Usando la segmentación de red para reducir el alcance de PCI DSS

A pesar de que las mejores prácticas de seguridad deberían ser aplicadas en todos los sistemas de una empresa, ya sean críticos o no, las necesidades del negocio y las capacidades limitadas de las organizaciones para mantener rigurosos controles de seguridad provocan que el equilibrio deseado entre los objetivos de negocio y los requisitos de seguridad no se logre a menudo. Este problema abre la necesidad de disponer de una arquitectura de seguridad distribuida en niveles de criticidad, donde los controles de seguridad estrictos se apliquen a sistemas críticos y aquellos controles más flexibles puedan aplicarse a sistemas menos críticos o sensibles. En el caso de PCI DSS, el cumplimiento de los mandatos requiere que las organizaciones (comercios, proveedores de servicio y adquirentes) inicien un análisis detallado del ámbito de aplicación del estándar descubriendo, en la mayoría de los casos, la necesidad de tomar medidas para aislar los procesos afectados y los sistemas que limitan el ámbito de aplicación de PCI DSS.

Marc Segarra López

Normalmente, la reducción y limitación del alcance de PCI DSS se logra a través de una adecuada segmentación de la red, pero antes de llevarla a cabo es necesario entender cómo establecer límites en el área de cumplimiento de PCI DSS y qué aspectos serán evaluados por el auditor QSA en una evaluación PCI DSS. De hecho, la mala interpretación del alcance de PCI DSS hace que las organizaciones crean que el cumplimiento de esta norma parezca mucho más fácil de lo que realmente es, provocando que estas organizaciones insistan en llevar a cabo directamente una auditoría de cumplimiento PCI DSS, sin haber tenido previamente un asesoramiento adecuado, concluyendo en una auditoría con resultados negativos y un aumento de los costes finales.

Abordar el cumplimiento de PCI DSS

Uno de los problemas comunes en la adecuación de PCI DSS es conseguir que los clientes entiendan que este estándar no solo se aplica a los componentes de sistema que almacenan, transmiten o procesan datos de tarjetas de pago, sino que por lo general el alcance de PCI DSS es mucho mayor, incluyendo los sistemas de gestión, sistemas de seguridad y en muchos casos todos los procesos e infraestructura del cliente.

Una segmentación de red adecuada puede ayudar a las organizaciones a reducir el alcance y el coste de la adecuación y evaluación del estándar. El objetivo es acotar los sistemas donde se procesan, almacenan y transmiten los datos de tarjetas de pago para limitar el alcance de PCI DSS, logrando:

- Reducir el riesgo, ya que la atención se centra en las áreas que requieren controles adicionales.
- Reducir el tiempo, esfuerzo y coste.
- Evitar multas elevadas, pérdidas financieras y daños en la reputación.
- Establecer estrategias efectivas de coste para administrar y proteger los datos de tarjetas de pago.

Figura 1

La intención es proteger los datos contra amenazas de otras redes o entornos que podrían afectar a los datos de tarjetas de pago. Es necesario evaluar las posibles interacciones entre el entorno PCI DSS de la organización y cualquier otro entorno, como una red de gestión de un proveedor de servicios administrados.

Un escenario que puede complicar enormemente los esfuerzos de cumplimiento de una organización se produce cuando no se analizan en profundidad los servicios contratados a terceros, viendo cómo una opción que idealmente hubiera sido válida para reducir el alcance de PCI DSS mediante la externalización de servicios en algunos casos actúa totalmente en contra, ampliando el alcance de PCI DSS más allá de los límites de la compañía. Para comprender mejor este escenario vamos a dar un ejemplo (ver **Figura 2**):

- Una organización "A", con el fin de reducir el alcance de PCI DSS, contrata con la compañía "B" servicios de gestión de cortafuegos, IDS y sincronización de tiempo.
- La empresa "B" ofrece los mismos servicios sobre una base compartida para varios clientes. La empresa "B" no administra los servidores de los clientes, o el acceso a ellos en absoluto, ni siquiera las copias de seguridad.
- Como la empresa "B" no procesa o gestiona datos de tarjetas de pago, ya que ningún cliente comparte estos datos con esta empresa, la compañía "B" no está obligada a validar el cumplimiento de PCI DSS como un proveedor de servicios.
- Normalmente los clientes, dentro de su proceso anual de auditoría PCI DSS, incluyen los servicios de la empresa "B" en su propia evaluación, como es el caso de la organización "A".
- La empresa "B" tiene en sus instalaciones (red) la consola de gestión de cortafuegos, otra consola de administración para el IPS, el servidor de tiempo NTP y un servidor Radius para la autenticación de los usuarios en cada una de las consolas de administración.
- En la misma red también hay otros servidores y dispositivos de la empresa "B" que no son utilizados para los servicios prestados a la organización "A".
- Como la empresa "B" no tiene la obligación de validar el cumplimiento de PCI DSS en su propia red, no hay garantías de que los componentes de sistema de su red estén protegidos con los últimos parches de seguridad, antivirus, control de accesos, etc.
- Esto significa que, por ejemplo, un compromiso potencial de la seguridad para la empresa "B" desde el punto de acceso inalámbrico, en el que no se ha cambiado la configuración por defecto, incluyendo el servidor NTP. Los usuarios de Radius que se utilizan para administrar los servidores de seguridad de los clientes como la consola de cortafuegos y la consola del IPS, llegando desde este punto a comprometer la red PCI DSS de la organización "A".
- Por esta razón y con este escenario, toda la red de la empresa "B" estaría dentro del alcance de PCI DSS de la organización "A", provocando que el cumplimiento de PCI DSS sea algo inalcanzable.

Esto no significa que las empresas no deban externalizar los servicios del entorno PCI DSS, todo lo contrario, ya que esto permite reducir el alcance; pero es esencial asegurar que la externalización no va a suponer un riesgo para la seguridad y, por tanto, una extensión del ámbito de aplicación del estándar. De hecho, el mismo escenario no plantearía los problemas de seguridad detallados anteriormente si la empresa "B" hubiera aplicado técnicas de segmentación de red para los servicios afectados por PCI DSS de aquellos que no lo están (ver **Figura 3**).

El alcance de PCI DSS

Para determinar cómo afecta PCI DSS a la organización es necesario llevar a cabo una ***evaluación que permita conocer cómo los datos de titulares de tarjetas de pago fluyen a través de la organización*** y analizar dónde es crítico el almacenamiento, procesamiento o tratamiento de esta información, eliminando aquellos flujos que no sean críticos. Es necesario que en la evaluación de cada uno de los flujos, donde aparezcan datos de tarjetas de pago, se considere el punto inicial (qué, cuándo y cómo llegan los datos de tarjetas a la organización), los estados intermedios (todos los tratamientos y ubicaciones por las que fluyen los datos) y el punto final (si existe, cómo salen de la organización los datos).

Este análisis debe llevarse a cabo en todas las áreas de la compañía, ya que es común que un área de la organización desconozca qué otras áreas también interaccionan con datos de tarjetas de pago. A continuación, se enumeran algunos ejemplos de flujos o servicios en los que pueden aparecer datos de tarjetas de pago en algún momento:

– Procesado, almacenado o transmisión de transacciones de pago.

– Proveedores de servicio (*cualquier servicio ofrecido sobre el cual se pueda transmitir, almacenar o procesar datos de tarjetas por parte del proveedor de servicio o del propio cliente*); como:

• Alojamiento de espacios web, servidores dedicados, *Housing*, *Datacenter.*

• Servicios de red, administración y gestión de sistemas.

• Desarrollo de aplicaciones.

– Facturación/pago de servicios mediante tarjeta por Internet, teléfono, móvil, etc.

– Servicios de atención al cliente donde aparezcan datos de tarjetas, por ejemplo:

• *Call-centers* (conversaciones grabadas).

• Incidencias recibidas en papel, por ejemplo fax.

• Incidencias recibidas electrónicamente (correo-e, aplicaciones, etc.).

– Hospedaje y/o gestión de servicios de clientes que contengan datos de tarjetas de pago.

– Programas de lealtad.

– Gestión de fraude con datos de tarjetas.

– Gestión de reservas.

Una vez identificados todos los flujos, es importante buscar las áreas donde pueden consolidarse datos de tarjetas de pago y/o eliminarlos. Con esta información se consigue determinar el alcance de PCI DSS, teniendo en cuenta que cualquier otro sistema, que se encuentre en la misma zona de red que los componentes identificados en los flujos, también se encontrará dentro del alcance de PCI DSS (aunque no intervenga de ningún modo en la gestión de los datos de titulares de tarjetas de pago).

Sin la adecuada segmentación de red (a veces denominada "red simple"), toda la infraestructura se encuentra dentro del alcance de la evaluación de las PCI DSS. La segmentación de red se puede alcanzar mediante diversos medios físicos o lógicos, tales como cortafuegos internos de red, *routers* con sólidas listas de control de acceso u otras tecnologías con la apropiada configuración que restrinjan el acceso a un segmento particular de la red.

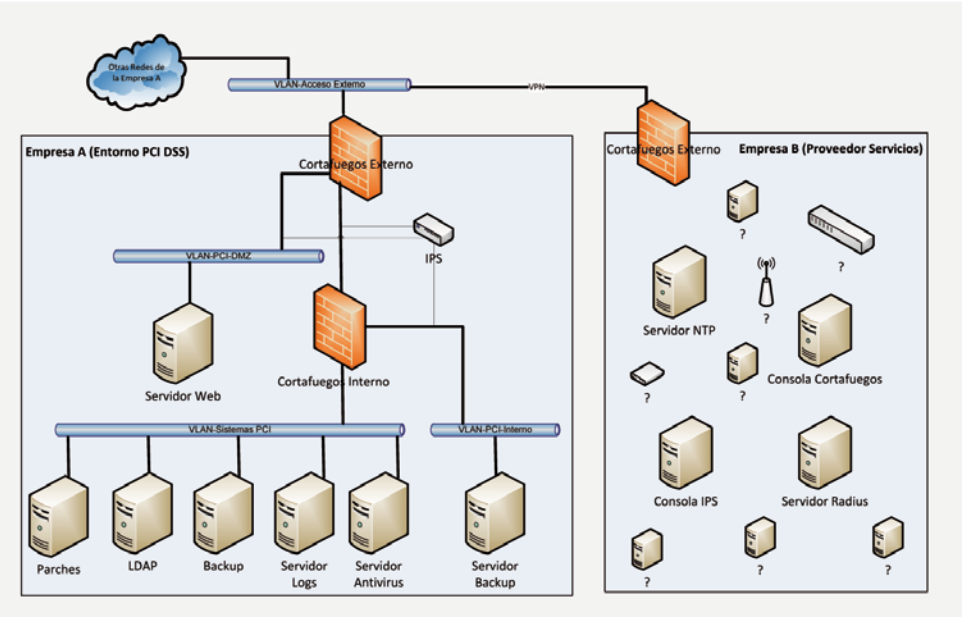

Figura 2

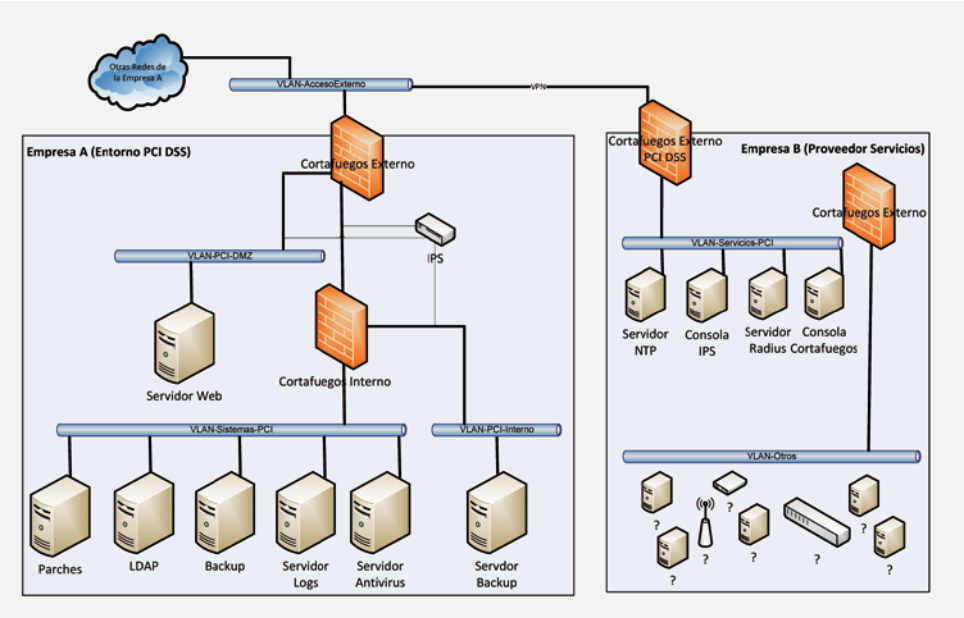

Figura 3

Requisitos y procedimientos de evaluación de seguridad Versión 2.0

Como se ha comentado anteriormente, los requerimientos de PCI DSS aplican a todos los componentes de sistema. Los componentes de sistema se definen como cualquier componente de red, servidor o aplicación que se incluya o esté conectado en el entorno de los datos de titulares de tarjetas de pago.

El entorno de los datos de titulares de tarjetas de pago es la zona de la red que posee información de datos de tarjetas o datos sensibles de autenticación, incluyendo:

• Cortafuegos, *switches*, *routers*, puntos de acceso inalámbricos y cualquier otro dispositivo de red y seguridad.

• Servidores, por ejemplo: web, aplicación, base de datos, autenticación, correo, Proxy, NTP, DNS, etc.

• Aplicaciones, compradas, personalizadas o propias, ya sean internas o externas (Internet).

• Todos los equipos de usuario, portátiles, etc.

Importancia de la segmentación de red

Las redes planas (o simples) incrementan significativamente la exposición potencial de una única violación de datos sin una protección adecuada de la red.

• Una violación a datos de tarjetas de pago puede ocurrir en cualquier tienda, oficina o sitio que acepte tarjetas de pago.

• Una red plana deja todos los sistemas vulnerables al punto "más débil". Una vez conseguido el acceso en cualquier punto a través del punto más débil, un intruso puede alcanzar otros sistemas críticos en otras ubicaciones.

Por otra parte, es necesario tener en cuenta que la segmentación de red no es un requerimiento obligatorio de PCI DSS pero una red única, plana o una segmentación de red errónea o incompleta puede provocar en todos los componentes existentes en la red, aunque no tengan nada que ver con datos de tarjetas de pago:

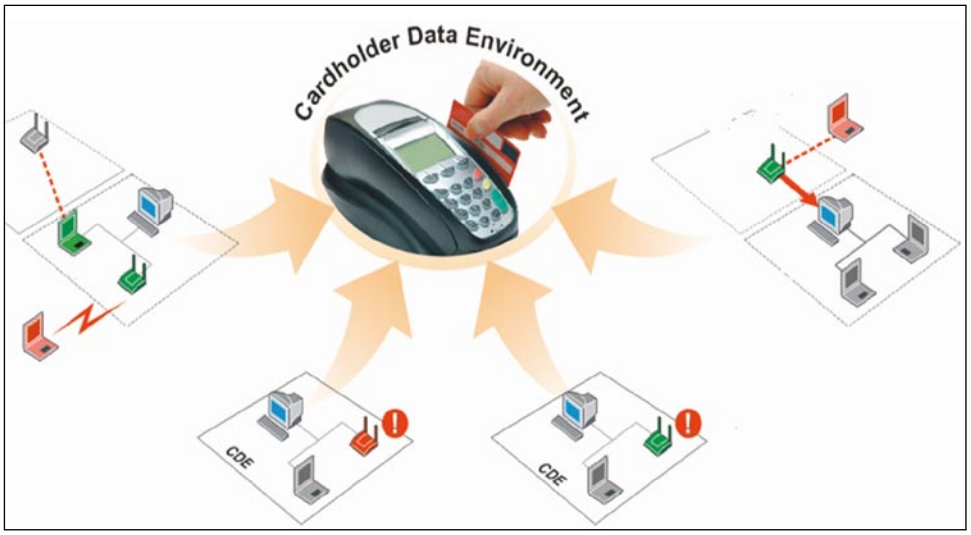

Figura 4

• Aumento de riesgo por la organización (mayor número de datos de tarjetas de pago, más ubicaciones con datos, más ubicaciones que controlar).

• Mayor coste y dificultad de implementar y mantener los controles de PCI DSS.

• Requerimiento de realizar test de intrusión de red y aplicación.

• Requerimiento de escaneos de vulnerabilidades internos y externos.

• Implementación de registros de auditoría y *logs* estrictos.

• Configuración de modo seguro de los componentes.

• Revisiones de código o necesidad de cortafuegos de aplicación para aplicaciones que nada tienen que ver con datos de tarjetas de pago.

• Gestión de usuarios y políticas de cuentas estricta para todos los componentes de la red.

Beneficios de reducir el alcance

Segmentar el entorno de datos de tarjetas de pago puede reducir significativamente el alcance de PCI DSS. A continuación, se describen algunos elementos que pueden verse reducidos si la red está debidamente segmentada:

• **Reducir el alcance**. De una situación donde cualquiera puede tener acceso a la red corporativa, a una situación con usuarios específicamente autorizados para acceder al entorno de datos de tarjetas de pago.

• **Número de sistemas (servidores, aplicaciones, dispositivos)**. Depende de cada organización, por ejemplo una red plana que contiene 100 servidores aunque solo 4 tratan con datos de tarjetas de pago. En una arquitectura de red plana o inadecuadamente segmentada, todos los sistemas se encuentran dentro del alcance. Sin embargo, aislando los cuatro servidores en un segmento seguro, solo estos servidores y el tráfico hacia/desde ese segmento se encuentra dentro del alcance.

• **Esfuerzo menor.** Es necesario menor esfuerzo para desarrollar y aplicar políticas de seguridad para proteger el segmento de lo que sería necesario para una red completa.

• **Coste menor**. A menor número de componentes, menor coste a asumir referente a auditorías de seguridad, como análisis de vulnerabilidades, test de intrusión, etc.

• **Menor esfuerzo forense.** En el caso de que ocurra un incidente de seguridad, la investigación forense en un segmento de red limitado es mucho más rápida y efectiva.

Sin segmentar adecuadamente la red, el cumplimiento de los requerimientos de PCI impacta a cualquier sistema y empleado con acceso a la red y puede requerir:

• Dos factores de autenticación para la autenticación mediante VPN y acceso a la red.

• 'Securización' de los sistemas, gestión de la aplicación de cambios; gestión de *logs* y registros de auditoría; y uso de cortafuegos personal y antivirus, incluso en sistemas y aplicaciones que no traten con datos de tarjeta de pago.

• Incremento de procesos y procedimientos para todos los cambios y tareas IT.

• Reducción de la inclusión de todas las aplicaciones que no tratan con datos de tarjeta de pago en futuras evaluaciones. *El requerimiento 6.6 requiere que todas las aplicaciones web sean protegidas por un* firewall *de aplicación o realizar revisiones de seguridad de vulnerabilidades*.

Ejemplo gráfico

En la **Figura 5** se muestra un ejemplo muy simple de una segmentación de red, en la que se mostrará la afectación de PCI DSS sobre cada segmento:

En el segmento de red correspondiente a "VLAN 2" no se almacena, procesa, ni transmite ningún dato de tarjeta por ningún componente de sistema. Además ningún componente del segmento "VLAN 2" puede acceder al segmento "VLAN 1", donde el cortafuegos implementa un control de acceso seguro y estricto para garantizar una segmentación adecuada. Como resultado, el segmento de red "VLAN 2" queda fuera del alcance de PCI DSS.

Por otro lado, en el segmento de red "VLAN 1" se transmiten y almacenan datos de tarjetas. A continuación se describe la funcionalidad de los componentes mostrados en el diagrama:

• **Srv DB:** Almacena en base de datos el PAN, nombre titular y fecha de caducidad.

• **Srv Ficheros B**: Servidor de ficheros para los empleados, nunca se almacenan datos de tarjetas.

• **Srv Ficheros A**: Contiene ficheros con extracciones de la base de datos, en ocasiones puede contener datos de tarjetas.

• **Servidor de Correo:** En ocasiones se reciben incidencias por correo electrónico que contienen el PAN de tarjetas de pago.

• **AP:** Punto de acceso inalámbrico conectado al segmento de red, por tanto pueden transmitirse datos de tarjeta por este canal.

• **Mvl:** Terminal blackberry de algunos empleados para acceder al correo-e.

El resultado es que todos los componentes se encuentran dentro del alcance de PCI DSS por formar parte del mismo segmento de red que aquellos que sí tratan datos de tarjetas:

• **Srv Ficheros B.** Aun no tratando de ningún modo con datos de tarjetas se encuentra dentro del alcance por encontrarse en el mismo segmento de red.

• **Mvl.** Al acceder al correo electrónico, pudiendo acceder a datos de tarjetas, también se encuentra dentro del alcance.

• **Resto.** El resto trata directamente con datos de tarjetas por lo que su implicación es directa.

La conclusión es que deben aplicarse todos los requerimientos PCI DSS (por ejemplo: *test* de intrusión, escaneos de vulnerabilidades, monitorización, etc.) a todos los componentes, incluidos el "Srv Ficheros B" y "Mvl" derivando en más esfuerzo y coste.

Consideraciones

La idea o concepto principal a tener en cuenta en todo momento es "¿Cómo puede afectar al entorno de datos de tarjeta la seguridad existente en el resto de entornos?". Por ejemplo, ¿un problema de seguridad en la red de ofimática, podría afectar la seguridad del entorno PCI DSS?

A continuación se describen algunos conceptos que hay que analizar:

¿Cómo se controla el tráfico de red? Pueden usarse controles lógicos o físicos para aislar PCI DSS de sistemas fuera del ámbito de aplicación. Los controles pueden ser cortafuegos, redes de área local virtuales (VLAN) y redes totalmente independientes del resto. Las técnicas más comunes son los cortafuegos y VLAN. Sin embargo, para separar las redes es necesario que haya listas de control de acceso fuertes (ACL), restricciones a nivel de puerto/servicio u otros controles que puedan ponerse en marcha para limitar y/o restringir el acceso de la red dentro del ámbito de aplicación de PCI DSS al resto de redes.

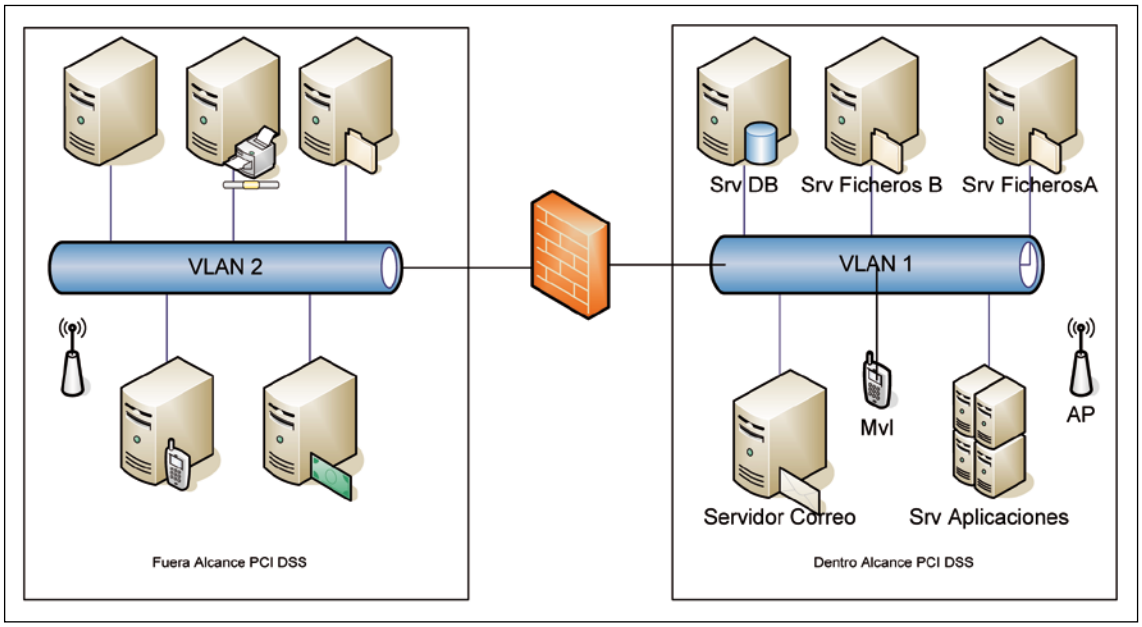

Figura 5

¿Cómo se monitoriza el tráfico de red? Es necesario que existan controles para monitorizar/supervisar el tráfico de red, con la capacidad de generar alertas cuando el tráfico no autorizado es bloqueado o detectado.

¿Quién tiene acceso a los dispositivos? Cualquier tipo de controles que puedan utilizarse son ineficaces si no se limita el acceso a los dispositivos de red. Es necesario establecer mecanismos para controlar cómo se accede a estos dispositivos y cómo se monitorizan dichos accesos.

Lo primero que hay que realizar para verificar el alcance de PCI DSS es comprobar la conectividad existente entre el entorno de datos de tarjetas y cualquier otro sistema. Si existen conexiones con otros entornos potencialmente inseguros, el alcance de PCI DSS es susceptible de ampliarse, por lo que será necesario analizar cualquier conexión entrante al entorno PCI DSS para evaluar los riesgos de seguridad inherentes a dicha conexión. Hay que tener en cuenta que el hecho de que una red se encuentre separada de otra mediante un cortafuegos no garantiza que una esté totalmente protegida sobre la otra. Por ejemplo, si es posible acceder a la red protegida a través del puerto 22 del cortafuegos desde una red insegura, la red segura podría estar en peligro si en la red potencialmente insegura hubiera *malware* capaz de trasmitirse a través de ese puerto.

Además, cualquier consola o herramienta de administración de componentes de sistema del entorno PCI DSS debe incluirse en el alcance, ya que pueden afectar a la seguridad de los mismos.

Algunas consideraciones a tener en cuenta para una buena segmentación de red:

– Una adecuada autenticación de usuario para acceder al segmento de red seguro.

– Listas de acceso (ACL) debidamente configuradas, definiendo:

- Por defecto a denegación absoluta.
- Permitir acceso a puertos/servicios específicos (no debe usarse "any").
- Desde orígenes concretos (IP's concretas, no rangos).
- A destinos concretos (IP's concretas, no rangos).

– Registro de accesos adecuado.

– Cualquier 'elemento' que traspase los límites del segmento de red seguro debe ser comprobado, ya sean:

- Dispositivos.
- Paquetes.
- Protocolos.
- Aplicaciones.
- Usuarios.

– Además las comprobaciones deben aplicarse tanto al tráfico de entrada como al tráfico de salida.

– No debe permitirse la salida de datos de tarjetas de pago a otro segmento de red que se encuentre fuera del alcance de PCI DSS.

– Políticas de seguridad basadas en la identidad del usuario o la aplicación, para identificar quién tiene acceso a qué datos, no basándose únicamente en direcciones IP, puertos y protocolos.

Ejemplos de **malas prácticas**:

- ***Servidor de correo fuera de segmento de red seguro, pero a veces se envían correos electrónicos con el PAN cifrado.*** Aunque los datos estén cifrados siguen siendo datos, así que tanto el servidor de correo como cualquier otro servidor, equipo o componente de red que se encuentre dentro del mismo segmento de red se consideran dentro del entorno de PCI DSS.
- ***Una aplicación dentro del entorno de PCI DSS permite generar extracciones de datos en ficheros para que el usuario los pueda manipular. Estos ficheros se almacenan en el equipo del empleado o en un servidor de ficheros fuera del alcance de PCI DSS.*** Si estas extracciones de datos contienen el PAN Completo, aunque sea cifrado, el servidor de ficheros, equipo del empleado o cualquier otro dentro de ese segmento de red estará dentro del alcance de PCI DSS.
- ***Una aplicación considerada fuera del alcance de PCI DSS es capaz de conectarse a otra aplicación o servidor dentro del alcance de PCI DSS.*** Si es necesario que la aplicación se conecte al entorno PCI DSS, entonces la aplicación también está dentro del alcance de PCI DSS, así como cualquier otro equipo o componente de red dentro del mismo segmento de red. ■

Marc Segarra López
Director de Consultoría Barcelona
INTERNET SECURITY AUDITORS
msegarra@isecauditors.com