TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 4 UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Lección 4- Dispositivos y controles de seguridad

Los miembros que comparten datos en una red son los dispositivos. Para realizar nuestras tareas laborales, entretenimiento y comunicaciones necesitamos de dispositivos conectados a nuestras redes. Casi siempre todos los dispositivos que empleamos almacenan información confidencial sobre nosotros. Para poder proteger los datos es necesario entender cómo los dispositivos que tenemos capturan y comparten datos en las redes locales y en internet.

Los dispositivos pueden ser:

- Memorias USB
- Cualquier dispositivo que tenga conexión inalámbrica a una red, esto abarca computadores, teléfonos móviles, relojes inteligentes, tabletas, asistentes domésticos, sistemas de sonido, televisores, enrutadores, cámaras, dispositivos de grabación de video, relojes digitales, robots de limpieza y todo electrodoméstico administrable por red (cafeteras, neveras, lavadoras, entre otros).
- Paneles de los automóviles, sistemas de infotainment, sistemas de control de voz en los autos, sistemas de localización en los autos.
- Zonas WiFi.

Así mismo, servicios como los de publicidad, que permiten a grandes corporaciones (como es el caso de las redes sociales y buscadores) al recopilar datos de los dispositivos de los usuarios pueden generar recomendaciones de cosas que comprar o sitios para visitar basado en nuestros datos y la probabilidad calculada de que consumamos esos productos.

A pesar de todas las oportunidades que los dispositivos permiten, también se convierten en vectores de amenazas proporcionando formas para que se lleven a cabo ataques. Por ejemplo:

Telefonos, computadores portátiles y tablets: Un atacante puede intentar engañar al usuario para que descargue aplicaciones malintencionadas. Estas aplicaciones pueden filtrar datos de usuario almacenados localmente como son contraseñas, usuarios, números de tarjetas, entre otros. Un ciberdelincuente puede aprovechar estos datos para robar dinero e información, pedir rescates y hacer daños.

En esencia, todo dispositivo que pueda interactuar con datos y que pueda conectarse entre equipos es un dispositivo. Cada dispositivo tiene información que puede ser susceptible de robos y expuesta. Por ejemplo, olvidar que alguna vez se realizó la conexión inalámbrica a una red WiFi abierta puede ser una falla de seguridad ya que los dispositivos suelen conectarse automáticamente sin pedir permisos al usuario.

Es importante recordar que los dispositivos, al ser parte integral de nuestras vidas, recopilan y guardan mucha información personal.

Un ejemplo son las aplicaciones de mapas que muestran el tráfico en tiempo real. Esto es posible gracias a que los servicios de mapas recopilan datos de miles de nuestros dispositivos como la geolocalización en tiempo real, los datos de los sensores internos tales como los acelerómetros y giroscopios que permiten identificar patrones de movimiento (frenar, acelerar) y variables físicas como desplazamiento, velocidad y aceleración que sufre el dispositivo a lo largo del tiempo.

Memorias USB: En una memoria USB es fácil colocar cualquier categoría de malware que se instale al instetarlo en un computador, por ejemplo key loggers (aplicaciones de registro de teclado), software espía, backdoors, ransomware, entre otros.

Dispositivos de asistencia que están siempre en línea: Equipos como asistentes en el hogar (Google home, Alexa, siri) pueden ser empleados por atacantes ya que están siempre con el micrófono abierto escuchando lo que los usuarios dicen. También equipos como cámaras y grabadores de video de seguridad pueden ser atacados para que reporten información a otros servidores sin que los usuarios se den cuenta. Esto puede exponer la vida privada y la seguridad de las personas que sean monitoreadas con los dispositivos mencionados.