TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 5 UNIDAD 1

Universidad Tecnológica de Pereira | faceIT

Lección 5–Vulnerabilidades en los dispositivos:

Un dispositivo puede tener fallas de seguridad internas. Por ejemplo, dispositivos que no tengan actualizado el software para cubrir fallas de seguridad descubiertas, dispositivos con sistemas de autenticación débiles e incluso dispositivos que tengan vulnerabilidades no reveladas públicamente, pero que atacantes conozcan y estén esperando el momento preciso para usarlas (a esto se conoce como vulnerabilidad del día cero).

En un dispositivo con fallas en la seguridad, los atacantes pueden ejecutar programas, instalar malware y controlar a voluntad el equipo de forma remota. Incluso hay dispositivos cuyas fallas en la seguridad permiten que el atacante siga teniendo el control a pesar de que haya sido actualizado con la última versión de actualizaciones de seguridad.

Hay programas que ciertos usuarios usan para tomar mayor control sobre los dispositivos y personalizarlos o ejecutar código propio. A estas prácticas se les conoce como jailbreaking y consiste en que un usuario, de forma no oficial, obtiene acceso a los sistemas principales de un dispositivo. Algunos casos conocidos son el jailbreak de Iphone e Ipod que permitía a los usuarios instalar aplicaciones sin pagar, o software que se ejecuta en consolas de juegos para que lean discos piratas. Estas acciones evitan las medidas de seguridad del fabricante facilitando que un atacante tome el control del dispositivo y pueda ejecutar instrucciones e instalar software malicioso. Los mismos desarrolladores de los programas de jailbreaking insertan vulnerabilidades como puertas traseras para hacerse con el control de los dispositivos a cambio de que el usuario tenga las capacidades extra. Evidentemente, sin que el usuario se de cuenta.

Medidas de protección de dispositivos

Para proteger los datos en los dispositivos se deben tomar ciertas medidas de seguridad como:

- Actualizar constantemente el software y el firmware de los dispositivos, en especial instalar las actualizaciones relacionadas con la seguridad informática.
- Apagar los dispositivos que no se encuentran en uso.
- Habilitar las características de seguridad que los dispositivos integran.
- Habilitar múltiple factor de autenticación en los dispositivos
- Utilizar software antivirus
- Evitar la instalación de software pirata y sin licencias

- Evitar la instalación de software de desconocidos
- Utilizar firewalls por software
- Cifrar el contenido de los medios de almacenamiento de los dispositivos. Un sistema con un disco duro cifrado no puede ser leído por atacantes, así se hagan con el control de la información no la podrán ver ni entender.
- Limitar el acceso al dispositivo. Muchas fallas de seguridad se dan porque el usuario descuida unos instantes de tiempo el equipo en estado desbloqueado, lo que facilita que un atacante mande un mensaje, inserte una memoria USB, o instale un programa y robe información. Para evitar esas vulnerabilidades basta con bloquear los equipos que no están siendo usados así se hagan pausas breves. Si los dispositivos son portátiles, llevarlos en todo momento evita que un atacante pueda tener acceso no autorizado