internet security auditors

2ª JORNADA SOBRE SEGURIDAD

EN MEDIOS DE PAGO

PCI DSS
PA DSS

ASPECTOS CLAVE DE SEGURIDAD EN PCI

VICENTE AGUILERA DÍAZ
DTOR. DEPARTAMENTO AUDITORÍA
INTERNET SECURITY AUDITORS

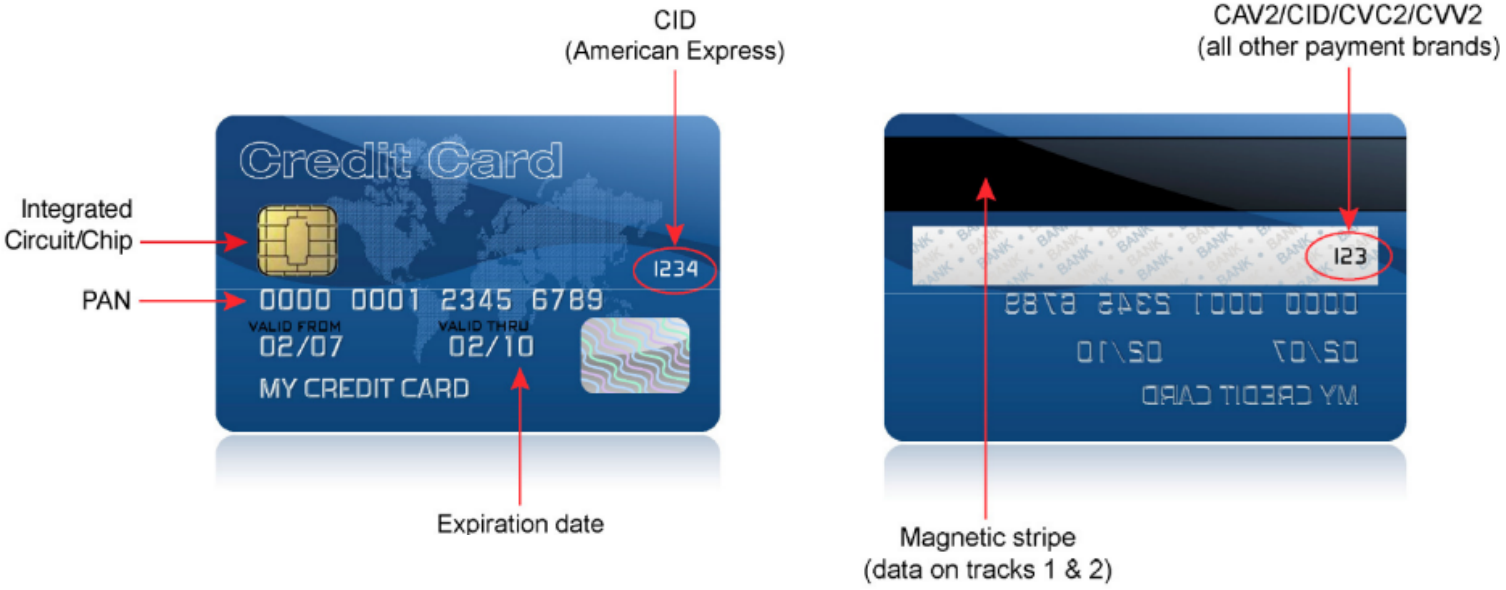
miércoles, 10 de Noviembre de 2010
Hotel Holiday Inn (Madrid)

Índice

- Objetivos y eficacia de la normativa
- Aspectos clave de la seguridad en PCI
- Mitos sobre PCI DSS
- Conclusiones

Objetivos y eficacia de la normativa

- **Objetivo:**
  - Fomentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

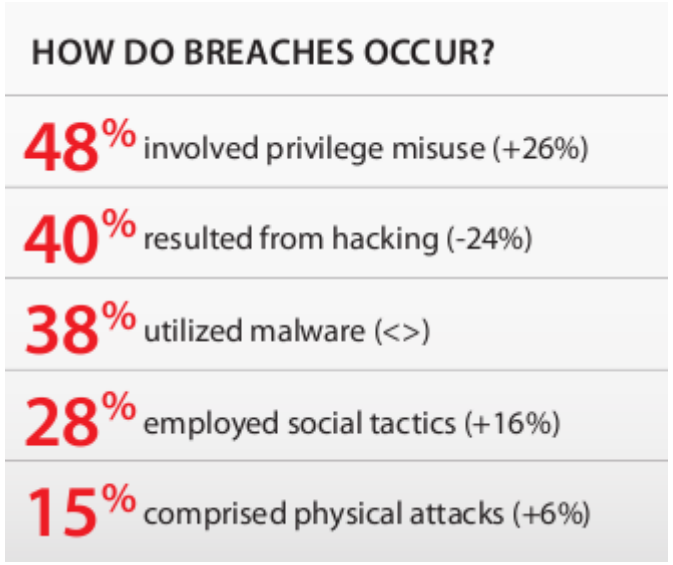


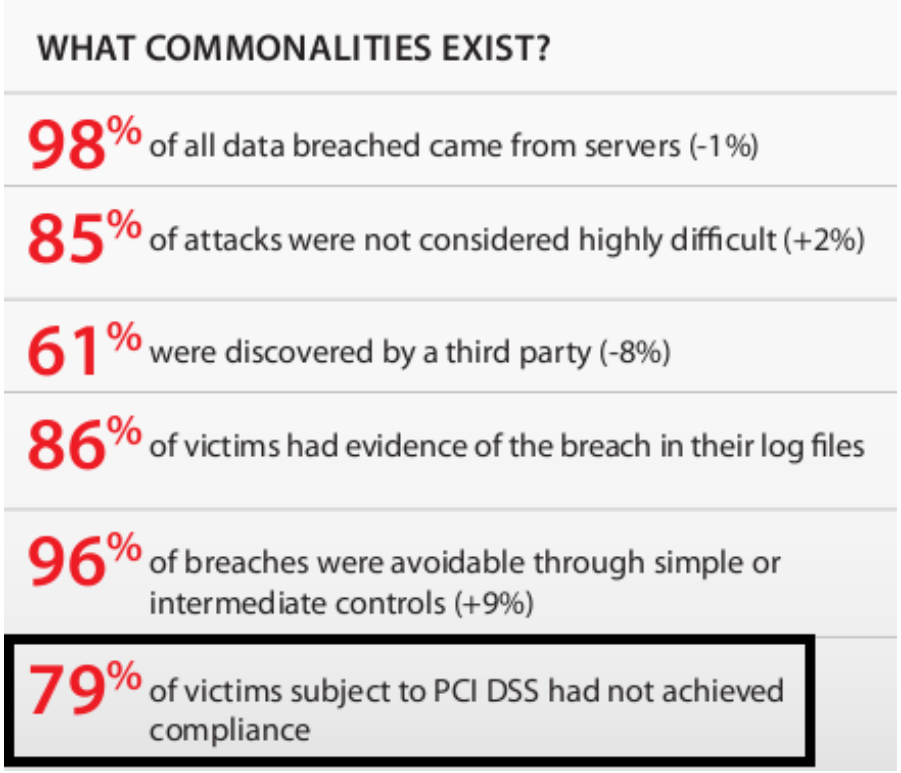
Objetivos y eficacia de la normativa

- **Controles:**
  1. Crear y mantener una red segura
  2. Proteger los datos del titular de la tarjeta
  3. Desarrollar un programa de gestión de vulnerabilidades
  4. Implementar medidas sólidas de control de acceso
  5. Monitorizar y probar las redes de forma periódica
  6. Mantener una política de seguridad de la información

Objetivos y eficacia de la normativa

- **Incidentes de seguridad:**

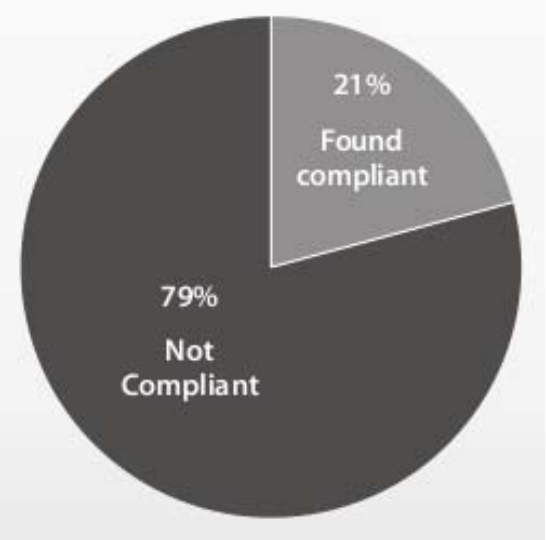




Fuente:
2010 Data Breach Investigations Report
http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Objetivos y eficacia de la normativa

- **Incidentes de seguridad:**
  - Estado de cumplimiento con PCI DSS



  - El cumplimiento es un **proceso continuo** que debe mantenerse. La validación es un evento temporal.

Aspectos clave de la seguridad en PCI

- **Consideraciones:**
  - ¿Qué actuaciones debemos realizar para alcanzar el cumplimiento?
  - ¿Con qué periodicidad debemos realizar dichas actuaciones?
  - ¿Qué requerimientos abordamos con cada una de estas actuaciones?

Aspectos clave de la seguridad en PCI

- **Actuaciones:**

Control	Req.	Tarea	Periodicidad					
			Anual	Semestral	Trimestral	Mensual	Semanal	Diario
1	1.1.2	Diagrama de red						
	1.1.6	Revisión normas del firewall/routers		X				
2	3.1	Revisión de retención de datos almacenados			X			
	3.6.4	Cambios de claves cifradas	X					
	3-5.2	Actualización de antivirus						X
	3-5.2	Análisis de los sistemas por los antivirus						

Aspectos clave de la seguridad en PCI

- **Actuaciones:**

Control	Req.	Tarea	Periodicidad					
			Anual	Semestral	Trimestral	Mensual	Semanal	Diario
3	6.1	Instalación de parches de seguridad			no críticos	críticos		
	6.6	Revisión de vulnerabilidades de las aplicaciones web	X					
4	8.5.4	Cancelar accesos a usuarios cesantes						
	8.5.5	Eliminar/desactivar cuentas de usuario			90 días			
	8.5.9	Cambio de contraseñas			90 días			
	9.1.1	Guardar videos			3 meses /ley			

Aspectos clave de la seguridad en PCI

- **Actuaciones:**

Control	Req.	Tarea	Periodicidad					
			Anual	Semestral	Trimestral	Mensual	Semanal	Diario
4	9.4	Conservar los registro de visitas			3 meses mín./ley			
	9.4	Registro de visitas físicas						
	9.5	Revisión de seguridad del lugar de almacén de copias de seguridad	X					
	9.9.1	Realización de registro de inventario	X					
	9.10	Destrucción de medios con datos						
5	10.6	Revisión de registros de componentes del sistema						X

Aspectos clave de la seguridad en PCI

- **Actuaciones:**

Control	Req.	Tarea	Periodicidad					
			Anual	Semestral	Trimestral	Mensual	Semanal	Diario
5	10.7	Conservar registro de auditoría	1 año					
	10.7	Disponibilidad del registro de auditoría			X			
	11.1	Verificación del analizador inalámbrico			X			
	11.2	Análisis internos y externos de vulnerabilidades			X			
	11.2	Mantener los datos de análisis	1 año					
	11.3	Pruebas de penetración internas y externas	X					

Aspectos clave de la seguridad en PCI

- **Actuaciones:**

Control	Req.	Tarea	Periodicidad					
			Anual	Semestral	Trimestral	Mensual	Semanal	Diario
5	11.3.1	Pruebas capa de red	X					
	11.3.2	Pruebas aplicación	X					
	11.5	Comparación de archivos críticos					X	
6	12.1.2	Identificación de amenazas, vulnerabilidades y resultadlo de riesgos	X					
	12.1.3	Revisión de actualizaciones del entorno	X					
	12.2	Mantenimientos de cuentas y registros						X

Aspectos clave de la seguridad en PCI

- **Actuaciones:**

Control	Req.	Tarea	Periodicidad					
			Anual	Semestral	Trimestral	Mensual	Semanal	Diario
6	12.6.1	Educación y concienciación de empleados en seguridad	X					
	12.6.2	Lectura y que ha entendido la política de seguridad por el empleado	X					
	12.9.2	Prueba del plan de seguridad	X					
	12.9.4	Capacitación sobre responsabilidad y respuesta frente a fallos de seguridad						
Realización del SAQ o Auditoría PCI DSS			X					

Mitos sobre PCI DSS

- **Los 10 mitos más comunes:**
  1. Un fabricante y producto nos permitirá alcanzar el cumplimiento.
  2. Externalizar el procesamiento de tarjetas nos permitirá el cumplimiento.
  3. El cumplimiento con PCI es un proyecto de TI
  4. PCI nos hará estar seguros
  5. PCI es inalcanzable; requiere demasiado
  6. PCI nos obliga a contratar un QSA
  7. No realizamos suficientes transacciones como para tener que cumplir con PCI

Mitos sobre PCI DSS

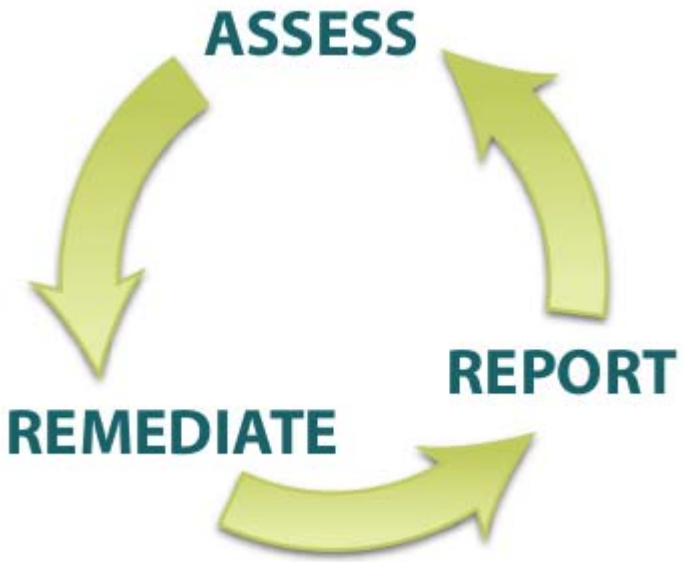
- **Los 10 mitos más comunes:**
  8. Hemos completado un SAQ, entonces cumplimos
  9. PCI nos obliga a almacenar datos de titulares de tarjeta
  10. PCI es demasiado exigente

Conclusiones

- **Comentarios finales:**
  - Una evaluación positiva de los requerimientos de PCI no garantiza que dispongamos de un elevado nivel de seguridad.
  - Las organizaciones que cumplen con PCI sufren menos incidentes de seguridad.
  - Cumplir con PCI DSS/PA DSS va más allá de realizar un escaneo o *pentest*.
  - Se recomienda disponer de un equipo multidisciplinar para abordar los distintos requerimientos.
  - ASVs y QSAs asumen distintas reponsabilidades.

Conclusiones

- **Comentarios finales:**
  - El cumplimiento de PCI es un proceso continuo



  - Este proceso **permite verificar el nivel de seguridad** de los datos de los titulares de tarjeta.

internet security auditors

2ª JORNADA SOBRE SEGURIDAD

EN MEDIOS DE PAGO

PCI DSS
PA DSS

PREGUNTAS

miércoles, 10 de Noviembre de 2010

Hotel Holiday Inn (Madrid)