Guía esencial para el cumplimiento de PCI

La seguridad de datos en las transacciones es fundamental para sus usuarios, descubra todo lo que necesita saber sobre PCI.

El Estándar de Datos de Seguridad de la Industria de las Tarjetas de Pago (PCI DSS) se actualizó por última vez en octubre 28 de 2010. Desde entonces hemos visto algunos cambios, incluyendo la política de cumplimiento por parte de VISA hasta la fuerte adopción de nuevas tecnologías como los pagos móviles. ¿Qué significan exactamente estos cambios para el cumplimiento regulatorio?

En esta guía esencial de PCI usted puede entender desde lo más básico de PCI hasta los detalles, nuevas tecnologías y consejos para usar las mejores prácticas en la implementación de PCI 2.0.

Contenido

PCI DSS 2.0

Artículo por: Maggie Sullivan

PCI DSS 2.0 (Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago, versión 2.0) es la segunda versión del Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS). El PCI DSS fue lanzado por primera vez el 26 de octubre de 2010. La tercera revisión está prevista para 2014.

De acuerdo con el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI), la versión 2.0 no introduce cambios importantes en los 12 requisitos. Se introdujeron algunos ajustes lingüísticos menores para aclarar el significado de los requisitos. La versión 2.0 refuerza la necesidad de un profundo alcance antes de una evaluación y promueve una gestión de registro más eficaz. También amplía los requisitos de validación para la evaluación de vulnerabilidades en un entorno comercial. Como resultado, los comerciantes pueden ahora utilizar las mejores prácticas de la industria para priorizar las vulnerabilidades.

Contenido

Los 12 requisitos PCI DSS

Artículo por: Maggie Sullivan

Los 12 requisitos PCI DSS son un conjunto de controles de seguridad que las empresas están obligadas a implementar para proteger los datos de las tarjetas de crédito y cumplir con el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS). Los requisitos han sido desarrollados y mantenidos por el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI).

Cualquier organización que reciba tarjetas de pago, incluyendo tarjetas de débito y crédito, deberá cumplir con los 12 requisitos de forma directa o bien a través de un control de compensación. No obstante, los controles de compensación no siempre se admiten y deben ser aprobados bajo un criterio de caso por caso, por parte de un asesor de seguridad cualificado de la PCI (QSA PCI). El incumplimiento de los 12 requisitos PCI DSS puede derivar en multas o en la finalización de los privilegios de procesamiento de tarjetas de crédito.

He aquí los 12 requisitos PCI DSS:

1. Instalar y mantener una configuración de firewall para proteger los datos de los titulares de tarjetas.

2. No utilizar los valores predeterminados suministrados por el proveedor para las contraseñas del sistema y otros parámetros de seguridad.

3. Proteger los datos almacenados de los titulares de tarjetas.

4. Cifrar la transmisión de los datos de los titulares de tarjetas a través de redes públicas abiertas.

5. Usar y actualizar con regularidad el software antivirus.

6. Desarrollar y mantener sistemas y aplicaciones seguras.

7. Limitar el acceso a los datos de los titulares, únicamente a lo que los negocios necesiten saber.

8. Asignar una identificación única a cada persona con acceso a una computadora.

9. Restringir el acceso físico a los datos de los titulares de tarjetas.

10. Rastrear y monitorear todo acceso a los recursos de la red y a los datos de titulares de tarjetas.

11. Probar con regularidad los sistemas y procesos de seguridad.

12. Mantener una política que aborde la seguridad de la información.

Contenido

Cambios en la política de cumplimiento de Visa PCI: ¿El Final de las evaluaciones PCI?

Artículo por: Mike Chapple

No hace mucho que Visa Inc. ha cambiado su política de evaluación de cumplimiento para el estándar de seguridad de pagos de la industria de tarjetas de crédito (PCI DSS).

Existen numerosos movimientos relacionados que pueden limitar el número de empresas necesarias para cumplir esta evaluación y que puede reducir el tiempo necesario para cumplir con sus requisitos.

En concreto, VISA ha decidido cambiar los criterios de sus clientes, incluyendo la necesidad de procesar el 75% de sus operaciones mediante terminales dotadas de “chip y PIN”, que ya no es un aspecto de esa evaluación PCI. Por desgracia no todos los comerciantes están al tanto del cambio y muy pocos entienden lo que supone para ellos. En este consejo no solo explicamos los cambios y sus implicaciones sino que también vemos las posibilidades con las que las empresas pueden hacer mucho más sencillo el cumplimiento de la PCI.

Contenido

¿El fin de la evaluación PCI?

La “muerte” de la evaluación PCI DSS seguramente sea una buena noticia para muchos profesionales que sentían por este tipo de evaluación el mismo entusiasmo que ante una visita al dentista o a un inspector de Hacienda. Aunque todos apreciamos el celo por una seguridad estricta respecto de los datos sensibles, como los números de tarjeta de crédito, también solemos agotarnos ante los interminables cuestionarios de autoevaluación (SAQS). Para quienes no estén al tanto de los PCI DSS, los comerciantes normalmente tienen que rellenar un SAQ como parte del proceso de validación y evaluación. Para muchos comerciantes, este SAQ se envía y efectúa a través de su banco con todos los requisitos necesarios. Sin embargo, los comerciantes más grandes deben realizar una evaluación en el comercio con un asesor de seguridad PCI cualificado y usar el SAQ para preparar esa visita.

Con el cambio en las políticas de VISA, ¿podemos ver el fin inminente de esa evaluación PCI? Veremos los detalles sobre los cambios realizados por Visa, pero lo que sí debe quedar claro es que el programa PCI DSS desaparecerá tarde o temprano, aunque las evaluaciones SAQs en el comercio seguramente sigan siendo una parte integral del programa en los próximos años. Dicho esto, hay numerosos movimientos relacionados que pueden provocar que los comerciantes no tengan que rellenar más autoevaluaciones al uso y que reducirán el tiempo empleado por aquellos que aun tengan que seguir rellenando esos formularios.

Definiendo claramente el entorno del titular de la tarjeta

El primero de los factores sobre el que las empresas de tarjetas de crédito se han esforzado notablemente es el de reducir el ámbito de sus operaciones con tarjeta de crédito. Cuando apareció el primer PCI DSS allá por 2004, muchos de nosotros protestamos por el tipo de lenguaje incluido en ámbito de cumplimiento que incluía “cualquier componente de red, servidor o aplicación que estuviera conectada con el entorno del titular de la tarjeta”. Después de “mucho llanto y crujir de dientes” por fin pudimos saber exactamente a qué se referían con eso de “conectar con el entorno del titular de la tarjeta”.

Contenido

Durante los últimos años la industria ha pasado de interpretar el idioma como un requisito intimidatorio para incluir prácticamente cualquier aspecto de la computación empresarial dentro de los esfuerzos del cumplimiento de la PCI a ser una oportunidad para crear y gestionar sistemas de pago mucho más seguros. Para hacer las evaluaciones PCI menos dolorosas, muchas empresas ahora segmentan a sus clientes, dejando a un lado a aquellos sistemas que acceden a los datos de la tarjeta de crédito del resto de la red de la empresa y limitando el acceso a estos sistemas al personal que necesite de acceso expreso a esta información sensible.

Esto ha permitido reducir el ámbito de numerosas evaluaciones PCI DSS a un número concreto de sistemas bien definidos. No es algo que reduzca el número de preguntas que la empresa debe responder pero sí limita notablemente los sistemas que quedan obligados a responder a las mismas.

Proceso externo de pagos

Una de las formas más sencillas de reducir dramáticamente el alcance de la PCI es mediante la externalización no solo de los principales componentes de la infraestructura del procesado de tarjetas de crédito, sino de todo el proceso. Al elegir un proveedor de servicio certificado para todo el proceso de gestión de tarjetas de crédito, puede externalizarse el alcance de la prueba. En algunos casos es posible eliminar por completo los datos relativos a las tarjetas del entorno, siempre que aseguremos que nunca vamos a encontrar en el sistema números de tarjeta sin encriptar.

Cuando elegimos un socio para procesar las tarjetas de crédito, debemos considerar solo aquellos proveedores certificados como PCI DSS y controlar su estado de manera que garanticen el cumplimiento de la política durante todo el contrato. Visa ofrece un registro global de proveedores de servicio PCI DSS certificado; cualquier socio potencial debe figurar en esta lista.

La externalización del procesado de tarjetas es una forma de extraer los datos de tarjeta de crédito de los sistemas empresariales y de reducir el número de respuestas a rellenar durante el proceso de cumplimiento PCI DSS. EL punto de partida de esta evaluación es un cuestionario completo --

SAQ D– que contiene, nada menos, 49 páginas de preguntas. Sin embargo, la empresa puede reducir la dimensión del cuestionario si:

- No almacena datos de las tarjetas. En este caso el cuestionario pasa a ser el SAQ C, de "solo" 26 páginas.
- Se traslada a un entorno virtual donde el procesamiento de tarjetas de crédito usa una interfaz web que cumple con las obligaciones del proveedor del servicio. En este caso el formulario es de 23 páginas, el SAQ C-VT.
- Usa solo equipos "imprint" o sistemas sencillos de marcado remoto. Con este planteamiento el comerciante pasa al formulario SAQ B y solo necesita un formulario de 20 páginas.
- Alcanza el auténtico nirvana del PCI DSS y externaliza por completo todo el proceso. No todos pueden hacerlo, pero quienes lo logran disfrutan del formulario SAQ A de 15 páginas.

Externalizar la gestión de tarjetas de crédito fuera de los sistemas de TI y sus componentes puede reducir dramáticamente el tiempo y esfuerzo necesario para cumplimentar el SAQ: cuando se combinan tales esfuerzos para limitar el alcance de los sistemas que deben ser conformes a la PCI es posible reducir notablemente el tiempo empleado en la evaluación de rendimiento.

Usando terminales EMV

Aunque es difícil, es posible eliminar todas las responsabilidades de evaluación PCI DSS. Tanto Visa como Master Card han publicado guías que permiten a los comerciantes utilizar la tecnología de PINC y Chip de Europay, MasterCard y Visa (EMV) para eliminar por completo la necesidad de evaluaciones. Es la forma de estas empresas de fomentar la adopción de estas nuevas tecnologías inteligentes de pago.

Las empresas que cumplan los siguientes criterios pueden solicitar la exención de las evaluaciones PCI DSS:

Contenido

- El 75% de sus operaciones se realizan mediante terminales de chip y PIN (aunque no se requiere un porcentaje equivalente de operaciones realizadas usando chip y PIN).
- Los comerciantes no deben almacenar información sensible.
- Los comerciantes deben segmentar los procesos mediante tarjeta presente y ausente.
- Los comerciantes no deben haber tenido incidencias de pagos durante el último año.
- Los comerciantes deben haber realizado su evaluación PCI en el año anterior.

Es importante destacar que aunque una empresa no cumpla con todos los requisitos de la evaluación todavía es posible cumplir con los requisitos del programa PCI DSS. Por otro lado, aunque Visa y Master Card han acordado poner en marcha este programa en 2012, American Express no empieza a ofrecer el programa hasta octubre de 2013.

Además, se ven buenas nuevas en el horizonte. A medida que los comerciantes se sienten más cómodos con los requisitos PIC DSS y con el ámbito de su entorno, la comunidad PCI está empezando a adoptar planteamientos basados en riesgos que permiten a los comerciantes no verse implicados en actividades de alto riesgo. Por eso está previsto ver más cambios en estos aspectos en el futuro.

Contenido

Combine el procesamiento de pagos móviles y cumpla la normativa PCI

Artículo por: Mike Chapple

Las pequeñas empresas alrededor del mundo están aceptando tarjetas de crédito debido a las nuevas tecnologías que permiten la aceptación de las mismas a través de teléfonos inteligentes y tabletas.

Nuevos proveedores, como Square Inc. y Sail, de VeriFone Inc., proporcionan pequeñas llaves de hardware que se conectan directamente a los dispositivos móviles y proporcionan un procesamiento barato y sencillo de pagos con tarjeta de crédito. Si todavía no ha visto uno de estos

dispositivos en un taxi, en una pequeña tienda o con un comerciante de acera, no pasará mucho tiempo hasta que note la nueva tecnología en uso.

Sin embargo, aunque esta tecnología sea algo tan fascinante y revolucionario, existen algunas ramificaciones que debemos considerar. ¿Qué significa exactamente el uso de esta tecnología para el cumplimiento regulatorio? Eso es lo que vamos a cubrir en este artículo.

PCI sigue siendo vigente; P2PE hace más sencillo el cumplimiento

En primer lugar, el Payment Card Industry Data Security Standard (PCI DSS) todavía se aplica en estas situaciones. Cualquiera que acepte una tarjeta de crédito, independientemente de la tecnología utilizada, debe cumplir con el PCI DSS. Aunque la probabilidad de que los puestos callejeros de perritos calientes estén sujetos a una inspección de PCI DSS es bastante baja, los bancos comerciales solicitarán anualmente la validación del cumplimiento de PCI DSS.

Lo más importante que pueden hacer los comerciantes que están considerando el uso de sistemas de procesamiento de pagos móviles es asegurarse de que utilizan un escáner de tarjetas que esté certificado por el PCI Security Standards Council (SSC), conforme con su cifrado punto-a-punto (P2PE) estándar. Los dispositivos que utilizan P2PE deben asegurarse de que el teléfono inteligente nunca vea la información sensible de la tarjeta de crédito sin cifrarla, lo que haría que el dispositivo no cumpliese el PCI DSS.

Esto es un gran problema, de lo contrario tratar que los teléfonos inteligentes cumplan con el PCI DSS dentro del alcance del sistema de procesamiento de pagos sería muy difícil. El Payment Card Industry Security Standards Council (PCI SSC) publicó un conjunto de requisitos para P2PE, pero aún no ha publicado una lista de productos o fabricantes P2PE validados.

Visite su sitio web para encontrar esa lista en los próximos meses. Algunos podrían considerar posponer el lanzamiento de esta tecnología hasta que la lista se haga pública. De lo contrario, existe un pequeño riesgo de que el

Contenido

equipo tenga que ser reemplazado si el producto inicialmente elegido no es validado con éxito.

Con P2PE, el lector de tarjetas en sí mismo utiliza tecnología de cifrado para proteger los detalles de una transacción con tarjeta de crédito. El número de tarjeta y otro tipo de información sensible se transforman en un mensaje cifrado que no puede ser leído sin la clave secreta. El lector entonces utiliza el teléfono inteligente para transmitir este mensaje cifrado al procesador de la transacción de tarjeta de crédito, el cual posee la clave de descifrado.

La belleza de este enfoque es que ninguno de los puntos de transacción entre el lector de tarjetas y el procesador de transacciones tienen acceso a la información sensible y, por lo tanto, no están sujetos a los rigurosos procedimientos de cumplimiento exigidos por la norma PCI DSS.

Proceso simplificado de validación

Los comerciantes que utilizan dispositivos de cifrado P2PE homologados se alivian de una carga significativa de exigencias de PCI DSS. El Consejo PCI reconoce esto y permite a los comerciantes utilizar un proceso de validación de cumplimiento simplificado si reúnen cuatro requisitos:

1. El comerciante está utilizando un producto P2PE en la lista, que será publicada próximamente, de productos P2PE validados por PCI SSC.

2. El comerciante no almacena, procesa o transmite ninguna información del titular en ningún sistema aparte del producto P2PE validado.

3. El comerciante no almacena datos de titulares de tarjetas en formato electrónico, incluyendo datos de titulares provenientes de sistemas de pago anteriores.

4. El comerciante ha obtenido una copia del manual de instrucciones P2PE PCI SSC (proporcionado por el proveedor) para su producto P2PE específico y conoce todos los requisitos descritos en este manual.

Contenido

Contenido

Los comerciantes que cumplan con estos cuatro requisitos son elegibles para rellenar el Cuestionario de autoevaluación P2PE-HW (SAQ) abreviado. En resumen, esta versión de la SAQ sólo hace preguntas sobre:

• El contenido de las políticas comerciales y los procedimientos relacionados con la retención de datos del titular, respuestas a incidentes, eliminación y almacenamiento seguros de los datos de los tarjetahabientes.

• Aplicación y revisión de las políticas y procedimientos de la organización.

• Uso y almacenamiento de códigos/valores de verificación de tarjeta ("código de seguridad" de tres o cuatro dígitos en el reverso de la tarjeta).

• Enmascaramiento de números de tarjetas de crédito cuando se muestran en papel.

• Prohibir la transmisión de números de tarjetas a través del correo electrónico, de mensajería instantánea y de tecnología de chat.

• Asegurar el soporte físico que contenga información de los tarjetahabientes.

• Entrenamiento del personal sobre concienciación de seguridad.

• Uso de proveedores de servicios.

• Planificación de respuestas a incidentes.

Las siete páginas de preguntas en este SAQ son un alivio en comparación con los largos cuestionarios requeridos para los sistemas más complejos de procesamiento de información de tarjetahabientes.

Conclusión

Los pequeños comerciantes que pueden satisfacer sus necesidades de negocio con los sistemas de pago móviles, encontrarán que su carga de

cumplimiento de exigencias puede reducirse significativamente si utilizan un producto P2PE válido de procesamiento de tarjetas de crédito.

Mediante la eliminación de los datos de la tarjeta del entorno del comerciante, los productos P2PE proporcionan a los clientes un alto grado de seguridad y reducen dramáticamente el riesgo de que un comerciante sea la fuente de una brecha de la seguridad de la información.

Contenido

¿La gestión de contraseñas afecta la conformidad PCI DSS?

Artículo por: Mike Chapple

En términos generales el Estándar de Seguridad de Datos para el Sector de Pagos con Tarjeta (PCI DSS) es el único criterio fundamental que establece requisitos claros sobre seguridad de contraseñas. Estos requisitos se encuentran en el apartado 8 de esa PCI DSS. Las mejores prácticas de seguridad para gestión de contraseñas que indica establecen las siguientes recomendaciones:

- Se prohíbe el uso de contraseñas de grupo, genéricas o compartidas. Algo que no debería sorprender a nadie, ya que es una práctica estándar en cualquier sector. Las contraseñas compartidas desactivan la seguridad de las contraseñas y la individualidad de las cuentas.
- Las contraseñas deben cambiarse cada 90 días como mínimo. Una de las cuestiones más conflictivas de la PCI DSS por las molestias que genera a los usuarios. En muchas empresas que no deben cumplir estos requisitos las contraseñas se cambian cada año o cada semestre. LA PCI DSS es mucho más estricta.
- Las contraseñas deben ser de al menos siete caracteres, con números y letras. Otra práctica de seguridad estándar presente en todas las empresas. No es necesario usar caracteres especiales o signos de puntuación.
- Los usuarios no deben volver a usar ninguna de las cuatro últimas contraseñas. Este requisito establece la prohibición de “reciclar” contraseñas usadas durante el último año.

Contenido

Si está sujeto a las prácticas de PCI DSS entonces todo esto no debe ser nuevo para usted. Los fallos en el cumplimiento de estas reglas le perjudicarán en su próxima auditoria. Y si está trabajando en el cumplimiento de otro estándar diferente que no le ofrezca una orientación concreta, también es un excelente juego de recursos para conocer las mejores prácticas usadas en la empresa actual.

La transparencia en la nube sigue siendo problema para el cumplimiento del PCI DSS, según expertos

Artículo por: Robert Westervelt

La transparencia en la nube sigue siendo el mayor problema a la hora de adoptar servicios basados en la nube, según informa un experto, que afirma que mantener el cumplimiento de PCI en la nube es posible, pero que los comerciantes todavía deben levantar un muro a la hora de obtener visibilidad entre los sistemas y procesos en la nube.

"Se ha hablado mucho sobre la transparencia, pero realmente no se han visto muchos cambios prácticos," afirma Diana Kelley, Socia de la consultora Security Curve de Amherst, New Hampshire.

Asistimos a una asunción lenta de los servicios basados en la nube. Los comerciantes que están moviendo sus sistemas de pago a la nube, o lo están considerando, están esperando la orientación del PCI Security Standards Council (PCI SSC) para asegurarse de que cumplen con las normas PCI durante y después de la transición. Según Kelley se ha logrado cierto progreso. La Alianza de Seguridad en la Nube (CSA), una entidad no lucrativa, está liderando un movimiento para estandarizar la transparencia de las prácticas de seguridad de los proveedores en la nube.

Sin embargo, los proveedores de pagos en la nube siguen obligando a sus clientes a firmar contratos donde la responsabilidad última de los datos de las tarjetas de crédito recae en el comerciante. Sin embargo no proporcionan la visibilidad y documentación necesaria para mantener ese cumplimiento.

Contenido

Muchos servicios basados en la nube se niegan a ser auditados, según Kelley. Las grandes empresas sí pueden forzar a su proveedor en la nube para que acepte una auditoría, pero las pequeñas empresas no. “Si no eres lo suficientemente grande para ellos, no les importa dejarte ir”, afirma Kelley.

La orientación en cumplimientos PCI está copando el gasto en tecnología, según la experta

Aunque no se prevén actualizaciones de PCI DSS hasta finales de 2012, las empresas ya están trabajando en las iniciativas de cumplimiento, según Diana Kelley de Security Curve.

En una entrevista concedida a *SearchSecurity.com*, Kelley explica cómo las empresas están usando los últimos documentos de cumplimiento PCI y por qué el uso de encriptación punto a punto (P2P) y de informes de virtualización puede ayudar eficazmente a los comerciantes a reducir los entornos de gestión de tarjetas de crédito y a purgar los datos de esas tarjetas de sus sistemas.

La PCI DSS no será actualizada hasta finales de 2013. ¿Están las empresas invirtiendo ya en tecnologías relacionadas con el cumplimiento de las PCI?

Diana Kelley: De momento tenemos una PCI DSS, y aunque se actualiza en ciclos de tres años, ya está empleando cierta tecnología emergente. Algunas cuestiones que merecen cierta priorización están siendo gestionadas a través de grupos especiales de interés (SIGs) y requieren de orientación por separado. En este punto da igual que se publique algo por separado de la PCI DDS, pero creo que sí estarán muy relacionadas. Es posible echar un vistazo a las orientaciones, tenerlas en cuenta y hacerlas parte del programa global de cumplimiento de PCI pero todavía tienen que cumplir con la PCI DSS. Por eso se ven como un paraguas general.

Algunas de estas organizaciones de tecnología emergente están priorizando áreas como la virtualización. Existe una guía separada que trata concretamente de los avances en el último año sobre virtualización. Todo sobre la nube. La nube va a ser la estrella de este año. La “tokenizacion” es

Contenido

otro ejemplo de esas tecnologías emergentes insertadas dentro del CDE (Entorno de gestión de tarjetas) que no figura en concreto en el PCI DSS.

Hablemos del cumplimiento de la PCI en la nube. ¿Hay problemas de arquitectura a la hora de adoptar soluciones en la nube por parte de los comerciantes?

Kelley: Sí y no. Sabemos que hay tres modelos de arquitectura en la nube: infraestructura, plataforma y uso de software como servicio (SaaS). Cuando vemos cómo está adoptando la gente la PCI, vemos que la mayoría usa el software como si usaran una puerta de acceso. Con este modelo concreto, si usted es el proveedor de esa puerta de enlace, se preocupa del cumplimiento PCI DSS, está certificado y entiende las necesidades reales –y por supuesto no almacena datos de tarjetas– puede ser algo muy beneficioso, especialmente para las pequeñas empresas e incluso para algunas grandes. Estamos reduciendo el ámbito de lo que se necesita para cumplir con PCI. Si no almacena datos de tarjetas y tampoco las gestiona entonces no tiene más que demostrar qué es lo que ocurre con los datos de las tarjetas cuando acceden al proveedor de pagos y probar que ese proveedor de pagos está trabajando tal como indica el acuerdo. Cuando lo que usamos es un software propio de pagos, como Plataforma de Servicios (PaaS) o mediante infraestructura (IaaS), entonces las cosas cambian un poco.

Si está usando algo similar a una infraestructura, entonces usted es responsable de la protección de los datos y configuración, de cómo los datos se usan en esta infraestructura y de ver que toda la gestión sea segura. Pero quizá tampoco tenga demasiado control sobre lo que necesita saber para ver si todo se hace correctamente. En los entornos en la nube no se permiten las auditorías y es posible que no disponga de toda la información de acceso necesaria. Así que surge un poco de confusión…Tampoco existe una gran transparencia a la hora de enfrentarse a los problemas que surgen y a poder entender cómo funciona esa nube ya que el proveedor afirma: “es mi centro de datos”. Así que ¿hasta qué punto podemos ser capaces de saber qué es lo que está pasando?

Contenido

El 30 de junio la PCI DSS 6.2 se convierte en un requisito. Requiere la creación de un proceso para asignar un nivel de riesgo a las vulnerabilidades recientemente descubiertas. ¿Puede comentarnos algo al respecto?

Kelley: Es algo significativo a la hora de actuar y evaluar vulnerabilidades para lograr entenderlas mejor. En el sistema de parcheo de vulnerabilidades anterior del PCI DSS tenías 30 días para hacerlo. Ahora te dicen que tienes que hacer una evaluación de riesgos, priorizar los parches e instalarlos en cierto tiempo. Por eso es necesario estar al tanto de que vulnerabilidades hablamos y tener la información sobre las mismas. Es necesario aceptar esa fuente de información. Puede ser mediante información pública o de los propios fabricantes que gestionan vulnerabilidades [proporcionado una lista de fuentes de información]. Esto es algo que las empresas pueden hacer y deberían implementar. El cambio es que ahora la gestión de vulnerabilidades se realiza por completo sobre la PCI. Las empresas ya lo veían venir: lo estaban haciendo y estaban preparados para ello

Se han emitido gran cantidad de documentos orientativos. El mensaje principal parece ser una reducción en el ámbito de actuación. ¿Es correcto?

Kelley: Uno de los aspectos fundamentales es como poder reducir el ámbito y mejorar las funciones de protección. Si vemos la encriptación de punto a punto, permite encriptar los datos desde el inicio sin tener que preocuparnos ya que los puntos salen encriptados desde el punto de venta así se transmiten hasta el punto de gestión donde el CDE (entorno de gestión de datos de tarjetas) comienza. No es necesario tener el CDE en todas partes cuando tienes solo un punto de venta. Es algo que ha dado varios problemas. Algunas brechas de seguridad han estado relacionadas con los terminales de punto de venta WiFi, a pie de tienda, cuando transferimos los datos a través del aire; puede haber alguien capaz de robarlos.

Las orientaciones para la encriptación de punto a punto parecen tener un lenguaje interesado. En el documento se afirma que “el comerciante

Contenido

debería actuar junto con el banco." ¿Es un nuevo mensaje desde la junta?

Kelley: Creo que puede ser un mensaje bastante directo desde la junta. Realmente no es algo nuevo para el mundo PCI, ya que se nos lleva diciendo desde hace mucho tiempo. He hablado con muchos QSA y analistas que ofrecían mensajes parecidos desde hace mucho tiempo. La razón es que pronto llegaremos a un punto en que queramos desempatar la cuestión. Un punto en el que las personas, de forma razonable, no estén conformes con los procesos de cumplimiento de la certificación. ¿Y entonces quien resuelve ese desacuerdo? Si no se expresa de forma clara en el DSS todo lo que está escrito queda abierto a interpretación. La junta hace todo lo que puede por ser clara en el lenguaje. Los programas de cumplimiento, sin embargo, siguen estando en manos de solo cinco empresas de tarjetas. Son quienes tienen el mando pero sin embargo no quieren implicarse. Así que muchas veces vuelcan la responsabilidad en el banco. Que la entidad quiera ser juez, o no, es otra cuestión.

Contenido

¿Qué hace único a TechTarget?

TechTarget se enfoca específicamente en el segmento de TI empresarial. Nuestro equipo de editores y nuestra red de expertos en la industria proveen el contenido más relevante e importante para los profesionales y administradores de TI. Balanceamos las comunicaciones en línea con las oportunidades de contacto en persona, para permitirle hacer contactos en eventos presenciales y virtuales, y para que pueda tener la capacidad de interactuar con compañeros, todo esto con el fin de crear información valiosa y relevante para los profesionales de TI en todas las industrias y mercados.