TIC

TALENTO TECH

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 6 UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

TIC

Lección 6-Seguridad en las aplicaciones

Las aplicaciones permiten el uso de los dispositivos para comunicarse con internet de forma fácil y amigable para el usuario. Es con aplicaciones que podemos compartir fotos, ver multimedia, realizar transacciones bancarias y realizar tareas en internet.

Sin embargo, las aplicaciones pueden ser vectores de ataque para ciberdelincuentes, por eso es necesario identificar qué hacen las aplicaciones para comunicar datos en internet y cómo podemos protegernos.

Las aplicaciones son software. El software son comandos ordenados que un dispositivo ejecuta para hacer algún tipo de trabajo. El software necesita de componentes físicos (hardware) de un dispositivo. Generalmente el software se divide en dos categorías. El software del sistema y el software de la aplicación.

Software de sistema:

Son los componentes de software que se ejecutan en primer lugar al encender un dispositivo. Este software se encarga de manejar los periféricos del software y hace que todo funcione, también reacciona cuando algo deja de funcionar.

El software de sistema suele ejecutarse en segundo plano y controla dispositivos como las pantallas, teclados, mouse, controladores de red y todos los programas físicos. Este software incluye el sistema operativo, el firewall y los antivirus. Puede ser objeto de ataques, sin embargo, es importante distinguir los ataques al software del sistema respecto al software de aplicación.

Software de aplicación:

Son todos los programas que tienen un propósito específico. Por ejemplo, un programa de procesamiento de texto, uno de hojas de cálculo, programas de correo electrónico, programas para mandar mensajes instantáneos y cualquier programa instalable que no haga parte del software del sistema.

El software de aplicación se caracteriza por:

- Realiza un trabajo especializado (escribir textos, editar videos, enviar mensajes, videojuegos)
- Está diseñado para que el usuario interactúe directamente con él.
- No se ejecuta por si mismo, necesita el software del sistema y que el usuario lo invoque.
- Debe ser instalado por un usuario.

Las aplicaciones están diseñadas para todo tipo de sistemas. Teléfonos móviles, computadores, televisores, relojes inteligentes entre otros. Gracias a internet, las aplicaciones también intercambian datos con los proveedores de aplicaciones. Por ejemplo, los juegos suelen recopilar datos de los jugadores, así como las aplicaciones de mapas recopilan la información de la ubicación de los usuarios. Algunas aplicaciones recopilan datos en segundo plano, cuando el usuario no está interactuado con ella. Esta información se comparte con otras aplicaciones. Por ejemplo, las redes sociales suelen revisar y compartir el historial de navegación web para generar anuncios y recomendaciones de compra.

Como las aplicaciones manejan tipos de información privada, los ciberdelincuentes suelen ponerlas en peligro para robar información.

Aplicaciones de Orígenes No Confiables

Hoy en día, descargar aplicaciones en dispositivos como computadoras, teléfonos inteligentes o tabletas es más fácil que nunca. La mayoría de las personas utiliza tiendas de aplicaciones reconocidas, que verifican la autenticidad de las apps antes de publicarlas y bloquean aquellas que no cumplen con sus normas de seguridad.

Sin embargo, también existen sitios menos regulados donde puedes descargar aplicaciones. En estas plataformas, las apps suelen tener pocas restricciones y escasas verificaciones de seguridad. Aunque no todas las aplicaciones disponibles en estos lugares son maliciosas, los ciberdelincuentes pueden aprovechar la falta de control para subir programas dañinos disfrazados de apps legítimas. Por ejemplo, pueden crear una copia de una aplicación popular y cargarla en un sitio poco confiable.

Instalar apps desde orígenes no verificados aumenta el riesgo de sufrir un ataque cibernético, por lo que es fundamental evitar descargar aplicaciones fuera de tiendas oficiales.

Aplicaciones con Vulnerabilidades

Aunque los desarrolladores hacen todo lo posible por proteger sus aplicaciones, es imposible garantizar que sean 100 % seguras. Los ciberdelincuentes buscan constantemente errores o vulnerabilidades que puedan aprovechar. Dos tipos comunes de vulnerabilidades son las de **código abierto** y las de **día cero.**

Vulnerabilidades de Código Abierto

Los desarrolladores suelen utilizar bibliotecas de código abierto, que son soluciones compartidas y de acceso libre para resolver problemas específicos. Una de las ventajas del código abierto es que cualquier vulnerabilidad encontrada se identifica y corrige públicamente. Sin embargo, este mismo acceso público permite que los ciberdelincuentes exploren estas vulnerabilidades para atacarlas.

Por eso, es esencial que los desarrolladores mantengan actualizadas las bibliotecas de código abierto que utilizan en sus aplicaciones para reducir riesgos.

Vulnerabilidades de Día Cero

Los errores desconocidos en una aplicación, llamados vulnerabilidades de día cero, son otro objetivo común. Si un ciberdelincuente detecta una de estas vulnerabilidades antes que los desarrolladores, puede explotarla sin que los usuarios o los responsables del software se den cuenta. Por ejemplo, un ciberdelincuente podría encontrar un error en una app bancaria y aprovecharlo para robar información personal o dinero de los usuarios.

El término "día cero" hace referencia a que los desarrolladores no tienen tiempo previo para reaccionar, ya que la vulnerabilidad se explota desde el primer día en que se descubre.

Amenazas Basadas en Navegadores

El navegador es la puerta principal al Internet, pero también puede ser un blanco para amenazas. Entre las más comunes están

Ataques Basados en Cookies

Las cookies son pequeños archivos de texto que almacenan información como credenciales de usuario o historial de búsquedas. Su función es mejorar la experiencia de navegación. Sin embargo, si un ciberdelincuente logra interceptar tus comunicaciones, podría robar estos datos y utilizarlos para hacerse pasar por ti en sitios web legítimos.

Typosquatting (Errores Tipográficos Deliberados)

El typosquatting consiste en registrar dominios mal escritos de sitios web populares para engañar a los usuarios. Por ejemplo, si alguien escribe mal el nombre de un sitio legítimo, podría terminar en una página falsa diseñada para robar información personal o infectar el dispositivo con malware.

Hay algunas prácticas que pueden ayudar a proteger las aplicaciones:

1. Aplicación rápida de actualizaciones

Los sistemas operativos y muchas aplicaciones populares, como procesadores de texto o plataformas de streaming, publican actualizaciones frecuentes. Estas no solo introducen nuevas funciones, sino que corrigen vulnerabilidades conocidas.

Ejemplo: Imagina que usas una app de banca móvil que lanza una actualización para corregir una brecha de seguridad. Si no actualizas, podrías ser víctima de un ataque que permita a un ciberdelincuente acceder a tu cuenta.

Recomendación: Configura tus dispositivos para que instalen actualizaciones automáticamente y asegúrate de revisar periódicamente si hay pendientes.

2. Revisión de la configuración de las aplicaciones

La mayoría de las aplicaciones vienen con configuraciones predeterminadas diseñadas para facilidad de uso, pero estas pueden ser una puerta de entrada para atacantes.

Ejemplo: Un sistema de videoconferencias podría tener habilitada una cuenta predeterminada con una contraseña genérica. Un ciberdelincuente podría usarla para infiltrarse en tus reuniones privadas.

Recomendación: Cambia las contraseñas por defecto y ajusta las configuraciones para maximizar la seguridad. Por ejemplo, enrutadores, cámaras inteligentes o aplicaciones empresariales suelen tener ajustes críticos que deben modificarse.

3. Configuración de privacidad

Muchas aplicaciones recopilan datos de los usuarios para mejorar sus servicios o, en algunos casos, para dirigir anuncios personalizados.
Ejemplo: Una app de mapas podría registrar todas las rutas que tomas, mientras que una tienda en línea podría rastrear tus búsquedas para enviarte recomendaciones.
Recomendación: Ve a la configuración de privacidad de cada aplicación y ajusta lo que deseas compartir. Por ejemplo, desactiva el historial de ubicaciones en apps de mapas o limita los permisos de las redes sociales para evitar un exceso de recopilación de datos.

4. Gestión de cookies

Las cookies almacenan información de tus actividades en sitios web, como contraseñas o preferencias. Aunque son útiles, también pueden ser explotadas si caen en manos equivocadas.

Ejemplo: Un ciberdelincuente podría acceder a tus cookies almacenadas en el navegador y obtener datos sensibles, como tus credenciales de inicio de sesión.

Recomendación: Borra regularmente las cookies desde la configuración de tu navegador y usa el modo de navegación privada (como "Incógnito" en Chrome) para evitar que se almacenen datos innecesarios.

5. Uso exclusivo de aplicaciones de confianza

Hoy en día, puedes descargar aplicaciones fácilmente desde diversas tiendas en línea, pero no todas son seguras.

Ejemplo: Supongamos que encuentras una versión "gratuita" de una aplicación popular en una tienda desconocida. Podría funcionar como la original, pero incluir malware que acceda a tus datos bancarios.

Recomendación: Descarga siempre aplicaciones desde tiendas oficiales como Google Play Store, Apple App Store o Microsoft Store. Antes de instalar una app, verifica las reseñas, la reputación del desarrollador y los permisos que solicita.
La seguridad de las aplicaciones no depende solo de los desarrolladores; como usuarios, también debemos tomar medidas proactivas para proteger nuestros datos y dispositivos. Implementar estas prácticas simples puede marcar la diferencia entre disfrutar de una experiencia segura o caer en manos de un ciberdelincuente.