Security Standards Council™

Norma: Normas de Seguridad de Datos (DSS)
Requisito: 11.3
Fecha: marzo de 2008

Suplemento informativo: requisito 11.3 sobre pruebas de penetración

Fecha de publicación: 2008-04-15

Descripción general

El requisito 11.3 de PCI DSS aborda las pruebas de penetración, a diferencia del requisito 11.2 de PCI DSS, que aborda las evaluaciones de vulnerabilidades internas y externas. Una evaluación de vulnerabilidades simplemente identifica y notifica las vulnerabilidades detectadas, mientras que una prueba de penetración intenta explotar las vulnerabilidades para determinar la posibilidad de que ocurra un acceso no autorizado u otra actividad maliciosa. Las pruebas de penetración deben incluir pruebas de la capa de aplicación y la capa de red, además de los controles y los procesos de las redes y las aplicaciones, y deben realizarse tanto desde el exterior de la red (pruebas externas) como desde el interior de la red.

Quién realiza las pruebas de penetración

Las normas PCI DSS no requieren que un Asesor Certificado de Seguridad (QSA) o un Proveedor Aprobado de Escaneo (ASV) realicen las pruebas de penetración; estas pueden ser realizadas por un recurso interno calificado o por un tercero calificado. Si se utilizan recursos internos para llevar a cabo las pruebas de penetración, esos recursos deben contar con experiencia en el área. Los individuos que realicen las pruebas de penetración deben estar separados, desde el punto de vista organizativo, de la administración del entorno que se está evaluando. Por ejemplo, el administrador del firewall no debe realizar la prueba de penetración del firewall.

Elaboración de informes y documentación

Se recomienda documentar tanto las metodologías de las pruebas de penetración como sus resultados. Las normas PCI SSC no cuentan con requisitos de elaboración de informes respecto a las pruebas de penetración; sin embargo, se deben conservar los resultados para realizar un seguimiento de los problemas identificados y como evidencia para aquellos que realicen la evaluación de PCI DSS.

Alcance

Las pruebas de penetración abarcan el entorno de datos de los titulares de tarjetas de crédito y todos los sistemas y todas las redes conectados a él. Si existe segmentación de red, de modo que el entorno de datos de los titulares de tarjetas de créditos está separado del resto de los sistemas, y dicha segmentación ha sido verificada en la evaluación de PCI DSS, el alcance de las pruebas de penetración puede limitarse al entorno de datos de titulares de tarjetas de crédito.

Frecuencia

Las pruebas de penetración deben realizarse, como mínimo, una vez al año y cada vez que haya actualizaciones o modificaciones importantes de las aplicaciones o la infraestructura (por ejemplo, instalaciones de nuevos componentes en el sistema, incorporación de una subred o incorporación de un servidor web). Aquello considerado como “importante” depende en gran medida de la configuración de un entorno determinado y no puede ser definido por PCI SSC. Si la actualización o modificación puede afectar los datos de los titulares de tarjetas de crédito, o permitir el acceso a ellos, debe considerarse importante. La importancia dentro de una red altamente segmentada

en donde los datos de los titulares de tarjetas de crédito están claramente separados de otros datos y otras funciones es muy diferente de la importancia dentro de una red simple en donde todas las personas y todos los dispositivos pueden acceder a los datos de los titulares de tarjetas de crédito. Como una mejor práctica de seguridad, todas las actualizaciones y modificaciones deben ser sometidas a pruebas de penetración para garantizar que los controles existentes sigan funcionando con eficacia después de implementarlas.

Preparación

Hay varias metodologías que se pueden utilizar para realizar las pruebas de penetración. La primera decisión que debe tomarse es cuánto conocimiento tiene la persona que realiza la prueba sobre el sistema que se está evaluando. Cuando no se cuenta con conocimiento previo, las pruebas se conocen como “pruebas de caja negra”, en donde la persona que realiza la prueba debe identificar la ubicación de los sistemas antes de intentar probarlos. Cuando se cuenta con conocimiento explícito previo, las pruebas se conocen como “pruebas de caja blanca”.

Si se establece que sería beneficioso para la persona que realiza la prueba tener conocimiento previo, hay varios puntos exigidos por otros requisitos de PCI DSS que brindan información que se puede utilizar. Entre estos puntos, se incluyen:

- El diagrama de una red (1.1.2).
- Los resultados de una revisión realizada por un QSA o de un Cuestionario de Autoevaluación (SAQ).
- Las pruebas anuales de controles para identificar vulnerabilidades y detener acceso no autorizado (11.1).
- Los resultados de análisis trimestrales de vulnerabilidades internas y externas (11.2).
- Los resultados de las últimas pruebas de penetración (11.3).
- La identificación anual de amenazas y vulnerabilidades que derivan en una evaluación de riesgos (12.1.2).
- La revisión anual de políticas de seguridad (las políticas que deben actualizarse pueden identificar nuevos riesgos en una organización) (12.1.3).

Se debe evaluar la documentación relacionada con todo lo antes mencionado y se debe considerar la inclusión de las amenazas y las vulnerabilidades consideradas como parte de los procesos de evaluación normales.

Metodología

Una vez que las amenazas y las vulnerabilidades hayan sido evaluadas, diseñe las pruebas para abordar los riesgos identificados en el entorno. Las pruebas de penetración deben adaptarse a la complejidad y al tamaño de una organización. Se deben incluir todas las ubicaciones de los datos de los titulares de tarjetas de crédito, todas las aplicaciones clave que almacenan, procesan o transmiten dichos datos, todas la conexiones de red clave y todos los puntos de acceso clave. Las pruebas de penetración deben intentar explotar las vulnerabilidades y las debilidades del entorno de los datos de

titulares de tarjetas de crédito, que intentan penetrar tanto en el nivel de la red como en el de las aplicaciones clave. El objetivo de las pruebas de penetración es determinar si se puede lograr el acceso no autorizado a los sistemas y archivos clave. Si esto es posible, se deben corregir las vulnerabilidades y se deben volver a realizar las pruebas de penetración hasta que salgan perfectas y ya no permitan el acceso no autorizado ni otro tipo de actividad maliciosa.

Componentes

Considere la posibilidad de incluir todas estas técnicas para las pruebas de penetración (entre otras) en la metodología, como ingeniería social y explotación de vulnerabilidades expuestas, controles de acceso en sistemas y archivos clave, aplicaciones web, aplicaciones personalizadas y conexiones inalámbricas.

Consideraciones importantes

- Respecto al cumplimiento de PCI, las pruebas de vulnerabilidades o configuraciones erróneas que pueden provocar ataques de negación de servicio contra la disponibilidad de recursos (redes/servidores) no deben tenerse en cuenta en las pruebas de penetración, ya que estas vulnerabilidades no pondrán en peligro los datos de los titulares de tarjetas de crédito.
- Se deben comunicar el tiempo y el alcance de las pruebas de penetración a todas las partes afectadas en la organización.
- Se deben realizar pruebas de acuerdo con los procesos críticos de la empresa, incluidos el control de cambios, la continuidad de la actividad empresarial y la recuperación después de un desastre.
- Se deben realizar todas las pruebas de penetración durante el período de mantenimiento monitorizado.

Acerca del PCI Security Standards Council (Consejo sobre Normas de Seguridad de la Industria de Tarjetas de Pago)

El objetivo del PCI Security Standards Council es mejorar la seguridad de las cuentas de pago impulsando la educación y la concienciación sobre las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago y otras normas que aumentan la seguridad de los datos de pago.

El PCI Security Standards Council fue creado por las principales marcas de tarjetas de pago, American Express, Discover Financial Services, JCB International, MasterCard Worldwide y Visa Inc., con el fin de proporcionar un foro transparente en el cual todas las partes interesadas pudieran proporcionar información sobre el desarrollo, la mejora y la difusión continuos de las Normas de Seguridad de Datos de la Industria de las Tarjetas de Pago (PCI DSS), los requisitos de seguridad para los Dispositivos de Entrada de PIN (PED) y las Normas de Seguridad de Datos para las Aplicaciones de Pago (PA-DSS). Los comerciantes, los bancos, los procesadores y los proveedores de puntos de venta son alentados a asociarse como organizaciones participantes.