

Gestión de eventos y monitoreo en el estándar PCI DSS

David Eduardo Acosta R.

Con el fin de definir una estrategia común para la protección contra fraudes y pérdida de datos relacionados con tarjetas bancarias, se conformó en 2006 el Payment Card Industry - Security Standard Council (PCI SSC) [1], integrado por American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc.

Como resultado, se han publicado tres diferentes estándares, orientados a garantizar la seguridad en el procesamiento, almacenamiento y transmisión de información confidencial asociada con tarjetas:

- Data Security Standard (DSS), dirigido a entidades bancarias, comerciantes y proveedores de servicios implicados en el procesamiento, almacenamiento y/o transmisión de datos de tarjetas de pago.
- Payment Application Data Security Standard (PA-DSS), orientado a vendedores y desarrolladores de soft-

ware que procesen datos de tarjetas de pago.

- PIN-Entry Device requirements (PED), enfocado a empresas que desarrollan dispositivos para la captura de PIN (Personal Identification Number).

Cada uno de estos estándares es de obligatorio cumplimiento para las entidades a las cuales les apliquen. Para efectos prácticos, nos centraremos en el primer estándar: PCI DSS, que se puede descargar libremente desde el sitio web del Council. PCI DSS versión 1.2 fue publicado en Octubre de 2008 y actualmente se encuentra en fase de despliegue. Es importante co-

mentar que el objetivo final del PCI SSC es lograr que cualquier ente que procese, almacene o transmita datos de tarjetas cumpla con DSS.

DSS fue desarrollado para definir una serie de controles homogéneos que le permitieran a las organizaciones afectadas, implementar contramedidas de forma sistemática y auditable, además de facilitar la adopción de dichos controles a nivel mundial, para la protección de los datos del tarjetahabiente (Personal Account Number (PAN), nombre del titular, código de servicio y fecha de vencimiento de la tarjeta). Así mismo, DSS se enfoca en garantizar cuáles datos confidenciales, como la información de la banda magnética, los códigos de validación (CVC2/CVV2/CID) y el PIN/PIN-BLOCK, no sean almacenados bajo ninguna circunstancia, con el fin de reducir el fraude relacionado con tarjetas de pago.

Para ello, se definió un conjunto de 12 requisitos, organizados de acuerdo con su área de cobertura, en 6 grupos u “objetivos de control”:

Desarrollar y mantener una red segura

Requisito 1: Instalar y mantener una configuración de firewall para proteger los datos de los tarjetahabientes.

Requisito 2: No usar contraseñas del sistema y otros parámetros de seguridad provistos por los proveedores.

Proteger los datos de los tarjetahabientes

Requisito 3: Proteger los datos de los tarjetahabientes que estén almacenados.

Requisito 4: Cifrar los datos de los tarjetahabientes transmitidos a través de redes públicas abiertas.

Mantener un programa de gestión de vulnerabilidad

Requisito 5: Utilizar software antivirus y actualizarlo regularmente.

Requisito 6: Desarrollar y mantener sistemas y aplicaciones seguras.

Implementar medidas sólidas de control de acceso

Requisito 7: Restringir el acceso a los datos de los tarjetahabientes conforme con la necesidad del funcionario de conocer la información.

Requisito 8: Asignar una Identificación única a cada persona que tenga acceso al sistema informático.

Requisito 9: Limitar el acceso físico a los datos de los tarjetahabientes.

Monitorear y probar regularmente las redes

Requisito 10: Rastrear y monitorizar todo el acceso a los recursos de la red y datos de los tarjetahabientes.

Requisito 11: Probar los sistemas y procesos de seguridad regularmente.

Mantener una política de seguridad de la información

Requisito 12: Mantener una política que contemple la seguridad de la información.

Así mismo, en el estándar DSS se ofrece una serie de recomendaciones para restringir el entorno de sistemas involucrados con datos de tarjetas. Dentro de ellas se encuentra una

correcta segmentación de red, para aislar aquellos elementos que procesan, almacenan o transmiten datos de tarjetas, de los que no lo hacen. Así mismo, la tercerización de servicios y separación de información, teniendo en cuenta que cualquier elemento que no intervenga en el proceso, puede ser excluido del cumplimiento de los controles, obligatorios por defecto.

En términos metodológicos, el proceso de implementación de PCI DSS puede asumirse siguiendo el “Ciclo de Deming”, es decir, un modelo para el mejoramiento continuo que consiste en una secuencia lógica de cuatro pasos repetidos, para la optimización y aprendizaje: Plan (Planear), Do (Hacer), Check (Revisar) y Act (Actuar), tal como se muestra en la figura No. 1.

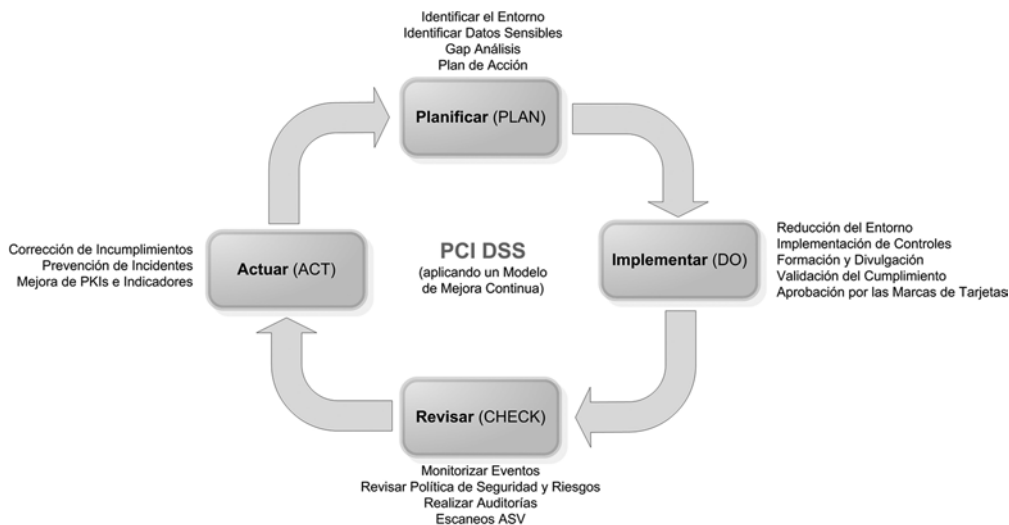


Figura No. 1. Ciclo de Deming orientado al cumplimiento de PCI DSS.

Para efectos de auditoría y evaluación, PCI SSC homologa empresas como Qualified Security Assessors (QSAs), personas encargadas de realizar una revisión del sistema y reportar al ente solicitante los resultados del análisis y Approved Scanning Vendor (ASV); empresas dedicadas a realizar escaneos de seguridad externos. Dependiendo del nivel de transacciones con tarjetas de pago que la organización realice anualmente, se deben realizar escaneos de seguridad trimestrales por un ASV, estar sujetos a auditoría anual por parte de un QSA o diligenciar un Self-Assessment Questionnaire (SAQ) [2], para garantizar que los controles se encuentran satisfactoriamente desplegados y son monitoreados en forma continua.

Controles de PCI DSS orientados al monitoreo y gestión de eventos

PCI DSS fue creado para proteger la confidencialidad, integridad y trazabilidad de los datos relacionados con tarjetas de pago. De allí, la importancia en contar con una buena gestión de eventos y registros que permita prevenir, detectar, contener, corregir y evaluar cualquier amenaza que afecte a dicha información y soporte cualquier proceso investigativo y/o actividad legal posterior a un incidente.

En este sentido, existe dentro de la especificación el Requisito 10: “Rastrear y monitorizar todo el acceso a

los recursos de la red y datos de los tarjetahabientes”, orientado hacia la definición de mecanismos de registro y su gestión. Es precisamente hacia allí hacia donde enfocaremos el presente artículo.

En dicho requisito se especifican las directrices y procedimientos de auditoría para garantizar que se cuenta con los siguientes controles definidos, implementados y en ejecución:

Procesos de vinculación de todos los accesos de cada usuario a los componentes del sistema: mediante este control se pretende garantizar que cada acceso al sistema, corresponde a un usuario plenamente identificable y rastreable, especialmente aquellos de tipo administrativo. Obviamente, este control depende de que anteriormente se haya ejecutado una labor de asociación inequívoca de una cuenta de



acceso a un usuario, de que se hayan eliminado las cuentas grupales y establecido los controles sobre cuentas por defecto, controles contemplados en el Requisito 7 y 8 del estándar.

Implementación de pistas de auditoría automatizadas para todos los componentes del sistema: la determinación de la causa de un incidente es muy difícil, si no se cuenta con registros de la actividad realizada sobre el sistema. Por ello, es necesario garantizar la existencia de un registro de todos los accesos al sistema, todas las acciones de tipo administrativo realizadas por cuentas interactivas, cualquier acceso a los registros de auditoría, intentos de acceso lógico no válidos, uso de mecanismos de identificación y autenticación, inicialización de registros de auditoría y creación y eliminación de objetos a nivel del sistema.

Elementos a ser registrados en las pistas de auditoría: con el propósito de certificar que los registros de auditoría cuentan con suficiente información para tener trazabilidad completa, se requiere que los siguientes elementos estén presentes en cada entrada: identificación del usuario, tipo de evento, fecha y hora, reporte del resultado (éxito o error), origen del evento e información acerca de los datos, componentes o recursos afectados por la acción ejecutada.

Sincronización de relojes y horarios en el sistema: con el fin de poder correlacionar en forma satisfactoria los eventos generados por cada componente del sistema, independientemente de su ubicación, se requiere que exista un elemento de sincronización central. Para ello, se recomienda implementar NTP (Network Time Protocol)[3] o tecnologías similares, definir uno o varios servidores que se sincronicen con elementos externos y confiables y distribuyan internamente dicha sincronización, empleando de forma opcional cifrado y listas de control de acceso (ACL) con estos hosts.

Resguardo y protección de los registros de auditoría: para prevenir que los registros de auditoría sean modificados y garantizar su integridad, inclusive bajo los privilegios del administrador del sistema, se deben implementar controles orientados hacia la separación de roles y la “necesidad de saber”. Para ello, se debe limitar la visualización de los registros de auditoría únicamente a aquel personal que por consideraciones operativas o administrativas lo requiera, aplicar controles para proteger la integridad de dichos registros, emplear un servidor central de registros como repositorio de datos relacionados con eventos de servidores, aplicaciones, bases de datos, equipos activos de red y de seguridad perimetral. De igual manera, es importante emplear un soft-

ware de monitorización de integridad de archivos, que permita identificar cualquier cambio realizado sobre los registros de eventos.

Revisión de los registros de eventos de los componentes por lo menos una vez al día:

la clave de los registros de eventos está en su revisión. Es un esfuerzo vano definir una arquitectura robusta de monitoreo, si no se ejecutan acciones sobre las alertas generadas. Para esto, PCI DSS requiere que los registros de eventos sean revisados por lo menos una vez al día y es precisamente en este punto donde las herramientas de centralización y generación de reportes automatizadas entran en acción, como se explicará más adelante.

Conservar los registros de auditoría:

finalmente, para el cumplimiento de PCI DSS es necesario que los registros de auditoría sean almacenados como mínimo durante un año, con disponibilidad inmediata de por lo menos los últimos tres meses para análisis.

Recomendaciones generales para la aplicación de controles de PCI DSS, orientados al monitoreo y gestión de eventos

Dada la complejidad inicial que se presenta frente a la implementación de una infraestructura de monitoreo y gestión de eventos en una organiza-

ción que procese, almacene o transmita datos de tarjetas, es necesario establecer un modelo metodológico que permita orientar el trabajo hacia la optimización de recursos y tiempos, con base en las necesidades detectadas. Para ello, es importante enfocarse en las siguientes labores:

1. Identificar aquellos controles en los cuales se tiene un cumplimiento parcial o total:

antes de empezar con la implementación de controles, es primordial identificar aquellos elementos que se encuentran actualmente en la infraestructura, y que pueden ser reutilizados o reconfigurados para cumplir con PCI DSS. De igual manera, en términos de procesos y recursos se debe plantear el mismo interrogante, con el fin de no incurrir en gastos y esfuerzos innecesarios. Se recomienda partir de la guía de auditoría y los procedimientos de evaluación que hacen parte integral del estándar, empleando estos criterios para la realización de un diferencial de estado actual vs. objetivo y definiendo labores para lograr el cumplimiento.

2. Definición e identificación del personal que requiere acceder a la información contenida en los registros de eventos:

por cuestiones de arquitectura y operatividad, los administradores tienen funciones y privilegios altos que les permiten interactuar con los registros de eventos. Para evi-

tar problemas con estos privilegios, además de facilitar la detección de errores involuntarios, prevenir potenciales fraudes y ocultamiento de rastros, es necesario segregar funciones (roles) en varias personas y definir una serie de restricciones, de acuerdo con los perfiles identificados.

3. Acciones técnicas para la configuración de los registros en equipos, servidores, aplicaciones, equipos activos de red y seguridad perimetral: todos los elementos presentes en la red son heterogéneos, generan diferentes tipos de eventos y los formatos de registro de eventos son diferentes. Es necesario definir estrategias de tipo técnico para configurar cada elemento conforme con los requerimientos de PCI DSS. Para ello, se puede apoyar la labor en la definición de procedimientos de configuración y/o guías de aseguramiento y listas de validación.

4. Determinar y cuantificar los recursos requeridos para el almacenamiento: Los tamaños de los archivos de registro y monitoreo son directamente proporcionales a la cantidad de eventos generados y servicios/servidores gestionados. Por ello, se debe estimar un espacio de almacenamiento en local de dichos registros, de por lo menos tres meses. Para presupuestar las necesidades, se recomienda utilizar varios servidores representativos (por sistema operativo

o por función) como pilotos, hacer un seguimiento estadístico por hora/día/semana del uso de disco y extrapolar dichos resultados en la totalidad de elementos técnicos del entorno. Teniendo en cuenta que es obligatorio el uso de un servidor centralizado de registros, dicho servidor debe tener espacio suficiente en disco, para almacenar los archivos de eventos de todos los equipos del entorno durante el tiempo estipulado (3 meses), además de contar con una estrategia de respaldo (backup) que permita mantenerlos durante un año.

Así mismo, se deben tener en cuenta recomendaciones generales de seguridad en almacenamiento de registros:

- Definición de un disco/partición/sistema de archivos (Filesystem) independiente para el almacenamiento en local.
- Aplicación de controles de acceso y permisos. Se recomienda emplear características y funcionalidades propias de los sistemas de archivos, como restricciones de ejecución de binarios, controles de inmutabilidad, permisos de “sólo agregación” en archivos (append-only) y controles para evitar el borrado.
- Activar funcionalidades como “registro cíclico” por tiempo, no por tamaño. Esto permitirá que después de un tiempo específico, los eventos

más recientes sobrescriban a los más antiguos de forma circular en el mismo archivo.

5. Contemplar el impacto en el desempeño de los servicios y servidores causados por la generación de registros de eventos: debido a que la generación de registros de eventos consume recursos del sistema (memoria intermedia, uso de procesador, uso de recursos de I/O), se debe contemplar el impacto que tiene dicho consumo sobre la capacidad general del servidor y los servicios asociados. El mismo proceso de seguimiento estadístico empleado para la cuantificación en el almacenamiento puede ser empleado para identificar el desempeño e impacto en aplicaciones y servidores.

6. Definir el método de transporte de registros a un servidor central: uno de los aspectos importantes es el transporte de los registros de eventos de un servidor gestionado a una ubicación central. Se debe garantizar la integridad y confidencialidad de dicha información, por lo que se recomienda el uso de canales cifrados empleando tecnologías como SSL, TLS, SSH, etc. y con control de integridad.

7. Definir los métodos de análisis y correlación: después de tener activados y almacenados correctamente los archivos de registro de eventos,

es necesario definir una estrategia de análisis y correlación de información, que permita obtener datos específicos frente a una acción en concreto. Dependiendo de la complejidad del entorno, miles de registros de eventos son generados por todos los elementos monitorizados, haciendo inmanejable la ubicación de un dato concreto. Es precisamente en este punto en donde entran en juego tecnologías como SIEM (Security Information and Event Management), herramientas que proveen capacidades de captura, filtrado, automatización, correlación, presentación, reportes y alertas.

8. Identificar los criterios de alarma, alertas y umbrales a ser activados: Finalmente, se requieren establecer criterios por los cuales un evento será considerado como un incidente y su impacto relacionado. Dependiendo de ello, se debe fijar una serie de alertas, establecer tiempos en los cuales dichas alertas deben ser atendidas y los procesos asociados. Todo ello en función de la criticidad y del impacto que el evento pueda tener en la confidencialidad e integridad de los datos de tarjetas relacionados con PCI DSS.

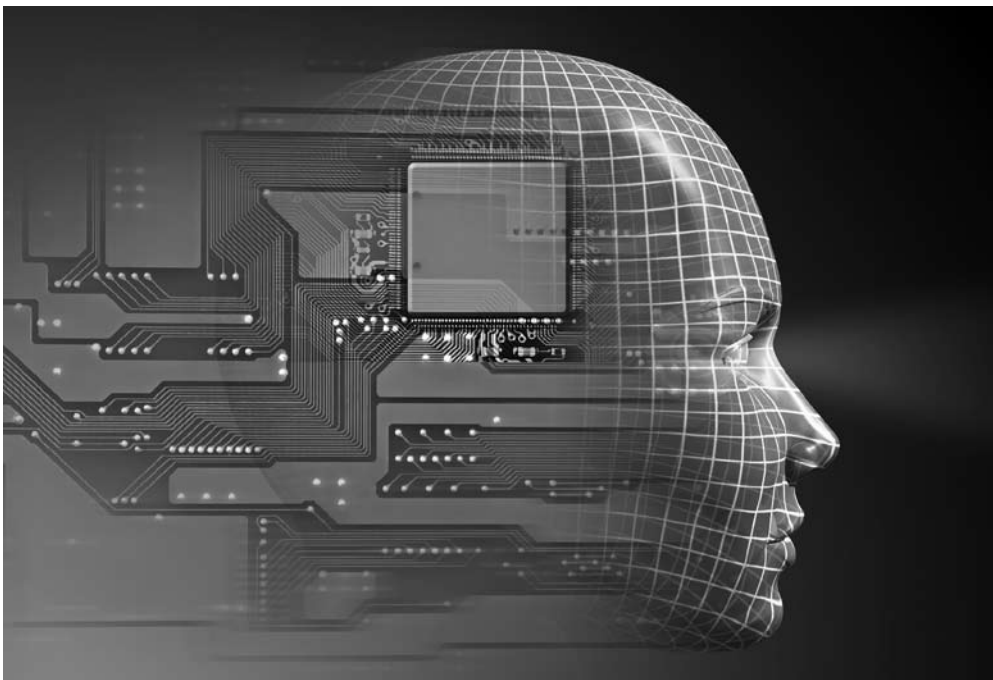
9. Aplicar controles orientados al aseguramiento de los registros de eventos: Con el fin de garantizar la idoneidad e integridad de los archivos de registro de eventos, es imprescindible implementar controles que

permitan la identificación de eventos sospechosos durante la manipulación de dichos archivos, tales como modificación intencional, no intencional, extracción de información, cambio de permisos y/o propietarios, borrado total o parcial y agregación. En este sentido, el requerimiento se orienta hacia la instalación de un sistema de monitorización de integridad o detección de cambios.

10. Evaluar qué tipo de herramientas pueden ser útiles, bajo qué conceptos y su ámbito de acción: para el cumplimiento de los controles se requiere implementar un sistema centralizado de registros, software de monitoreo de integridad, software de sincronización de tiempos y software de recolección, análisis y ge-

neración de alertas. Dependiendo de la complejidad del entorno afectado por el cumplimiento de PCI DSS, la cantidad de elementos involucrados y el número promedio de eventos generados en umbrales de tiempo predefinidos (minutos, horas, días) y el personal y recursos disponibles, se puede optar por el uso de software OpenSource, herramientas comerciales o una mezcla de ambos, siempre bajo el concepto costo-beneficio.

11. Definir prioridades en la implementación de controles globales: debido a la alta interacción e interdependencia entre todos los controles del estándar, se deben identificar a nivel general, aquellas acciones que preceden a otras, para no duplicar el trabajo. En este sentido, PCI SSC ha



publicado una guía denominada “PCI Prioritized Approach for DSS 1.2” [4], para definir el enfoque de prioridades en todos los requerimientos de DSS. Dicha guía y su hoja de cálculo de soporte pueden ser descargadas libremente. En esta guía se definen 6 hitos organizados de acuerdo con la prioridad de implementación. Cada hito abarca una serie de controles y son presentados a manera de recomendación, ya que cada organización puede definir sus propias prioridades conforme con el escenario de cumplimiento. Dichos hitos son:

- 1) Remover datos sensitivos y limitar los periodos de retención
- 2) Proteger las redes perimetrales, internas e inalámbricas
- 3) Asegurar las aplicaciones de pago con tarjetas
- 4) Monitorear y controlar el acceso a los sistemas
- 5) Proteger los datos del tarjetahabiente almacenados
- 6) Finalizar las tareas restantes de cumplimiento y asegurarse que los controles están implementados satisfactoriamente.

Para nuestro caso, el proceso de implementación de una plataforma de monitorización viene posterior al desarrollo de proyectos de asegura-

miento de datos, redes y aplicaciones, por lo que es primordial identificar cuándo se deben aplicar estos controles para no incurrir en errores.

Es importante resaltar que una entidad que haya implementado los controles de ISO/IEC 27002:2005 -sobre todo el control 10.10 “Supervisión”-, puede estar en capacidad de lograr una adopción sencilla de los requerimientos de monitoreo de PCI DSS.

Gestión de eventos en PCI DSS: un ejemplo de implementación

Para complementar el marco teórico expuesto anteriormente, describiremos un ejemplo real en el cual una empresa multinacional, dedicada a la gestión de pagos con tarjetas en compras en línea (pasarela de pagos), ha logrado implementar un sistema de gestión de eventos y monitoreo para cumplir con los requerimientos definidos en PCI DSS y lograr su certificación de manera satisfactoria, luego de un proceso de alineamiento de aproximadamente un año.

Dicha empresa ha definido como política corporativa el uso de software OpenSource en sus sistemas de información, por lo que los sistemas operativos están basados en GNU/Linux y todos los aplicativos relacionados (bases de datos, servidores web, servidores de aplicación, entre otros.) siguen la misma línea. En el entor-

no de cumplimiento se identificaron aproximadamente 30 activos entre equipos de red, seguridad perimetral, servidores y aplicativos dentro del alcance de cumplimiento. Cuentan con dos administradores senior de tiempo completo y la operación se encuentra a cargo de un tercero. Toda la infraestructura se encuentra en un Centro de Procesamiento de Datos (CPD) y la operación y administración se efectúa de forma remota.

Para lograr los objetivos de cumplimiento del requerimiento 10 de PCI DSS, se empleó como marco de trabajo la metodología y pasos descritos en este documento, con los siguientes resultados:

1. Identificar aquellos controles en los cuales se tiene un cumplimiento parcial o total:

al iniciar, se procedió con la ejecución de un diferencial con PCI DSS que permitió identificar aquellos elementos que pertenecían al ámbito de cumplimiento, permitiendo una reducción de entorno e identificando controles que se encontraban implementados y que podían ser alineados con los requerimientos del estándar. Así mismo, se identificaron las falencias y se generaron proyectos para asumir su corrección y gestionar el riesgo.

2. Definición e identificación del personal que requiere acceder a la información contenida en los regis-

tros de eventos: con el fin de evitar potenciales problemas de conflicto en la gestión de eventos, se definieron responsabilidades sobre los archivos de registro de eventos locales a cada administrador de la plataforma, segregando las funciones y privilegios y se nombró a dos operadores como encargados del servidor centralizado de registros, dividiendo la contraseña maestra de administrador entre estas dos personas.

3. Acciones técnicas para la configuración de los registros en equipos, servidores, aplicaciones, equipos activos de red y seguridad perimetral:

el paso siguiente fue generar documentación técnica de referencia y soporte para la configuración del subsistema de registro de eventos de cada uno de los elementos presentes en el entorno de cumplimiento. Para ello, se utilizó información de referencia del fabricante o proveedor, guías de aseguramiento (SANS, CIS, NIST, NSA, etc.) y listas de validación. Esta documentación se publicó en la Intranet, se puso a disposición del personal técnico a cargo y su implementación fue revisada por un tercero mediante una lista de validación. Cada no conformidad llevaba una labor de corrección asociada, hasta lograr el cumplimiento total.

4. Determinar y cuantificar los recursos requeridos para el alma-

cenamiento: para cuantificar las necesidades técnicas en términos de almacenamiento, se tomó como muestra un elemento representativo de cada grupo de activos identificados en el entorno. Para recolección de información y análisis estadístico de consumo de espacio se empleó la herramienta NAGIOS [5], que permite generar reportes históricos de uso y comportamiento de discos. Con estos datos se hicieron cálculos y se presupuestó el uso de espacio en un término de un año por cada elemento del entorno. La sumatoria de estos espacios en disco determinó el almacenamiento que se debería disponer para el servidor centralizado de logs.

Así mismo, se definieron particiones especiales en los sistemas operativos dedicadas exclusivamente al almacenamiento de registros de eventos y se activaron las funcionalidades de control en el filesystem (EXT3): Noexec, Nosuid y Nodev, funcionalidades de journaling e indicadores (flags) extendidos, para evitar eliminación y permitir únicamente adición de datos en archivos de registro. Se hizo uso del aplicativo SYSLOG a nivel local, configurando que los ficheros de registro se reutilizaran a los 3 meses y que se hiciera copia en el servidor central.

5. Contemplar el impacto en el desempeño de los servicios y servido-

res causados por la generación de registros de eventos: la misma estrategia empleada para la recolección de información de uso en almacenamiento (NAGIOS) se usó para analizar el desempeño en términos de uso de procesador, memoria intermedia, etc. Los resultados fueron revisados y se agregó nuevo hardware conforme con las necesidades.

6. Definir el método de transporte de registros a un servidor central: como servidor centralizado de registros se empleó un equipo independiente con SYSLOG. Gracias a la funcionalidad de consolidación central de eventos a través de la red que ofrece SYSLOG, se definieron canales de comunicación seguros entre un extremo y otro empleando túneles de Secure Shell (SSH).

7. Definir los métodos de análisis y correlación: después del despliegue de la arquitectura de almacenamiento y centralización, se hizo empleo de la herramienta OpenSource Epylog [6] en el servidor central de SYSLOG y en cada uno de los servidores que por arquitectura eran soportados. Esta herramienta permite analizar de forma periódica todos los registros de auditoría almacenados, ejecutar validaciones y activar alertas, junto con reportes de actividades vía correo electrónico.

8. Identificar los criterios de alarma, alertas y umbrales a ser activados: para la generación de alertas se configuraron los parámetros necesarios en Epylog, conforme con las necesidades de la empresa y los niveles de criticidad de los eventos analizados.

9. Aplicar controles orientados al aseguramiento de los registros de eventos: finalmente, se empleó el aplicativo Samhain [7] como analizador de integridad en aquellos archivos relacionados con el subsistema de registro de eventos en cada uno de los servidores identificados y en el servidor central de registros, asociando alertas, responsables y acciones frente a acciones sospechosas. Las alertas eran gestionadas de forma centralizada a través de Beltane [8], complemento de Samhain para visualizar los reportes, a través de una consola web y almacenar las alertas y reportes en una base de datos.

Adicional a las herramientas citadas en esta implementación, vale la pena enumerar las siguientes soluciones que pueden ser empleadas en el despliegue de una arquitectura de gestión de registros con similares prestaciones (lista no exhaustiva):

• **Herramientas de análisis de desempeño y consumo de recursos:** Zabbix (www.zabbix.com - Open-

Source), IBM Tivoli (Comercial), HP OpenView (comercial)

• **Gestión de eventos a nivel local y centralizado:** SYSLOG (www.syslog.org - OpenSource), syslog-ng (www.balabit.com/network-security/syslog-ng - OpenSource)

• **Análisis de eventos, consolidación y alertas:** OSSIM (www.ossim.net - OpenSource), Prelude (www.prelude-ids.com - Opensource), RSA eView (www.rsa.com - Comercial), Netforensics (www.netforensics.com - Comercial), GFI EventsManager (www.gfi.com - Comercial).

• **Monitoreo de integridad:** Tripwire (www.tripwire.com - Comercial), Osiris (osiris.shmoo.com - OpenSource), INTEGRIT (integrit.sourceforge.net - OpenSource), AIDE (www.cs.tut.fi/~rammer/aide.html - OpenSource)

Una lista bastante completa de herramientas puede ser encontrada en <http://www.loganalysis.org>.

Conclusiones

El estándar PCI DSS define una serie de requerimientos de obligatorio cumplimiento para cualquier elemento que almacene, procese o transmita información relacionada con tarjetas. Uno de los puntos más importantes de dicho estándar es

precisamente la gestión de eventos y monitoreo, para garantizar la trazabilidad y auditoría en cada una de las acciones que se llevan a cabo en el sistema, partiendo desde la definición básica de los componentes del registro de eventos, las características que debe cumplir, cómo se debe almacenar y proteger y quiénes los pueden acceder.

Como en cualquier proceso de alineamiento con normativas, los administradores se pueden ver envueltos en problemas durante el análisis, el diseño, la implementación, la puesta en marcha y el monitoreo de una plataforma de gestión de eventos, por lo que se requiere definir una serie de acciones que conlleven a la implementación de la infraestructura, soportadas en personal, recursos y herramientas (OpenSource o comerciales) que permitan una gestión óptima de las alertas y faciliten las acciones preventivas y correctivas, frente a cualquier amenaza que pueda sufrir la organización.

Finalmente, es buena práctica contar con el soporte y asesoramiento de

una empresa homologada QSA, para guiar el proceso de implementación PCI DSS, de forma que las actuaciones realizadas garanticen alcanzar en forma exitosa el cumplimiento de la norma.

Referencias

[1] PCI Security Standards Council <https://www.pcisecuritystandards.org/>. Abril de 2009.

[2] PCI QSA y ASV https://www.pcisecuritystandards.org/qa_asv/index.shtml y SAQ <https://www.pcisecuritystandards.org/saq/index.shtml> Abril de 2009.

[3] IETF RFC 1305 “Network Time Protocol (Version 3) Specification, Implementation and Analysis”. Marzo de 1992.

[4] PCI Prioritized Approach for DSS.

<https://www.pcisecuritystandards.org/education/prioritized.shtml>. Abril de 2009.

[5] NAGIOS Open Source Monitoring www.nagios.org. Abril de 2009.

[6] Epylog Log Analyzer <http://fedorahosted.org/epylog/>. Abril de 2009.

[7] Samhain File Integrity Monitoring <http://la-samhna.de/samhain>. Abril de 2009.

[8] Beltane Web Console for Samhain <http://la-samhna.de/beltane/index.html>. Abril de 2009.

David Eduardo Acosta R. Consultor en seguridad de la información, CISSP, CISM, OPST, CCNA y PCI QSA. Màster en Seguretat de les Tecnologies de la Informació y Master in Project Management de la Universitat de La Salle – Ramón Llull (Barcelona – España). Es Miembro de la IEEE, del ISMS Forum Spain y trabaja actualmente con Internet Security Auditors en Barcelona (España). Puede ser contactado en deacosta@isecauditors.com.