LIBRO BLANCO | ABRIL DE 2016

Cierre de las puertas traseras de las redes

Cinco prácticas recomendadas para controlar los riesgos que plantean los distribuidores externos

Dale R. Gardner
CA Security Management

ca technologies

Índice

Resumen ejecutivo

Reto

Las grandes infracciones de datos que se produjeron en Target, Home Depot, eBay y en la Oficina de gestión de personal de la Administración estadounidense (OPM), entre otros, se pudieron materializar gracias a credenciales de usuario comprometidas o robadas que pertenecían a usuarios con privilegios con un acceso amplio a sistemas confidenciales. Casi en dos de cada tres casos, la infracción inicial se debió a la relajación en las prácticas de seguridad de un tercero (por ejemplo, un distribuidor o un partner empresarial que tenía acceso a una red interna). Con las credenciales robadas de un partner, los atacantes estudiaron la infraestructura de TI en busca de las cuentas con privilegios que, posteriormente, explotaron para obtener acceso no autorizado a sistemas esenciales y provocar daños en la empresa.

Oportunidad

Al igual que las compañías que fueron víctimas de estas infracciones, muchas organizaciones se enfrentan a una mezcla frustrante y compleja de distribuidores externos, contratistas y partners empresariales con acceso de red a su infraestructura de TI y a diversas cuentas con privilegios usadas para ejecutar aplicaciones de misión crítica. En el mundo interconectado actual, el acceso no puede bloquearse por completo y las cuentas con privilegios no se pueden eliminar, así que la única opción es proteger mejor las cuentas con privilegios frente a usuarios no autorizados, lo que significa proteger los activos de información confidencial.

Ventajas

Externalizar los ahorros de costes, las mejoras de calidad y las eficiencias es posible gracias a la empresa interconectada. Restringir el acceso de red en el cortafuegos a todo el mundo ya no es una opción. Los recursos relevantes deben estar a disposición de los partners empresariales para que disfruten de las ventajas empresariales. Deben implementarse las mejores prácticas de seguridad para bloquear las infracciones, a la vez que se permiten las actividades empresariales legítimas.

Sección 1

Riesgos creados por el acceso de terceros

Actualmente, casi todas las organizaciones tienen un número de "no empleados" con cierto nivel de acceso con privilegios a redes y sistemas internos. Con frecuencia, el equipo de seguridad de la información de la empresa puede que no conozca de nada a esas personas, excepto que trabajan para otros distribuidores de la empresa, proveedores de servicios externalizados o partners empresariales. Normalmente, estos usuarios externos constituyen el mayor riesgo para la empresa porque sus cuentas suelen ser la ruta más sencilla para comprometer la empresa. Ejemplos de estas infracciones se encuentran en los casos de Target, Home Depot y otros aparecidos en todos los titulares. Un acceso de usuario comprometido de un tercero relativamente pequeño puede aprovecharse para conseguir un mayor acceso a las redes y sistemas de la organización, lo que puede tener unos resultados catastróficos. Estas infracciones no son algo improbable. Según Troy Leach, del PCI Council, aproximadamente, el 65 % de las infracciones están provocadas por algún tercero.

Los reguladores son conscientes de estos riesgos y están trabajando con el sector para desarrollar las regulaciones y los controles oportunos que permitan hacer frente a este problema. Por ejemplo, la versión 3 de PCI del Data Security Standard introdujo nuevos controles cuyo objetivo era hacer frente a los riesgos planteados por terceros. Benjamin Lawsky, superintendente de asuntos financieros del estado de Nueva York, indicó: **"La ciberseguridad de un banco con frecuencia es solo tan buena como la ciberseguridad de sus distribuidores. Por desgracia, estas empresas externas pueden convertirse en una puerta trasera para la entrada de los piratas que pretenden robar datos confidenciales de los clientes de los bancos".** En consecuencia, los servicios financieros, el sector sanitario y otros reguladores del sector están desarrollando nuevos requisitos de conformidad para reducir los riesgos y mejorar la seguridad.

> "La ciberseguridad de un banco con frecuencia es solo tan buena como la ciberseguridad de sus distribuidores. Por desgracia, estas empresas externas pueden convertirse en una puerta trasera para la entrada de los piratas que pretenden robar datos confidenciales de los clientes de los bancos".
>
> – Benjamin Lawsky, superintendente de servicios financieros, estado de Nueva York

---

Sección 2

Cinco prácticas recomendadas para controlar los riesgos que plantean los distribuidores externos

Avanzar, controlar y gestionar el acceso de terceros a las redes y sistemas se está convirtiendo en un requisito cada vez más importante, tanto para la gestión de los riesgos de seguridad de la información como para la conformidad normativa.

> "Los piratas accedieron a las redes de OPM mediante las credenciales robadas del contratista KeyPoint Government Solutions".
>
> Exclusiva: los detalles de la infracción de OPM que no se conocían, 21 de agosto de 2015

Práctica recomendada 1: implementar procesos y controles de apoyo

Al igual que con la mayoría de los problemas relacionados con la seguridad de la información, un buen punto de partida es definir los procesos y los controles que ayudan a gestionar los riesgos. Esto es particularmente importante para gestionar los riesgos que plantean los terceros porque la mayoría de las actividades se producen fuera del control y la supervisión directa del equipo de seguridad de la información. Como estas relaciones empresariales pueden establecerse y el acceso puede proporcionarse sin que el equipo de seguridad de la información tenga conocimiento de ello o haya revisado el caso, dicho equipo debe involucrarse durante las negociaciones del contrato con objeto de que se desarrollen y apliquen las políticas adecuadas, como parte de la estructura general de gestión de accesos e identidades.

La parte más sencilla del proceso es el aprovisionamiento, el desaprovisionamiento y la definición de políticas adecuadas para usuarios con privilegios que no sean empleados. Al igual que con otros usuarios con privilegios, se deben clarificar las siguientes áreas:

- Formación y definición del usuario
- Sistemas y recursos a los que se debe acceder
- Nivel de privilegios necesario para realizar el trabajo
- Cualquier restricción que se deba aplicar
- Monitorización, grabación de sesiones, alertas y frecuencia de revisión de las sesiones

La mayoría de las organizaciones ya cuentan con políticas de este tipo para los usuarios con privilegios. En caso de que no existan, deberán crearse. Los mismos procesos y controles que se aplican a los usuarios con privilegios que son empleados deben aplicarse a los que no lo son. En función de la estructura organizativa y el tamaño, suelen ser los responsables de las operaciones de TI o de la gestión de las identidades o un grupo de contratación quienes gestionan estos procesos. Estos grupos deben ser conscientes de los procesos de formación, aprovisionamiento, monitorización y desaprovisionamiento de los usuarios con privilegios de terceros, y comprometerse con su cumplimiento.

Estándares de seguridad

Por lo general, la seguridad es solo tan fuerte como su eslabón más débil. Mediante un usuario con privilegios de un partner, la infraestructura del partner y sus procesos pasan a ser parte de la propia infraestructura de TI de la organización. Un simple partner que tenga unos controles débiles o una seguridad deficiente puede facilitar que los piratas informáticos vulneren la protección de la organización, como quedó de manifiesto en el caso de la Oficina de gestión de personal de la Administración estadounidense, que se produjo mediante las credenciales robadas al contratista KeyPoint Government Solutions. Por consiguiente, desde el punto de vista de la gestión de riesgos, es importante efectuar una evaluación de la seguridad de cada partner según los estándares que la organización tenga establecidos. En un número de casos cada vez mayor, PCI, HIPAA y otros requisitos de conformidad exigen la realización de evaluaciones de las prácticas de los distribuidores externos y se señalan los requisitos específicos.

La mayoría de las organizaciones ya cuentan con estándares de seguridad de la información. Estos estándares deben aplicarse a los distribuidores externos. Para desarrollar nuevos estándares de seguridad de la información, hay disponibles varias fuentes:

- Shared Assessments publica un documento Standard Information Gathering (SIG) que ayuda a estandarizar la seguridad de la información recopilando y evaluando los procesos.
- Office of the Comptroller of the Currency (OCC) publica una guía sobre la gestión de riesgos en general, con secciones específicas sobre TI que pueden ser útiles.
- Federal Financial Institutions Examination Council (FFIEC) publica documentos con estándares relevantes.
- Herramienta de evaluación de riesgos de seguridad del departamento de servicios sanitarios y sociales.
- Controles de privacidad y seguridad 800-53 del NIST para los sistemas de información federal.

- Autoridades normativas estatales.
- Estructuras de control y políticas COBIT o ISO 27002.

Además, las normativas de conformidad específicas del sector pueden incluir requisitos para trabajar con terceros:

- Normas de seguridad de datos de la industria de las tarjetas de pago (PCI)
- HIPAA HITECH

Implementación, formación y aplicación

Una vez que se han definido los procesos y las evaluaciones, estos deben implementarse y aplicarse por parte de los responsables de TI, finanzas, asuntos legales y las unidades de negocio que se encargan de las relaciones con los distribuidores, como una parte normal de la definición e implementación del contrato con terceros. A continuación, se especifican los elementos básicos que se deben incluir en los contratos con terceros:

- Garantías: referencias a los propios procedimientos y políticas que un distribuidor se compromete a aplicar, por ejemplo: comprobar los antecedentes de sus empleados con acceso a los sistemas de su organización y formarlos.
- Soluciones: sanciones por incumplimiento de la conformidad y los procesos de corrección.
- Provisiones de auditoría: comprobaciones y balances disponibles para validar la conformidad y frecuencia de las auditorías.

Estas provisiones de gestión de riesgos fundamentales deben incorporarse en las partes relevantes de los contratos y los procesos de implementación. La naturaleza detallada de la política y su aplicación varían según el área empresarial, el equilibrio de riesgos y los costes.

Práctica recomendada 2: autenticar mejor a los usuarios

La oportunidad más importante para mitigar los riesgos con el menor coste y esfuerzo que puede ofrecer la mayor reducción de riesgos es la identificación y autenticación del usuario. Como se ha indicado previamente, casi dos tercios de las infracciones se deben a una identificación y autenticación inadecuadas del usuario externo, incluida la gestión de credenciales (o la ausencia de ella). Por lo general, las organizaciones externas suelen ser empresas más pequeñas que carecen de la experiencia y la madurez en cuestiones de seguridad propias de las organizaciones más grandes. Esto genera problemas con frecuencia. Las credenciales de los usuarios pueden verse comprometidas de estas dos formas: credenciales débiles y mal gestionadas o revelación de las credenciales por error a una persona equivocada.

- **Credenciales débiles:** incluso si se elige una contraseña fuerte, el proceso de aplicación de las reglas de las contraseñas y su caducidad puede ser tedioso. Las personas, especialmente los pequeños distribuidores, no aplican estos procesos. Por ejemplo, un tercio de los distribuidores utilizan las mismas credenciales de ID de usuario y contraseña para todos los clientes. Una vez que los atacantes comprometen ese conjunto de credenciales de un cliente, simplemente tienen que acceder a la lista de clientes del distribuidor (que probablemente estará publicada en el sitio web de este) y elegir el resto de las organizaciones una a una.
- **Revelación por error:** según estadísticas recientes, el índice de éxito de los intentos reiterados de suplantación de identidad se cifra en torno al 100 %, tras 5-7 intentos solo. Esto es un reflejo de lo sofisticados que han llegado a ser estos esfuerzos y de la naturaleza humana de, incluso, los usuarios más experimentados y sofisticados. Un único error puede comprometer la seguridad, tal y como se ilustró en la infracción de la red eléctrica de Ucrania en diciembre de 2015. Esto significa que, incluso el partner empresarial más avezado, puede ser objeto de ataques de robos de identidad (phishing).

La mejor forma de proteger las credenciales que se usan para acceder a los sistemas es gestionarlas y controlarlas de manera proactiva mediante la definición y la aplicación de políticas, entre ellas:

- Complejidad
- Frecuencia de cambio
- Autenticación mediante varios factores

Una práctica recomendada para la gestión de credenciales es la autenticación mediante varios factores para todos los terceros (y los usuarios internos con privilegios). Una vez que una organización se encuentra en el punto de mira de un atacante, es cuestión de tiempo que se vulneren las credenciales usadas por un distribuidor externo. Por ejemplo, en el caso de la red eléctrica ucraniana, parece que se había enviado malware BlackEnergy a un usuario con privilegios que no sospechaba nada mediante un adjunto de Microsoft Office infectado, lo cual se usó como vector de acceso inicial para adquirir credenciales legítimas. El mejor modo de evitar que ocurra esto consiste en incorporar otro factor al proceso de autenticación. Existen diferentes opciones de autenticación mediante varios factores. La opción específica que sea más efectiva depende de una combinación de requisitos de conformidad, regulaciones y aspectos económicos. Por ejemplo, el Gobierno federal de Estados Unidos aplica requisitos específicos para el uso de tarjetas PIV/CAC por parte de usuarios administrativos y con privilegios. En otros entornos, existen otras opciones, por ejemplo, los certificados, los tokens basados en hardware y software o los procesos de verificación que utilizan el teléfono móvil del usuario. La economía de la autenticación mediante varios factores es muy favorable, por lo que el caso empresarial es fácil de crear.

La gestión eficaz de las credenciales de terceros depende de que los usuarios de los distribuidores tengan sus credenciales individuales, lo que no encaja con las prácticas empresariales actuales de muchas organizaciones. En muchos casos, en lugar de crear una cuenta para cada usuario, se crea una cuenta para cada distribuidor, por lo que todos los empleados del distribuidor utilizarán la misma cuenta y las mismas credenciales. Esto puede ser más fácil desde el punto de vista administrativo, pero se pueden producir los siguientes problemas cuando varias personas comparten una cuenta:

- La autenticación mediante varios factores es más complicada.
- Se dificulta la capacidad para controlar el acceso y el uso de las credenciales, especialmente en los casos en los que una persona deja la organización o cambia de rol. Es muy fácil filtrar o robar unas credenciales compartidas.
- Además, resulta imposible determinar qué persona realizó una acción concreta en la red. Si una cuenta está compartida entre varias personas, no hay forma de saber cuál de ellas realizó una acción problemática.

Implementar un proceso donde las credenciales se emiten para los individuos en lugar de para los distribuidores elimina en gran parte estos problemas y simplifica el proceso de incorporación y cese de los usuarios. Cuando alguien se incorpora a la organización de un partner empresarial, se crea una cuenta y se le concede acceso. Dicha cuenta y acceso se puede eliminar de forma fácil y rápida cuando el individuo deja la organización o cambia de rol. Una correcta gestión de los accesos y la autenticación de los usuarios no son solo cuestiones tecnológicas, sino que también tienen implicaciones con las personas, los procesos y la formación que se deben definir al negociar los acuerdos con los distribuidores y al establecer los procesos. Los distribuidores deben informar de los cambios en el personal, lo cual es un trabajo extra para ellos. Además, deben implementarse procedimientos de notificación para que el distribuidor informe de estos hechos. En general, el esfuerzo administrativo adicional merece la pena por la mejora de la seguridad y el control que ofrecen estos enfoques. De hecho, las exigencias normativas requieren un control de acceso y una autenticación a nivel individual porque son más efectivos.

El último aspecto, que puede que no sea habitual en las organizaciones, es el requisito de realizar comprobaciones de antecedentes y de identidades de los individuos externos que acceden a los sistemas de la organización. De nuevo, se trata de una cuestión de gestión: el coste que supone (tanto financiero como administrativo) está justificado generalmente, en especial en los entornos confidenciales.

Una tecnología que centraliza y automatiza las reglas de complejidad de las contraseñas, sus cambios y la integración de sistemas de autenticación de varios factores es un almacén de credenciales. El siguiente elemento tras la gestión de las credenciales es separar la autenticación del control de acceso.

Práctica recomendada 3: separar la autenticación del control de acceso

En la mayoría de las redes, una vez que una persona consigue acceso a la red, tiene visibilidad de una amplia gama de dispositivos y sistemas, así como acceso potencial a ellos. Entre los resultados de esta arquitectura de red figuran infracciones como las de Target, Home Depot o la red eléctrica de Ucrania, entre otras. Estas infracciones se llevan a cabo mediante una cadena de ciberataques. Con la cadena de ciberataques, los atacantes llevan a cabo una serie de pasos (en ocasiones, iterativamente) para llevar a buen puerto la infracción. El ataque comienza con la obtención del acceso inicial a una red, a menudo comprometiendo las credenciales de un distribuidor o de un tercero. Una vez dentro, el atacante puede buscar dentro de la red atacada para localizar vulnerabilidades o credenciales adicionales cuya explotación le permitirá obtener un mayor acceso a niveles cada vez mayores de privilegios, hasta que finalmente alcanza su objetivo definitivo, como fue el caso de la red eléctrica de Ucrania.

> "Las tres empresas indicaron que los actores borraron algunos sistemas ejecutando el malware KillDisk al finalizar el ciberataque. El malware KillDisk borra determinados archivos de los sistemas objetivo y daña el sector de arranque principal, por lo que los sistemas quedan inoperables. Además, se informó de que, al menos en un caso, las interfaces humano-máquina (HMI) basadas en Windows integradas en unidades de terminal remotas también se sobrescribieron con KillDisk. Los infractores también dejaron inoperables los dispositivos Serie-Ethernet de las subestaciones al dañar su firmware. Además, parece que también programaron la desconexión de los servidores de la fuente de alimentación ininterrumpida (UPS) mediante la interfaz de gestión remota de UPS. El equipo considera que estas acciones se realizaron en un intento de interferir en los esfuerzos de restauración esperados".
>
> Ciberataque a infraestructuras críticas en Ucrania
> Fecha de publicación original: 25 de febrero de 2016

Como se ha indicado en la práctica recomendada número 2, una forma de romper esta cadena de ciberataque es controlar el acceso a la red y dificultar la entrada del atacante con la autenticación mediante varios factores. Otra capa de defensa consiste en limitar la visibilidad y el acceso a los recursos de la red. La mayoría de los distribuidores solo necesita acceder a sistemas concretos. No necesitan acceder a toda la red o ni siquiera a una subred ni tener visibilidad de ella.

La visibilidad de la red y el acceso se pueden limitar usando la segmentación de red física. Esto se suele hacer con frecuencia para cumplir con una exigencia normativa. Al segmentar la red y controlar el acceso, el ámbito de los recursos disponibles se limita. Aunque este puede ser un enfoque eficaz, tiene sus carencias:

- Sobrecarga administrativa para configurar y mantener esta arquitectura de red.
- Vulnerabilidad de las conexiones entre las distintas partes de la red: un atacante puede encontrar la forma de atravesar las conexiones de red para obtener acceso a su objetivo.

Una mejor alternativa consiste en usar la segmentación lógica con una solución de gestión de identidades con privilegios, como CA Privileged Access Manager, que puede limitar el acceso a los recursos. Esta solución funciona con la implementación de un "cuello de botella" por el que tenga que pasar el usuario externo para obtener acceso a los recursos protegidos. Este enfoque tiene varias ventajas:

- **Control de acceso de "confianza cero":** un inicio de sesión correcto no ofrece acceso a toda la red. En lugar de ello, el sistema aplica las políticas que especifican qué recursos están disponibles para un usuario, lo que limita el acceso del usuario solo a esos sistemas. Este enfoque posibilita un control muy exhaustivo de la visibilidad y el acceso: un usuario nunca podrá ver recursos a los que no tenga derecho de acceso. El usuario solo ve una lista de sistemas predefinidos para los que tiene permiso de acceso y visualización.
- **Evita que los delincuentes sorteen las defensas:** para controlar los movimientos laterales en una red, el sistema intercepta diversos comandos de red, como TELNET o SSH, y evita que se ejecuten. Esta capacidad limita el acceso de terceros solo a sistemas previamente especificados, lo que evita que tengan visibilidad del resto de la red y que puedan intentar acceder a otros sistemas.

Es importante estandarizar y consolidar los métodos de acceso con un "cuello de botella", ya sea mediante una solución de gestión de accesos con privilegios, con una VPN o con alguna otra solución que canalice el acceso mediante rutas conocidas. Si define rutas aceptables de acceso a los recursos desde el exterior, la monitorización le resultará más sencilla. Al contener protocolos no aprobados y dirigir las sesiones aprobadas a una ruta predefinida, las anomalías son más fáciles de identificar para investigarlas en profundidad, aspectos en los que SIEM y las herramientas de registro pueden ayudar a detectar eventos anormales.

Práctica recomendada 4: evitar errores y comandos no autorizados

Se pueden usar permisos y derechos de acceso para limitar el acceso a los recursos tecnológicos de información. En ocasiones, este enfoque no ofrece el grado de precisión necesario para controlar realmente lo que hace alguien en el sistema. Por ejemplo, un administrador externo puede que necesite iniciar sesión en un servidor usando el acceso "raíz" o "administrador", que es un tipo de cuenta de superusuario con muchos privilegios. Este enfoque de acceso puede estar avalado por razones administrativas o técnicas, por lo que genera una situación de riesgo. Con este alto nivel de privilegios, el individuo puede hacer cualquier cosa en el sistema, incluso borrarlo por completo, lo que supone un riesgo inaceptable para la mayoría de las organizaciones, incluso si esta persona es un empleado de la empresa.

Un enfoque diferente con una solución de gestión de accesos con privilegios ofrece un enfoque más asumible al habilitar un control de permisos muy detallado con el que gestionar mejor este tipo de usuarios. El sistema de gestión de accesos con privilegios permite que se establezcan sesiones en nombre de una persona en diversos sistemas de destino con distintas cuentas (por ejemplo, la cuenta raíz), cada una con diferentes niveles de permisos.

El filtrado de comandos y las listas negras y blancas también se pueden usar para limitar qué comandos puede utilizar un usuario concreto. Una lista negra contiene comandos que no están permitidos, mientras que una lista blanca contiene comandos que sí se pueden ejecutar. Las listas blancas y negras se usan juntas para ofrecer un alto nivel de control y flexibilidad. De esta forma, el uso con privilegios puede mantener el recurso informático sin generar un daño inaceptable. Una ventaja inesperada del filtrado de comandos es evitar errores inadvertidos. En el ejemplo anterior, el superusuario puede mover archivos, pero no reformatear el disco.

Los filtros de comandos combinados con funciones de registro facilitan la monitorización y las alertas, para que el sistema responda del modo adecuado. Cuando alguien intenta infringir alguno de los filtros, se puede mostrar una advertencia o terminar la sesión causante del problema. Por ejemplo, si una persona decide hacer pruebas antes de alcanzar el límite establecido por los filtros de comandos, cuando se alcanzan los límites, el sistema puede generar una alerta que inicie una investigación sobre las acciones de la persona. Estas son algunas de las respuestas posibles:

- Bloquear y advertir al usuario
- Finalizar la sesión
- Desactivar la cuenta del usuario
- Generar una alerta o alarma para el SOC

Práctica recomendada 5: monitorizar e investigar

Siempre se requiere cierto nivel de monitorización. El nivel y el alcance específico de la monitorización dependen de las consideraciones de gestión de la conformidad y del riesgo.

Incluso en casos con pocos riesgos intrínsecos, las funciones de registro ayudan a resolver problemas e investigar la actividad sospechosa. El registro básico recopila lo que ha sucedido y es útil para revisar actividades inapropiadas o no autorizadas. Ofrece esta información:

- Hora de inicio y finalización de sesión
- Sistemas a los que se ha accedido
- Comandos emitidos
- Respuestas recibidas

En cualquier tipo de situaciones confidenciales, la monitorización aprovecha los registros para aplicar las políticas establecidas sobre el acceso a los sistemas, ya que los esfuerzos por infringir estas políticas merecen atención. Se pueden realizar varias acciones en respuesta a un intento de infracción de una política. En un nivel básico, estos intentos generan una investigación para averiguar qué ha sucedido. Se puede necesitar formación adicional para que los usuarios sepan qué tareas se espera que hagan y cómo deben realizarlas. Una infracción puede deberse a un simple error o ser un indicador de un intento de comportamiento malintencionado. La monitorización permite detectar eventos sospechosos para que se investiguen.

Las investigaciones son muy importantes, tal y como indica JPMorgan Chase, cuyo personal detectó que se habían producido infracciones tras investigar a uno de sus distribuidores.

> "JPMorgan descubrió que los piratas informáticos habían accedido a sus sistemas en agosto, después de averiguar que el mismo grupo de piratas había vulnerado un sitio web de una carrera benéfica que patrocinaba el banco... Solo después de averiguar que el sitio web de Corporate Challenge había sido vulnerado, JPMorgan supo que su propia red también había sido objeto de ataque de los mismo piratas".
>
> "Neglected Server Provided Entry for JPMorgan Hackers"
> The New York Times, 22 de diciembre de 2014

En situaciones más confidenciales, se puede requerir la captura o grabación de sesiones para recopilar toda la información sobre lo sucedido en una sesión concreta, lo que será útil para futuras investigaciones. Una práctica habitual consiste en capturar las grabaciones a pantalla completa de las sesiones confidenciales. Estas grabaciones se pueden estudiar posteriormente, en casos de infracciones conocidas de políticas o problemas que surjan posteriormente relacionados con el sistema, para valorar qué sucedió en la sesión original. Según la confidencialidad del entorno, puede ser aconsejable realizar comprobaciones puntuales. Uno de los problemas asociados tradicionalmente con la grabación de sesiones es que los archivos grabados y la sobrecarga del sistema pueden ser importantes. Otro reto es contar con un plan de acción para revisar las sesiones grabadas. Dado que tanto el gasto tecnológico como de tiempo aumenta con la grabación de sesiones, el análisis de costes y beneficios ayuda a identificar situaciones que son adecuadas para este nivel de inversión. Como punto de partida, es útil identificar los siguientes aspectos:

- Cuándo se debe grabar y durante cuánto tiempo.
- Cuándo y con qué frecuencia se deben revisar las grabaciones.
- Cuál es la política de conservación de las grabaciones.

Si decide implementar técnicas de grabación de sesión, hay que tener en cuenta varias capacidades:

- Fácil acceso a los metadatos de la sesión (inicio y finalización).
- Capacidad para desplazarse por la sesión y acceder a un punto específico de una grabación.
- Posibilidad de destacar una actividad "interesante", como infracciones de políticas y actividades confidenciales.

Las situaciones de mayor riesgo pueden exigir la monitorización "por encima del hombro" o acceso de una segunda parte, lo que requiere que otra persona vea en tiempo real lo que hace un usuario con privilegios. Normalmente, este tipo de situaciones de riesgo extremo no se producen con terceros u otros usuarios externos. La monitorización "por encima del hombro" plantea también problemas técnicos. Además, la persona que realice la monitorización debe tener mucha experiencia en el tema para comprender las acciones realizadas y sus repercusiones en el entorno a gran escala. Desde una perspectiva de gestión del riesgo, la monitorización "por encima del hombro" puede ser adecuada para un número muy pequeño de situaciones.

Las tareas típicas de monitorización suelen ser un proceso de dos pasos:

- **Respuesta en tiempo real a las infracciones de políticas:** se pueden producir varias acciones: generación de una alerta que se remite a un centro de operaciones de seguridad o cierre de una sesión o cuenta.
- **Investigación y análisis después de los hechos:** una revisión de los registros o las grabaciones de la sesión para respaldar las investigaciones forenses o la resolución de problemas.

El análisis y la investigación después de los hechos pueden incluir esfuerzos para relacionar los registros y las alertas generadas por un sistema de gestión de accesos con privilegios y una herramienta de seguridad para eventos inesperados. Por ejemplo, en organizaciones donde se haya implementado una solución de gestión de accesos con privilegios, toda la actividad administrativa está centralizada en el sistema de gestión de accesos con privilegios. Si alguna solicitud SSH o TELNET procede de otras partes de la red, se considera como alerta inmediata de que algo va mal y requiere investigación. Al eliminar o prohibir herramientas administrativas no autorizadas, la actividad sospechosa es relativamente fácil de identificar. Un cortafuegos de última generación puede ayudar a identificar las aplicaciones y los protocolos que están prohibidos. Otras actividades sospechosas pueden ser el acceso a horas inesperadas o comportamientos inusuales, como la realización de descargas.

A lo largo del tiempo, las revisiones y las auditorías manuales en curso permiten buscar y perfeccionar herramientas y políticas para ignorar falsos positivos y automatizar activadores y alertas a fin de que sean más eficaces.

Sección 3

Ventajas de gestionar los riesgos relacionados con terceros

Ninguna organización moderna puede estar aislada y desconectada de Internet. Las relaciones empresariales requieren colaboración electrónica para intercambiar información confidencial entre partners. Actualmente, las empresas utilizan proveedores externos para servicios de contabilidad, procesamiento de tarjetas de crédito, asesoramiento legal, administración de planes de retirada, servicios de marketing, fabricación y cientos de trabajos más. La colaboración electrónica entre partners empresariales permite ahorrar tiempo y dinero, habilita los procesos automatizados y los sistemas que mejoran la precisión, la calidad y la eficiencia. Restringir el acceso de red de un tercero en el cortafuegos no es una opción. Los recursos relevantes deben estar a disposición de los partners empresariales para que disfruten de las ventajas empresariales. Al mismo tiempo, las compañías se enfrentan a riesgos reales al conectarse con terceros.

Las infracciones de seguridad son caras. Según la revista Fortune, tras el robo en 2013 de 40 millones de tarjetas de pago y 70 millones de otros registros, Target calcula unos costes de 162 millones de dólares tras los reembolsos del seguro. Sony calculó un gasto de 35 millones de dólares en la "restauración financiera y de los sistemas de TI" tras una infracción sufrida en 2014. Home Depot registró 28 millones de dólares en gastos netos antes de impuestos. Los costes expuestos no incluyen los daños en la reputación ni el aumento de las primas de los seguros. Además de estos costes "físicos", la vida de las personas se altera. Muchas personas pierden sus trabajos y el resto debe trabajar de día y de noche para investigar y mitigar las infracciones.

> "Con independencia del modo en que lo evaluamos o de si miramos hacia adelante o hacia atrás, estamos de acuerdo en que el punto central en que deben invertir las empresas es en seguridad de la información".
>
> Benjamin Dean, School of International and Public Affairs de la Columbia University, Fortune Magazine, 27 de marzo de 2015

Es evidente que ninguna empresa quiere aparecer en la portada del Wall Street Journal como ejemplo de otra gran infracción de seguridad. Las cinco prácticas recomendadas pueden bloquear las infracciones a la vez que permiten las actividades empresariales legítimas garantizando la reputación y la seguridad de los activos de información de su organización.

Sección 4

Conclusiones

Según el informe Data Breach Investigations Report (DBIR) de Verizon del año 2015, se estima que 400 millones de dólares son las pérdidas resultantes de los 700 millones de registros que se han visto comprometidos. Las 70 organizaciones que han contribuido a este informe han documentado 79 790 incidentes de seguridad, de los cuales 2122 fueron infracciones confirmadas en 61 países. Dos tercios de los incidentes se produjeron en Estados Unidos. Aunque la gran mayoría de las amenazas siguen procediendo de fuentes externas, las amenazas internas y de partners han aumentado levemente entre 2013 y 2014. Los riesgos son reales, tal y como pone de manifiesto la megainfracción que se produjo en la Oficina de gestión de personal de la Administración estadounidense (OPM).

El método de ataque empleado en la OPM seguía una fórmula: definición de un subcontratista como objetivo de un ataque de ingeniería social y robo de credenciales para obtener acceso a la red. Instalación de malware en un sistema y creación de una puerta trasera. Extracción de datos durante meses sin ser detectados.

La infracción de OPM también pone de manifiesto la vulnerabilidad de las organizaciones ante la ingeniería social. Los contratistas y los empleados gubernamentales deben someterse ahora a programas de formación sobre seguridad y conocer los peligros del "spear phishing" y otras amenazas de las redes sociales.

> "The most innovative and damaging hacks of 2015".
>
> CSO Magazine, 28 de diciembre de 2015

Muchos riesgos se pueden paliar siguiendo las cinco prácticas recomendadas que se describen en este documento para crear una defensa de seguridad de la información más potente, flexible, sólida y de varios niveles. Estas prácticas son las siguientes:

- Implementar procesos y controles de apoyo que definan y apliquen políticas para usuarios con privilegios de terceros.
- Autenticar mejor a los usuarios mediante la tecnología de autenticación de varios factores, de modo que resulte más difícil vulnerar las credenciales con privilegios, incluso en el caso de ataques de suplantación de identidad e ingeniería social.
- Separar la autenticación del control de acceso para que los usuarios con privilegios solo tengan una visibilidad limitada en las redes internas, con lo que se minimizan los posibles daños que puede acarrear un usuario o un conjunto de credenciales robadas.
- Evitar errores y comandos no autorizados de forma que los desencadenantes en tiempo real actúen como la primera línea de defensa para proteger la infraestructura frente a los errores inadvertidos y a la actividad malintencionada.
- Monitorizar e investigar actividades sospechosas para detectar rápidamente infracciones, mejorar la formación cuando se necesite, y perfeccionar continuamente la automatización y los procesos a fin de eliminar falsos positivos.

Los sistemas de gestión de accesos con privilegios tienen funciones y características automatizadas que ayudan a definir, automatizar y aplicar las cinco prácticas recomendadas descritas en este documento en toda la empresa en entornos físicos, virtuales o en la nube, lo que ayuda a las organizaciones a implementar procesos coherentes en todos los sistemas, las aplicaciones y los dispositivos.

Sección 5

Referencias

https://www.brighttalk.com/webcast/9017/156931

http://www.xceedium.com/solutions/privileged-identity-management/432-2

http://www.bankinfosecurity.com/occ-more-third-party-risk-guidance-a-7233/op-1

http://www.bankinfosecurity.com/banks-vendor-monitoring-comes-up-short-a-8103

Informe del 9 de abril del NYS Financial Services Department, "Update on Cyber Security in the Banking Sector: Third Party Service Providers"
http://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html?emc=edit_tu_20160301&nl=bits&nlid=59970007

https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

http://www.cnbc.com/2015/07/22/4-arrested-in-schemes-said-to-be-tied-to-jpmorgan-chase-breach.html

How Much do Data Breaches Cost Big Companies? Shockingly Little
http://fortune.com/2015/03/27/how-much-do-data-breaches-actually-cost-big-companies-shockingly-little/ 27 de marzo de 2015

http://fortune.com/tag/data-breach 2 de marzo de 2016

http://www.crn.com/slide-shows/security/300077563/the-10-biggest-data-breaches-of-2015-so-far.htm/pgno/0/10?itc=refresh 27 de julio de 2015

https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx 21 de agosto de 2015

http://www.csoonline.com/article/3018343/security/the-most-innovative-and-damaging-hacks-of-2015.html

Sección 6

Acerca del autor

Dale R. Gardner tiene más de dos décadas de experiencia en software empresarial, desde la gestión de redes y sistemas hasta múltiples segmentos de seguridad, como la gestión de identidades, la seguridad de las aplicaciones, la gestión de vulnerabilidades, la seguridad de redes y la conformidad normativa. Se trata de un antiguo analista de investigación y escritor. Ha definido, creado y comercializado diversas soluciones de gestión y seguridad, que mejoran las operaciones y contribuyen a garantizar la integridad y fiabilidad de las infraestructuras corporativas de las tecnologías de la información. Actualmente es responsable del marketing a nivel global de la cartera de productos de gestión de accesos con privilegios de CA Technologies.