

¿Por que un cortafuegos no es un dique permeable,
y un ordenador sin cortafuegos, seguramente será traspasado?

Recientemente encontré un artículo* muy interesante, y un tanto polémico, acerca de los beneficios e inconvenientes de los cortafuegos personales.

✍ El artículo en cuestión es [Why home firewall is a leaky dike](#)
(¿Por qué un cortafuegos personal es un dique permeable?)

El autor, por supuesto, es una persona muy inteligente, pero me parece que carece del sentido de la previsión cuando comenta que “Los programas cortafuegos para uso hogareño, no son más que un dique permeable”.

Yo diría que un ordenador sin un cortafuegos es una caja perforada. Es decir, el cortafuegos protege a la caja contra pérdidas que, de otro modo, serían inevitables.

Por supuesto que (el cortafuegos) no puede resolver todos los problemas.

Ningún programa o equipo, o cualquier otro elemento, es perfecto. Pero pueden brindar una protección adicional que mantenga la integridad de los datos personales almacenado en el ordenador.

Junto con el cortafuegos, se recomiendan otras medidas de seguridad, como por ejemplo antivirus, aplicaciones contra programas espía y la instalación de parches para su sistema operativo y para las aplicaciones, instalando las últimas actualizaciones de seguridad.

En la cima de esto encontramos el conocimiento del usuario acerca de los elementos básicos de seguridad, y la aplicación de un poco de sentido común en el uso de su ordenador.

A continuación, encontrará algunas afirmaciones realizadas en el artículo, el cual, se basa en el análisis de seis cortafuegos, efectuado este a comienzos de este año por la revista alemana **PC Professionell's**.

Si bien Outpost 4.0 no estaba disponible al momento de la creación del mismo, creí que sería útil identificar cómo Outpost Firewall Pro 4.0 contrarrestaría los reclamos del autor:

✍ Outpost Firewall Pro 4.0 se encuentra en sus últimas etapas de desarrollo y será lanzado próximamente.

1. “Los cortafuegos no lo protegen contra los análisis de fuga”

La futura versión 4 de Outpost Firewall Pro fue diseñada para brindar protección contra todas las técnicas conocidas que puedan permitir pérdidas de información, incluso aquellas que utilizan un programa de confianza como disfraz. Específicamente, hemos probado el código contra casi 20 de las herramientas disponibles para análisis de fuga y Outpost aprobó todas.

Por lo tanto, creo que los usuarios de Outpost pueden estar seguros que los cortafuegos **realmente** los protegen contra los análisis de fuga.

2. “El código malicioso puede desactivar el programa de seguridad antes de causar otros daños”

Sí, esto puede suceder, y, en realidad, sucedió con varios de los antivirus y aplicaciones contra programas espía más conocidos. Pero Outpost Firewall Pro 4.0 ha sido diseñado con amplia capacidad de auto-protección.

Por lo tanto, ningún código malicioso podrá desactivar, de manera temporal, el funcionamiento del cortafuegos antes de realizar su trabajo sucio.

3. “El antivirus es más importante que el cortafuegos porque los troyanos pueden explotar las vulnerabilidades”

Un buen cortafuegos cierra **todos** los puertos a redes externas que no se consideren seguras.

De forma tal que, incluso si el programa que utiliza estos puertos tiene una vulnerabilidad de seguridad, el cortafuegos bloqueará a los piratas que traten de inyectar un troyano, u otro código malicioso en su ordenador. (Pero, no olvide que de todas formas, el usuario debería también utilizar un antivirus para incrementar su seguridad).

4. **“El antivirus es el último recurso, después que todas las otras herramientas de seguridad han fallado”**

La defensa de la última brecha es, a mi entender, pensar (y disponer) de un cortafuegos, no del antivirus. Y es así, porque (en la gran mayoría de los antivirus) este último debe contar con las últimas firmas para identificar las posibles infecciones, de manera confiable, y así poder eliminarlas de manera precisa.

Si no hay firma, el antivirus no verá al código malicioso (salvo escasas soluciones de seguridad que cuentan con una adecuada defensa proactiva).

Pero el cortafuegos verá un comportamiento anormal y cerrará el puerto que este código está tratando de utilizar.

5. **“Los cortafuegos de escritorio no son necesarios si los usuarios siguen las reglas básicas de la navegación segura”**

Existen muchas personas conocedoras, y con experiencia, que disientirían por completo con esta afirmación.

La mayoría de los usuarios no son concientes de las reglas básicas de la navegación segura e, incluso si tienen conciencia de ello, a menudo las ignoran. Es parte de la naturaleza humana.

El cortafuegos está allí para salvar la brecha y ayudar a proteger a los usuarios cuando ellos mismos no lo hacen.

Es como una bolsa de aire en un automóvil: ayudará a proteger a los pasajeros si tienen un accidente y no estaban utilizando el cinturón de seguridad.

6. **“Una cuenta pública no necesita derechos de administrador y debería iniciar una sesión como tal solamente cuando instala algún programa”**

Sí, esto es cierto acerca de los derechos de administrador, pero Windows XP, por defecto agrega usuarios como administradores. Windows Vista corregirá esta situación en su momento.

7. **“Los usuarios que aún prefieren un cortafuegos deberían primero verificar si están utilizando un enrutador con esta funcionalidad”**

De ser así, entonces no se necesita un cortafuegos, ni siquiera el que se encuentra integrado en Windows XP.

Los enrutadores y dispositivos con funcionalidad de cortafuegos físico, no cuentan con monitorización de datos por aplicación. Solamente pueden verificar el tráfico de acuerdo con las condiciones generales.

No pueden evitar que un registrador sofisticado de pulsaciones, transmita los datos personales fuera del equipo.

Sin embargo, un cortafuegos personal sí lo hace.

8. **“De todas formas, la configuración de un cortafuegos personal representa, por lo general, más de los que los usuarios pueden administrar”**

Sí, este es un problema importante con muchos cortafuegos.

Los errores en la configuración, junto a que los usuarios suelen ignoran los mensajes incomprensibles del cortafuegos, son responsables de la mayoría de las *fallas* de estos programas.

Nuestros ingenieros han trabajado duro para eliminar este problema, por lo tanto, un asesor inteligente ayuda a los usuarios de Outpost cuando deben decidir si autorizan o bloquean ciertas actividades de los programas.

Me gustaría saber cómo responderá este autor cuando vea la versión mejorada de ImproveNet en Outpost 4.0.

Bien, esta es mi opinión acerca del valor de los cortafuegos. Por suerte, al menos algunas de las personas entendidas en el tema que lean esta nota compartirán mi opinión.

Igor Pankov

Gerente, en Agnitum, de mercado de productos.

Traducción y adaptación: Ontinet.com, S.L.