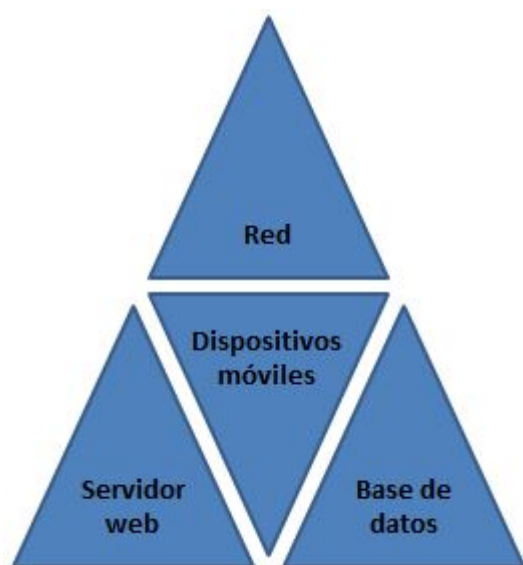


Factores de riesgo en las aplicaciones móviles y algunos controles básicos con los que abordarlos

Con la continua evolución tecnológica, especialmente en el ámbito empresarial, la auditoría del TI y los profesionales de seguridad deben adaptarse al escenario de las amenazas cambiante creado por las aplicaciones móviles adelantándose al riesgo. Para ello deben poner controles apropiados y probar las aplicaciones móviles desde su concepción hasta su lanzamiento. Es por ello que he seguido leyendo sobre la **Gestión del Riesgo Institucional en el Mundo Móvil**, y esta vez he investigado acerca de los **factores de riesgo** en las aplicaciones móviles y algunos **controles básicos** con los que abordarlos. En este Post he utilizado como fuente un artículo de una revista llamada **“ISACA Journal: mobile apps”**.

Los riesgos en las aplicaciones móviles se pueden dividir en cuatro categorías:



Riesgos y controles en la categoría de Dispositivos móviles:

1. Almacenamiento de datos:

- **Riesgo:** Pérdida y divulgación de datos.
- **Control:** El cifrado de los datos en reposo en el dispositivo móvil se establece en el Estándar de Cifrado Avanzado (Advanced Encryption Standard: AES) de 128, 192 o 256. Mediante este control los datos se almacenan de forma segura para evitar la extracción maliciosa de la aplicación cuando los datos están en reposo.

2. Transmisión de datos:

- **Riesgo:** Pérdida y divulgación de datos.
- **Control:** El cifrado de datos se aplica para los datos en transmisión a través de la Capa de Puertos Seguros (Secure Sockets Layer: SSL) y fuertes protocolos de seguridad tales como:
 - Acceso Web – HTTPS vs. HTTP
 - Transferencia de archivos – FTPS, SFTP, SCP, WebDAV sobre HTTPS vs. FTP, RCP
 - Protocolos de seguridad – Seguridad en la Capa de Transporte (Transport Layer Security: TLS)

Mediante este control la transmisión de datos de la aplicación móvil está cifrada cuando no se dispone de datos en reposo.

IMPORTANTE: Estos dos primeros riesgos tratan sobre la pérdida y la divulgación de datos, tema que hace referencia a la **DLP** y a la gestión de contenido móvil (**MCM**).

3. Aplicación de gestión de acceso y seguridad:

- **Riesgo:** Acceso no autorizado y fraude.
- **Control:** La gestión de aplicaciones móviles (**MAM**) se utiliza para gestionar el acceso y el

despliegue de la aplicación. Además, se mantienen unas adecuadas listas blancas y listas negras. Mediante este control la aplicación está configurada para limitar el acceso y configurada adecuadamente para uso autorizado limitado.

4. Llevar dispositivos móviles fuera del perímetro empresarial:

- **Riesgo:** Pérdida o robo del dispositivo móvil, haciendo posible el acceso no autorizado a las aplicaciones móviles del dispositivo y al fraude de los datos de éstas.
- **Control:** (MAM) *Leer el control 3.2 de esta categoría.

Riesgos y controles en la categoría de Red:

1. Conectividad inalámbrica:

- **Riesgo:** Pérdida y divulgación de datos (**DLP & MCM**).
- **Control:** La transmisión de datos utiliza, como mínimo, SSL o TLS. Ambos protocolos criptográficos para la transmisión segura de datos. Mediante este control el cifrado se aplica cuando se activa la conexión Wi-Fi.

2. Secuestro de sesión (Session hijacking):

- **Riesgo:** Pérdida y divulgación de datos y acceso no autorizado (**DLP & MCM**).
- **Control:** Los protocolos de conexión para el Localizador Uniforme de Recursos (Uniform Resource Locator: URL) a través de TLS son a través de HTTPS en lugar de HTTP para conectarse de forma segura a una URL. Mediante este control se evita el secuestro de una sesión debido a un protocolo de conexión inseguro.

Riesgos y controles en la categoría de Servidor web:

1. Gestión de acceso:

- **Riesgo:** Pérdida y divulgación de datos y acceso no autorizado (DLP & MCM).
- **Control:** Todos los servidores web aplicables se asignan a los propietarios de sistemas técnicos y empresariales. Los roles y responsabilidades definidos son adecuados, especialmente para el personal interno y de terceros. Mediante este control los roles y responsabilidades de la propiedad son establecidos, documentados y comunicados.

2. Ataque de fuerza bruta:

- **Riesgo:** Acceso no autorizado y fraude, disponibilidad de la aplicación.
- **Control:** Los protocolos de bloqueo están habilitados para cuentas con varios intentos de contraseña incorrectos. Se recomienda la utilización de CAPTCHA (programa que distingue entre seres humanos y ordenadores) para evitar DoS (Denegación de Servicio). Mediante este control la gestión de la estrategia de DoS abarca programas adecuados para bloquear los protocolos no autorizados.

Riesgos y controles en la categoría de Base de datos:

1. Acceso privilegiado:

- **Riesgo:** Acceso no autorizado y fraude.
- **Control:** El acceso a la BD está limitado a las personas apropiadas, y las revisiones de acceso adecuadas y las cuentas del sistema documentadas

se mantienen archivadas. Todas las cuentas y contraseñas predeterminadas se deshabilitan al aplicar controles de contraseña estrictos. Mediante este control el acceso elevado a las BBDD se asegura adecuadamente utilizando las mejores prácticas.

2. Inyección SQL (SQL injection):

- **Riesgo:** Acceso no autorizado y fraude.
- **Control:** Se da lugar a la técnica de validación de entrada; existen reglas específicamente definidas para el tipo y la sintaxis contra las reglas clave de negocio. Mediante este control el acceso a la BD del Back-end está protegido adecuadamente de vulnerabilidades utilizando técnicas de validación de entrada apropiadas.

3. Validación de la entrada de la aplicación (cliente):

- **Riesgo:** Acceso no autorizado y fraude.
- **Control:** La limpieza de los datos de usuario de la aplicación procedentes de la aplicación móvil se protege adecuadamente mediante comprobaciones de lógica incorporada dentro de la aplicación. La correcta implementación de las comprobaciones lógicas está habilitada en el lado del servidor. Mediante este control los datos procedentes de aplicaciones móviles son examinados antes de confiar en ellos para extraerlos o enviarlos a la capa de BD.

4. Servicios de BD de aplicaciones.

- **Riesgo:** Acceso no autorizado y fraude.
- **Control:** El servidor de BD se prueba adecuadamente y se protege contra ataques maliciosos. Los formularios de inicio de sesión requieren HTTPS. Las conexiones SSL son obligatorias.

¿Y el último post?:

No se han tratado amenazas como el **Phishing**. Puesto que considero que es fundamental tener ciertas nociones de esta amenaza, mi último post, tratará sobre ésta.

Referencia:

Revista de ISACA:

J. Khan, Mohammed «Mobile App Security Audit Framework», *ISACA Journal: mobile apps*, nº 4 (2016): 14-17.