Implicaciones de Seguridad Informática en el Cumplimiento de Regulaciones Bancarias

Manuel López Arredondo
Specialist-Info Security Engr
manuel.lopez_arredondo@bankofamerica.com
+52 (33) 5350 5241

OWASP
Noviembre 11, 2011

The OWASP Foundation
http://www.owasp.org

Contenido

- Incidentes de seguridad en el Sistema Bancario Internacional
- Regulación Internacional
- Regulación Mexicana
- Esfuerzos de la Banca
- Riesgos Emergentes
- Comentarios

Incidentes de Seguridad en el Sistema Bancario

Nov, 2011
Capital One
Anonymous ejecutó un DDOS

Sep, 2011
Bank of Melbourne
La cuenta de Twitter fue hackeada para enviar phishing a los clientes

Jun, 2011
Citi Bank
El 1% de sus clientes (1.5 mm) pudo ser robada

Regulación Internacional

- Basilea III
  - Requerimientos de Capital Mínimos
    - Riesgo de Crédito
    - Riesgo Operacional
    - Riesgo de Mercado
  - Proceso de Revisiones Regulatorias
    - Marco de Control Regulatorio
    - Marco de Control Interno
      - Evaluación Interna de Sistemas
  - Disciplina de Mercado

Regulación Internacional

- Payment Card Industry (PCI)
  - Promovido por VISA, MasterCard, AMEX y Discover
  - Define los tipos de evaluaciones que deben de realizarse así como los escaneos a ejecutarse
  - Especifica frecuencias de ejecución de controles
  - Mantiene un estándar de controles para compañías emiten tarjetas de crédito

Regulación Internacional

- Estados Unidos
  - La ley Gramm-Leach-Bliley (GLBA) en el 1999 permitió la afiliación entre entidades bancarias, de valores y de seguros.
  - Sarbanes-Oxley Act nació en el 2002 para regular a todas las entidades que cotizan en la bolsa de Nueva York (NYSE)
    - Sección 404 enfocada a la revisión de los controles internos
- Argentina
  - Comunicado A4609 del BCRA
    - Establece los requisitos mínimos para la administración de TI así como de la seguridad de la información

Regulación Mexicana

- Circular Única de Bancos de la CNBV
  - Capítulo X (Medios Electrónicos)
    - Incorpora la definición de medios electrónicos
    - Define requisitos para contraseñas
    - Establece los componentes para el doble factor de autenticación
    - Medios de comunicación cifrada para la transmisión de información en internet
    - Bitácoras de accesos de usuarios y personal, manejo y almacenamiento seguro de solo lectura de dichos registros.
  - Capítulol IV (Administración de Riesgos)
    - Administración del Riesgo Tecnológico

Regulación Mexicana

- Código Penal Federal
  - Contempla que constituye el delito sólo si se accesa un sistema informático protegido por un mecanismo de seguridad.
  - El Código Penal no define qué debe entenderse por "mecanismo de seguridad".
  - Nuestro Código no contempla todos los tipos más comunes de ataques informáticos.

Regulación Mexicana

- Ley de Instituciones de Crédito
  - Artículo 112 Quáter.- Se sancionará con prisión de tres a nueve años y de treinta mil a trescientos mil días multa, al que sin causa legítima o sin consentimiento de quien esté facultado para ello:
    - I. Acceda a los equipos o medios electrónicos, ópticos o de cualquier otra tecnología del sistem bancario mexicano, para obtener recursos económicos, información confidencial o reservada, o
    - II. Altere o modifique el mecanismo de funcionamiento de los equipos o medios electrónicos, ópticos o de cualquier otra tecnología para la disposición de efectivo de los usuarios del sistema bancario mexicano, para obtener recursos económicos, información confidencial o reservada.

Esfuerzos de la Banca

- Alinieación a Marcos de Control como COSO, COBIT, ISO27001
- En instituciones globales se ha implementado el modelo
  - Top-down
  - Bottom-Up

Riesgos Emergentes

Comentarios