

Revisión de la seguridad en Windows Vista, a un año de su lanzamiento

Ha pasado casi un año desde el lanzamiento de Windows Vista, pero aún no se han analizado en detalle muchas mejoras en la seguridad que Microsoft implementó para este sistema operativo. Ahora, es un buen momento para ocuparse de ellas.

El tema cobra particular importancia en vísperas del lanzamiento del primer Paquete de mantenimiento (SP1, *Service Pack 1*), ya que será interesante ver las mejoras que este introducirá con respecto a la protección del usuario y del sistema operativo. Mientras esperamos estas novedades, analizaremos en detalle el estado actual de la seguridad de Windows Vista.

En documentos anteriores, ya hemos tratado dos aspectos clave sobre la seguridad de este sistema: el [cortafuegos integrado](#) y la [protección de 64 bits](#).

En esta oportunidad, hablaremos de otras medidas de protección también implementadas en Vista.

Nuestro análisis se centrará especialmente en la protección destinada al usuario hogareño y de pequeñas empresas. Como algunas mejoras están pensadas especialmente para el uso corporativo, no serán tenidas en cuenta por el momento.

A continuación presentamos las características principales, agrupadas de acuerdo con su impacto en la seguridad del sistema.

Políticas de interacción local

Control de cuentas de usuario (UAC, *User Account Control*)

Uno de los problemas más serios en las versiones anteriores de Windows es que, una vez que los usuarios se registran en sus sistemas como administradores, obtienen acceso ilimitado a los recursos y pueden efectuar cualquier tipo de modificación que deseen. Esto es positivo cuando se realiza de manera controlada y con la autoridad apropiada, ya que los usuarios no podrán, por ejemplo, instalar un programa, a menos que cuenten con permisos de administrador. Sin embargo, esta característica puede resultar extremadamente peligrosa si un código malicioso se activa bajo este tipo de cuenta y comienza a trabajar con privilegios de alto nivel.

Esto ocurre ya que, cuando se ejecuta dentro de la cuenta del administrador, el código malicioso automáticamente hereda el mismo nivel de acceso que tiene el propietario del sistema. Así, puede instalar programas, cargar controladores, cambiar la configuración del registro, asociarse con aplicaciones legítimas, escribir áreas críticas del sistema, y realizar todo tipo de actividades no autorizadas sin ser notado.

Tal deficiencia es explotada a menudo por los piratas y otros delincuentes informáticos, debido a que la mayoría de los usuarios de Windows XP designan sus propias cuentas como de administrador (que es la opción predeterminada), exponiéndose a las amenazas de los códigos maliciosos cada vez que se conectan a la red.

En un intento por detener este abuso de privilegios, Microsoft introdujo una nueva función llamada **Control de cuentas de usuario** (UAC, *User Account Control*).

Esencialmente, esta característica reduce al mínimo los derechos de cualquier programa dado, aun cuando el usuario esté trabajando con la cuenta del administrador.

Los programas se ejecutan en este estado de derechos reducidos y, si necesitan permisos adicionales, solicitan el consentimiento del usuario. Esto asegura que las aplicaciones trabajen en un entorno mucho más limitado, conteniendo de forma efectiva a los códigos maliciosos.

Desafortunadamente, aun cuando el Control de cuentas de usuario incrementó la capacidad de los usuarios para aislar los códigos maliciosos, se convirtió en una molestia para el usuario promedio, debido a la excesiva cantidad de avisos emergentes que solicitan una respuesta.

En Vista, casi todas las actividades, incluyendo aquellas tan simples como cambiar el protector de pantalla del escritorio, generan una ventana de alerta que pide la confirmación del usuario autorizado, distrayendo constantemente su atención.

El Control de cuentas de usuario debería implementar algún método que memorice las respuestas apropiadas para cada actividad particular, eliminando la necesidad de volver a pedir indicaciones una y otra vez.

Aislamiento de aplicaciones y modo restringido para Internet Explorer

Windows Vista evita que un proceso con menor privilegio se comunice con otro de mayor privilegio. Esto asegura que los códigos maliciosos no puedan secuestrar una aplicación legítima, o usar comandos entre procesos, para controlar su actividad.

Esta función se conoce como **Control obligatorio de integridad** (*Mandatory Integrity Control*), y bloquea algunas operaciones tales como el desvío de procesos (*hooking*), la inserción de archivos DLL (componentes ejecutables externos), y la monitorización o manipulación de la actividad de aplicaciones importantes.

Esta restricción resulta particularmente útil cuando se aplica a Internet Explorer. Si esta aplicación está siendo aprovechada por códigos maliciosos, pero se ha iniciado con credenciales de bajo privilegio, no podrá dispersar la infección hacia otras áreas del ordenador.

Disposición aleatoria de la dirección asignada (ASLR, *Address Space Layout Randomization*)

Esta función carga los archivos de sistema en ubicaciones aleatorias de la memoria, haciendo más difícil para los códigos maliciosos predecir dónde están ubicadas las funciones privilegiadas del sistema.

La **Disposición aleatoria de la dirección asignada** ayuda a evitar la mayoría de los ataques de ejecución remota, ya que el código malicioso no tiene forma de localizar el objeto buscado, el cual puede encontrarse bajo cualquiera de las 256 direcciones existentes.

Refuerzo de los servicios de Windows (WSH, *Windows Service Hardening*)

Esta función evita que los servicios de Windows realicen operaciones no autorizadas, bloqueando así la posibilidad de que los códigos maliciosos los utilicen con fines dañinos. Adicionalmente, estos servicios ya no se ejecutan desde la cuenta del sistema, sino desde las cuentas con menores privilegios.

En términos de la comunicación con los recursos internos de Windows, los servicios de Windows ahora necesitan permisos para escribir en ciertos objetos del sistema, y Windows solamente les permite acceder a los recursos que incluyen en su diseño el permiso para ser modificados.

En el sistema operativo Vista, Microsoft también les ha permitido a los desarrolladores de aplicaciones independientes usar esta función para que refuercen sus propios servicios, especificando los permisos de escritura.

Opciones de control parental

A continuación haremos una breve revisión de las nuevas características del control parental.

- Bloqueo de categorías específicas con contenido delicado, tales como “tiroteo en escuela” o “drogas”.
- Definición personalizada de direcciones permitidas o bloqueadas.
- Restricción opcional de la descarga de archivos de la red, usando el control de las cuentas de usuario.
- Creación de listas de juegos permitidos de acuerdo con las clasificaciones proporcionadas por autoridades competentes. También permite que los propios usuarios definan los criterios para la restricción de juegos.
- Especificación de límites de tiempo para las cuentas, definiendo cuándo y por cuánto tiempo pueden ser usadas.
- Control de ejecución de programas, que restringe el uso de las aplicaciones a una lista de títulos permitidos. Esto se implementa por medio de las políticas de restricción de aplicaciones de Windows.
- Registro de actividades, incluyendo información contenida en los sitios web visitados, aplicaciones iniciadas, tiempo de uso, y otras estadísticas.

Cifrado de los discos

Los usuarios ahora pueden cifrar las unidades de disco con una llave USB o el módulo de **plataforma confiable** (*Trusted Platform Module*) de Intel, incluido en algunas placas madre.

El sistema **Bitlocker** de cifrado de discos está disponible solamente en las versiones **Enterprise** y **Ultimate** de Windows Vista.

Sin embargo, la necesidad de cifrar los contenidos importantes de los dispositivos móviles para proteger la información del acceso no autorizado, es cada vez mayor.

El primer Paquete de mantenimiento, próximo a ser lanzado, aumentará la funcionalidad de esta característica.

Defensa contra los programas espía

Vista incluye **Windows Defender**, una aplicación gratuita contra programas espía que promete proteger el ordenador de estas amenazas.

En la práctica, sin embargo, no alcanzó un buen desempeño en las pruebas independientes.

Por lo tanto, los usuarios aún deben instalar alguna solución de otro fabricante para garantizar una mayor seguridad.

Conclusión

Vista presenta mejoras muy importantes en relación a Windows XP, incluyendo varias características de seguridad orientadas principalmente a reforzar las defensas internas del ordenador contra las actividades maliciosas locales.

No obstante, esto no significa que sea una solución integral que garantice un 100% de seguridad (aunque, como todos sabemos, este concepto no existe en realidad).

Conocer y comprender la importancia de usar el ordenador de forma segura es vital para los usuarios. Esto los ayudará a mantenerse libres de preocupaciones cuando están en línea.

El uso de soluciones de seguridad desarrolladas por otras compañías, que muchas veces llenan algunos huecos dejados por Microsoft, resultará también un aporte fundamental en este aspecto.