PCI DSS, estándar para combatir el fraude en compras online

En la era en la que vivimos, la mayoría de las personas no suelen pensar en las consecuencias que actos tecnológicos como puede ser la compra online pueden acarrear. Con el paso del tiempo la gente ha ido evolucionando y se va sintiendo más *segura* a la hora de realizar compras por internet pero, aun así, las vulnerabilidades del pago por internet siguen estando presentes.

Con el comienzo de la era de internet, las diferentes operadoras de tarjetas de crédito ampliaron sus servicios para poder comprar por internet pero no fue hasta octubre de 1999 que Visa aprobó el desarrollo de la primera medida contra el fraude. Esta medida era CISP (Cardholder Information Security Program) y es una de las precursoras del PCI DSS (*Payment Card Industry Data Security Standard*).

Dado que los mecanismos de seguridad inicialmente implantados eran muy sencillos, Visa y Master Card, entre los años 1988 y 1998, reportaron un total de 750 millones de dólares en concepto de fraude con las tarjetas de crédito. Para poder combatir ese cibercrimen, con el paso de los años se han implantado diferentes medidas de seguridad, entre las que podemos destacar:

- Diciembre de 2004. Debuta la primera versión de PCI DSS (PCI DSS 1.0). Es un día distintivo en la historia de la seguridad de la información dado que éste es el primer estándar de seguridad unificado respaldado por las cinco principales marcas de tarjetas (Visa, Master Card, JCB, American Express y Discover,). Éstas fundaron el comité PCI SSC (Payment Card Industry Security Standards

Council) para proporcionar un foro transparente en el que todas las partes interesadas puedan aportar información para el desarrollo, la mejora y la difusión en curso de las PCI DSS.

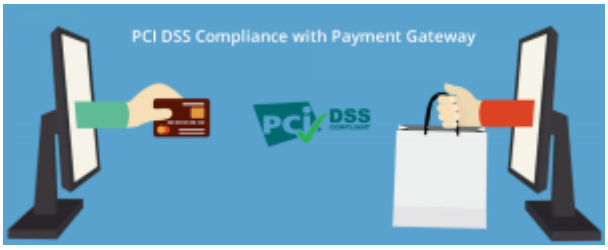
- Septiembre de 2006. Se lanza la versión PCI DSS 1.1. El código de la aplicación personalizado debe revisarse profesionalmente para detectar vulnerabilidades. Es en este punto donde las cinco principales compañías deciden tener un grupo independiente que les audite. Este grupo pasará a ser conocido como QSA (*Qualified Security Assessor*).
- Octubre de 2008. Se lanza la versión PCI DSS 1.2. En esta nueva versión se incluyen nuevos requisitos respecto a 802.1x para la protección de redes inalámbricas. Este puede llegar a ser un cambio muy costoso para algunos minoristas.
- Junio 2010. Se decide que los cambios se van a realizar periódicamente cada tres años en vez de cada dos como hasta el momento.
- Octubre 2010. Debuta la versión PCI DSS 2.0. Según Ed Moyle, manager senior de CTG, "*Esta versión del estándar representa una simplificación del proceso de evaluación, que debería ayudar a aliviar un poco la carga de cumplimiento de las normas PCI DSS*".
- Noviembre 2013. Debuta la versión PCI DSS 3.0. Se enfatiza la necesidad de evaluaciones internas de vulnerabilidad, agrega flexibilidad a los requisitos de contraseña y resalta la creciente importancia del cumplimiento del proveedor.
- Abril 2015. Se publica la versión PCI DSS 3.1. Se incluían los cambios a realizar para abordar las vulnerabilidades dentro del protocolo de cifrado SSL (Secure Sockets Layer) que puede poner en riesgo los datos de pago.
- Abril 2016. Se publica la versión PCI DSS 3.2. Se incluyeron las fechas de migración revisadas para abordar los datos generados con el protocolo SSL.

Ya conocemos los cambios que se han ido realizando en las diferentes versiones del estándar pero, *¿qué es realmente PCI DSS?*

PCI DSS es el estándar de seguridad de datos para la industria de tarjeta de pago y fue desarrollado por el comité PCI SSC como una guía para ayudar a las diferentes organizaciones que procesan, almacenan y/o transmiten datos de titulares de la tarjeta para asegurar los datos con el fin de evitar fraudes. Éste es un proceso continuo de mejora en el que se evalúan los procesos de negocio para poder resolver las vulnerabilidades que se observan en los mismos.

Toda compañía que procese, guarde o transmita cualquier tipo de dato de tarjetas de crédito y débito debe cumplir con lo que los estándares dictaminen o se arriesgan a perder los permisos que tienen para procesar las tarjetas de crédito y débito, auditorías o pagos de multas. No obstante, los proveedores de servicios de tarjetas de crédito y de débito deben ser los que validen el cumplimiento de los estándares.

Esta validación la realizan los auditores autorizados (QSAs). Los QSA son organizaciones de seguridad independientes que han sido calificadas por el consejo de normas de seguridad de PCI.



Referencias:

The history of the PCI DSS standard: A visual timeline: https://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

ISACA PCI DSS CC Virtualization Guidelines: https://www.pcisecuritystandards.org/documents/Virtualization_

InfoSupp_v2.pdf

PCI SSC Qualified Security assesors: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors