Dispositivos Móviles

1. Consejo de Seguridad Informática ST04-017

Protección de Dispositivos Portátiles: Seguridad Física

Muchos usuarios de computadora, especialmente aquellos que viajan por negocios, confían en laptops y Asistentes Digitales Personales (PDA - Personal Digital Assistant) debido a que son pequeños y fáciles de transportar. Pero mientras estas características los hace populares y prácticos, también los hace ideales como objetivo de robo. Asegúrese de proteger sus dispositivos portátiles, tanto la máquina como la información que contiene.

¿Qué está en riesgo?

Sólo usted puede determinar lo que está realmente en riesgo. Si un ladrón le roba su laptop o PDA, la pérdida más obvia es la máquina. Sin embargo, si el ladrón puede acceder a la información de su computadora o PDA, toda la información almacenada en el dispositivo está en riesgo, tanto como la información adicional a la que se puede acceder a partir de los datos almacenados en ese dispositivo.

Las personas no autorizadas no deberían tener acceso a información delicada o de cuenta de cliente. Probablemente escuchó noticias sobre organizaciones que entran en pánico porque les robaron o perdieron laptops conteniendo información confidencial. Pero aún si no hay información empresarial delicada en su laptop o PDA, piense acerca de otra información en riesgo: información acerca de citas, contraseñas, direcciones de correo electrónico y otra información de contacto, información personal para cuentas online, etc.

¿Cómo puede proteger su laptop o PDA?

- **Contraseña –proteja su computadora** - Asegúrese que tenga que ingresar una contraseña para iniciar su sesión en su computadora o PDA.
- **Mantenga su laptop o PDA junto a usted todo el tiempo** – Cuando viaje, mantengan su laptop junto a usted. Los horarios de comidas son los momentos óptimos para que los ladrones revisen las habitaciones de un hotel buscando laptops. Si está en una conferencia o feria comercial, esté especialmente alerta – estos acontecimientos ofrecen a los ladrones una selección más amplia de dispositivos que muy probablemente contengan información delicada, y las sesiones de una conferencia ofrecen más oportunidades para que los ladrones ingresen a las salas de invitados.

- **Oculte su laptop o PDA** – No hay necesidad de que publique a los ladrones que tiene una laptop o PDA. Evite usar su dispositivo portátil en áreas públicas, y considere tener bolsos no tradicionales para llevar su laptop.
- **Esté alerta a sus alrededores** – Si utiliza su laptop o PDA en una zona pública preste atención a la gente que lo rodea. Tome precaución de esconderse de los que "surfean por encima de los hombros "—asegúrese que nadie pueda verlo cuando tipea sus contraseñas o ver cualquier información importante y delicada en su pantalla.
- **Considere una alarma o un candado** – Muchas empresas venden alarmas o candados que se puede usar para proteger o asegurar su laptop. Si viaja a menudo o estará en un área de alta población, tal vez quiera considerar invertir en una alarma para el bolso de su laptop o un candado para asegurar su laptop a algún mueble.
- **Haga back up de sus archivos** – Si le roban su dispositivo portátil, además es bastante malo que alguien pueda acceder a su información. Para evitar perder toda la información, haga backups y almacénelos en un lugar separado. No sólo aún podrá tener acceso a su información, sino que podrá identificar e informar exactamente qué información está en riesgo.

¿Qué puede hacer si le roban o pierde su laptop o PDA?

Informe sobre la pérdida o robo a las autoridades correspondientes. Estas autoridades pueden ser representantes de la fuerza policial, tanto como al personal del hotel o el personal de la conferencia. Si su dispositivo contenía información delicada de la empresa o una cuenta de cliente, informe inmediatamente la pérdida o el robo a su organización para que puedan actuar rápidamente.

2. Consejo de Seguridad Informática ST04-020

Protección de Dispositivos Portátiles: Protección de Datos

Además de tomar precauciones para proteger sus dispositivos portátiles, es importante agregar otra capa de seguridad protegiendo a los datos.

¿Por qué necesita otra capa de protección?

Aunque hay varias formas de proteger físicamente su laptop, PDA, u otro dispositivo portátil, no hay garantía de que no serán robados. Después de todo, como el nombre lo sugiere, los dispositivos portátiles están diseñados para ser fácilmente transportados. El robo en sí mismo, como mínimo, es frustrante, inconveniente y desconcertante, pero la exposición de la información en el dispositivo podría traer consecuencias serias. También recuerde que cualquier dispositivo conectado a Internet, especialmente si es una conexión inalámbrica, es también susceptible a ataques de red.

¿Qué puede hacer?

- **Usar contraseñas correctamente** – En el proceso de llegar a la información en su dispositivo portátil, probablemente usted encuentre varías solicitudes de contraseñas. Aproveche esta seguridad. No elija las opciones que permiten a su computadora recordar contraseñas, no elija contraseñas que los ladrones podrían adivinar fácilmente, use diferentes contraseñas para programas diferentes, y aproveche los métodos de autenticación adicionales.
- **Considerar almacenar datos importantes en forma separada** – Hay muchos medios para almacenar, incluyendo CDs, DVDs, y drives extraíbles (también conocidos como drives USB o *thumb drives* – haciendo referencia a que tienen el tamaño de un dedo pulgar (*thumb*). Al guardar sus datos en un medio extraíble y manteniéndolo en un lugar diferente (por ejemplo en su portafolio en lugar del bolso/valija de la laptop), puede proteger sus datos aún si le roban su laptop. Debería asegurarse de proteger el lugar donde guarda sus datos para prevenir un fácil acceso. Puede ser útil llevar estos medios de almacenamiento con otros objetos valiosos que usted tiene en su poder todo el tiempo y que naturalmente protege, tales como la billetera o llaves.
- **Encriptar archivos** – Encriptando archivos, usted asegura que gente no autorizada no pueda ver los datos aunque tengan acceso físico a ellos. También puede considerar opciones para encriptación de todo el disco, que previene que un ladrón inicie su laptop sin una frase contraseña. Cuando usa el encriptado, es importante que recuerde sus contraseñas o frases contraseñas; si se olvidara de ellas o las perdiera, podría perder sus datos.
- **Instalar y mantener el software anti-virus** – Proteja las laptops y PDAs de virus de la misma forma en que protege su computadora de escritorio. Asegúrese que tiene las definiciones de virus actualizadas. Si su software anti-virus no incluye software anti-spyware, considere instalar un software separado para protegerse contra esa amenaza.
- **Instalar y mantener un firewall** – Aunque un firewall es siempre importante para restringir el tráfico que ingresa y sale de su computadora, es especialmente importante si usted está viajando y usando distintas redes. Los firewalls pueden ayudar a prevenir que extraños ganen un acceso no deseado.
- **Haga un back up de sus datos** – Asegúrese de hacer un back up de cualquier dato que tenga en su computadora en un CD-ROM, DVD-ROM, o red. Esto no sólo asegurará que podrá tener acceso a la información si le roban su dispositivo, sino que podría ayudar a identificar exactamente a qué información podría acceder un ladrón. Puede también tomar medidas para reducir la dimensión del daño que podría provocar esa exposición.

3. Consejo de Seguridad Informática ST08-001

Tener Precaución con los Drives USB

Los drives USB son populares para almacenar y transportar datos, pero algunas de las características que los hacen prácticos también introducen riesgos de seguridad.

¿Qué riesgos de seguridad están asociados con los drives USB?

Debido a que los drives USB, también llamados *thumb drives* -haciendo referencia a que tienen el tamaño de un dedo pulgar (*thumb*)-, son pequeños, fáciles de tenerlos a mano, son de bajo precio y extremadamente portátiles, son populares para almacenar y transportar archivos de una computadora a otra. Sin embargo, estas mismas características los hace atractivos para los atacantes.

Una opción es que los atacantes usen su drive USB para infectar otras computadoras. Un ataque podría infectar una computadora con código malicioso, o malware, que puede detectar cuando un drive USB se enchufa en su computadora. El malware luego baja código malicioso al drive. Cuando se enchufa el drive USB a otra computadora, el malware infecta esa computadora.

Algunos atacantes también han apuntado a los dispositivos electrónicos, infectando objetos tales como cuadros de foto y drives USB durante la producción. Cuando los usuarios compran productos infectados y los conectan a sus computadoras, el malware se instala en sus computadoras.

Los atacantes también pueden usar drives USB para robar información directamente de una computadora. Si un atacante puede tener acceso físico a una computadora, puede bajar información sensible e importante a un drive USB. Aún las computadoras que fueron apagadas pueden ser vulnerables, porque la memoria de una computadora está aún activa durante varios minutos luego de desconectarla de la corriente. Si un atacante puede enchufar un drive USB en la computadora durante este tiempo, rápidamente puede rebootear el sistema desde el drive USB y copiar la memoria de la computadora, incluyendo contraseñas, llaves de encriptado, y otros datos sensibles al drive. Las víctimas pueden aún no darse cuenta de que sus computadoras fueron atacadas.

El riesgo de seguridad más obvio para los drives USB, sin embargo, es que son fáciles de perder o de que los roben. Si los datos no tenían un backup, la pérdida de un drive USB puede significar horas de pérdida de trabajo y el potencial de que la información no pueda ser replicada. Y si la información del drive no está encriptada, cualquiera que tenga el drive USB puede acceder a todos los datos que éste contiene.

¿Cómo puede proteger sus datos?

Hay pasos que puede tomar para proteger los datos de su drive USB y en cualquier otra computadora a la que usted puede enchufarle el drive:

- **Aproveche la ventaja de las opciones/configuraciones de seguridad** - Use contraseñas y encriptado en su drive USB para proteger sus datos, y asegúrese de tener un backup de la información por si pierde su drive.
- **Mantenga separados los drives USB personales y de negocios/trabajo** – No use drives USB personales en computadoras de su organización/empresa y no enchufe drives USB que tengan información de la empresa en su computadora personal.
- **Use y mantenga el software de seguridad, y mantenga todo software actualizado** - Use un firewall, un software anti-virus, y un software anti-spyware para que su computadora sea menos vulnerable a los ataques, y asegúrese de mantener las definiciones de virus actualizadas. También, mantenga el software de su computadora actualizado aplicando los parches necesarios.
- **No enchufe en su computadora un drive USB desconocido** - Si encuentra un drive USB, entréguelo a las autoridades apropiadas (el personal de seguridad del lugar, el departamento TI de su organización, etc.). No lo enchufe a su computadora para ver los contenidos o tratar de identificar al propietario.

4. Consejo de Seguridad Informática ST05-003

Asegurar las Redes Inalámbricas

Las redes inalámbricas son cada vez más populares, pero introducen riesgos de seguridad adicionales. Si tiene una red inalámbrica, asegúrese de tomar las precauciones apropiadas para proteger su información.

¿Cómo funcionan las redes inalámbricas?

Como las mismas lo sugieren, las redes inalámbricas, a veces denominadas WiFi, le permiten conectarse a Internet sin cables. Si su hogar, su oficina, el aeropuerto, o aún un café tienen una conexión inalámbrica, usted puede acceder a la red desde cualquier lugar dentro del área de cobertura inalámbrica.

Las redes inalámbricas se sostienen sobre ondas de radio más que de cables para conectar computadoras a Internet. Un transmisor, conocido como un punto de acceso inalámbrico o *gateway*, está cableado a una conexión de Internet. Esto brinda un "hotspot" o zona interactiva, que transmite la conectividad por ondas de radio. Los hotspots tienen información de identificación, incluyendo un ítem llamado SSID (*service set identifier*), que permite a las computadoras localizarlos. Las computadoras que tienen una tarjeta inalámbrica y tienen permiso para acceder a la frecuencia

inalámbrica, pueden aprovechar la conexión de la red. Algunas computadoras pueden identificar automáticamente las redes inalámbricas abiertas en un área dada, mientras que otras pueden requerir que usted localice e ingrese la información tal como el SSID.

¿Qué amenazas de seguridad están asociadas con las redes inalámbricas?

Como las redes inalámbricas no requieren de un cable entre una computadora y la conexión de Internet, es posible que los atacantes que estén dentro del rango tomen control o intercepten una conexión no protegida. Una práctica conocida como búsqueda de redes inalámbrica (*wardriving*) se trata de personas equipadas con una computadora, una tarjeta inalámbrica, y un dispositivo, que se mueven por las áreas en busca de redes inalámbricas e identifican las coordenadas específicas de una ubicación de red. Esta información generalmente es luego publicada online. Algunos individuos que participan en, o se aprovechan de la búsqueda de redes inalámbrica tienen intenciones maliciosas y podrían usar esta información para tomar control de su red inalámbrica hogareña o interceptar la conexión entre su computadora y un *hotspot* en particular.

¿Qué puede hacer para minimizar los riesgos de su red inalámbrica?

- **Cambiar las contraseñas por default** – La mayoría de los dispositivos de red, incluyendo los puntos de acceso inalámbricos, están pre-configurados con contraseñas del administrador por default para simplificar la instalación. Estas contraseñas por default son fácilmente encontradas online, por lo tanto no ofrecen protección. El cambio de las contraseñas por default hace más difícil a los atacantes controlar el dispositivo.
- **Restringir el acceso** –Permita que sólo los usuarios autorizados accedan a su red. Todos los componentes de hardware conectados a una red tienen una dirección MAC (*media access control*). Usted puede restringir o permitir acceso a su red filtrando las direcciones MAC. Consulte su documentación de usuario para obtener información específica referida a la habilitación de estas funciones. También hay varias tecnologías disponibles que requieren autenticación de los usuarios inalámbricos antes de acceder a la red.
- **Encriptar los datos en su red** - WEP (Wired Equivalent Privacy) y WPA (Wi-Fi Protected Access) encriptan información en dispositivos inalámbricos. Sin embargo, WEP tiene una cantidad de temas de seguridad que lo hacen menos efectivo que el WPA, por lo tanto usted debería buscar específicamente los engranajes que soporten el encriptado vía WPA. El encriptado de los datos prevendría que cualquiera que pudiera tener acceso a su red no pueda mirar sus datos.
- **Proteger su SSID** - Para evitar que gente de afuera acceda fácilmente a su red, evite publicar su SSID. Consulte su documentación de usuario para ver si puede cambiar el SSID por default para que sea más difícil de adivinar.
- **Instalar un firewall** – Aunque es una buena práctica de seguridad instalar un firewall en su red, debería instalar también un firewall directamente en sus dispositivos (un firewall basado en el host). Los atacantes que directamente puedan pinchar su red inalámbrica también podrán sortear su firewall de red –

un firewall basado en el host agregará una capa de protección a los datos de su computadora.

- **Mantener el software anti-virus** – Para reducir el daño que los atacantes puedan infligir sobre su red y computadora inalámbrica puede instalar un software anti-virus y mantener sus definiciones de virus actualizadas. Muchos de estos programas también tienen rasgos adicionales que pueden protegerlo contra o detectar spyware y Troyanos.

5. Consejo de Seguridad Informática ST05-017

Seguridad Informática para los Dispositivos Electrónicos

Cuando piense en seguridad informática, recuerde que los dispositivos electrónicos tales como teléfonos celulares y PDAs también pueden ser vulnerables a ataques. Tome las precauciones apropiadas para limitar su riesgo.

¿Por qué la seguridad informática se extiende más allá de sus computadoras?

En realidad, el tema no es que la seguridad informática se extienda más allá de sus computadoras; es que las computadoras se extienden más allá que las laptops y desktops (computadoras de escritorio) tradicionales. Muchos dispositivos electrónicos son computadoras – desde teléfonos celulares y PDAs a video juegos y sistemas de navegación para automóviles. Mientras que las computadoras ofrecen mayores características y funcionalidad, también introducen nuevos riesgos. Los atacantes pueden aprovechar estos avances tecnológicos para apuntar a dispositivos previamente considerados "seguros." Por ejemplo, un atacante puede infectar su teléfono celular con un virus, robar su teléfono o servicio inalámbrico o acceder a los datos de su PDA. No sólo estas actividades tienen consecuencias para su información personal, sino que podrían también tener serias consecuencias si usted almacena información de empresas en ese dispositivo.

¿Qué tipo de electrónicos son vulnerables?

Cualquier dispositivo electrónico que usa algún tipo de componente computarizado es vulnerable a las imperfecciones y vulnerabilidades del software. Estos riesgos aumentan si el dispositivo está conectado a Internet o a una red a la que un atacante puede tener acceso. Recuerde que una conexión inalámbrica también introduce estos riesgos. La conexión externa ofrece un camino para que un atacante envíe o extraiga información desde su dispositivo.

¿Cómo puede protegerse a sí mismo?

- **Recordar la seguridad física** – Tener acceso físico a un dispositivo facilita a un atacante que extraiga o corrompa la información. No deje su dispositivo

delante del público o en áreas fácilmente accesible sin prestarle atención o abandonado.

- **Mantener el software actualizado** – Si el proveedor larga parches para el software que hace operar su dispositivo, instalarlo lo antes posible. Estos parches pueden llamarse actualizaciones *firmware*. Al instalarlos puede prevenir que los atacantes aprovechen los problemas o vulnerabilidades conocidos.
- **Usar buenas contraseñas** – Elija dispositivos que le permitan proteger su información con contraseñas. Seleccione contraseñas que serán difíciles de adivinar para los ladrones y use diferentes contraseñas para diferentes programas y dispositivos. No elija opciones que permitan que su computadora recuerde sus contraseñas.
- **Deshabilitar la conectividad remota** – Algunos PDAs y teléfonos están equipados con tecnologías inalámbricas, tales como Bluetooth, que pueden usarse para conectarse con otros dispositivos o computadoras. Debería deshabilitar estas funciones cuando no están en uso.
- **Encriptar archivos** – Aunque la mayoría de los dispositivos no ofrecen una opción de encriptar archivos, usted puede tener un software para encriptar en su PDA. Si está almacenando información personal o de empresas, ver si tiene la opción de encriptar los archivos. Encriptando los archivos, se asegura que gente no autorizada no pueda ver los datos aunque tengan acceso físico a ellos. Cuando use el encriptado, es importante que recuerde sus contraseñas y frases contraseña; si se las olvidara o las perdiera, podría perder sus datos.

6. Consejo de Seguridad Informática ST06-007

Defender los Teléfonos Celulares y PDAs Contra los ataques

Como los teléfonos celulares y PDAs han pasado a ser más avanzados tecnológicamente, los atacantes están encontrando nuevas formas de apuntar a sus víctimas. Usando mensajes de texto o correo electrónico, un atacante podría atraerlo hacia un sitio malicioso o convencerlo de que instale un código malicioso en su dispositivo portátil.

¿Qué riesgos únicos presentan los teléfonos celulares y los PDAs?

La mayoría de los teléfonos celulares actuales tienen la función de enviar y recibir mensajes. Algunos teléfonos celulares y PDAs también ofrecen la función de conectarse a Internet. Aunque éstas son funciones que usted podría encontrar útiles y practicas, los atacantes pueden tratar de aprovecharlas. Como resultado, un atacante puede llegar al lograr lo siguiente:

- **Abusar de su servicio** – La mayoría de los planes de teléfonos celulares limitan la cantidad de mensajes que puede enviar y recibir. Si un atacante manda

spams con sus mensajes de texto, a usted le podrían cobrar cargos adicionales. Un atacante también puede infectar su teléfono o PDA con código malicioso que les permitirá usar su servicio. Como el contrato está a su nombre, usted será responsable de los costos.

- **Atraerlo a un sitio web malicioso** – Mientras que los PDAs y teléfonos celulares que le dan acceso al correo electrónico son blancos para los ataques phishing estándares, ahora los atacantes están enviando mensajes de texto a teléfonos celulares. Estos mensajes, supuestamente de una empresa legítima, pueden tratar de convencerlo de que visite un sitio malicioso proclamando que hay un problema con su cuenta o diciéndole que usted se ha suscripto a un servicio. Una vez que usted visite el sitio, puede ser engañado para brindar información personal o bajar un archivo malicioso.
- **Usar su teléfono celular o PDA en un ataque** – Los atacantes que ganan control de su servicio pueden usar su teléfono celular o PDA para atacar a otros. No sólo esto oculta la identidad real del atacante, sino que permite que el atacante aumente la cantidad de objetivos o blancos.
- **Ganar acceso a la información de la cuenta** – En algunas áreas, los teléfonos celulares están pudiendo hacer ciertas transacciones (desde pagar el estacionamiento o compras en comercios hasta llevar a cabo grandes transacciones financieras). Un atacante que puede ganar acceso a un teléfono que se utiliza para estos tipos de transacciones puede descubrir la información de su cuenta y usarla o venderla.

¿Qué puede hacer para protegerse?

- **Seguir las pautas generales para proteger dispositivos portátiles** - Tomar precauciones para asegurar su teléfono celular y PDA de la misma forma que lo debería hacer con su computadora.
- **Tener cuidado con publicar su teléfono celular o dirección de correo electrónico** – Los atacantes a menudo usan software para navegar por sitios web buscando direcciones de correo electrónico. Estas direcciones luego se convierten en blancos para los atacantes y spam. También se pueden recolectar números de teléfonos celulares automáticamente. Limitando la cantidad de personas que tienen acceso a su información, usted limita su riesgo de convertirse en una víctima.
- **No siga los links enviados en correo electrónico o en mensajes de texto** – Sospeche de los URLs enviados en correos electrónicos no solicitado o mensajes de texto. Aunque estos links puedan parecer legítimos, en realidad podrán dirigirlo a un sitio web malicioso.
- **Esté atento al software que se baja de Internet** – Hay muchos sitios que ofrecen juegos y otros software que se pueden bajar a su teléfono celular o PDA. Estos software podrían incluir un código malicioso. Evite bajar archivos de sitios en los que no confía. Si está obteniendo archivos de un sitio supuestamente seguro, busque un certificado del sitio web. Si baja un archivo de un sitio web, considere guardarlo en su computadora y escanearlo manualmente para detectar si tiene virus antes de abrirlo.

- **Evaluar sus configuraciones de seguridad** – Asegúrese de aprovechar las configuraciones de seguridad ofrecidas en su dispositivo. Los atacantes pueden aprovechar las conexiones de Bluetooth para acceder o bajar información en su dispositivo. Deshabilite el Bluetooth cuando no lo está usando para evitar un acceso no autorizado.