.

Algunos programas, por ejemplo, pueden perder temporalmente la capacidad de acceso a Internet o desactivar parte de su funcionalidad.

Pero estas situaciones no son muy comunes y el desarrollador de la aplicación en cuestión brindará habitualmente un parche a los usuarios. También es un buen motivo para registrar su programa con el desarrollador, para que sepan dónde encontrarlo cuando necesiten enviarle información urgente y/o de gran importancia.

Puntos importantes a realizar junto con la actualización

Aún cuando esté siguiendo de cerca las recomendaciones de actualización y, actualice sus programas regularmente, existen algunos pasos adicionales que debería seguir:

1. **Instale un cortafuegos personal de calidad**, como por ejemplo Outpost Firewall Pro, que puede cerrar los canales de conexión de su ordenador, y proteger sus datos de las personas que inician conexiones de Internet no autorizadas o innecesarias;

2. **No ejecute programas desconocidos**, si no reconoce el programa o no confía en sus creadores, utilice las herramientas de búsqueda de Internet para realizar una pequeña investigación acerca de la compañía y la aplicación antes de permitirle que se ejecute en su sistema;
3. **No abra archivos adjuntos sospechosos** tanto de personas conocidas como desconocidas, y no navegue en sitios de Internet de dudosa reputación.

Programas con mayor tendencia a tener problemas de seguridad

1. Todos los servicios de Windows que utilizan la funcionalidad de acceso remoto (Servicio Servidor, Telnet, Escritorio remoto, entre otros).
2. Todos los programas integrados en Windows que acceden a Internet (Internet Explorer, Windows Messenger, entre otros).
3. Cualquier programa de terceros que confíe en la funcionalidad de acceso a Internet (navegadores, reproductores de contenido multimedia remoto, entre otros).

Conclusiones

La actualización de seguridad es uno de los procedimientos clave de mantenimiento, que debería realizar regularmente en su ordenador. Los beneficios de contar con un sistema actualizado y bien configurado superan, en gran medida, el tiempo que lleva ejecutar las actualizaciones.

Considerando que puede realizar la mayoría de las actualizaciones automáticamente y en segundo plano, no existe una excusa real para no instalar los parches y tener un ordenador funcionando en perfectas condiciones.

Enlaces útiles:

- Servicio de informes de vulnerabilidad Secunia: <http://secunia.com/>.
- Boletín de seguridad de Microsoft <http://www.microsoft.com/technet/security/current.aspx>:
Un solo lugar con toda la información acerca de los últimos desarrollos de seguridad de Microsoft.
- Servicio de actualizaciones de Windows: <http://windowsupdate.microsoft.com/>.
- Actualizaciones de programas para productos de Microsoft Office: <http://www.officeupdate.com/>.