Medidas de defensa ante los principales vectores de ataque en dispositivos móviles

Si hemos llegado hasta este punto, ya somos conscientes de las distintas tácticas mediante las cuales nuestros dispositivos móviles, y por tanto nuestra información personal, pueden verse comprometidos. Para evitar que estos riesgos se conviertan en amenazas reales, es fundamental conocer y aplicar mecanismos de defensa eficaces. A continuación, se explican cinco de los vectores de ataque más comunes y los mecanismos existentes para protegernos frente a ellos:

1. Aplicaciones maliciosas

Durante la instalación de aplicaciones, especialmente aquellas descargadas desde fuentes no oficiales, se solicitan permisos como el acceso a la cámara, al micrófono o a la ubicación. Si se aceptan sin revisar, la aplicación puede tener acceso total al dispositivo.

Mecanismo de defensa:
Una forma eficaz de protegernos es revisar manualmente los permisos de cada aplicación y revocar aquellos que no son necesarios para su funcionamiento.
Además, se recomienda instalar aplicaciones únicamente desde tiendas oficiales, como Google Play o App Store, donde los sistemas de revisión detectan comportamientos maliciosos y retiran aplicaciones potencialmente peligrosas.

2. Spyware (como Pegasus)

El spyware es un tipo de software espía que se instala sin conocimiento del usuario y recopila información privada, como mensajes, ubicaciones o patrones de comportamiento.

Mecanismo de defensa:
La mejor defensa es mantener siempre actualizado el sistema operativo y las aplicaciones instaladas, ya que los fabricantes lanzan parches de seguridad para corregir vulnerabilidades que este tipo de malware aprovecha.
También es recomendable contar con antivirus móviles de confianza, que analicen el comportamiento de las apps e identifiquen software espía en segundo plano.

3. Uso de redes Wi-Fi públicas

Las redes Wi-Fi abiertas, muy comunes en cafeterías o aeropuertos, pueden ser manipuladas por atacantes para interceptar información confidencial.

Mecanismo de defensa:
Para evitarlo, se debe utilizar una VPN (Red Privada Virtual) al conectarse a redes públicas.
La VPN cifra toda la información que se envía y se recibe, creando un canal seguro que impide que terceros puedan ver o modificar el tráfico.
Adicionalmente, se recomienda evitar realizar transacciones sensibles (como acceder al banco) desde redes públicas sin protección.

4. Aplicaciones inactivas

Las aplicaciones que ya no usamos pueden seguir funcionando en segundo plano, mostrando publicidad engañosa o recopilando datos sin permiso.

Mecanismo de defensa:
Una medida sencilla y efectiva es desinstalar las aplicaciones que no se utilizan, reduciendo así la superficie de ataque.
Esto no solo elimina posibles procesos maliciosos en segundo plano, sino que también mejora el rendimiento del dispositivo y libera espacio.

5. Falta de contraseña o contraseñas débiles

Muchas personas no protegen sus dispositivos móviles con contraseña o utilizan claves fáciles de adivinar, lo que facilita el acceso no autorizado.

Mecanismo de defensa:
La solución más efectiva es configurar una autenticación fuerte, combinando una contraseña segura con métodos biométricos, como la huella dactilar o el reconocimiento facial.
También se recomienda activar el cifrado del dispositivo, de forma que, aunque el móvil caiga en manos de otra persona, no se pueda acceder a su contenido sin la clave de desbloqueo.

Bibliografía

1. Centro Criptológico Nacional (CCN-CERT) – Guía CCN-STIC-1406: Seguridad en Dispositivos Móviles

https://www.ccn-cert.cni.es

2. Agencia Española de Protección de Datos (AEPD) – Recomendaciones para el uso seguro del móvil

https://www.aepd.es/guias

3. National Institute of Standards and Technology (NIST) – Special Publication 800-124 Rev. 2: Guidelines for Managing the Security of Mobile Devices

https://csrc.nist.gov/publications/detail/sp/800-124/rev-2/final