INFORME OFICIAL | DICIEMBRE DE 2015

Abordar el cumplimiento de la PCI

A través de la administración de accesos con privilegios

ca technologies

Resumen ejecutivo

Reto

Las organizaciones que gestionan transacciones que involucran tarjetas de crédito o débito se están enfrentando a crecientes presiones para cumplir con los mandatos de cumplimiento normativo. En particular, deben cumplir con la Norma de seguridad de datos del sector de las tarjetas de pago (PCI DSS) versión 3, que entró en vigor en enero de 2015.[1] PCI DSS v3 estableció diversos requisitos para proteger los sistemas y las redes importantes de una organización, incluido el Entorno de datos de titulares de tarjetas (CDE). Con requisitos para el control estricto de autenticación y acceso al CDE, las organizaciones están desafiadas por las difíciles tareas de implementar autenticación de diversos factores, control de acceso y generación de reportes o prácticas sobre actividades, particularmente para el acceso administrativo o con privilegios de estos sistemas.

Oportunidad

Los requisitos de PDI DSS que pertenecen a la administración de accesos con privilegios indican los riesgos asociados con el uso incorrecto de las cuentas con privilegios y el acceso que proporcionan a activos empresariales críticos. Casi todos los incidentes de seguridad recientes señalan a las credenciales o los usuarios con privilegios como un vector de ataque principal en la ejecución exitosa de una brecha. Una estrategia eficaz de administración de accesos con privilegios le permite a una organización restringir, registrar y monitorear todas las actividades realizadas por cuentas con privilegios, como administradores de bases de datos, sistemas y redes. Como resultado, obtienen mayor control y visibilidad sobre los usuarios con privilegios y su acceso de “superusuario” a los elementos más valiosos de la empresas. Sin esto, muchas organizaciones no solo luchan por cumplir con los requisitos de control de acceso, autenticación e identificación de PCI DSS v3, sino que también no logran minimizar su exposición de riesgos a brechas y ataques.

Beneficios

Una estrategia de defensa exhaustiva para la administración de accesos con privilegios entregada en una solución fácil de implementar, como CA Privileged Access Manager, puede ayudar a las organizaciones a abordar los requisitos de PCI DSS v3 y proteger mejor no solo sus CDE sino también su empresa de TI híbrida completa, que abarca redes, servidores, entornos virtuales y en la nube. Como resultado, las organizaciones obtienen mayor seguridad para protegerse de brechas y reducen los riesgos de infracciones o fallas en el cumplimiento de PCI DSS.

Sección 1:

La necesidad de contar con administración de accesos con privilegios

La necesidad de contar con administración de accesos con privilegios nunca ha sido mayor. En numerosos estudios se han mostrado las fallas sistemáticas de las defensas de seguridad tradicionales. Algunos incluso sugieren que casi todas las organizaciones corrieron riesgo al menos alguna vez.[2] Los medios informan con regularidad importantes brechas de datos, como la brecha de Target a finales de 2013, la brecha de Home Depot en 2014 y la brecha de la Oficina de administración de personal en 2015, que involucran credenciales robadas utilizadas por terceros. De hecho, el reporte de investigaciones sobre la brecha de datos de Verizon 2014 citó el uso de credenciales robadas como la principal amenaza de las organizaciones.[3]

Las organizaciones a menudo ignoran los peligros planteados por sus cuentas con privilegios y la gran cantidad de cuentas con privilegios que pueden tener. Las cuentas con privilegios no solo son utilizadas por los empleados de una organización, sino también por terceros como proveedores, contratistas y otros que realizan soporte técnico para sistemas, dispositivos de red y aplicaciones. Una única empresa podría tener miles o incluso decenas de miles de cuentas con privilegios, las cuales plantean su propio riesgo de seguridad a la organización.

La idea detrás de la administración de accesos con privilegios es proporcionar mayor control y visibilidad para las acciones del administrador. El modelo tradicional se ha diseñado para confiar completamente en todos los administradores, pero este punto de vista ingenuo pasa por alto dos grandes problemas: la posibilidad que un administrador disgustado se convierta en una amenaza interna y las consecuencias de una cuenta administrativa puesta en peligro por un atacante externo, especialmente cuando el administrador en cuestión es un proveedor o un tercero.

Una manera de superarlo es mediante la adopción de un modelo de “confianza cero”, una estrategia que CA Privileged Access Manager (anteriormente Xceedium Xsuite), un componente clave de las soluciones de administración de accesos con privilegios de CA Technologies, adopta donde no se supone una confianza plena en los administradores. Con este modelo, se reducirá la cantidad de brechas y la gravedad de las brechas que aún ocurren. Los requisitos de PCI DSS reflejan este modelo de confianza cero en cierta medida, como el Requisito 7.1.2 “Restringir el acceso de los Id. de usuarios con privilegios a la menor cantidad de privilegios necesaria para realizar las responsabilidades laborales”.

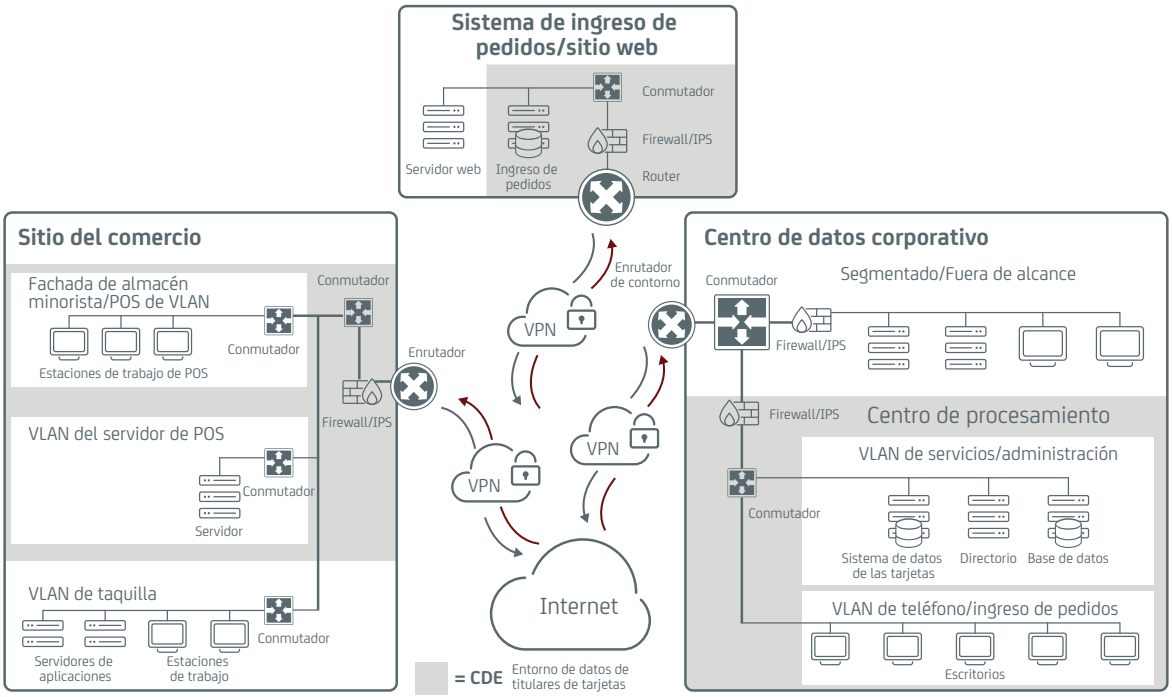
Sin embargo, aunque el cumplimiento de PCI proporciona una base sólida para la protección de CDE, solo “marcar la casilla” y cumplir únicamente los requisitos mínimos no es una defensa suficiente para las amenazas actuales. La administración de accesos con privilegios va más allá de los requisitos de PCI para proteger de mejor manera el CDE de una organización.

Además de lograr el cumplimiento de PCI, otros motivos principales por los que se necesita la administración de accesos con privilegios incluyen: interrumpir la cadena de ataque, mitigar amenazas internas, registrar y monitorear comandos y eliminar contraseñas preprogramadas.

Ilustración A:

El alcance de los requisitos de PCI DSS

PCI DSS v3 requiere medidas para proteger el Entorno de datos de titulares de tarjetas (CDE).



Cómo interrumpir la cadena de ataque

El concepto básico de una cadena de ataque es que un atacante sigue un patrón repetitivo para obtener acceso a un sistema (o ampliar ese acceso) y aumentar los privilegios. Esos privilegios se utilizan luego para obtener acceso a otro sistema o ampliar el acceso existente, aumentar los privilegios nuevamente y continuar esta cadena de explotación hasta que se alcanza el objetivo final. Si esta cadena de explotación puede romperse en cualquier punto del ciclo, el ataque puede detenerse antes de que alcance su objetivo final.

CA Privileged Access Manager proporciona las capacidades que ayudan a interrumpir la cadena de ataques. Por ejemplo, CA Privileged Access Manager es compatible con la autenticación de diversos factores para las cuentas con privilegios, lo que hace que ponerlas en peligro sea mucho más difícil ya que un atacante necesita poner en peligro diversas credenciales para una única cuenta. También, el uso de privilegios mínimos cuando se trata de cuáles son los comandos que cada cuenta con privilegios puede emitir en cada componente de CDE reduce el acceso a información confidencial, lo que dificulta aún más que un atacante obtenga acceso no autorizado a datos de interés.

Otra manera en que CA Privileged Access Manager ayuda a interrumpir la cadena de ataque es el respaldo de la segmentación de redes. Esto limita cuáles son las subredes a las que una cuenta con privilegios particular puede acceder y cuáles son los sistemas de cada subred que pueden ser administrados. La segmentación de redes ayuda a limitar la propagación lateral de ataques de un sistema a otro, y también a restringir la visibilidad que un atacante tiene de la red de la organización. De manera similar, CA Privileged Access Manager ofrece un agente de filtro de socket (SFA), que previene que un administrador abra una conexión de red no autorizada en otro sistema, como intentar un comando SSH o Telnet con un host no autorizado por las políticas de CA Privileged Access Manager.

Todas estas capacidades de CA Privileged Access Manager están recomendadas específicamente por fuentes como Mandiant para reducir el fraude de tarjetas de crédito.[4]

Cómo mitigar las amenazas internas

Aunque los requisitos de PCI se centran en los atacantes externos, también pueden reconocer la importancia de amenazas internas que son un problema apremiante para las organizaciones de la actualidad. Un estudio indicó que más del 10 por ciento de los empleados había robado la información de su empleador con ánimo de lucro o conocían a alguien que lo había hecho.[5]

CA Privileged Access Manager ayuda a mitigar las amenazas internas en diversas maneras. En primer lugar, su implementación de principios de privilegios mínimos limita estrictamente los comandos que una persona dentro del sistema puede emitir y sobre cuáles componentes de CDE dichos comandos pueden ser emitidos. Esto, en efecto, minimiza el daño que puede causar una persona dentro del sistema. En segundo lugar, el registro y monitoreo de todas las actividades de cuentas con privilegios proporcionan un documento detallado de todos los comandos emitidos, que permite la rastreabilidad de una persona en particular, no un Id. genérico (compartido).

Comandos de registro y monitoreo

Independientemente de la solidez de los controles de seguridad, siempre habrá debilidades; por esto, las brechas son inevitables en todos los entornos. Debido a que CA Privileged Access Manager registra y monitoreo todas las actividades involucradas en las cuentas con privilegios, simplifica considerablemente los procesos forenses para determinar lo que hizo un atacante exitoso mediante el uso de credenciales administrativas no autorizadas.

Cómo eliminar contraseñas preprogramadas

Muchos desarrolladores de software, administradores y otros han aplicado durante mucho tiempo la práctica de contraseñas preprogramadas en scripts, códigos fuente y en otros lugares. Esta es una gran vulnerabilidad ya que los desarrollares de software, evaluadores y otros pueden acceder a estas contraseñas, y los atacantes saben cómo buscarlas cuando se infiltran en un sistema con el fin de poder usarlas para obtener acceso a otros sistemas, como bases de datos de titulares de tarjetas. CA Privileged Access Manager proporciona capacidades de autenticación entre aplicaciones que eliminan la necesidad de contraseñas preprogramadas.

Sección 2:

Cómo la administración de accesos con privilegios puede ayudar a cumplir con PCI

Como analizamos anteriormente, la administración de accesos con privilegios es una parte fundamental para abordar el cumplimiento de PCI. No se puede cumplir simplemente con una gran cantidad de requisitos de PCI en entornos empresariales típicos sin emplear una solución de administración de accesos con privilegios. Por ejemplo, un minorista grande se estaba enfrentando a $100 000 por mes de multas debido a su incumplimiento de los requisitos de PCI para el control de acceso, identificación y autenticación. Al agregar CA Privileged Access Manager a su cartera de soluciones de seguridad, el minorista pudo cumplir con los requisitos faltantes y evitó recibir más multas.

CA Privileged Access Manager aborda cada uno de los siguientes requisitos de PCI.[6]

Requisito 2: No utilizar las opciones predeterminadas suministradas por el proveedor respecto de contraseñas de sistemas ni de otros parámetros de seguridad.

CA Privileged Access Manager aborda este requisito de dos maneras. En primer lugar, cuando se utiliza durante la implementación del sistema, puede tomar control de cuentas predeterminadas con privilegios y ordenar que se restablezcan todas las contraseñas predeterminadas para estas cuentas. En segundo lugar, limita los protocolos que pueden usarse para el acceso administrativo remoto, como SSH o SSL/TLS. Esto previene el uso de la administración del sistema en redes que usan protocolos no seguros.

Requisito 6: Desarrollar y mantener aplicaciones y sistemas seguros.

Una parte importante de este requisito es el manejo adecuado de credenciales y la separación de tareas en los entornos de desarrollo, prueba y producción. CA Privileged Access Manager aplica el control de acceso basado en roles para las cuentas con privilegios de todos estos entornos, respaldando la separación de tareas mientras facilita la eliminación simple de cuentas de desarrollo, prueba y otros tipos de cuentas que ya no se necesitan cuando se implementa un sistema o una aplicación.

Requisito 7: Restringir el acceso a los datos de los titulares de tarjeta tomando como base la necesidad de conocer la información.

CA Privileged Access Manager permite que las organizaciones implementen el principio de privilegios mínimos para el acceso con privilegios, un área ignorada con frecuencia. Específicamente, el modelo de confianza cero de CA Privileged Access Manager aplica control de acceso detallado para los usuarios individuales con privilegios o para los grupos de dichos usuarios (por ejemplo, administradores de bases de datos). Esto limita los componentes del sistema a los que cada usuario o grupo con privilegios puede acceder (servidores, dispositivos de red y aplicaciones) y los comandos que cada usuario o grupo con privilegios puede ejecutar en cada uno de estos componentes. CA Privileged Access Manager puede integrar Active Directory, LDAP y otros directorios empresariales para volver a utilizar sus definiciones de grupo y roles.

Requisito 8: Identificar y autenticar el acceso a componentes del sistema.

Casi todas las partes del Requisito 8 están respaldadas explícitamente por CA Privileged Access Manager. CA Privileged Access Manager requiere un Id. único para cada usuario con privilegios, proporciona todas las características de la administración de contraseña estándar y respalda una gran variedad de tecnologías de autenticación con un único factor y con diversos factores. Específicamente, CA Privileged Access Manager respalda el Requisito 8 de la siguiente manera:

- **8.1:** La administración de accesos con privilegios de CA proporciona una autenticación única para cada usuario con privilegios, incluso cuando las organizaciones utilizan “cuentas compartidas” para ciertos componentes de infraestructura, como los enrutadores. Aplica la separación de tareas entre los usuarios con privilegios. Proporciona características estándar para finalizar inmediatamente los privilegios de acceso revocados, deshabilitar las cuentas con privilegios inactivas y aplicar políticas de bloqueo para los intentos fallidos de autenticación y políticas de reautenticación para las sesiones inactivas.
- **8.2:** Se integra con diversos métodos de autenticación, solicitando la autenticación de todos los usuarios con privilegios. Almacena contraseñas y otras credenciales (por ejemplo, claves criptográficas privadas) en un almacén fuertemente cifrado y las transmite solo a través de canales cifrados. Aplica políticas de reutilización, caducidad, seguridad y longitud de contraseñas estándar.
- **8.3:** Respalda varios métodos de autenticación de diversos factores, RADIUS, certificados X.509 y tarjetas inteligentes.
- **8.5, 8.6:** Permite que las organizaciones usen “cuentas compartidas” detrás de escena mientras requieren que cada usuario con privilegios, incluidos terceros, se identifique y autentifique de manera única. Esta identificación única incluye el uso de tarjetas inteligentes, certificados digitales, tokens criptográficos y otras formas de credenciales que no están relacionadas a contraseñas.
- **8.7:** Limita el acceso directo a la base de datos de los titulares de tarjetas solo a los administradores de la base de datos autorizados. Ofrece compatibilidad entre aplicaciones para garantizar que los individuos no puedan acceder o volver a usar credenciales de la aplicación.

Requisito 10: Monitorear y hacer un seguimiento de todo acceso a los recursos de red y los datos de titulares de tarjetas.

Como el Requisito 8, CA Privileged Access Manager respalda casi todas las partes del Requisito 10. CA Privileged Access Manager registra y guarda todas las actividades realizadas con cada cuenta con privilegios. Esto incluye los documentos de auditoría con formato de registro de sistema y las grabaciones similares a DVR de las sesiones del administrador,

con etiquetas en las grabaciones que indican posibles incumplimientos a la política para acelerar la revisión. CA Privileged Access Manager respalda el Requisito 10 de la siguiente manera:

- **10.1:** CA Privileged Access Manager vincula cada instancia de acceso con privilegios a una persona específica. Le otorga pistas de auditoría a cada persona para el acceso con privilegios a todos los componentes del sistema.
- **10.2:** Usa registro nativo y registro de sistema para generar pistas de auditoría automatizadas que registren cada acción que cada usuario con privilegios realiza en los servidores, dispositivos de red, bases de datos y otras aplicaciones. Incluye todas las actividades de identificación y autenticación para las cuentas con privilegios. Limita el acceso a pistas de auditoría para que únicamente los usuarios autorizados puedan revisarlas y registra todas las revisiones.
- **10.3:** Registra todos los campos obligatorios de PCI para cada evento registrado, incluidos autenticación del usuario, tipo de evento, fecha y hora, éxito o falla, origen del evento e identidad de los recursos afectados (nombre de host, etc.).
- **10.4:** Usa tecnología de sincronización de hora (es decir, Protocolo de tiempo de red [NTP]) para realizar una sincronización de hora.
- **10.5:** Usa técnicas de hashing para identificar alteraciones en los registros y grabaciones de auditoría. Proporciona redireccionamiento de registro de sistema para realizar copias de seguridad de los registros en un almacenamiento de registros centralizado.
- **10.7:** Usa registro de sistema y respalda el redireccionamiento de registro de sistema para que los registros de auditoría puedan mantenerse durante el tiempo que se desee.

Requisito 12: Mantener, para todo el personal, una política que aborde la seguridad de la información.

CA Privileged Access Manager permite la captura y aplicación de políticas de usuarios con privilegios.
CA Privileged Access Manager también registra todos los intentos de infracciones a las políticas, que son aportes naturales a un proceso de evaluación de riesgos.

Proteger el CDE: Desde una perspectiva del control del servidor

La administración de accesos con privilegios de CA Technologies también aborda requisitos adicionales para el control de acceso localizado y muy detallado en el host para proteger más los recursos de alto valor, incluido el CDE. El control del servidor de CA Privileged Access Manager proporciona una importante capa adicional de protección de seguridad en las plataformas del servidor, lo que permite el control de acceso detallado, la administración basada en políticas y la auditoría segura fundamental para proteger los activos electrónicos. Las políticas de acceso pueden diseñarse para regular el acceso a recursos del servidor, programas, archivos y procesos mediante el uso de una variedad de criterios.

Sección 3:

Cambios de PCI DSS v2 a v3

Cuando se actualizó PCI DSS de la v2 a v3, se agregaron protecciones significantes para el CDE, incluido lo siguiente:

- Implementar segmentación de red para el CDE con el fin de aislar mejor las porciones del CDE. Esto incluye garantizar que se registren todos los flujos de datos de los componentes del sistema y auditar todas las actividades realizadas por usuarios con privilegios.
- Realizar una prueba de penetración de perímetro de CDE.
- Administrar las credenciales e implementar el control de acceso de privilegios mínimos y auditoría para todos los accesos de CDE.
- Reforzar los controles de seguridad para los proveedores de servicio.[7]

Estas protecciones destacan la necesidad de tener una solución de administración de accesos con privilegios como CA Privileged Access Manager para proteger al CDE y abordar los requisitos de PCI. Para la mayoría de entornos, la administración de accesos con privilegios es la única manera de implementar de manera eficaz el principio de privilegios mínimos para el control de acceso de nivel de administrador y el registro granular de las actividades del administrador. Además, la administración de accesos con privilegios puede ser valiosa para implementar la segmentación de red y monitorear todas las actividades que involucran flujos de datos entre los segmentos de red.

La actualización de PCI DSS contenía otros cambios relacionados con la administración de accesos con privilegios. Principalmente, el Requisito 8 sobre identificación y autenticación se reestructuró en gran medida, por lo que a primera vista parece que el requisito se cambió de forma masiva. Sin embargo, los cambios involucraron fundamentalmente una reestructuración del requisito.

El cambio más importante es la adición del Requisito 8.6. "Cuando se usan mecanismos de autenticación diferentes a las contraseñas, como tokens criptográficos o tarjetas inteligentes, el mecanismo de autenticación solo debe estar disponible para un usuario; no se permiten los mecanismos de autenticación compartidos". CA Privileged Access Manager aborda este nuevo requisito de la manera que analizamos en la sección anterior.

Sección 4:

Beneficios

Las organizaciones que implementan soluciones de administración de accesos con privilegios obtienen un mayor nivel de seguridad, menor riesgo de amenazas internas y externas, y mejor cumplimiento con las regulaciones, incluida PCI DSS.

Más específicamente, CA Privileged Access Manager puede ayudar a las organizaciones de las siguientes maneras, no solo para abordar el cumplimiento con PCI DSS, sino también para mejorar su postura de seguridad general de la manera más rentable:

- **Reducción de los costos.** CA Privileged Access Manager puede ayudar a reducir considerablemente el costo de las auditorías de PCI DSS, especialmente al proporcionar una manera simple y rentable de segmentar lógicamente la red de una organización. Es un dispositivo similar a proxy que funciona en la capa de la aplicación de la red y controla los usuarios con privilegios que pueden acceder a los sistemas. La segmentación lógica del plano de administración permite que las organizaciones mantengan topologías de la red física existente mientras segregan sistemas con los datos de los titulares de tarjetas en islas cuyo acceso está estrictamente controlado. Con esta estrategia, CA Privileged Access Manager permite que las organizaciones aíslen sistemas de manera lógica con datos de titulares de tarjetas, y de este modo limita el alcance de las auditorías de PCI sin incurrir en el elevado costo requerido para segmentar de manera física las redes.
- **Seguridad mejorada.** La estrategia de defensa exhaustiva de CA Privileged Access Manager para la seguridad ayuda a las empresas a implementar un conjunto exhaustivo de controles para reducir los riegos de los usuarios con privilegios y proporcionar mayor protección ante amenazas externas, lo que permite prevenir que sucedan brechas o minimizar su impacto.
- **Administración y respuesta de protección más rápida.** La facilidad de implementación y administración desde dentro de una única plataforma permite el control mejorado y acelerado de accesos con privilegios y la protección de credenciales para sistemas de toda la empresa híbrida (de centros de datos tradicionales a entornos virtualizados, nubes públicas o cualquier combinación) sin los gastos generales innecesarios que se asocian normalmente con las estrategias alternativas.

Sección 5:

Conclusiones

La administración de accesos con privilegios es necesaria para abordar el cumplimiento de PCI. Pero, su importancia va más allá de solo cumplir con los requisitos de PCI ya que permite que una organización mejore su postura de seguridad general ante amenazas internas y externas. CA Privileged Access Manager proporciona una manera eficaz de implementar la administración de accesos con privilegios a favor del cumplimiento de PCI y otras necesidades de seguridad.

Al utilizar CA Privileged Access Manager, las organizaciones pueden:

- Reducir de mejor manera sus costos de cumplimiento de PCI abordando muchos requisitos de PCI con una única solución lista para usar que se integra sin problemas con las soluciones existentes de la organización.
- Ahorrar gastos relacionados con las brechas y preservar la reputación de una organización al prevenir diversas brechas de datos y minimizar el impacto de cualquier brecha que pudiera ocurrir.

1 PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

2 Reporte de seguridad anual de 2014 de Cisco, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

3 Reporte de investigaciones sobre las brechas de datos de 2014 de Verizon, http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR

4 M-Trends 2014: Beyond the Breach (Más allá de la brecha), https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

5 Data Leakage Worldwide: The High Cost of Insider Threats (Fuga de datos en todo el mundo: El elevado costo de las amenazas internas), http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf

6 PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

7 Resumen de cambios de PCI DSS v2.0 a v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

CS200-163851_1215