Información Sobre Seguridad Box Party

Actualización: 1 Mayo 2018

Utilice siempre un navegador actualizado. Los principales navegadores de hoy en día se actualizan automáticamente bien de forma transparente al usuario o mediante notificaciones que deberán ser aprobadas. Las actualizaciones automáticas del sistema operativo deberán también estar habilitadas.

Compruebe que los complementos y extensiones están configurados para actualizarse automáticamente. Asimismo, asegúrese que la instalación de estos complementos se realiza desde fuentes fiables.

Se aconseja deshabilitar complementos como Adobe Flash y Java para aquellos servicios y sitios desconocidos. Mecanismos que permitan pinchar y ejecutar o el uso de determinadas extensiones permiten facilitar esta tarea. Asimismo, se recomienda deshabilitar JavaScript para navegar por páginas web desconocidas. Para agilizar esta configuración pueden utilizarse extensiones que permiten aplicar políticas de contenido para habilitar y deshabilitar lenguajes de scripting.

Se aconseja revisar las opciones de seguridad y privacidad del navegador. Actualmente los navegadores disponen de medidas tan interesantes como: no aceptar cookies de terceros, bloquear pop-ups, evitar la sincronización de contraseñas, evitar el autocompletado, borrar los ficheros temporales y cookies al cerrar el navegador, bloquear la geolocalización, filtrar ActiveX, etc.

Se recomienda hacer uso de HTTPS (SSL/TLS) frente a HTTP incluso para aquellos servicios que no manejen información sensible. Existen funcionalidades que servirán de gran ayuda para garantizar el uso preferente de HTTPS sobre HTTP durante la navegación web.

Se recomienda proteger el navegador y los complementos con soluciones que impidan aprovechar debilidades de seguridad para mitigar posibles ataques derivados de programas que intenten aprovechar dichas debilidades. En algunos casos, este tipo de herramientas podrán proteger al usuario frente a “0-days”. Esta solución no debe verse como un sustituto al antivirus sino como una capa de seguridad adicional.

Proteja sus contraseñas, no las revele a terceros por escrito ni verbalmente, cambie de contraseña periódicamente y nunca atienda a peticiones de contraseña que le lleguen por correo electrónico.

Use combinaciones de números, letras y símbolos para sus contraseñas. No almacene contraseñas de forma predeterminada por medio del navegador y utilice herramientas más seguras para su gestión (por ejemplo, gestores de contraseñas que implementen un sistema de cifrado robusto). En el caso de que se decida utilizar el navegador es importante hacer uso de una llave maestra que cifre el repositorio de credenciales.

Es importante verificar que los certificados remitidos por servicios HTTPS que manejen información sensible han sido remitidos por una CA de confianza. Cualquier error o alerta generada por el navegador como consecuencia de la validación del certificado (por ejemplo, certificados autofirmados) deberá revisarse cuidadosamente.

Para mejorar la seguridad frente a ataques de intermediario se recomienda el uso de políticas de “Certificate Pinning”.

Valore el uso de extensiones o complementos adicionales que implementen funcionalidades no contempladas por el navegador. Por ejemplo, aquellas que mejoran la privacidad durante la navegación o que bloquean en la medida de lo posible anuncios, banners publicitarios y determinadas técnicas de seguimiento utilizadas por terceros.

(Fuente: Elaboración propia y Centro Criptológico Nacional ”Informe de Buenas prácticas CCN- CERT BP-06/2016”)