

Como Lograr La Prevención de Fraude Para Móvil

Sesión en Español

Octubre 3, 2016

11:00 a 12:00 del Día

Sergio Piñón
Director de Seguridad y Vice Presidente Senior
Ocean Bank

Dos Tipos de Riesgos a Considerar y Su Importancia

- Riesgo al teléfono o dispositivo móvil interno del usuario empresarial
- Riesgo at teléfono o dispositivo móvil del consumidor o cliente

Identificación de riesgos

- Dirigido a todo tipo de móvil, productos, servicios y tecnología a la empresa
 1. El móvil esta completamente disponible a ataques y sin seguridad
 2. Tipo de comunicación para las diferentes funciones
 3. Uso de WiFi
 4. Transacciones financieras
 5. Correo electrónico
 6. Aplicaciones
 7. Protección al cliente o consumidor

Tipos de Riesgos

- Riesgo estratégico – no documentado en el plan estratégico
- Riesgo operacional – transacción iniciada, autenticación, y autorización
- Riesgo de SMS tecnológico – usualmente no cifrado
- Riesgo asociado a los sitio web – que pueden causar incumplimiento (breach)
- Riesgo de las aplicaciones al usuario – pueden comprometer las transacciones
- Riesgo de pago – falta de autenticación múltiple
- Riesgo de cumplimiento regulatorio
- Riesgo de reputación
- Falta de medición del riesgo
- Falta de Mitigación de riesgos

Mitigación

- Desarrollar estrategia para la seguridad de los servidores, base de datos, transacciones, prevención de fraude, técnicas geográficas, y identificación de anómalos
- Considerar autenticación mas fuerte y segura, cifrado máximo AES 256 bits para evitar acceso no autorizado a la información del cliente o al consumidor
- Implementar políticas y procedimientos para el inicio o inscripción al programa
- Procedimiento para controlar el fraude al consumidor o usuario de la aplicación
- Seguridad para el inicio de la sesión (Login Parameters) parámetros para la contraseña
- Monitorea de la actividad del usuario
- Entrenamiento a todos usuarios

Protección al móvil

- Aplicación “Lookout” - Permitido por Apple para los iPhones y Ipad
- Asegura el teléfono o equipo móvil total
 1. Localiza el equipo via GPS
 2. Seguridad a plataforma operacional del sistema
 3. Detecta aplicaciones con virus y con malware
 4. Guardia copias de todo los datos para la recuperación por si hay una perdida
 5. Alerta si la tarjeta de sim es removida
 6. Alerta si la conexión es terminada
 7. Alerta si se adquiere acceso no autorizado

Muchas Gracias!

FOLLOW US



@fiba_bankers