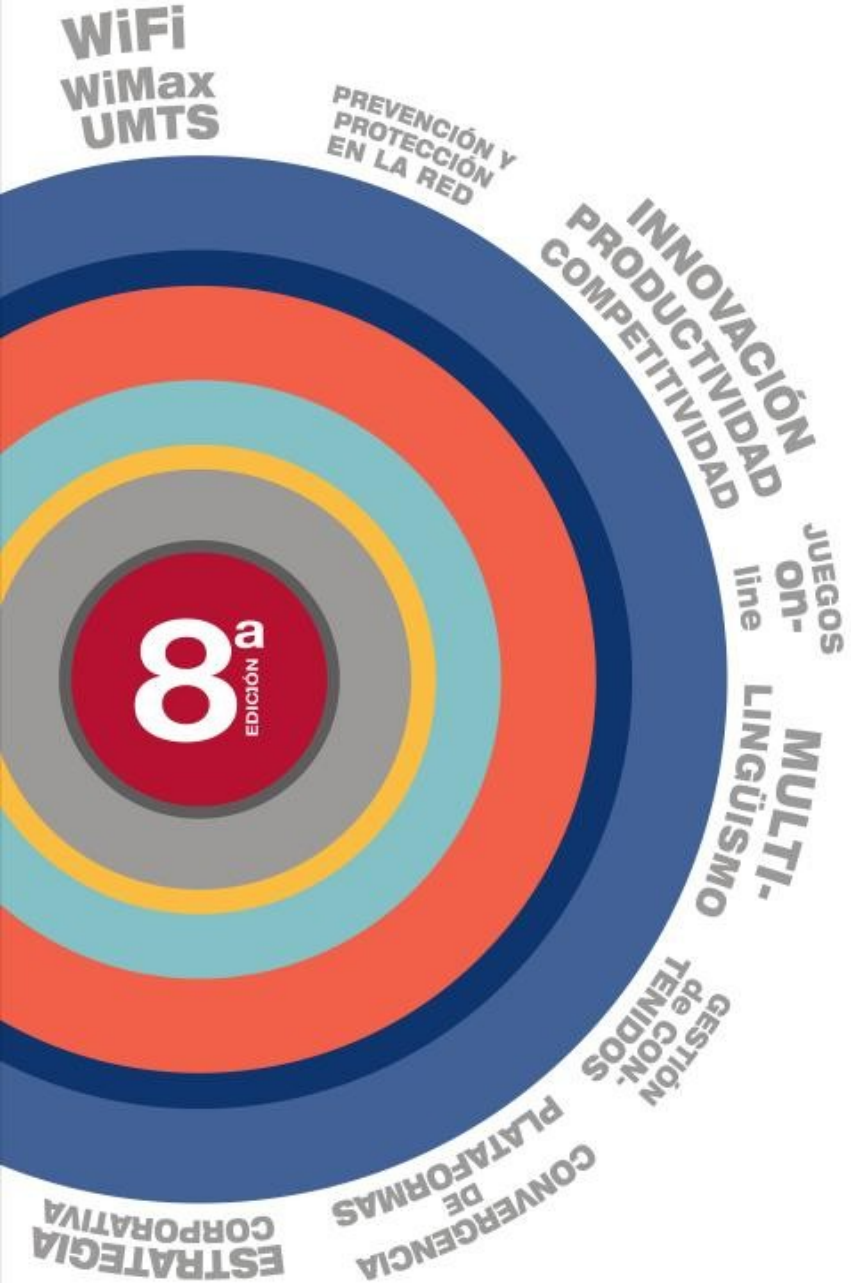

Innovación y Conocimiento en la Sociedad Digital

8ª Edición Internet Global Congress

Barcelona, 29 de mayo - 1 de junio, 2006

PALACIO DE CONGRESOS, FIRA BARCELONA, PZA. DE ESPAÑA

PCI DSS: Las leyes de Seguridad de VISA y Mastercard

Daniel Fernández Bleda
CISA, CISSP, ISO27001 Lead Auditor
OPST/A Trainer, CHFI Instructor

Internet Security Auditors
Socio Fundador
dfernandez@isecauditors.com

internet security auditors

IGC
www.igcweb.net

UN PROYECTO DE:
Fundació Barcelona Digital

www.isecauditors.com

internet security auditors

Índice

- Antecedentes
- La Respuesta
- El Resultado ¿esperado?
- PCI DSS
  - Evolución
  - Clasificación
  - Responsabilidades
  - Requerimientos
- Tareas Básicas
- Estado Actual en España
- El Futuro del Pago Electrónico

internet security auditors

Antecedentes

- Los robos de tarjetas de crédito en servidores de Internet se incrementan a finales de 1999. En algunos casos, la razón principal es la dejadez de los responsables de estos websites.

Defunct Web site leaks credit card info

By Joris Evers

IDG News Service, 07/25/00

BREAKING NEWS

SEND PRINT FEEDBACK REPRINT

Full details of hundreds of credit cards are out in the open. At the time of this writing Monday, all customer orders of a U.S. e-commerce site, with pornography as the best-selling item, were openly any protection.

The site lists information on m placed last year. More than 60 credit card. The numbers and e can be viewed by anyone. Orde customers' names, mailing adc ordered.

IGC
www.igcweb.net

A stick is needed

By Scott Bradner

Network World, 03/27/00

BREAKING NEWS

SEND PRINT FEEDBACK REPRINT

The information is only just coming out, but it seems like there has been another massive theft of credit card information from an e-commerce site.

There are a number of troubling parts to this story, and if other e-commerce companies do not learn something from this incident, e-commerce will continue to get more dangerous for users.

Credit card numbers stolen via known security hole

Web sites that fail to patch are still vulnerable.

By Ann Harrison

Computerworld, 03/10/00

BREAKING NEWS

SEND PRINT FEEDBACK REPRINT

A 2-year-old security hole in Microsoft Corp.'s Internet ware let a computer cracker -card numbers from d post them on the Internet.

n available for 18 months. panies say they don't have all of the patches needed , also known as crackers.

ave one sys/admin guy who ters, and you can't keep up said Eric Geiler, a principal

dad digital

La Respuesta (I)

- El año 2000 VISA y Mastercard inician la "carrera contra el fraude".

Visa, MasterCard plan anti-fraud initiatives

By Ellen Messmer
Network World, 08/18/00

BREAKIN
SEND PRINT FEEDBACK

Visa and MasterCard have separately drafted new plans to wage against online credit-card fraud, a costly burden for merchants w fooled into accepting phony card numbers over the Web.

Visa this week trumpeted a list of security "best practices" for e-merchants that accept Visa cards, requiring them to use encry and firewalls to protect card data. In a different approach, Maste next year plans to require that credit-card purchases on the 'Net include a special three-digit cardholder identification number that printed on the back of their cards. This change, expected to go i effect next April, will require alterations to card-processing softw networks, MasterCard says.

Visa issues 10 'commandments' for online merchants

By Maria Trombly
Computerworld, 08/11/00

BREAKING NEWS
SEND PRINT FEEDBACK REPRINT

In an attempt to reduce online credit-card fraud, Visa U.S.A. in San Francisco announced 10 "commandments" for online merchants to guard its cardholders' information. And, next week, Visa will follow up by releasing the details of a broad online security program.

John Shaughnessy, Visa's senior vice president for risk management, said merchants would be required to obey these rules or face fines, sales restrictions or loss of membership.

The rules won't go into effect immediately but will be phased in over the course of a year, starting in the fourth quarter, Visa spokeswoman Angie Grothoff said.

La Respuesta (II)

- Estas iniciativas se plasman en un programa de seguridad en cada uno de los fabricantes de más peso mundial:
  - VISA CISP (Cardholder Information Security Program), aplicable en USA, y el VISA AIS (Account Information Security), aplicable en el resto del mundo:
    - Se publican el 2000 y es obligatorio su cumplimiento desde Junio de 2001.
  - Mastercard SDP (Site Data Protection):

La Respuesta (III)

- En USA, existen dos fabricantes más en juego: American Express y Discover:
  - American Express DSOP (Data Security Operating Policy)
  - Discover DISC (Discover Information Security and Compliance)
- Ambos son similares y proponen directrices o recomendaciones de seguridad, más simples ¿realistas? que las de VISA y Mastercard.
- También son menos precisas por lo que deja más margen a la interpretación.

El Resultado ¿esperado?

- Aunque se ha aplicado más control, nuevos incidentes se continuan produciendo.

Registrar's database said to have exposed data

By Jeremy Kirk, IDG News Service, 04/07/06

A database problem with a U.S. domain name registrar exposed sensitive financial and personal information relating to thousands of domain name registrations, a Dutch company said Friday.

DiscountDomainRegistry.com, of New York, fixed the problem shortly after being notified Thursday, said Nico Vandendrie: CEO of Strongwood, a private investigation company based in the Netherlands.

Hacker hits up to 8M credit cards

Secret Service and FBI probe security breach of Visa, MasterCard, Amex and Discover card accounts.

February 27, 2003: 4:20 PM EST

NEW YORK (CNN) - The Secret Service and the FBI confirmed Wednesday they have been involved for the past two weeks in trying to track down the computer hacker who breached the security system of Data Processors International, which processes credit card transactions on behalf of merchants.

MasterCard, Visa, Discover Financial Services and American Express all have said this week that some of their card accounts had been affected by the breach.

MasterCard estimated that the hacker may have gotten access to information on as many as 8 million credit card accounts overall, including 2.2 million of its own cards. Visa said 3.4 million of its

40 Million Credit Card Numbers Hacked

Data Breached at Processing Center

By Jonathan Krim and Michael Barbaro
Washington Post Staff Writers
Saturday, June 18, 2005; Page A01

More than 40 million credit card numbers belonging to U.S. consumers were accessed by a computer hacker and are at risk of being used for fraud, MasterCard International Inc. said yesterday.

IGC
www.igcweb.net

ociedad digital

Evolución

- VISA y Mastercard alinean sus programas CISP/AIS y SDP bajo unas únicas directrices:
  - PCI DSS (Payment Card Industry Data Security Standard).
  - Se publica la primera documentación a principios del año 2004.
  - En Enero de 2005 se publica el documento definitivo.
  - En Junio de 2005 se fija la fecha de obligado cumplimiento.

Clasificación (I)

- Tenemos tres principales agentes implicados en el tratamiento de tarjetas:
  - Merchants:
    - Empresas que tienen acceso y pueden almacenar “account data”. Son los “vendedores” de tarjetas.
    - Deben asegurar que esta información de cuentas (números, PINs, etc.) se almacena y trata de forma segura.

Clasificación (II)

- Service Providers:
  - Third Party Processor (TPP): Los vendedores web contratan a estas entidades para ofrecer sus contenidos y vender sus servicios online.
  - Data Storage Entity (DSE): Una entidad que no sea un merchant o TPP que almacena y tiene acceso a los datos de las tarjetas. Ejemplos: empresas de hosting, pasarelas de pago, terminal drivers and processors.

Clasificación (III)

- Vendors:
  - Empresas que hayan pasado los procesos de “homologación” de VISA y Mastercard para ofrecer Escaneos de Red y Auditorías OnSite. Adicionalmente pueden ofrecer Assessments objetivos.
  - Mastercard homologa Escaneadores y Auditores externos.
  - VISA homologa y forma a los Auditores OnSite (QDSP, *Qualified Data Security Professional*) y a las empresas Auditoras (QDSC, *Qualified Data Security Company*).

Clasificación (IV)

- Clasificación de los vendedores (*merchants*):

Nivel de la Empresa	Descripción por VISA	Descripción por Mastercard	Responsabilidades			Fecha Límite
			Auditoría Anual On-Site	Escaneos de la Red	Self Assess-ment	
1	Cualquier vendedor que supere los 6MM transacciones/año. Vendedores que hayan sido hackeados o sufrido cualquier tipo de ataque que haya resultado en un compromiso de datos de tarjetas. Cualquier vendedores que VISA/Mastercard decidan que debe cumplir los requerimientos del Nivel 1. Cualquier empresa identificada por otro fabricante como de Nivel 1.	La misma	✓	✓ (trimestrales)	✗	30-jun-05
2	Cualquier vendedores que procesa de 150K a 6MM de transacciones/año.	Cualquier empresa que procesa de 150K a 6MM transacciones/año Cualquier empresa clasificada por otro fabricante como de Nivel 2	✗	✓ (trimestrales)	✓ (anuales)	
3	Cualquier empresa que procesa de 20K a 150K transacciones/año.	Cualquier empresa que procesa de 20K a 150K transacciones/año Cualquier empresa clasificada por otro fabricante como de Nivel 3				
4	Cualquier empresa que procesa menos de 20K transacciones/año.	Cualquier otra empresa	✗	≈ (anuales)	≈ (anuales)	No aplicable

Clasificación (V)

- Clasificación de los proveedores de servicios:

Nivel de la Empresa	Descripción por VISA	Descripción por Mastercard	Responsabilidades			Fecha Límite
			Auditoría Anual On-Site	Escaneos de la Red	Self Assess-ment	
1	Todos los procesadores VisaNet (miembros y no miembros) y todas las pasarelas de pago.	Incluye todos los TPPs. Todos los DSEs que almacenan datos de merchants de Nivel 1 o Nivel 2.	✓	✓ (trimestrales)	✗	30-jun-04
2	Cualquier proveedor de servicios que no sea de Nivel 1 y almacena, procesa o transmite más de 1 MM de cuentas/transacciones / año.	Todos los DSEs que almacenan datos de merchants de Nivel 3.	✓	✓ (trimestrales)	✗	30-jun-05
3	Cualquier proveedor de servicios que no sea de Nivel 1 y almacena, procesa o transmite menos de 1 MM de cuentas/transacciones / año.	Todos aquellos DSEs no incluidos en el Nivel 1 o Nivel 2.	✗	✓ (trimestrales)	✓ (anuales)	Opcional

Responsabilidades (I)

- Las empresas debe llevar a cabo alguna o varias de estas tareas para asegurar el cumplimiento del PCI DSS:
  - Análisis propios (Self Assessments).
  - Escaneos de la red (Network Scans).
  - Auditorías Internas (OnSite Audit).

Responsabilidades (II)

- Self Assessments:
  - Permite conocer si la organización incurre en incumplimientos con la norma y el grado.

Payment Card Industry Self-Assessment Questionnaire

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

	DESCRIPTION	RESPONSE		
1.1	Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?	☐ Yes	☐ No	
1.2	If wireless technology is used, is the access to the network limited to authorized devices?	☐ Yes	☐ No	☐ N/A
1.3	Do changes to the firewall need authorization and are the changes logged?	☐ Yes	☐ No	
1.4	Is a firewall used to protect the network and limit traffic to that which is required to conduct business?	☐ Yes	☐ No	

Responsabilidades (III)

- Escaneos de Red:
  - Deben identificar todas las vulnerabilidades que puedan estar presentes en los sistemas.
  - En la versión publicada a mediados del 2005 se incide en la diversidad de operativos y sistemas en general.
  - Un aspecto al que se presta especial atención en la seguridad de las aplicaciones, haciendo especial incapie en el seguimiento de recomendaciones de referencia como los de la OWASP (Open Web Application Security Project).

Responsabilidades (IV)

- Auditorías OnSite:
  - Implican la auditoría del cumplimiento de todos los aspectos de la norma.
  - Debe se llevadas a cabo por un QDSC.
  - En las empresas de Nivel 1 son la herramienta básica para demostrar el cumplimiento o las salvedades delante de VISA y Mastercard.

Requerimientos (I)

- El PCI DSS se compone de requerimientos, agrupados en 6 “dominios”.
- En total tenemos 75 controles de los que debemos revisar su cumplimiento.

Requerimientos (II)

- Construir y mantener una Red segura:
  - Requerimiento 1: Instalar y mantener la configuración del firewall para proteger los datos.
  - Algunas tareas:
    - Revisar la estructura de la red.
    - Revisar la configuración del firewall y otros sistemas de red, incluyendo los inalámbricos.
    - Documentar la configuraciones y cambios.
    - Revisar el tráfico que puede alcanzar los servidores.
    - Revisar que la información no está accesible desde la red externa de forma directa.

Requerimientos (III)

- Requerimiento 2: No emplear opciones por defecto en contraseñas y valores de configuración.
- Algunas tareas:
  - Revisar los Sistemas Operativos, servicios de red, dispositivos de red y filtrado en busca de configuraciones, ficheros, usuarios y contraseñas, etc. por defecto (especialmente usuarios de administración, comunidades SNMP, clave WEP, etc.).
  - Revisar que los servidores no acumulan la prestación de servicios y que estos emplean servicios seguros.

Requerimientos (IV)

- Proteger los Datos de los Usuarios (Cardholder)
  - Requerimiento 3: Proteger los datos almacenados
  - Algunas tareas:
    - Revisar las políticas y procedimientos de seguridad.
    - Revisar el cumplimiento legal vigente (p.e. LOPD).
    - Revisar el cumplimiento de las normas de retención (y destrucción) de los datos de tarjetas.
    - Asegurar que no se almacena ningún tipo de información relativa a las bandas magnéticas, códigos CVV y CVV2 y PINs.
    - Revisar que se emplean métodos válidos de encriptación de información y claves.

Requerimientos (V)

- Requerimiento 4: Encriptar las transmisiones de datos y datos sensibles de usuarios a través de redes públicas.
- Algunas tareas:
  - Revisar el uso de la encriptación adecuada en las aplicaciones web.
  - Revisar el uso de los protocolos de encriptación (algoritmos, claves, rotación de claves, etc.) adecuados en las redes inalámbricas.
  - Revisar el uso de encriptación en la transmisión de información sensible a través de correo electrónico.

Requerimientos (VI)

- Mantener un Programa de Gestión de Vulnerabilidades
  - Requerimiento 5: Usar y actualizar regularmente software anti-virus.
  - Algunas tareas:
    - Revisar el uso adecuado de software anti-virus en los puntos adecuados de la red: ordenadores de usuario, tráfico y servidores de red, correo electrónico, etc.
    - Revisar la actualización periódica y adecuada de todo este software.

Requerimientos (VII)

- Requerimiento 6: Desarrollar y mantener sistemas y aplicaciones seguras.
- Algunas tareas:
  - Revisar que las políticas de actualización aseguran la aplicación de parches críticos en menos de 30 días.
  - Revisar que se dispone de las herramientas y procedimientos adecuados para la identificación de vulnerabilidades (entre estas las identif. en el Req. 2).
  - Asegurar que se dispone de entornos de desarrollo y producción separados y que la información y las medidas de seguridad adecuadas se amplican en ambos.
  - Asegurar que en el desarrollo de las aplicaciones no aparecen vulnerabilidades documentadas por la **OWASP**.

Requerimientos (VIII)

- Implementar Medidas de Control de Acceso Robustas
  - Requerimiento 7: Restringir el acceso a los datos según need-to-know.
  - Algunas tareas:
    - Revisar la Política de seguridad en busca de la definición de los controles de acceso para todos los sistemas, aplicaciones e información.
    - Revisar la documentación de los sistemas y aplicaciones para aseguran que permiten implementar los controles de acceso adecuados y se basan en la premisa “deny-all” por defecto.

Requerimientos (IX)

- Requerimiento 8: Asignar un ID único a cada persona con acceso a los sistemas.
  - Algunas tareas:
    - Revisar que las personas que acceden a la información de usuarios tienen ID único.
    - Revisar el uso de accesos basados en autenticación de factor-2 en información crítica.
    - Asegurar que los passwords se almacenan encriptados.
    - Revisar los procedimientos de asignación y gestión de claves y verificar la robustez de éstos y las claves.
    - Auditar todos los sistemas para revisar la implementación de opciones de seguridad en la autenticación.

Requerimientos (X)

- Requerimiento 9: Restringir el acceso físico a los datos de los usuarios.
  - Algunas tareas:
    - Revisar las medidas de seguridad física (cámaras, tarjetas de acceso, cerraduras, etc.) a los sistemas y la red, sobre todo los que tratan o almacenan datos de usuarios.
    - Revisar los sistemas de control de acceso para las visitas.
    - Revisar los registros e instalaciones que almacenan copias de seguridad para comprobar el uso de la seguridad física y sistemas de protección adecuada.

Requerimientos (XI)

- Monitorizar y Auditar las Redes Regularmente
  - Requerimiento 10: Auditar y monitorizar todos los accesos a los recursos de red y los datos de usuarios.
  - Algunas tareas:
    - Verificar la existencia de la auditoría de eventos de todo tipo relativos a la información de usuarios.
    - Verificar los accesos a la información de auditoría así como su almacenamiento en copias de seguridad.
    - Revisar que la Política de Seguridad detalla los aspectos relativos a configuración y retención de datos de auditoría.

Requerimientos (XII)

- Requerimiento 11: Auditar regularmente la seguridad de los sistemas y procesos.
  - Algunas tareas:
    - Asegurar que se realizan auditorías de seguridad y escaneos de vulnerabilidades de forma regular.
    - Revisar los procedimientos de búsqueda de Puntos de Acceso furtivos o dispositivos inalámbricos peligrosos.
    - Revisar la corrección de las vulnerabilidades previamente detectadas.
    - Revisar el uso, mantenimiento y gestión de Sistemas de Detección/Prevención de Intrusiones.
    - Verificar el uso de sistemas de integridad de ficheros.

Requerimientos (XIII)

- Mantener un Política de Seguridad de la Información
  - Requerimiento 12: Mantener una política que gestione la seguridad de la información.
  - Algunas tareas:
    - Revisar los procedimientos de acciones del día a día en busca de deficiencias en la documentación.
    - Asegurar la existencia de un CSO o responsable de seguridad.
    - Revisar la existencia y documentación de los procedimientos de gestión de incidentes en la empresa.

Tareas Básicas

- Es necesario auditar en profundidad los sistemas de información de la empresa.
- Prestando especial atención a los dispositivos de red, servidores, servicios y aplicaciones web que puedan estar accesibles desde Internet.
- Es necesario documentar los procedimientos y políticas que deben seguirse en la organización.
- Debe auditarse el cumplimiento técnico y organizativo de las normas de seguridad de forma regular.

Estado Actual en España

- No se considera país crítico de acción: no se abren procesos de certificación empresas ni auditores.
- Hay pocas empresas “auto-clasificadas” de Nivel 1 (unas 20), pero se cree que hay muchas más que no declaran todas sus operaciones internas con T.C.
- Se va a trabajar personalmente con ellas durante el 2006 incrementando la presión sobre el cumplimiento a lo largo del año 2007.
- Quién no haya hecho esfuerzos en su implantanción podrá “ser castigado”.

El futuro

- Todos los fabricantes de tarjetas se han acabado alineando a la norma de una forma u otra: AMEX, JCB, Discover, etc.
- Además del PCI DSS, Europay, VISA y Mastercard fundaron EMVCo -con una demanda pendiente anti- monopolio-, para establecer estándares de seguridad para la nueva generación de tarjetas “inteligentes”.
- Entre PCI DSS y EMV se definen los requerimientos de seguridad en la implementación, fabricación y uso, transferencia y almacenamiento de su información.

Enlaces de Interés

VISA CISP:

http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html

VISA AIS:

http://www.visaeurope.com/acceptingvisa/datasecurity.html

Mastercard SDP:

https://sdp.mastercardintl.com

American Express DSOP:

http://www10.americanexpress.com/sif/cda/page/0,1641,17457,00.asp

Discover DISC:

http://www.discovernetwork.com/resources/data/data_security.html

EMV Co. LLC:

http://www.emvco.com

Ruegos y Preguntas

Muchas gracias por su asistencia

Innovación y Conocimiento en la Sociedad Digital

8ª EDICIÓN Internet Global Congress

Barcelona, 29 de mayo - 1 de junio, 2006

PALACIO DE CONGRESOS, FIRA BARCELONA, PZA. DE ESPAÑA

PCI DSS: Las leyes de Seguridad de VISA y Mastercard

Daniel Fernández Bleda
CISA, CISSP, ISO27001 Lead Auditor
OPST/A Trainer, CHFI Instructor

Internet Security Auditors
Socio Fundador
dfernandez@isecauditors.com

internet security auditors

IGC
www.igcweb.net

UN PROYECTO DE:
Fundació Barcelona Digital

www.isecauditors.com