Local Billing: implantación y certificación del estándar PCI DSS

Local Billing Solutions Limited, proveedor de servicios especializado en el procesamiento de pagos para empresas de comercio electrónico, ha implementado el estándar PCI DSS consiguiendo su certificación en enero de 2009. El proceso de implantación y certificación se ha realizado con la ayuda de Internet Security Auditors como empresa homologada QSA y ASV, tras un largo camino de estudio y adecuación de los diferentes procesos de negocio que trabajan con datos de tarjetas de pago.


Jordi Salvat i Alabart / Miguel Ángel Domínguez Torres

PCI DSS[1], estándar desarrollado por el PCI Security Standard Council (organismo creado por VISA, Mastercard, AMEX, JCB y DISCOVER), debe ser implantado por entidades bancarias, proveedores de servicio y comercios que tratan con datos de tarjetas de pago. Entre ellos se encuentra Local Billing, que concienciado de la necesidad de implementar mejoras de seguridad de forma continuada ha cumplido con las normas establecidas por el sector de las tarjetas de pago. Este cumplimiento del estándar de seguridad PCI DSS, permite a Local Billing mejorar el servicio a sus clientes garantizando, si cabe aún más, la seguridad de sus datos bancarios en todos los procesos en que trata con tarjetas de pago.

El estándar define el conjunto de requerimientos que permiten gestionar la seguridad y definir las políticas y los procedimientos de seguridad necesarios tanto a nivel de infraestructura, diseño de red o arquitectura de sistemas.

Servicios de Local Billing

Local Billing proporciona servicios de intermediación en el procesamiento de pagos en línea. Se estructura en varias áreas o grupos: el grupo de procesamiento de pagos, el grupo de servicio de atención al cliente y el grupo de consultoría. El grupo de Procesamiento de Pagos permite optimizar la aceptación del pago para comercios que desean vender sus productos en línea (software, información, música, vídeos, etc.)

Su plataforma de procesamiento de pago es capaz de transferir el tráfico a varios proveedores para maximizar el número de métodos de pago aceptados y optimizar el tiempo de actividad de sus comerciantes. La política de la compañía es garantizar un mínimo de dos proveedores de pago por cada método de pago y así poder garantizar la estabilidad y fiabilidad a sus clientes.

Local Billing, como proveedor de servicios que recoge, almacena, procesa y transmite datos de tarjetas de pago, adelantándose a la solicitud por parte de sus clientes, decidió apostar una vez más por el beneficio de éstos y entre sus prioridades decidió incluir la implantación de este estándar de seguridad que le ha permitido verificar, corregir y mejorar el correcto procesamiento, transmisión y almacenamiento de los datos relativos a tarjetas de pago. Para ello ha contado con el soporte de Internet Security Auditors, empresa experta en seguridad que le ha proporcionado el asesoramiento y soporte necesarios para implantar con éxito los proyectos que le han permitido alcanzar el cumplimiento del estándar PCI DSS. Internet Security Auditors posee las certificaciones de QSA[2] (Qualified Security Assessor) y de ASV[3] (Approved Scanning Vendor) concedidas por el PCI SSC, siendo avalado por todas las marcas de tarjetas de pago que apoyan éste organismo común.

El proyecto se ha desarrollado formando un equipo multidisciplinar formado por personal de Local Billing relacionado con departamentos técnicos de desarrollo, sistemas y base de datos, así como responsables de medios de pago, seguridad y cumplimiento normativo, complementando el equipo con consultores QSA de Internet Security Auditors.

Previo a emprender el proyecto se realizaron tareas formativas en PCI DSS con el objetivo de que todo el personal conociera el estándar y lo entendiera lo mejor posible, determinando también las herramientas de soporte a utilizar.

Como herramienta clave para todo el proyecto se decidió utilizar la Wiki corporativa con gestión de roles y permisos. El uso de esta herramienta se escogió por varios motivos: facilidad de uso, ya que todo el personal de Local Billing está acostumbrado a utilizarla en otros proyectos y por tanto no requería formación; es un repositorio ideal para centralizar la información y gestionar el ciclo de vida de la documentación; es accesible por todo el personal de Local Billing repartido geográficamente por todo el mundo; facilita el trabajo en equipo; y junto con otras herramientas de gestión de proyectos se utilizó también para centralizar las tareas que se definieron como parte de la implantación del estándar.

Tras establecer el entorno de trabajo, la primera tarea que se realizó fue analizar los procesos de negocio y establecer el ámbito de Local Billing sobre el que era necesario implementar los requerimientos PCI DSS. Posteriormente se analizaron cada uno de los requerimientos y se definieron las acciones necesarias para su cumplimiento, definiendo el **programa de cumplimiento** a ejecutar para la implantación y mantenimiento del estándar. (Ver **Figura 1**: Fases Implantación PCI DSS)

Minimización del ámbito de aplicación

La estrategia principal que se determinó necesaria e imprescindible para alcanzar con éxito la implantación del estándar, fue **minimizar al máximo el ámbito de aplicación** de PCI DSS. Esto implicó la necesidad de realizar cambios a nivel de segmentación de red entre los entornos de producción/preproducción situados en el CPD de Amsterdam y el entorno de desarrollo localizado en Barcelona. Requirió establecer controles de acceso estrictos a los componentes de sistemas localizados en el CPD de Amsterdam, para así poder garantizar los niveles de seguridad necesarios sobre los empleados de Local Billing así como para los usuarios de los proveedores de servicios que se conectan remotamente al entorno de producción donde se guardaban los datos de tarjetas.

Una medida que se determinó como obligatoria por el beneficio que aportaba, a pesar del gran esfuerzo que suponía y que aunque se trata uno de los requerimientos primarios del estándar en muchos casos se cubre con controles compensatorios debido a la complejidad de modificar las aplicaciones y bases de datos, fue el cifrado del PAN (Primary Account Number) en base de datos. Para ello se rediseñó la base de datos para contener los datos de tarjetas en formato truncado, hash y finalmente cifrado. Esto se hizo dado que el número de tarjeta completo, o PAN, se necesita únicamente para el

Figura 1

El informe de auditoría fue remitido a Visa y Mastercard para su estudio y publicación en sus listas de proveedores de servicio certificados, siendo el primer proveedor de servicios multinacional con sede en España incluido en estas listas.

[1] PCI DSS v1.2: https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf
[2] Lista de empresas homologadas QSA: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
[3] Lista de empresas homologadas ASV: https://www.pcisecuritystandards.org/pdfs/asv_report.html

procesamiento de los pagos y los empleados de Local Billing y Comercios no necesitan conocer nunca el PAN completo; por lo que ese dato, en lugar de ser enmascarado en su visualización, se extrae directamente truncado de la base de datos.

Para el cifrado se creó un módulo específico que permite gestionar los procesos de cifrado/descifrado del PAN cumpliendo los requerimientos de PCI DSS, acompañado de los procedimientos para la gestión de claves que garantizan la seguridad de las claves de cifrado (creación, regeneración, eliminación, custodia, etc.)

La finalidad fue eliminar, lo máximo posible, la necesidad de implementar requerimientos PCI DSS en los componentes de sistemas ubicados en las oficinas centrales en Barcelona y sobre los cuales era más complicado establecer unas medidas de seguridad tan exigentes como las que impone PCI DSS en algunos casos.

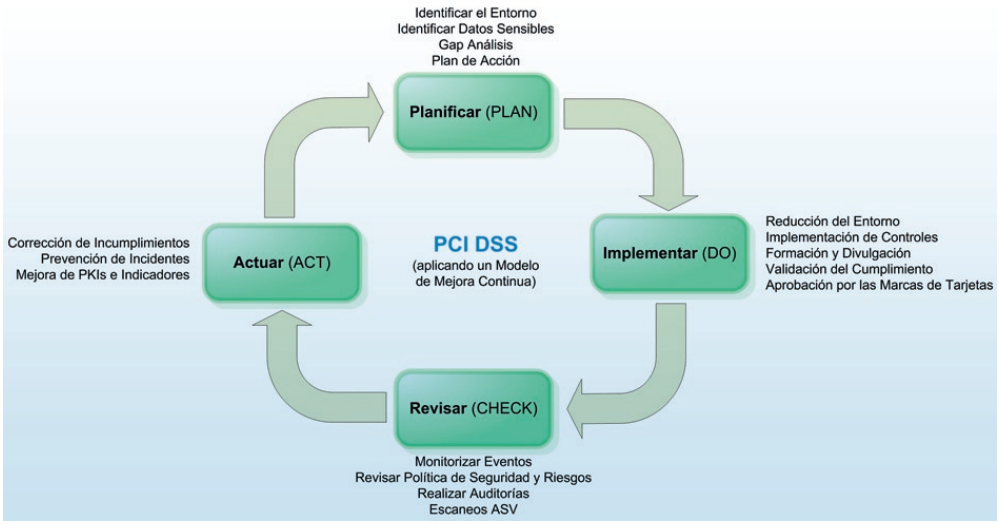

Figura 2

Además de los aspectos técnicos que se han implementado para el cumplimiento de PCI DSS, los aspectos referentes a la gestión y mantenimiento del cumplimiento con el estándar, se han cubierto definiendo procesos y procedimientos orientados a ser simples, fáciles de entender por todos los afectados, definiendo puntos de control para su correcta aplicación y accesibles a través de la Wiki.

Todo el personal de Local Billing y proveedores implicados han sido agrupados bajo roles de acceso y se les ha formado en las funciones y responsabilidades ligadas a PCI DSS. Se ha proporcionado formación en desarrollo seguro a los programadores por miembros expertos del equipo de Internet Security Auditors y se han definido materiales para realizar sesiones de concienciación en seguridad y en el buen uso de los datos de tarjetas de pago.

Local Billing es consciente de que el cumplimiento de PCI DSS es un proceso continuo por lo que se ha creado la figura de PCI Manager para garantizar dicho cumplimiento. (Ver **Figura 2**: PDCA PCI DSS).

Aspectos clave

Local Billing trabaja con un gran número de empresas a las que subcontrata servicios de espacio físico de CPD, mantenimiento de sistemas y dispositivos de red, pasarelas de pago, desarrollo de software, etc. Esto ha supuesto que la gestión del cumplimiento de los diferentes proveedores con PCI DSS haya sido un aspecto clave para garantizar el cumplimiento y la certificación de Local Billing, llegando a ser necesario rescindir el contrato con pasarelas de pago que no cumplían con el estándar PCI DSS.

Entre otros problemas que se tuvieron que solventar nos encontramos con proveedores de pasarela de pago que requerían el envío del CVV2 en cada transacción, con lo que obligaba a Local Billing a almacenar dicho dato en su base de datos y por tanto incumplir PCI DSS. Este inconveniente se pudo solventar redefiniendo junto con el proveedor de pasarela de pago el protocolo utilizado.

Además de los aspectos técnicos que se han implementado para el cumplimiento de PCI DSS, los aspectos referentes a la gestión y mantenimiento del cumplimiento con el estándar, se han cubierto definiendo procesos y procedimientos orientados a ser simples, fáciles de entender por todos los afectados, definiendo puntos de control para su correcta aplicación y accesibles a través de la Wiki.

Tras la implantación satisfactoria del programa de cumplimiento se realizó, por parte de un auditor QSA (Qualified Security Assessor) de Internet Security Auditors, la auditoría necesaria para poder validar ante Visa y Mastercard el cumplimiento de PCI DSS. El equipo auditor QSA definió y ejecutó las pruebas de auditoría mediante obtención de evidencias revisando documentación, analizando componentes de sistemas y entrevistando al personal de Local Billing, así como a personal de los proveedores más críticos para el cumplimiento de PCI DSS, incluyendo el personal en Amsterdam.

Gracias a la gran colaboración y disposición del equipo de Local Billing durante la implantación, la auditoría sólo detectó algunos problemas menores, principalmente de detalle de configuración de sistemas, que tras ser corregidos en pocos días permitieron obtener un informe de auditoría satisfactorio. Estos problemas de configuración de sistemas podrán evitarse en el futuro mediante una mejor gestión de configuración, incluyendo la total automatización de los procesos de instalación de sistemas y aplicaciones.

El informe de auditoría fue remitido a Visa[4] y Mastercard[5] para su estudio y publicación en sus listas de proveedores de servicio certificados, siendo el primer proveedor de servicios multinacional con sede en España incluido en estas listas. ■

Jordi Salvat i Alabart
VP Asociado de la Oficina Técnica
LOCAL BILLING SERVICES LTD.
jordi.salvat@localbillinglimited.com

Miguel Ángel Domínguez Torres
Director de Consultoría
CISA, CISSP, PCI QSA, BSI ISO27001 Lead Auditor
Experto Implantador SGSI (Applus+), OPST
INTERNET SECURITY AUDITORS
mdominguez@isecauditors.com

Marc Segarra López
Consultor en Seguridad
PCI QSA
msegarra@isecauditors.com

REFERENCIAS

PCI DSS v1.2: https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

Lista de empresas homologadas QSA: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

Lista de empresas homologadas ASV: https://www.pcisecuritystandards.org/pdfs/asv_report.html

Lista de proveedores de servicio certificados de VISA:
www.visaeurope.com/documents/ais/visa_europe_ais_certified_service_providers_march_2009.pdf

Lista de proveedores de servicio certificados de Mastercard:
www.mastercard.com/us/sdp/assets/pdf/Compliant%20Service%20Providers%20-%20March%203%202009.pdf

[4] Lista de proveedores de servicio certificados VISA: http://www.visaeurope.com/documents/ais/visa_europe_ais_certified_service_providers_march_2009.pdf

[5] Lista de proveedores de servicio certificados MasterCard: http://www.mastercard.com/us/sdp/assets/pdf/Compliant%20Service%20Providers%20-%20March%203%202009.pdf