REPORTE OFICIAL | ABRIL DE 2016

Cerrando las backdoors de la red

Las cinco mejores prácticas para controlar los riesgos de proveedores externos

Dale R. Gardner
Administración de Seguridad de CA

ca technologies

Tabla de contenidos

Resumen ejecutivo

Reto

Las principales filtraciones en Target, Home Depot, eBay, la oficina de administración de personal de los E. UU. y otras fueron posibles por credenciales de usuarios robadas o comprometidas, que pertenecían a un usuario con privilegios con acceso extensivo a sistemas sensibles. En casi dos tercios de los casos, la infracción inicial fue posible por las prácticas pobres de seguridad de un tercero, ya sea proveedor o socio de negocioso, con acceso a una red interna. Con las credenciales robadas del socio, los atacantes exploraron la infraestructura de TI infiltrada en busca de cuentas con privilegios que luego explotaron para obtener acceso no autorizado a sistemas importantes y causar daño grave en los negocios.

Oportunidad

De similar manera a las compañías infiltradas, muchas organizaciones enfrentan una mezcla frustrante y compleja de proveedores, contratistas y socios de negocios externos con acceso de red a su infraestructura de TI y una variedad de cuentas con privilegios usadas para ejecutar aplicaciones fundamentales para la misión. En el mundo interconectado actual, el acceso no puede ser completamente bloqueado y las cuentas con privilegios no pueden eliminarse, por eso, la única opción es proteger mejor las cuentas de los usuarios no autorizados, para proteger mejor los recursos de información sensible.

Beneficios

La tercerización de ahorros en costos, mejoras de calidad y eficiencias es posible gracias a la empresa interconectada. Restringir el acceso de red al firewall para todos ya no es una opción. Los recursos relevantes deben estar disponibles para socios de negocios, para obtener beneficios comerciales. Las mejores prácticas de seguridad de información deben estar establecidas para bloquear filtraciones, al mismo tiempo que permiten actividades comerciales legítimas.

Sección 1

Riesgos creados por el acceso de proveedores externos

Hoy en día, la mayoría de las organizaciones cuentan con 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 empresa puede saber poco o nada sobre estas personas, además de que trabajar para proveedores de la empresa, proveedores de servicios externos o socios de negocios. Por lo general, estos usuarios tercerizados representan el mayor riesgo para la empresa, porque sus cuentas suelen ser la ruta más fácil para comprometer a la empresa. Los ejemplos de estas filtraciones pueden verse en importantes noticias sobre Target, Home Depot y otras. Se puede aprovechar un acceso de usuario comprometido de terceros relativamente pequeño para obtener un acceso más amplio a las redes y sistemas de la organización y los resultados son terribles daños. Estas infracciones no son aberraciones. De acuerdo a Try Leach, del Consejo de Normas de la PCI, alrededor del 65 % de las infracciones pueden rastrearse a un proveedor externo.

Los reguladores conocen estos riesgos y están trabajando con la industria para desarrollar controles apropiados y regulaciones para abordar el desafío. Por ejemplo, la versión 3 de la PCI del estándar de seguridad de datos presentó nuevos controles apuntados a abordar el riesgo de terceros. Benjamin Lawsky, el superintendente de servicios financieros del estado de Nueva York, destacó lo siguiente: **"La seguridad cibernética de un banco suele ser solo tan buena como la seguridad cibernética de sus proveedores. Lamentablemente, esas firmas de terceros pueden brindar una entrada por las backdoors a los hackers que buscan robar datos sensibles de clientes bancarios".** Como resultado, los servicios financieros, atención médica y otros reguladores de la industria están desarrollando nuevos requisitos de cumplimiento para reducir el riesgo y mejorar la seguridad.

> "La seguridad cibernética de un banco suele ser solo tan buena como la seguridad cibernética de sus proveedores. Lamentablemente, esas firmas de terceros pueden brindar una entrada por las backdoors a los hackers que buscan robar datos sensibles de clientes bancarios".
>
> – Benjamin Lawsky, superintendente de servicios financieros del estado de Nueva York

---

Sección 2

Las cinco mejores prácticas para controlar los riesgos de proveedores externos

De ahora en adelante, controlar y administrar el acceso de terceros a redes y sistemas se está volviendo un requisito cada vez más importante, tanto para la administración de riesgos de seguridad de información como para el cumplimiento normativo.

> "Los hackers han accedido a las redes de OPM mediante credenciales robadas del contratista KeyPoint Government Solutions".
>
> Exclusivo: Los detalles que no vio de la infracción de OPM, 21 de agosto de 2015

Mejor práctica 1: Implemente procesos y controles de respaldo

Al igual que con la mayoría de los problemas de seguridad de la información, un buen punto de partida es definir los procesos y controles que ayudan a administrar el riesgo. Esto es particularmente importante para administrar riesgos de terceros, porque la mayoría de la actividad ocurre fuera del ámbito y control directos del equipo de seguridad de la información. Dado que las relaciones comerciales pueden establecerse y el acceso puede brindarse sin el conocimiento ni la revisión del equipo de seguridad de la información, el equipo tiene que estar involucrado durante las negociaciones de contratación, para que se desarrollen e implementen políticas apropiadas como parte del marco general de administración de acceso e identidades.

La parte simple del proceso es el aprovisionamiento, desaprovisionamiento y definición de políticas apropiadas para usuarios con privilegios que no son empleados. Al igual que otros usuarios con privilegios, deben aclararse las siguientes áreas:

- definición y capacitación del usuario;
- sistemas y recursos para los que se necesita acceso;
- nivel de privilegios necesario para realizar las tareas;
- restricciones a establecer;
- y frecuencia de control, registro de sesiones, alertas y revisión de sesiones.

La mayoría de las organizaciones ya tienen estas políticas establecidas para los usuarios con privilegios. Si estas políticas no existen, es necesario crearlas. Los mismos procesos y controles que aplican a los usuarios con privilegios que son empleados deben aplicar a los que no son empleados. De acuerdo a la estructura y tamaño de la organización, el grupo de operaciones de TI, los individuos responsables de la administración de identidad o un grupo contratista suelen manejar estos procesos. Estos grupos deben estar al tanto y aceptar los procesos de capacitación, aprovisionamiento, control y desaprovisionamiento de usuarios externos con privilegios.

Estándares de seguridad

En general, la seguridad solo es tan fuerte como el enlace más débil. A través de un usuario con privilegio de un socio, la infraestructura y los procesos del socio se vuelven parte de la infraestructura de TI propia de la organización. Solo un socio con controles débiles o seguridad pobre puede ser un intermediario para que los hackers rompan la protección de la organización, como queda demostrado por la infracción a la Oficina de administración de personal que ocurrió mediante las credenciales robadas del contratista KeyPoint Government Solutions. Por lo tanto, desde el punto de vista de la administración de riesgos, resulta imprescindible evaluar la seguridad de cada socio de negocios en relación con los estándares organizativos establecidos. En un número cada vez mayor de casos, la PCI, HIPAA y otros mandatos de cumplimiento requieren evaluaciones del rendimiento de proveedores externos y la enumeración de requisitos específicos.

La mayoría de las organizaciones ya tienen estándares de seguridad de la información establecidos. Estos estándares deben aplicar a proveedores externos. Para desarrollar un nuevo estándar de seguridad de la información, existen diversas fuentes disponibles:

- Evaluaciones compartidas publica un documento, Recopilación de información estándar (SIG), para ayudar a estandarizar la recopilación de seguridad de la información y el proceso de evaluación.
- La oficina de contralor de la moneda (OCC) publica amplias guías sobre la administración de riesgos, con secciones específicas para TI que se pueden aprovechar.
- El Consejo federal de certificación de instituciones financieras (FFIEC) publica documentos con estándares relevantes.
- Herramienta de evaluación de riesgos de seguridad del Departamento de servicios humanos y de salud.
- Controles de privacidad y seguridad 800-53 de NIST para sistemas de información federal.

- Autoridades normativas estatales.
- Marcos de control y política COBIT o ISO 27002.

Además, los mandatos de cumplimiento específicos de la industria pueden incluir requisitos para trabajar con terceros:

- Norma de seguridad de datos de la PCI.
- HIPAA HITECH.

Implementación, capacitación e implementación

Una vez que las evaluaciones y procesos estén establecidos, deben implementarse y hacerse cumplir por parte de TI, Finanzas, Legal y las unidades de negocios a las que pertenecen las relaciones con proveedores, como parte normal de la definición e implementación del contrato con terceros. A continuación, los elementos básicos que deben incluirse en todos los contratos con terceros:

- Garantías: referencias a las políticas y los procedimientos que un proveedor se compromete a aplicar, incluidas verificaciones de antecedentes y la capacitación de los empleados del proveedor que tienen acceso a los sistemas de la organización.
- Solución: penalizaciones por incumplimiento y procesos de corrección.
- Disposiciones de la auditoría: los mecanismos de control y equilibrio estarán disponibles para validar el cumplimiento y la frecuencia de auditoría.

Estas disposiciones de administración de riesgo fundamentales deben incorporarse a las partes relevantes de los procesos de contratación e implementación. La naturaleza detallada de esta política y su implementación varían de acuerdo al área comercial, los riesgos y los costos.

Mejor práctica 2: Autenticar usuarios con mayor eficacia

La mayor oportunidad de mitigación de riesgos en la que el menor costo y esfuerzo puede ofrecer la mayor reducción de riesgos es la identificación y autenticación de usuarios. Como se mencionó previamente, el origen de alrededor de dos tercios de infracciones es la identificación y autenticación inadecuada de usuarios externos, que incluye la administración de credenciales (o falta de la misma). Por lo general, las organizaciones de terceros tienden a ser firmas más pequeñas, que carecen de madurez en cuanto a la seguridad y la experiencia de grandes organizaciones. Esto suele generar problemas. Las credenciales de los usuarios pueden verse comprometidas de dos maneras: fortaleza inadecuada y administración de credenciales o divulgación inadvertida de credenciales a la persona incorrecta.

- **Credenciales débiles:** Incluso si se elige una contraseña fuerte, implementar las reglas y caducidad de las contraseñas puede ser un proceso tedioso. La gente, en especial los proveedores pequeños, no lo hace. Por ejemplo, un proveedor de terceros uso las mismas credenciales, ID de usuario y contraseña, para todos sus clientes. Una vez que los atacantes comprometieron ese juego de credenciales para ese cliente, pudieron revisar la lista de clientes del proveedor (que fue consideradamente pública en el sitio web del proveedor) y elegir del resto de las organizaciones, una a una.
- **Divulgación errónea:** Según estadísticas recientes, la tasa de éxito de los intentos repetidos de suplantación de identidad es cercana al 100 %, después de tan solo cinco a siete intentos. Esta es una reflexión sobre qué tan sofisticados pueden volverse estos esfuerzos y la naturaleza humana de hasta los usuarios más capaces y sofisticados. Solo un error lleva a una transigencia, como lo ilustró la infracción en la red de suministro eléctrico ucraniana en diciembre de 2015. Esto significa que incluso más socios comerciales capacitados pueden ser propensos a ataques de suplantación de identidad.

La mejor manera de proteger las credenciales usadas para acceder a sistemas es administrarlas y controlarlas de manera proactiva, definiendo e implementando políticas que incluyan lo siguiente:

- complejidad;
- frecuencia de cambio;
- y autenticación de múltiples factores.

Una mejor práctica para la administración de credenciales es la autenticación de múltiples factores para todos los terceros (y usuarios internos con privilegios). Una vez que se selecciona una organización como objetivo, es cuestión de tiempo hasta que las credenciales usadas por un proveedor externo se vean comprometidas. Por ejemplo, en la infracción de la red de suministro eléctrico ucraniana, parece que se envió malware de BlackEnergy a un usuario con privilegios no sospechoso mediante un adjunto de Microsoft Office infectado, que luego se usó como vector de acceso inicial para adquirir credenciales ilegítimas. La mejor forma de evitar que esto suceda es agregar otro factor al proceso de autenticación. Hay varias opciones de autenticación multifactor disponibles. La opción específica que es más efectiva depende de una combinación de economía y regulaciones o mandatos de cumplimiento. Por ejemplo, en el gobierno federal de los EE. UU., hay requisitos específicos para el uso de tarjetas PIV/CAC para usuarios administrativos y con privilegios. En otros entornos, hay otras opciones disponibles, que incluyen certificados, tokens basados en hardware e incluso tokens basados en software o procesos de verificación en los que se usa el teléfono celular de una persona. La economía de la autenticación de múltiples factores es muy favorable y hace fácil de crear el caso de negocios.

La administración de credenciales de terceros efectiva depende de que los usuarios de proveedores cuenten con credenciales individuales, lo que no es consistente con las prácticas comerciales actuales en muchas organizaciones. En muchos casos, en lugar de crear una cuenta para un usuario, se crea una cuenta para un proveedor, con el concepto de que cualquiera de los empleados del proveedor puede usar la misma cuenta y credenciales. Si bien esto puede ser sencillo administrativamente, los siguientes problemas ocurren cuando varias personas comparten una cuenta:

- La autenticación de factores múltiples es más complicada.
- La capacidad de controlar el acceso y usar las credenciales es más difícil, en especial en casos en los que alguien deja la organización o cambia roles. Las filtraciones o el robo de credenciales compartidas son demasiado fáciles.
- Se pierde la atribución, es decir, la capacidad de determinar qué individuo realizó una acción específica en la red. Si una cuenta es compartida entre muchas personas, no hay manera de saber cuál de los individuos realizó la acción problemática.

Implementar un proceso en el que las credenciales se emitan a los individuales en lugar de al proveedor elimina ampliamente estos problemas y simplifica el proceso de activación y desactivación de usuarios. Cuando una persona se une a la organización de un socio de negocios, se crea una cuenta y se otorga acceso a esta. Esa cuenta y ese acceso pueden ser finalizados fácil y rápidamente cuando ese individuo se vaya o cambie roles. La administración de acceso y autenticación de usuario exitoso no son solo problemas de tecnología, sino también de personal, procesos y capacitación, que deben abordarse cuando se negocien acuerdos con proveedores y se establezcan procesos. Los proveedores deben emitir notificaciones sobre cambios de personal, que es un trabajo adicional para ellos, y los procedimientos deben estar establecidos para facilitarle al proveedor el informe de estos eventos. En general, el esfuerzo administrativo adicional vale la pena, por la seguridad y los controles mejorados que ofrecen estos enfoques. De hecho, los mandatos normativos requieren autenticación a nivel individual y control de acceso, porque son muy efectivos.

La última zona, que puede ser atípica en las organizaciones, es un requisito para las verificaciones de antecedentes y evidencias de identidad para los individuos externos que acceden a los sistemas de las organizaciones. Otra vez, es un problema de administración de riesgos. El costo que involucra (tanto financiero como administrativo) suele justificarse, en especial en entornos sensibles.

Una tecnología que centraliza y automatiza las reglas de complejidad de contraseñas, los cambios de contraseña y la integración de los sistemas de autenticación de múltiples factores es una bóveda de credenciales. La siguiente solución más accesible después de la administración de credenciales es la separación de la autenticación del control de acceso.

Mejor práctica 3: Separar la autenticación del control de acceso

En la mayoría de las redes, una vez que la persona obtiene acceso a la red, él o ella cuenta con la visibilidad (y posible acceso) a una amplia gama de dispositivos y sistemas. Entre los resultados de esta arquitectura de red existen infracciones como Target, Home Depot, la red de suministro eléctrico ucraniana y muchos otros. Se logran con una cadena de ataque de infracción. Con la cadena de ataque de infracción, los atacantes completan una serie de pasos, a veces de manera iterativa, para llevar adelante una infracción exitosa. El ataque comienza obteniendo acceso a una red, con frecuencia a través de credenciales de proveedores o terceros comprometidas. Una vez dentro, el atacante puede buscar en la red infiltrada para encontrar vulnerabilidades o credenciales adicionales que explotar para obtener cada vez más acceso, a niveles cada vez más altos de privilegios, hasta llegar al objetivo final, como fue el caso en la infracción a la red de suministro eléctrico ucraniana.

> "Las tres compañías indicaron que los actores despejaron algunos sistemas ejecutando malware KillDisk al final del ataque cibernético. El malware KillDisk borra los archivos seleccionados en los sistemas tomados como objetivo y corrompe el registro de arranque principal, lo que deja a los sistemas inoperables. También se informó que, al menos en un caso, interfaces hombre-máquina (HMI) basadas en Windows, metidas en unidades terminales remotas, también se sobrescribieron con KillDisk. Los actores también dejaron inoperables dispositivos en serie Ethernet en subestaciones, corrompiendo el firmware. Además, los actores programaron desconexiones con informes del servidor Sistema de alimentación ininterrumpida (UPS) mediante su interface de administración remota. El equipo evalúa que estas acciones se realizaron en un intento de interferir con los esfuerzos de restauración esperados".
>
> Ataque cibernético contra importante infraestructura ucraniana
> Fecha de publicación original: jueves, 25 de febrero de 2016

Como se mencionó en Mejores prácticas 2, una manera de cortar con la cadena de ataques es controlar el acceso a la red y complicar el ingreso de un atacante con la autenticación de múltiples factores. Otra capa de defensa es limitar su visibilidad y acceso a recursos en la red. La mayoría de los proveedores solo necesitan acceso a sistemas muy específicos. No necesitan acceso ni visibilidad de toda la red ni de una subred.

La visibilidad y acceso de la red puede limitarse con segmentación física de redes. Esto suele realizarse para cumplir con un mandato normativo. Al segmentar la red y controlar el acceso, el alcance de recursos disponibles puede ser limitado. Si bien este puede ser un enfoque efectivo, tiene desventajas:

- los gastos administrativos requeridos para establecer y mantener la arquitectura de la red;
- y la vulnerabilidad de las conexiones entre distintas partes de la red, ya que un atacante puede encontrar un modo de atravesar las conexiones de la red para obtener acceso al objetivo.

Una mejor alternativa es usar segmentación lógica con una solución de administración de identidades con privilegios, como CA Privileged Access Manager, que puede limitar el acceso a los recursos. Esta solución funciona implementando un "punto conflictivo" que un usuario externo debe atravesar para obtener acceso a los recursos protegidos. Este enfoque logra una serie de beneficios.

- **Control de acceso confianza cero:** Un inicio de sesión exitoso no ofrece acceso a toda la red. En cambio, las políticas que especifican qué recursos están disponibles para un usuario son habilitadas por el sistema y limitan a un individuo a solo esos sistemas. Este enfoque permite un control muy cercano de la visibilidad y el acceso. Un individuo nunca ve los recursos a los que no puede acceder. El usuario solo ve una lista predefinida de los sistemas a los que tiene permitido el acceso.
- **Prevención del avance:** Para controlar el movimiento lateral dentro de una red, el sistema intercepta una variedad de comandos de red, como TELNET o SSH y evita que se ejecuten. Esta capacidad limita el acceso de terceros solo a sistemas previamente especificados y elimina formas de obtener visibilidad del resto de la red e intentos de llegar a otros sistemas.

Es importante estandarizar y consolidar los métodos de acceso con un punto conflictivo, con una solución de administración de acceso con privilegios o VPN o alguna otra solución que canalice el acceso a través de las vías conocidas. Al definir rutas aceptables para el acceso externo a recursos, el monitoreo se torna mucho más fácil. Al contener protocolos no aprobados y dirigir sesiones aprobadas a una ruta predefinida, las anomalías son fáciles de identificar para mayor investigación, donde las herramientas SIEM y de inicio de sesión pueden ayudar a marcar eventos anormales.

Mejor práctica 4: Prevenir los errores y comandos no autorizados

Los derechos y permisos de acceso pueden usarse para limitar el acceso a recursos de TI. A veces, este enfoque no ofrece el grado de precisión necesario para realmente controlar lo que alguien hace en un sistema. Por ejemplo, un administrador de sistema de terceros puede necesitar iniciar sesión en un servidor con algo como raíz o admin., algún tipo de cuenta de supe usuario con grandes privilegios. Motivos técnicos o administrativos pueden garantizar el enfoque de acceso y hacer que la situación sea riesgosa. Con ese nivel de poder, el individuo puede hacer casi cualquier cosa en el sistema, inclusive destruirlo por completo, que es un riesgo inaceptable para la mayoría de las organizaciones, incluso si esta persona es un empleado dentro de la compañía.

Un enfoque distinto, con una solución de administración de acceso con privilegios ofrece un enfoque más aceptable, ya que implementa controles específicos de permisos para administrar este tipo de usuarios. El sistema de administración del acceso con privilegios permite que se organicen las sesiones de una persona en varios sistemas de destino a través de una serie de cuentas diferentes, cada una con diferentes niveles de permiso.

El filtrado de comandos y las listas blancas y negras también pueden usarse para limitar qué comandos puede realizar un usuario específico. Una lista negra contiene comandos que no están permitidos y una blanca, comandos que pueden emitirse. Las listas blancas y negras usadas juntas brindan un alto nivel de control y flexibilidad. Así, el uso de privilegios puede mantener el recurso de computación sin causar daños inaceptables. Un beneficio inesperado del filtrado de comandos es la prevención de errores inadvertidos. En el ejemplo anterior, el supe usuario puede mover archivos, pero no reformatear el disco.

Los filtros de comandos combinados con el inicio de sesión facilita el control y las alertas, para que el sistema responda de manera apropiada cuando alguien intenta pasar uno de los comandos. Puede emitir una alerta o terminar con la sesión de un atacante. Por ejemplo, un individuo puede decidir experimentar un poco antes de llegar a los límites establecidos por los filtros de comando. Cuando se llega a los límites, el sistema puede generar una alerta que inste una investigación de las acciones del individuo. Estas son algunas de las respuestas posibles:

- bloquear y advertir al usuario;
- finalizar la sesión:
- desactivar la cuenta del usuario;
- y generar alerta/alarma para SOC.

Mejor práctica 5: Monitorear e investigar

Siempre se requiere cierto nivel de monitoreo. El nivel y alcance específicos de monitoreo dependen de sus consideraciones de administración de cumplimiento y riesgos.

Incluso en casos con poco riesgo intrínseco, iniciar sesión ayuda a solucionar problemas e investigar actividad sospechosa. El inicio de sesión básico es un registro básico de lo que sucedió y es útil para revisar actividad inapropiada o no autorizada. Incluye lo siguiente:

- frecuencia de inicio y fin de sesión;
- sistemas accedidos;
- comandos emitidos;
- respuestas recibidas.

En cualquier tipo de situaciones sensibles, el monitoreo aprovecha los registros para implementar políticas establecidas para el acceso del sistema, dado que los esfuerzos para violar estas políticas merecen atención. Pueden tomarse diversas acciones en respuesta a un intento de violación de política. A un nivel básico, los intentos de violar las políticas requieren una investigación para descubrir qué sucedió. Puede requerirse capacitación adicional para ayudar a la gente a comprender qué tareas se esperan de ellos o cómo deben realizarse. Una violación podría ser un simple error o podría ser un indicio de intento de comportamiento malintencionado. El monitoreo contribuye con la captura de eventos sospechosos, para que sean investigados.

Las investigaciones son muy importantes, como demuestra JPMorgan Chase, cuyo personal descubrió que había habido una infracción después de investigar a uno de sus proveedores.

> "JPMorgan descubrió hackers dentro de sus sistemas en agosto, después de descubrir que el mismo grupo de hackers se había metido en un sitio web de una carrera de beneficencia patrocinada por el banco. Recién después de descubrir que el sitio web Corporate Challenge había sido infiltrado, JPMorgan se enteró de que su propia red había sido atacada por los mismos hackers".

> "Un servidor desatendido permitió la entrada de los hackers de JPMorgan"
> The New York Times, 22 de diciembre de 2014

Para situaciones aún más sensibles, el registro o captura de sesiones puede ser necesario para brindar información completa sobre qué sucedió en una determinada sesión, para ayudar en posibles investigaciones futuras. Un caso de uso común es capturar los registros de pantalla completa de las sesiones sensibles. Estos registros pueden ser examinados después, en casos de violaciones conocidas de política o problemas que surjan después con un sistema, para evaluar qué sucedió en la sesión original. De acuerdo a la sensibilidad del entorno, pueden realizarse verificaciones. Uno de los desafíos que suele estar asociado con el registro de sesión es que los archivos de registro (y gastos del sistema) pueden ser significativos. El otro desafío es un plan de acción para revisar las sesiones registradas. Dado que los costos de tiempo y tecnología aumentan para el registro de sesión, el análisis costos-beneficios ayuda a identificar situaciones que son apropiadas para este nivel de inversión. Como punto de partida, es útil identificar lo siguiente:

- cuándo realizar un registro y durante cuánto tiempo;
- cuándo y con qué frecuencia revisar los registros;
- y cuál es la política de retención de registros.

Si elige implementar técnicas de registro de sesión, varias capacidades son importantes:

- fácil acceso a metadatos de la sesión (cuándo empezó y terminó);
- la capacidad de recorrer rápidamente sesiones e ir a un punto determinado en un registro;
- y la capacidad de destacar la actividad "interesante", como violaciones de políticas y actividades sensibles.

Las situaciones de mayor riesgo pueden requerir control "por encima de los hombros" o acceso de dos partidos, que requiere que otro individuo mire lo que un usuario con privilegios hace en tiempo real. Por lo general, estas situaciones de riesgo extremo no ocurren con terceros o usuarios externos. El control "por encima de los hombros" involucra desafíos técnicos. Sin embargo, asimismo, el control debe ser realizado con grandes capacidades, para que se comprendan ambas acciones tomadas y sus ramificaciones en el entorno mayor. Desde una perspectiva de administración de riesgos, el control "por encima de los hombros" puede ser apropiado para una cantidad muy limitada de situaciones.

El monitoreo típico consiste en un proceso de dos pasos:

- **Respuesta en tiempo real a violaciones de política:** pueden ocurrir varias acciones; advertir al usuario, generar una alerta a un centro de operaciones de seguridad o cerrar una sesión o cuenta.
- **Investigación y análisis posteriores al hecho:** una revisión de registros y registros de sesión para respaldar la resolución del problema o las investigaciones forenses.

La investigación y análisis posteriores al hecho pueden incluir esfuerzos para correlacionar registros y alertas generados por un sistema de administración del acceso con privilegios con otras herramientas de seguridad y red para eventos inesperados. Por ejemplo, en organizaciones en las que se ha implementado una solución de administración del acceso con privilegios, toda la actividad administrativa está centralizada en el sistema de administración de acceso con privilegios. Si las solicitudes de sesión SSH o TELNET vienen de otras partes de la red, se ven como alertas inmediatas de que algo está mal y se investigan. Al eliminar o prohibir herramientas administrativas no autorizadas, la actividad sospechosa es relativamente fácil de identificar. Un firewall de la próxima generación puede ayudar a marcar aplicaciones o protocolos prohibidos. Otras actividades sospechosas pueden incluir acceso en momentos inesperados o comportamiento inusual, como descargas de archivos.

Con el tiempo, las auditorías y revisiones manuales en curso ayudan a encontrar herramientas y políticas para ignorar los falsos positivos y automatizar disparadores y alertas para que sean más efectivos.

Sección 3:

Beneficios de manejar el riesgo de proveedores externos

Ninguna organización moderna puede ser aislada y desconectada de Internet. Las relaciones comerciales requieren colaboración electrónica, donde se intercambia información sensible entre socios. Hoy en día, las compañías usan proveedores externos para servicios de contabilidad, procesamiento de tarjetas de crédito, consejería legal, administración de planes jubilatorios, servicios de comercialización, fabricación y cientos de otros trabajos. La colaboración electrónica entre socios comerciales ahorra tiempo y dinero, y habilita procesos y sistemas automatizados que mejoran la precisión, calidad y eficiencia. Restringir el acceso de red de terceros al firewall no es una opción. Los recursos relevantes deben estar disponibles para socios de negocios, para obtener beneficios comerciales. Al mismo tiempo, las compañías se enfrentan a riesgos reales conectándose con terceros.

Las infracciones de seguridad son caras. De acuerdo a la revista Fortune, después del último robo del 2013 de 40 millones de tarjetas de pago y 70 millones de otros registros, Target estimó costos de USD $162 millones, después del reembolso de los seguros. Sony estimó haber gastado USD $35 millones en “restaurar sistemas financieros y de TI” después de una infracción en 2014. Home Depot registro USD $28 millones en gastos netos, sin impuestos. Los costos mencionados no incluyen el daño en la reputación y el aumento en las primas de seguro. Además de estos grandes costos, las vidas de las personas dan un vuelco. Muchos pierden sus trabajos y los que quedan tienen que trabajar contrarreloj, investigando y mitigando infracciones.

> “Más allá del modo en que lo midamos o si buscamos hacia atrás o hacia adelante, acordamos en el punto central: las compañías tienen que invertir en seguridad de la información”.
>
> Benjamin Dean, colega de Columbia University’s School of International and Public Affairs. Revista Fortune, 27 de marzo de 2015

Sin dudas, ninguna compañía quiere estar en la portada del Wall Street Journal como un ejemplo de otra gran infracción. Las cinco principales y mejores prácticas de seguridad pueden bloquear infracciones y permitir las actividades comerciales legítima, lo que mantiene seguros los recursos de información y la reputación de su organización.

Sección 4:

Conclusiones

De acuerdo al informe de investigaciones de infracción de datos (DBIR) de Verizon en 2015, de los 700 millones de registros comprometidos, hubo una pérdida financiera estimada de USD $400 millones. Setenta organizaciones que contribuyeron con este informe registraron 79 790 incidentes de seguridad, de los que 2122 fueron infracciones confirmadas en 61 países y dos tercios de los incidentes ocurrieron en los EE. UU. A pesar de que la vasta mayoría de amenazas siguen viniendo de fuentes externas, las amenazas internas y de socios aumentaron levemente entre 2013 y 2014. Los riesgos son reales, tal como quedó demostrado por la mega infracción en la Oficina de administración de personal (OPM) de los EE. UU.

El método del ataque a la OPM siguió una fórmula: apuntar a un subcontratista en un ataque de ingeniería social y robarle las credenciales para obtener acceso a la red; plantar malware en un sistema y crear una backdoor; Exfiltrar datos durante meses, sin ser detectados.

La infracción de OPM también enfatizó la vulnerabilidad de la ingeniería social de las organizaciones. Los empleados y contratistas del gobierno ahora son sujetos a programas de capacitación de seguridad, para conocer los peligros de la suplantación de identidad y otras amenazas a los medios.

> "Los hackeos más innovadores y perjudiciales del 2015"
> CSO Magazine, 28 de diciembre de 2015

Muchos riesgos pueden mitigarse usando cinco mejores prácticas descritas en este documento, que funcionan en conjunto para crear una defensa en capas más sólida, flexible y eficaz para la seguridad de la información. Estas prácticas incluyen las siguientes:

- implementar procesos y controles de respaldo con el objeto de definir y aplicar políticas de acceso para usuarios externos con privilegios;
- autenticar usuarios con mayor eficacia mediante el uso de tecnología de autenticación de múltiples factores, de modo que sea más difícil comprometer las credenciales con privilegios, incluso frente a ataques de suplantación de identidad e ingeniería social;
- separar la autenticación del control de acceso, de modo que los usuarios con privilegios tengan solo una visibilidad limitada de las redes internas, lo que limita el posible daño que un usuario —o un grupo de credenciales robadas— puede ocasionar;
- prevenir los errores y comandos no autorizados al aplicar disparadores en tiempo real como primera línea de defensa, con lo que se protege la infraestructura de errores inadvertidos e intentos malintencionados;
- y monitorear la actividad e investigar los eventos sospechosos para detectar rápidamente las violaciones, mejorar la capacitación cuando sea necesario y perfeccionar los procesos y la automatización en forma constante, para eliminar falsos positivos.

Los sistemas de administración del acceso con privilegios han automatizado funciones y capacidades que ayudan a definir, automatizar e implementar las cinco mejores prácticas descritas en este informe, a lo largo de toda la empresa, para entornos físicos, virtuales y en la nube, que ayuda a las organizaciones a implementar un proceso consistente a lo largo de sistemas, aplicaciones y 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 Departamento de servicios financieros del estado de Nueva York, "Actualización de seguridad cibernética en el sector bancario: proveedores externos de servicios"
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

¿Cuánto les cuesta a las grandes compañías las infracciones de datos? Sorprendentemente poco
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 cuenta con más de dos décadas de experiencia en software empresarial, y se enfocó en áreas como la red y los sistemas de administración, así como también múltiples segmentos de la seguridad, incluida la gestión de identidad, la seguridad de aplicaciones, la gestión de vulnerabilidades, el cumplimiento y la seguridad de red. Como ex-analista de investigación y escritor, ha definido, construido y comercializado diferentes soluciones de administración y seguridad que mejoran las operaciones y ayudan a garantizar la integridad y confiabilidad de la infraestructura de tecnología de la información de la empresa. En la actualidad es responsable de marketing a nivel mundial de la cartera de productos de administración de acceso con privilegios de CA Technologies.