



Principales ocho consejos de seguridad para Windows 8

Darren Teagles, director ejecutivo de productos

Microsoft ha sacado al mercado Windows 8, la versión más reciente del sistema operativo Windows, que lleva a disposición del público general desde el 26 de octubre. Aunque ofrece funciones de seguridad mejoradas, Windows 8 despierta también nuevas preocupaciones provocadas por los cambios en la interfaz gráfica de usuario y la nueva tienda de aplicaciones en línea. Los siguientes ocho consejos pueden ayudarle a seguir protegido al pasar a Windows 8.

1. Tenga cuidado con las aplicaciones para la nueva interfaz de usuario de Windows 8 (anteriormente conocida como Metro)

Algunas aplicaciones conocidas se han vuelto a desarrollar por completo para la nueva interfaz de Windows 8 y pueden funcionar de forma totalmente distinta aunque tengan el mismo aspecto. Por ejemplo, ciertas aplicaciones distribuidas anteriormente como archivos ejecutables pueden estar ahora totalmente basadas en Internet y no ser igual de visibles para las herramientas de seguridad y control existentes.

2. Utilice la versión de interfaz de usuario estilo Windows 8 de Internet Explorer

Los complementos están deshabilitados de forma predeterminada para evitar que se convierta en objetivo principal de ataques de Blackhole y kits de explotación.

3. Asegúrese de que el proveedor de seguridad marca las aplicaciones de la interfaz de usuario de Windows 8 maliciosas

Existen diferencias importantes entre las aplicaciones de la interfaz de usuario de Windows 8 y las aplicaciones normales, y el proveedor de seguridad debería ser capaz de diferenciarlas. El producto de seguridad debe marcar correctamente las aplicaciones modificadas o maliciosas (manipuladas, licencias inválidas, etc.) de la interfaz de usuario de Windows 8.

4. Desactive la hibernación del cifrado del disco duro

El cifrado del disco duro es fundamental para proteger los datos. Si es posible, desactive la opción de hibernación en Windows 8 mediante una política de grupo, ya que no siempre funciona correctamente con el cifrado.

5. Asegúrese de que el hardware cuenta con el logotipo "Diseñado para Windows 8"

Para llevar este logotipo, el hardware debe ser compatible con la interfaz UEFI, lo que permite hacer uso de la función de arranque seguro disponible en Windows 8. El arranque seguro está diseñado para garantizar que el entorno previo al sistema operativo es seguro y disminuir los riesgos de ataques del cargador de arranque.

6. Otorgue prioridad a la restricción de aplicaciones

La tienda de aplicaciones de Windows 8 hace que la restricción de aplicaciones sea cada vez más importante tanto para prevenir programas maliciosos como para controlar la productividad. Aunque la tienda de Windows estará protegida, la experiencia nos demuestra que es probable que se cuelen aplicaciones maliciosas. Impida el uso de aplicaciones que no sean relevantes para la empresa.

7. Trate los dispositivos de Windows RT (ARM) como cualquier otro dispositivo móvil

Asegúrese de que impone a los dispositivos de Windows RT los mismos niveles de seguridad que a cualquier otro tipo de dispositivo. Debería poder controlarlos, vigilarlos, borrarlos de forma remota y cifrarlos.

8. Revise los permisos de las aplicaciones en la tienda de Windows

Las aplicaciones de la tienda de Windows deben enumerar los recursos que necesitan. Revise detenidamente los permisos en la ficha de detalles, ya que algunos de ellos pueden permitir de forma predeterminada el acceso a la información de ubicación, el calendario, etc.

Además, es aconsejable utilizar una suite de seguridad completa para disponer de funciones avanzadas de filtrado, y gestión e informes centralizados. Aunque Microsoft ha incluido un antivirus y un cortafuegos básicos, la mayoría de las empresas seguirán necesitando seguridad de nivel comercial. Y, evidentemente, todas las reglas de seguridad antiguas también son aplicables a Windows 8. Permitir los inicios de sesión automáticos sigue siendo poco aconsejable. Pero, sobre todo, no baje la guardia.

Síguenos en:



Ventas en el Reino Unido:
Teléfono: +44 8447 671131
Correo electrónico: sales@sophos.com

Ventas en España:
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en Norteamérica:
Línea gratuita: +1 866 866 2802
Correo electrónico: nasales@sophos.com

Boston (EE. UU.) | Oxford (Reino Unido)
© Copyright 2012. Sophos Ltd. Todos los derechos reservados.
Todas las marcas registradas pertenecen a sus respectivos propietarios.

Artículos de Sophos 10.12v1.dNA

Más noticias de
seguridad y tendencias
Visite Sophos.com/es-es/

SOPHOS