Software y Aplicaciones

1. Consejo de Seguridad Informática ST04-006

Saber qué son los Parches

Cuando los proveedores advierten vulnerabilidades en sus productos, a menudo largan parches para solucionar el problema. Asegúrese de aplicar los parches que correspondan para su computadora lo antes posible para que su sistema esté protegido.

¿Qué son los parches?

Al igual que los parches de tela que se usan para reparar agujeros en la ropa, los parches de software reparan agujeros en los programas de software. Los parches son actualizaciones que enmiendan un problema o vulnerabilidad en particular dentro de un programa. A veces, en lugar de largar un parche, los proveedores largan una versión más avanzada de su software, aunque puedan referirse a esta mejora como un parche.

¿Cómo encontrar qué parches necesita instalar?

Cuando hay parches disponibles, los proveedores generalmente los ponen en sus sitios web para que los usuarios los bajen. Es importante instalar un parche tan pronto como fuere posible para proteger su computadora de los atacantes que aprovecharían la vulnerabilidad. Los atacantes pueden apuntar a las vulnerabilidades durante meses o aún algunos años luego de que los parches están disponibles. Algunos software automáticamente verificarán las actualizaciones, y muchos proveedores ofrecen a los usuarios la opción de recibir notificación de actualizaciones automáticas a través de una lista de correspondencia. Si estas opciones automáticas están disponibles, recomendamos que las aproveche. Si no están disponibles, periódicamente verifique si hay actualizaciones en los sitios web de los proveedores.

Asegúrese de bajar sólo software o parches de sitios web en los que confía. No confíe en un link en un mensaje de correo electrónico – los atacantes han usado mensajes de correo electrónico para dirigir a los usuarios a sitios web maliciosos donde hay usuarios que instalan virus disfrazados de parches. También esté alerta a los mensajes de correo electrónico que afirman que han adjuntado el parche al mensaje – estos adjuntos generalmente son virus.

2. Consejo de Seguridad Informática ST05-018

Saber qué es la Voz sobre Protocolo de Internet (VoIP)

Con la introducción de Voz sobre Protocolo de Internet (Voice over Internet Protocol - VoIP), usted puede usar Internet para hacer llamadas telefónicas en lugar de una línea telefónica separada. La tecnología no presenta riesgos de seguridad.

¿Qué es Voz sobre Protocolo de Internet (VoIP)?

Voz sobre Protocolo de Internet (VoIP), también conocida como telefonía IP, le permite usar su conexión de Internet para hacer llamadas telefónicas. En lugar de usar una línea análoga como los teléfonos tradicionales, VoIP usa tecnología digital y requiere una banda ancha de alta velocidad tal como DSL o cable. Hay una variedad de proveedores que ofrecen VoIP, y ofrecen distintos servicios. La aplicación más común de VoIP para uso personal o del hogar son los servicios de teléfono basados en Internet a través de una ficha de teléfono. Con esta aplicación, usted aún tendrá un número de teléfono, discará números de teléfono, y generalmente tendrá un adaptador que permite usar un teléfono común. La persona a la que usted llama probablemente no notará la diferencia con una llamada telefónica tradicional. Algunos proveedores de servicio también le ofrecen la posibilidad de usar su adaptador VoIP en cualquier lugar que tenga una conexión de Internet de alta velocidad, permitiéndole llevarlo con usted cuando viaja.

¿Cuáles son las consecuencias de seguridad de VoIP?

Como VoIP se apoya sobre su conexión de Internet, puede ser vulnerable a cualquier amenaza o problemas con los que se enfrenta su computadora. La tecnología aún es nueva, por lo tanto hay alguna controversia acerca del potencial para un ataque, pero VoIP podría hacer que su teléfono sea vulnerable a virus y otro código malicioso. Los atacantes podrían realizar actividades tales como interceptar sus comunicaciones, hacer escuchas ilegales, conducir ataques phishing manipuleando la identidad del que lo llamó, y provocar que su servicio colapse. Las actividades que consumen una gran cantidad de recursos de la red, como la bajada de archivos grandes, juegos online, multimedia, también afectarán su servicio VoIP.

También hay problemas inherentes al ruteo de su teléfono sobre la conexión de banda ancha. A diferencia de las líneas telefónicas tradicionales, que operan a pesar de un corte de corriente, si usted se queda sin corriente, su VoIP puede no quedar disponible. También hay preocupación de que los sistemas de seguridad del hogar o los números de emergencia tal como el 911 puedan no funcionar de la forma que usted espera.

¿Cómo se puede proteger?

- **Mantener el software actualizado** – Si el proveedor lanza parches para el software con el que opera su dispositivo, instalarlos lo antes posible. Estos parches pueden ser denominados actualizaciones de programa o *firmware*. Instalarlos prevendrá que los atacantes puedan aprovechar problemas o vulnerabilidades conocidas.
- **Usar y mantener el software anti-virus** – El software anti-virus reconoce y protege su computadora contra los virus más conocidos. Sin embargo, los atacantes están permanentemente lanzando nuevos virus, por lo tanto es importante mantener el software anti-virus actualizado.
- **Aprovechar las opciones de seguridad** – Algunos proveedores de servicio pueden ofrecer encriptado como uno de sus servicios. Si usted está preocupado acerca de la privacidad y confidencialidad, podría considerar ésta y otras opciones disponibles.
- **Instalar o habilitar un firewall** – Los firewalls pueden prevenir algunos tipos de infección bloqueando el tráfico malicioso antes de que entre en su computadora. Algunos sistemas operativos actualmente incluyen un firewall, pero necesita asegurarse que esté habilitado.
- **Evaluar sus valores/configuración de seguridad** – Tanto tu computadora como su equipo/software VoIP ofrecen una variedad de valores que usted puede ajustar a la medida de sus necesidades y requerimientos. Sin embargo, habilitar ciertos valores lo pueden dejar más vulnerable a ser atacado, por lo tanto deshabilite lo que no es necesario. Examine sus valores/configuración, particularmente los de seguridad y selecciones opciones que cumplan con sus necesidades sin exponerlo a un mayor riesgo.

3. Consejo de Seguridad Informática ST05-007

Riesgos de la Tecnología para Compartir Archivos

La tecnología para compartir archivos es una forma popular para que los usuarios intercambien o “compartan” archivos. Sin embargo, usar esta tecnología lo hace susceptible de riesgos tales como infección, ataque, o exposición de información personal.

¿Qué es compartir archivos?

Compartir archivos comprende usar la tecnología que permite a los usuarios compartir archivos que están alojados en sus computadoras individuales. Las aplicaciones Par-a-Par (P2P), tales como aquellas utilizadas para compartir archivos de música, son algunas de las formas comunes de la tecnología para compartir archivos. Sin embargo,

las aplicaciones P2P introducen riesgos de seguridad que pueden poner la información de su computadora en peligro.

¿Qué riesgos introduce la tecnología para compartir archivos?

- **Instalación de código malicioso** – Cuando usted usa aplicaciones P2P, es difícil, sino imposible, verificar que la fuente de los archivos es confiable. Estas aplicaciones generalmente son usadas por los atacantes para transmitir código malicioso. Los atacantes pueden incorporar spyware, virus, caballos Troyanos, o gusanos en los archivos. Cuando usted baja los archivos, su computadora se infecta.
- **Exposición de información personal o delicada** – Al usar las aplicaciones de P2P, usted puede estar dando a otros usuarios el acceso a su información personal. Ya fuere porque ciertos directorios están accesibles o porque usted brinda información personal a lo que usted cree que es una persona u organización confiable, personas no autorizadas pueden acceder a sus datos financieros o médicos, documentos personales, información de empresa delicada u otra información personal. Una vez que la información fue expuesta a gente no autorizada, es difícil saber cuánta gente accedió a ella. La disponibilidad de esta información puede incrementar su riesgo de robo de identidad.
- **Susceptibilidad al ataque** – Algunas aplicaciones P2P pueden solicitarle que abra ciertos puertos en su firewall para transmitir los archivos. Al abrir algunos de estos puertos puede darle a los atacantes acceso a su computadora o permitirles que ataquen su computadora tomando ventaja de cualquier vulnerabilidad que pudiera existir en la aplicación P2P. Hay algunas aplicaciones P2P que pueden modificar y penetrar los firewalls mismos, sin su conocimiento.
- **Denegación de servicio** – Bajar archivos provoca una cantidad significativa de tráfico sobre la red. Esta actividad puede reducir la disponibilidad de ciertos programas en su computadora o puede limitar su acceso a Internet.
- **Proceso/acusación**- Los archivos compartidos a través de aplicaciones P2P pueden incluir software pirateado, material con derecho de autor, o pornografía. Si usted los baja, aún sin saberlo, puede enfrentarse con multas u otra acción legal. Si su computadora está en la red de una empresa y expone información de clientes, tanto usted como su compañía podrían ser responsables.

¿Como puede minimizar estos riesgos?

La mejor forma de eliminar estos riesgos es evitar usar aplicaciones P2P. Sin embargo, si elige usar esta tecnología, puede seguir algunas buenas prácticas de seguridad para minimizar su riesgo:

- **Usar y mantener el software anti-virus** – El software anti-virus reconoce y protege su computadora contra los virus más conocidos. Sin embargo, los atacantes están permanentemente lanzando nuevos virus, por lo tanto es importante mantener el software anti-virus actualizado.

- **Instalar o habilitar un firewall** – Los firewalls pueden prevenir algunos tipos de infección bloqueando el tráfico malicioso antes de que ingrese en su computadora. Algunos sistemas operativos incluyen un firewall, pero debe estar seguro de que esté habilitado.

4. Consejo de Seguridad Informática ST05-005

Revisión de los Contratos de Licencia para Usuario Final

Antes de aceptar un contrato de licencia para usuario final, asegúrese de comprender y de sentirse cómodo con los términos del mismo.

¿Qué es un contrato de licencia para usuario final?

Un contrato de licencia para usuario final (*End-User License Agreement - EULA*) es un contrato entre usted y el proveedor o desarrollador de software. Algunos paquetes de software establecen que tan sólo sacando el envoltorio al vacío del paquete, usted está de acuerdo con el contrato. Sin embargo, usted puede estar más familiarizado con el tipo de EULA que se presenta como cuadro de diálogo que aparece la primera vez que abre el software. Generalmente requiere que usted acepte las condiciones del contrato antes de proceder. Algunos EULAs sólo se aplican a ciertas características del software, por lo tanto puede encontrarlas cuando intente usarlas.

Lamentablemente, muchos usuarios no leen este contrato antes de aceptarlo. Los términos de cada contrato difieren, y usted puede estar acordando condiciones que más tarde considerará injustas o que lo exponen a riesgos de seguridad que no esperaba.

¿Qué términos pueden incluirse?

EULAs son contratos legales, y el vendedor o desarrollador puede incluir prácticamente cualquier condición. Las condiciones a menudo están diseñadas para proteger al desarrollador o al proveedor de responsabilidades, pero también pueden incluir términos adicionales que le dan al proveedor cierto control sobre su computadora. Estos contratos generalmente cubren los siguientes tópicos:

- **Distribución** – Generalmente hay limitaciones puestas en la cantidad de veces que usted tiene permitido instalar el software y restricciones acerca de reproducir el software para distribución.
- **Garantía** – Los desarrolladores o proveedores a menudo incluyen cláusulas de descargo de responsabilidad estableciendo que no son responsables por cualquier problema que surja como resultado de haber usado el software incorrectamente. También pueden protegerse de responsabilidades por defectos del software, fallas del software, o incompatibilidad con otros programas de su computadora.

Los siguientes tópicos, aunque no son estándares, son ejemplos de otras condiciones que fueron incluidas en los contratos EULAs. Presentan consecuencias con respecto a la seguridad que usted debería considerar antes de aceptar el acuerdo.

- **Monitoreo** – Acordar con EULA puede darle al proveedor permiso para monitorear la actividad de su computadora y comunicar la información al proveedor o a otro tercero. Dependiendo de la información que se recolecta, este tipo de monitoreo podría tener consecuencias tanto de seguridad como de privacidad.
- **Instalación de software** – Algunos contrato permiten al proveedor instalar software adicional en su computadora. Esto puede incluir versiones actualizadas del programa de software que usted instaló (la determinación de qué versión usted está corriendo puede ser el resultado del monitoreo descripto arriba). Los proveedores también pueden incorporar cláusulas que les permiten a ellos o a terceros instalar programas de software adicionales en su computadora. Este software puede ser innecesario, puede afectar la funcionalidad de otros programas de su computadora, y puede introducir riesgos de seguridad.

5. Consejo de Seguridad Informática ST04-021

Conocimiento de su Computadora: Sistemas Operativos

El sistema operativo es el programa más fundamental que corre en su computadora. Sirve como la base de cómo funciona todo el resto.

¿Qué es un sistema operativo?

Un sistema operativo (SO) es el programa principal en una computadora. Realiza una variedad de funciones, incluyendo

- Determinar qué tipos de software puede instalar.
- Coordinar las aplicaciones que corren en su computadora en cualquier momento.
- Asegurarse que las partes individuales del hardware, tal como impresoras, teclados, unidades de disco, todas se comuniquen correctamente.
- Permitir aplicaciones tales como procesadores de la palabra, clientes de correo electrónico, y navegadores web para realizar tareas en el sistema (por ejemplo abrir ventanas en una pantalla, abrir archivos, comunicarse en una red) y usar otros recursos del sistema (por ejemplo, impresoras, unidades de disco)
- Informar mensajes de error .

El SO determina cómo usted ve la información y realiza las tareas. La mayoría de los sistemas operativos usan una interfaz gráfica (GUI), que presenta información a través

de figuras (íconos, botones, cuadros de diálogo, etc.) y también palabras. Algunos SO pueden sustentarse mejor sobre interfaz de texto que otros.

¿Cómo elegir un sistema operativo?

En términos muy simplificados, cuando usted elije comprar una computadora, está generalmente eligiendo un sistema operativo. Aunque usted lo pueda cambiar, los proveedores generalmente entregan las computadoras con un sistema operativo en particular. Hay múltiples sistemas operativos, cada uno con diferentes rasgos y beneficios, pero los tres siguientes son los más comunes:

- **Windows** - Windows, con las versiones incluyendo Windows XP, Windows Vista, y Windows 7, es el sistema operativo más común para el usuario de un hogar. Está producido por Microsoft y está generalmente incluido en máquinas compradas en negocios de electrónica o a proveedores tales como Dell o Gateway. El SO Windows usa una interfaz gráfica (GUI), que muchos usuarios encuentran más atractiva y fácil de usar que las interfases basadas en texto.
- **Mac OS X** – Producido por Apple, Mac OS X es el sistema operativo usado en las computadoras Macintosh. Aunque usa un GUI diferente, es conceptualmente similar a la interfase de Windows en la forma que opera.
- **Linux y otros sistemas operativos derivados de UNIX** - Linux y los otros sistemas derivados del sistema operativo UNIX frecuentemente se usan para estaciones de trabajo y servidores especializados, tales como servidores de web y correo electrónico. Como generalmente es más difícil para los usuarios en general o porque requieren un conocimiento y habilidades especializadas para funcionar, son menos populares en los usuarios de hogar que las otras opciones. Sin embargo, a medida que se continúen desarrollando y resulten más fáciles de usar, pueden pasar a ser más populares en los sistemas de usuarios de hogar.