La realidad de PCI DSS

Continuando con la idea del anterior Post, me parece apropiado tratar la realidad de los estándares, en mi caso **PCI DSS** (Payment Card Industry Data Security Standard). Como todo estándar, y PCI DSS no es una excepción, define un conjunto de normas o directrices que definen aspectos de un área determinada. Pero indudablemente un estándar no es una ley que, si se aplica, se debe cumplir y si no habrá sanciones o multas. Para nada, simplemente son recomendaciones.

En líneas generales la normativa que rige PCI DSS está basada en los siguientes aspectos **[1]**:

- Desarrollar y mantener una red segura, instalando y una configuración de firewall para proteger los datos del titular de la tarjeta y utilizando contraseñas de sistemas y otros parámetros de seguridad diferentes a los utilizados por defecto por los proveedores.
- Proteger los datos del titular de la tarjeta de crédito, mediante el **cifrado** durante la transmisión de los mismos a través de redes públicas abiertas.
- Mantener un programa de administración de vulnerabilidad, gracias a **software antivirus** y el desarrollo de **código seguro** para las aplicaciones.
- Implementar medidas solidas de control de acceso, a través de **restricciones de acceso** a los datos según la necesidad de la empresa y asignando un ID exclusivo a cada persona que tenga acceso mediante un ordenador, además de restringir el acceso físico.
- Supervisar y evaluar las redes con regularidad, mediante el **rastreo** y **supervisión** de todos los accesos a los recursos de la red y los datos.
- Mantener una **política de seguridad** de la información.

Cada empresa que utiliza datos relacionados con las tarjetas

de pago, es importante que siga las líneas generales del estándar PCI DSS, ya que, en gran manera, le garantiza cierto nivel de seguridad. De hecho, está comprobado, que las empresas que cumplen con PCI DSS, han conseguido minimizar en un porcentaje alto, el riesgo de pérdida o robo de los datos. Y no solo eso, sino que, cumplir con el estándar y que el **QSA** (Qualified Security Assessors) verifique dicho cumplimiento, proporciona cierto nivel de reputación a la empresa y la convierte en una compañía de confianza para los consumidores.

Un ejemplo reciente de empresa que cumple con PCI DSS es **BlackMesh**, que obtuvo el nivel 1 de certificación en el año 2015. Para las compañías que cumplen con el estándar, reunir los requisitos mínimos para obtener esta certificación, valida la seguridad de los procesos de pago de los sistemas e incrementa la protección de los datos de los titulares de las tarjetas **[2].**

En cambio, casos como el de la compañía **Home Depot** son muy significativos. Esta compañía, en el año 2014, fue víctima de un ciberataque, que permitió el acceso a datos de tarjetas de pago de 50 millones de usuarios de su sistema y que le supuso unas pérdidas de 19 millones de dólares **[3]**. Lo más llamativo de este caso, es que esta empresa cumplía con el estándar PCI DSS y tras el ataque, se comprometió a mejorar la seguridad de sus datos durante un periodo de dos años y a contratar a un especialista en seguridad, encargado de supervisar dichas mejoras.

Situaciones como la de **Home Depot** produce una sensación de vulnerabilidad en el resto de empresas que están cumpliendo el estándar y puede generar cierta alarma y confusión sobre cómo se están haciendo las cosas. Y, por consiguiente, son muchos los detractores y críticos que se pronuncian en contra del estándar. La mayoría de ellos opinan que, desde su creación, el estándar está orientado a la protección tanto de bancos como de proveedores de tarjetas de pago, de la responsabilidad

que cae sobre ellos ante la pérdida o robo de los datos, dejando de lado a los comerciantes, que son los que realmente tiene que afrontar la situación. Una noticia de apenas 15 días, anunciaba que el proveedor de telas **Vera Bradley**, había sufrido un ataque en sus sistemas de pago, y algo muy significativo, la empresa no contaba con los mecanismos de detección apropiados y fue el FBI quien descubrió el problema y lo comunicó a la empresa **[4]**.

Tal y como indican los expertos, los ataques no se hacen sobre un solo sistema, sino que se realizan en serie sobre múltiples vendedores, haciendo más difícil su detección. Además, cualquier punto en el ecosistema de pagos esta potencialmente en riesgo. Y es que sea cual sea el tamaño de la compañía, desde un minorista hasta grandes compañías están en riesgo. Podemos añadir más casos significativos a los anteriores, como los ataques a la cadena de comida rápida **Wendy**, al minorista de ropa **Eddie Bauer** y las cadenas de hoteles **Hilton**, **Trump**, **Hutton**, etc.

Por ello cada versión mejorada del estándar, en cierta manera es un alivio. Por ejemplo, en su última versión, se introdujo una novedad importante, como es la **autenticación multifactor** para cualquier usuario con permisos de administración de datos asociados a tarjetas, algo ya demandado por algunos expertos en seguridad. En versiones anteriores, este tipo de autenticación era necesaria únicamente en el acceso remoto a los datos, por lo que la seguridad de acceso no era la más apropiada **[5]**.

El CTO de PCI SSC, Troy Leach, señala *«El funcionamiento del estándar, siempre está acorde con los nuevos requerimientos en seguridad».* La evolución del estándar es muy sencilla: cada nuevo requisito definido, primeramente, se introduce como una buena práctica, de manera que las empresas se pueden ir preparando para adaptarse al cambio, y posteriormente, en la siguiente versión ya se introduce como una norma **[5 bis]**.

En conclusión, sabemos que el estándar PCI DSS ayuda a las empresas a mantener los datos de los titulares de tarjetas de pago seguros y que obtener una certificación de su uso y aplicación, otorga cierto nivel de confianza por parte del consumidor, pero que desde luego casos como el de **Home Depot**, nos abren los ojos y nos hacen darnos cuenta de que nunca es suficiente, y que incluso los estándares no contemplan todas las posibilidades y riesgos que existen en los sistemas.

Referencias

[1] PCI DSS v3.0 Normas de seguridad de datos: https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

[2] «BlackMesh Achieves PCI DSS Level 1 Certification»: http://search.proquest.com/docview/1735954442?OpenUrlRefId=info:xri/sid:primo&accountid=14529

[3] «Home Depot settels consumer lawsuit over big 2014 data breach»
(Océano): http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z

[4] «Retailed Vera Bradley: Payments System Hacked»: http://www.databreachtoday.com/retailer-vera-bradley-payments-system-hacked-a-9449

[5] «PCI DSS 3.2: The evolution continues»: http://www.csoonline.com/article/3083106/data-protection/pci-dss-3-2-the-evolution-continues.html