LIBRO BLANCO | NOVIEMBRE DE 2015

Rompamos la cadena de los ciberataques:

evite las violaciones de datos con la gestión de los accesos con privilegios

ca technologies

Resumen ejecutivo

Reto

Es imposible que transcurra un solo día sin que oigamos noticias de un nuevo robo de datos, con la consecutiva pérdida de secretos confidenciales, registros financieros o información personal. Estos incidentes se suceden en todos los sectores de la economía: comercio, educación, instituciones gubernamentales, etc. Suponen un auténtico freno a la economía mundial, responsable de costes por valor de cientos de miles de millones de dólares anuales,[1] tanto que, si no se prevé adoptar medidas inmediatas y agresivas, la factura derivada de la ciberdelincuencia subirá hasta los billones de dólares en menos de una década.[2] Más allá de las cifras figura también el devastador impacto que sufren las personas que han visto vulnerados los datos más íntimos de sus vidas privadas.

Los especialistas en seguridad han peleado por establecer defensas basadas en el perímetro. Dichas defensas, por decirlo de la forma más llana, dejan pasar a los buenos mientras cierran el paso y mantienen fuera a los malos. La concatenación sin fin de violaciones de la que somos testigos nos aporta pruebas de primera mano que demuestran que tales perímetros no han cumplido su objetivo primordial. Como consecuencia, las organizaciones se enfrentan a la necesidad de poner en pie una nueva capa de seguridad, fundamental, centrada específicamente en la protección y la gestión de las identidades. Un requisito nuevo y esencial en la lucha por contener la propagación de las infracciones. De entre todas estas identidades, ninguna es tan crucial como las que pertenecen a los usuarios con privilegios. En todas las violaciones, robar y explotar estas credenciales constituye el principal vector de ataque, ya que otorga las “llaves del reino”.

Oportunidad

Los equipos de seguridad tienen a su disposición un conjunto maduro de tecnologías y procesos, denominado en términos generales "gestión de accesos con privilegios", que les ofrece medios para derrotar y cortar el paso a los atacantes. Los usuarios malintencionados, tanto internos como externos, actúa de forma predecible y suelen seguir una serie de pasos lógicos para ejecutar sus ataques con éxito. Estas secuencias, que fueron identificadas y articuladas originalmente por los equipos de ciberseguridad de Lockheed Martin,[3] se han bautizado como cadenas de ciberataque o “kill chains”. El motivo del nombre es que, si es posible interrumpir o eliminar (del inglés "kill", matar) la secuencia de pasos de los atacantes en cualquier punto, se conseguirá evitar o mitigar el ataque definitivo. La gestión de los accesos con privilegios proporciona medios para frustrar los ataques en varios pasos del ciclo de vida del ataque. En este documento analizaremos una versión algo simplificada de una cadena de ciberataque y daremos ejemplos concretos de cómo contribuye la gestión de accesos con privilegios a detener ataques y proteger organizaciones frente a las violaciones.

Ventajas

Las ventajas financieras de evitar tales violaciones están claras. Más difíciles de cuantificar son los costes indirectos que conllevan los perjuicios sufridos por la marca y la reputación, pero a menudo más cuantiosos. Perjuicios como la pérdida de la confianza entre partners y clientes o los impactos sobre la valoración de la empresa en los mercados. Sin embargo, por significativos que sean dichos costes, palidecen al compararlos con la devastadora repercusión que la sustracción de información personal detallada puede tener sobre personas confiadas, que no sospechan nada. Queda claro entonces que la gestión de accesos con privilegios, con su capacidad de mitigar unos perjuicios tan extendidos, reporta ventajas extraordinarias.

Las violaciones de datos, un reto: riesgos cada vez mayores y daños incalculables

Cuando sopesamos la actual sucesión de incidentes de seguridad, es habitual referirse al incidente Target, que sucedió a finales de 2013. El caso Target supuso el robo de unos 70 millones de registros de tarjetas de pago, pero no fue la primera violación de datos ni la mayor de la historia. Ni tan siquiera de 2013. Sin embargo, una combinación de factores provocaron que el caso Target estimulase el interés de muchos actores esenciales acerca de la naturaleza tremendamente dañina de los ataques que se venían sucediendo. Desde el robo de datos de Target, hemos presenciado un sinfín de ataques más pequeños, con menos repercusión pública, además de una serie continuada de incidentes a gran escala, como los de Home Depot o JP Morgan Chase hace casi un año. Recientemente, mientras se redacta este documento, el robo de datos a Experian supuso la sustracción de datos personales confidenciales y muy sensibles de unos 15 millones de clientes de T-Mobile.

> "Para los negocios digitales, la gestión de identidades con privilegios se ha vuelto algo increíblemente importante y complicado. Es importante porque un solo administrador con malas intenciones o el robo de las credenciales de un administrador puede tener efectos desastroso sobre los clientes, los ingresos y la reputación a largo plazo".
>
> Forrester Research[4]

De acuerdo con Intel Security y el Center for Strategic and International Studies (Centro de estudios estratégicos e internacionales), se calcula que el monto de las pérdidas ocasionadas por este tipo de ciberdelincuencia en 2014 ascendió a unos 400 000 millones de dólares. Puede resultar difícil hacerse a la idea de qué representan cifras tan colosales. Así pues, para ponerlo en perspectiva, comparemos esos 400 000 millones de dólares con el volumen de ingresos que genera el tráfico de drogas a nivel mundial. Esta última actividad queda algo empequeñecida, puesto que se calcula que supone 300 000 millones anuales. El impacto de la ciberdelincuencia es incluso mayor que el PNB de muchas naciones prósperas. Por ejemplo, Singapur, país que repite la cifra anterior por pura coincidencia: 300 000 millones de dólares anuales. Esto constituye, a todas luces, un gran problema de índole financiera. Los datos sugieren que, si no se adoptan medidas inmediatas, la situación está abocada a empeorar. McKinsey prevé que la ciberdelincuencia provoque un impacto global anual por valor de 3 billones de dólares, 10 veces más que la cuantía que supone actualmente.

Está claro que estos incidentes resultan perjudiciales. Las organizaciones que han sufrido violaciones de datos y otras similares han experimentado pérdidas en su capitalización de mercado, han visto descender las ventas, han visto evaporarse la buena voluntad de los clientes y han notado que se reducían sus beneficios. Todo ello sin contar con los perjuicios financieros y emocionales que sufren los usuarios afectados por estas violaciones, fruto de los estragos causados por delitos como la suplantación de identidad. Ahora bien, por preocupante que sea todo esto, las noticias son todavía peores si nos fijamos en otros incidentes que han comenzado a suceder más recientemente.

En primer lugar, se han empezado a ver ataques que buscan claramente provocar un impacto material en las operaciones de las organizaciones agredidas. Tal vez no le suene de nada Code Spaces, pero era una pequeña empresa con sede en el Reino Unido, especializada en proporcionar servicios de control de versiones y copias de seguridad basadas en nube para desarrolladores. En junio de 2014, un atacante logró obtener las credenciales administrativas para acceder a la consola de gestión de los servicios web de Amazon (AWS) de Code Spaces. Tras crear una larga serie de cuentas y puertas traseras, el agresor exigió a los responsables de Code Spaces un rescate. Cuando los administradores autorizados intentaron expulsar al atacante del sistema era ya demasiado tarde. Con todos los accesos administrativos a su disposición para el sistema de gestión de Code Spaces completo, el agresor tomó represalias y destruyó rápidamente toda la infraestructura de tecnologías de la información de la empresa: servidores, aplicaciones y un componente fundamental: las copias de seguridad de datos

y sistemas. El ataque culminó en cuestión de horas. La empresa se vio forzada a suspender sus actividades en cuestión de días.[5] El ataque a Code Spaces es un ejemplo dramático, pero hay muchos más casos que ilustran esta tendencia. Como los incidentes de Sony Pictures Entertainment y Saudi Aramco.

A partir de este punto, tan solo un paso nos separa de la última tendencia, que según los expertos es el ciberespionaje. Entre las primera señales de estas violaciones destacaban las agresiones a compañías aseguradoras, como Anthem, Premera y CareFirst, sucedidos a principios de 2015. Formalmente, no se ha acusado formalmente a ningún estado-nación de ser responsable de estos ataques, pero hay especulaciones muy difundidas según las cuales, el robo de millones de registros de datos personales formaba parte de una campaña mayor, cuyo fin sería recopilar informes sobre personas que ocupaban cargos sensibles dentro de instituciones gubernamentales, contratistas de defensa o corporaciones financieras y de telecomunicaciones, así como responsables de toma de decisiones geopolíticas y otros. Estas violaciones de sustracción de datos coincidieron con la comunicación de un aviso confidencial del FBI en EE. UU., que advertía de que hackers chinos habían elegido como objetivo información personal identificable de redes comerciales y gubernamentales de los EE. UU.[6] Desde entonces, naturalmente, nos hemos enterado del robo de datos de la Oficina de Gestión de personal (Office of Personel Management u OPM) de EE. UU. En dicha acción se robaron datos personales, incluidos exhaustivos historiales biográficos, financieros, laborales y personales de personas solicitantes de autorizaciones de seguridad.

Oportunidad: Cuentas con privilegios, el nuevo frente de batalla

Vamos a detenernos un minuto y recapitular. Las violaciones de datos son un gran problema, cada vez mayor. Hay mucho en juego, cada vez más, y cada día que pasa nos enfrentamos a adversarios más sofisticados y mejor financiados. Llegados a este punto, no nos extrañaría que incluso el lector más optimista sienta una punzada de pesimismo. Ante un reto de estas dimensiones, ¿qué se espera que podamos hacer para combatirlo?

Ilustración A.

La gestión de accesos con privilegios ayuda a las organizaciones a lograr cinco objetivos de alto nivel.

Hay buenas noticias: existe un motivo para la esperanza, ya que prácticamente todos estos ataques muestran un rasgo común. Ese rasgo compartido son los usuarios con privilegios. Más específicamente, las cuentas y credenciales con privilegios que esas personas utilizan para configurar, mantener o utilizar nuestra infraestructura de tecnologías de la información. En todos los casos de violación que hemos tratado, ha quedado demostrado que robar y explotar esas credenciales, lo que proporciona un acceso con privilegios a la infraestructura de TI, constituye un factor esencial para el éxito de los agresores y un vector de ataque de primera magnitud.

> "En 2018, la incapacidad de las organizaciones para dimensionar y contener adecuadamente los accesos con privilegios será la raíz de hasta el 60 % de los usos indebidos internos y de los incidentes de robo de datos, lo que supone un gran auge respecto al 40 % actual".
>
> Gartner[7]

Antes de analizar el papel principal que desempeñan los accesos con privilegios en los intentos de violación de datos con éxito, sería útil examinar brevemente quiénes son los usuarios con privilegios, ya que la población de personas con accesos privilegiados, al igual que el número de cuentas reales y credenciales utilizadas para proporcionar esos accesos son cifras muy superiores a lo que se suele reconocer.

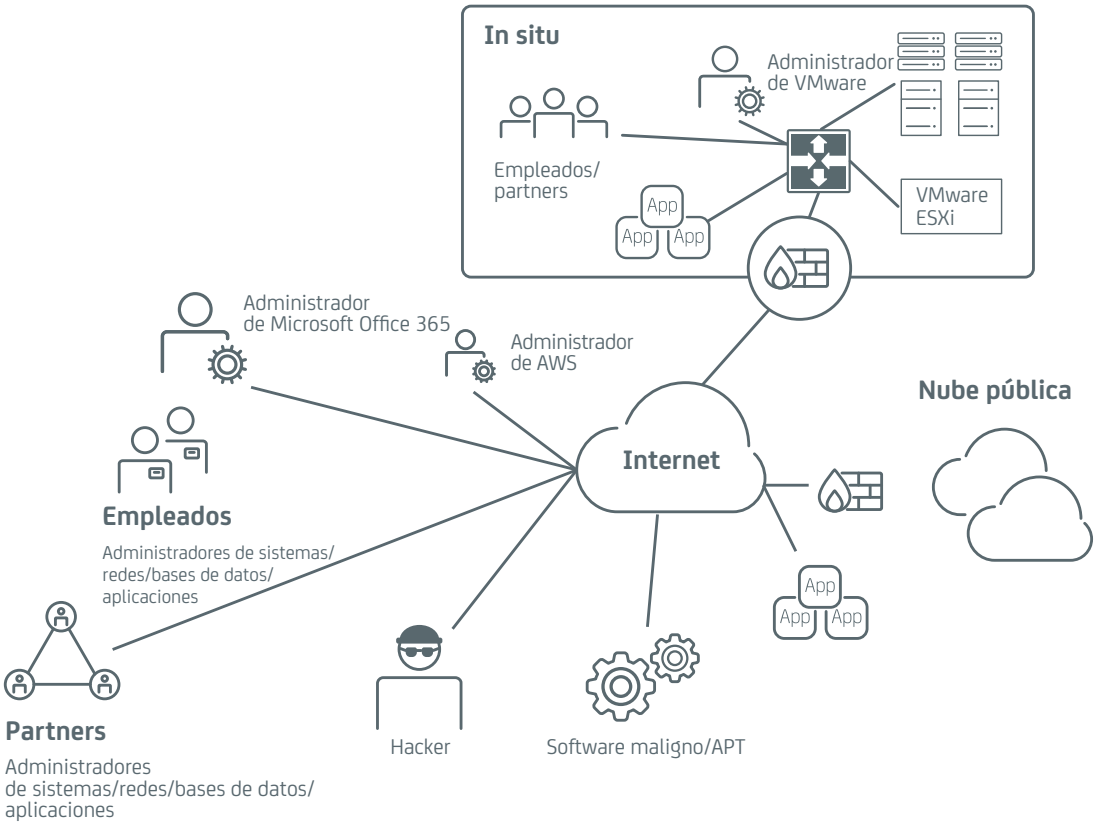


Ilustración B.

Cuentas con privilegios, el nuevo frente de batalla

Durante años, cuando pensábamos en usuarios con privilegios, generalmente solo nos fijábamos en personal interno de la organización con responsabilidades de primera mano relacionadas con la administración del sistema y las redes. Como consecuencia, mucha gente reducía el riesgo al mínimo y consideraba que el reto de gestionar los accesos con privilegios consistía en controlar la conocida como "amenaza interna". Es cierto que los usuarios internos con malas intenciones pueden provocar daños graves, pero este tipo de incidentes no son frecuentes y apenas representan una pequeña porción de las violaciones.

En realidad, muchos usuarios con privilegios no son internos. Se trata de distribuidores, contratistas, partners de negocio y otros, a quienes se han concedido accesos con privilegios correspondientes a sistemas internos de la organización. En muchas empresas, la cifra de usuarios de terceros bien puede superar a la de usuarios con privilegios "internos" convencionales. Asimismo, la experiencia sugiere que las terceras partes suponen una fuente de riesgos mayor. Pensemos en los casos de violaciones que hemos mencionado, incluidos los de Target, Home Depot y OPM entre otros. Se infringió la seguridad de las credenciales de un usuario de terceros con autorización y a continuación, se utilizaron para acceder ilícitamente a toda la red y sus recursos.

Además, el número de usuarios con privilegios ha ido aumentando, a medida que se da el salto a la nube y se adoptan tecnologías como la virtualización. Si nos fijamos en la nube, concretamente, muchos de estos usuarios con privilegios podrían en realidad no ser miembros del personal de TI convencional. Como ejemplo, pensemos en los representantes de líneas de negocio que adquieren ofertas basadas en servicios donde, en el peor de los casos, las organizaciones de seguridad y los departamentos de TI tradicionales podrían estar completamente desinformados del nivel de exposición.

Sin olvidar que, cada vez con más frecuencia, muchos usuarios con privilegios no son usuarios en realidad. O, como mínimo, no son personas. En los entornos virtualizados y en la nube, el auge de las herramientas de aprovisionamiento y configuración automatizadas, impulsada por scripts y programas, ha introducido todavía a más "usuarios" con notable autoridad sobre grandes secciones de la infraestructura y capacidad de acceso. Una consecuencia inmediata para estos sistemas automatizados son las cifras de scripts y programas (cuya cuenta a menudo se pierde) ensamblados durante años de operaciones, que requieren accesos administrativos o sensibles a recursos como bases de datos u otras aplicaciones y sistemas. En ambos casos, este acceso y estas operaciones están controlados por la autenticación, de un modo bastante adecuado. Por desgracia, las credenciales que se requieren suelen estar integradas como no modificables en los archivos de configuración de las aplicaciones. Así son objetivos fáciles para usuarios malintencionados, tanto internos como externos.

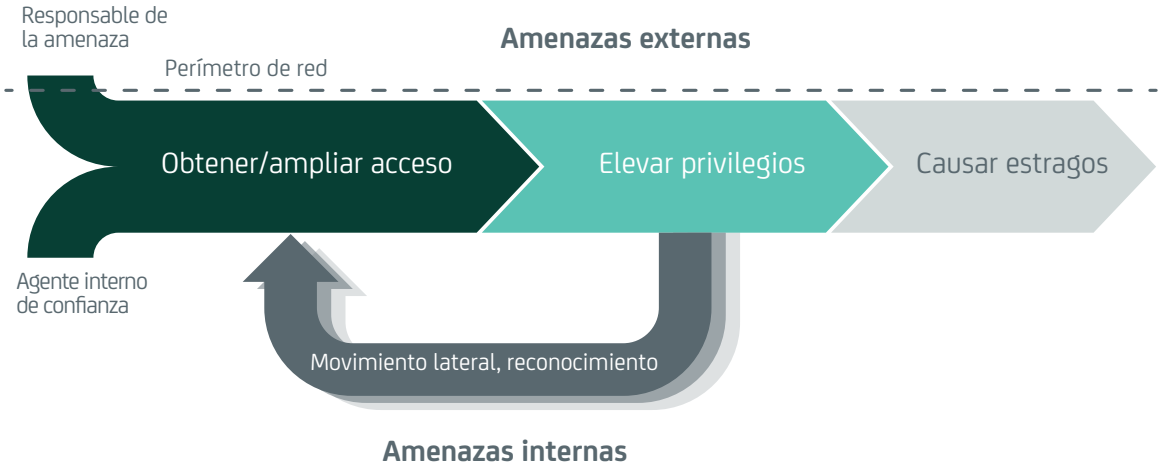
Lo último y tal vez más importante: hay que recordar que no hablamos solamente de usuarios con privilegios, sino de todas las cuentas con privilegios que existen en una organización típica y sus correspondientes credenciales. Esas credenciales suponen la amenaza más significativa, dado que explotarlas es esencial para determinar en qué modo se efectúan los ataques.

Conozcamos la cadena de ciberataque: ¿cómo funciona?

La cadena de ciberataque o "kill chain" de un intento de violación de datos está compuesta por una serie de pasos coherentes y predecibles, que un atacante debe dar para alcanzar correctamente su objetivo. Si bien la articulación de ciertas cadenas de ciberataque puede ser bastante compleja, es posible resumir los pasos clave asociados a la típica cadena de ciberataque de violación de datos de forma simplificada.

Ilustración C.

Ejemplo de una cadena de ciberataque (kill chain) simplificada



Existen cuatro pasos clave:

- **Obtener acceso:** En primer lugar, es necesario acceder a la red. Si es usted un usuario interno auténtico o quizás un tercero de confianza, resulta fácil. Basta con explotar las credenciales y el acceso que ya tiene. Para el resto de atacantes, no sería mucho más complicado. Gracias a la creciente popularidad de redes sociales como LinkedIn, es relativamente fácil identificar y marcar como objetivos individuos específicos entre los miembros de una organización que probablemente dispongan de acceso privilegiado a los sistemas. La creciente sofisticación de las estafas de robo de datos "spearphishing" implica que un atacante lo tiene más fácil que nunca para engañar incluso a las personas más experimentadas y habilidosas para que le entregue sus credenciales. Especialmente credenciales poco sofisticadas, como identificadores de usuario y contraseñas.
- **Elevar los privilegios:** Una vez que el atacante ha conseguido el acceso, uno de los primeros pasos es elevar de nivel los privilegios. Normalmente, se hace vulnerando la seguridad de otras credenciales con privilegios. Este paso sirve de apoyo para dos actividades esenciales. En primer lugar, otorga al atacante la capacidad de adoptar ciertas medidas, como alterar o inhabilitar el inicio de sesión o instalar software maligno, que le ayudarán a evitar que se descubra su existencia y su actividad. En segundo lugar, sienta las bases para el siguiente paso de la cadena de ciberataque, el reconocimiento y movimiento lateral.
- **Realizar movimientos laterales y reconocimiento:** Salvo que se trate de un atacante con muy buena suerte, es poco probable que el primer sistema al que haya conseguido acceder sea el auténtico objetivo del ataque. Casi con toda seguridad, la diana ansiada (sistemas de procesamiento de tarjetas de pago, datos confidenciales, registros personales y similares) estará ubicada en otro lugar de la red, en otros sistemas. Así que el siguiente paso de la cadena de ciberataque es efectuar un reconocimiento de la red y moverse hacia sistemas y servidores más próximos al objetivo definitivo.
- **Repetir el proceso según sea necesario:** A partir de aquí, es sencillo. Basta repetir el proceso hasta alcanzar el objetivo final, sea cual sea. Una vez más, la experiencia ha demostrado que los atacantes pueden ser muy pacientes y dedicar tiempo a investigar y navegar por las redes para desarrollar su misión. Los informes de violaciones de datos que se publican de forma rutinaria indican que los atacantes han pasado meses e incluso años trabajando en el interior de las redes de la víctima. Cuando por fin alcanzan su objetivo, pueden llevar a la práctica el ataque e inutilizar sistemas, robar datos u otras acciones.

Por desgracia, sobre todo cuando no están presentes ni tan siquiera herramientas y procesos rudimentarios de gestión de accesos con privilegios, existen una serie de cosas que hacen las organizaciones y que facilitan la ejecución de esta cadena de ciberataque por parte de los atacantes. Los errores más habituales son los siguientes:

- **Utilizar técnicas de autenticación débiles** para acceder a la red o a recursos específicos, incluido el error de no eliminar las cuentas y contraseñas administrativas predefinidas y confiar en credenciales poco sofisticadas, como sencillas combinaciones de identificador de usuario y contraseña, fáciles de robar o vulnerar.
- **Descuidar la gestión de las contraseñas y claves**, sin cambiar las credenciales de forma frecuente y periódica. En organizaciones con muchísimos recursos, esto puede resultar terriblemente problemático, ya que resulta tentador evitar los problemas operativos y reducir los gastos generales aplicando prácticas poco recomendables, como la reutilización de las credenciales y no rotar las credenciales de forma periódica.
- **Permitir el uso de cuentas compartidas**, especialmente en el caso de cuentas potentes con privilegios, como las cuentas de usuario raíz o administrador. Esta práctica introduce diversos riesgos, ya que para un usuario es fácil compartir una credencial con otros. Además, que muchas personas tengan acceso a una credencial determinada hace resulte prácticamente imposible atribuir la ejecución de una tarea concreta a una persona específica dentro de un sistema. Ello complica el análisis forense y la solución de problemas.
- **Equiparar la autenticación con el control de accesos.** Muchas redes están segmentadas de forma ineficiente y, como resultado, en cuanto una persona se introduce en la red, tiene visibilidad sobre muchos más recursos de los que sería necesario o prudente. Eso facilita las tareas de reconocimiento y movimiento lateral, lo simplifica la labor de un atacante en busca del objetivo final.
- **La falta de control y análisis de la actividad de los usuarios con privilegios** puede favorecer la aparición de múltiples problemas. Si no se monitorizan o analizan periódicamente las actividades, se corre el riesgo de pasar por alto comportamientos sospechosos, dándoles rienda suelta a los malhechores. Dada la naturaleza humana, es normal que la gente retuerza o incumpla las reglas si saben que hay pocas probabilidades de que se detecten sus actos.

Recomendaciones: Rompamos la cadena de ciberataque

En líneas generales, una solución de gestión de accesos con privilegios se subdivide en tres aspectos o pasos clave y proporciona medios para romper la cadena de ciberataque, detener a los atacantes e impedir las violaciones.

Primer paso: Impedir los accesos sin autorización

Obligar a que los accesos con privilegios superen una puerta de enlace basada en red para llegar a los recursos constituye un método sencillo de aplicar una autenticación robusta. Obviamente, un sistema de este tipo debería integrarse con la infraestructura de gestión de identidades existente. Por tanto, el sistema debería admitir enlaces con los almacenes de identidades existentes, como Active Directory, o con los directorios de LDAP e incluso con RADIUS o TACACS+ en algunos entornos. El sistema puede y debería admitir la autenticación local, pero generalmente su organización y contará con un almacén de identidades establecido y en uso. Dado que estos sistemas ya definen tanto los usuarios con autorización como las funciones y los permisos, conviene que aproveche esos datos como base para los accesos con privilegios.

Ahora bien, esto no es más que una línea de referencia. Dada lo relativamente fácil que es robar las credenciales de un usuario autorizado, superar una puerta de enlace como esta sería asequible para un atacante. Para impedirlo, es fundamental implantar obligatoriamente el uso de autenticación multifactorial (MFA, multi-factor authentication) para los accesos con privilegios. La adición de la MFA incrementa notablemente el nivel de dificultad que afrontará un atacante con intención de acceder a la red. Hace tiempo, la autenticación multifactorial era una tecnología cara y engorrosa desde el punto de vista administrativo. Sin embargo, los avances tecnológicos han cambiado drásticamente la economía de

implementar tecnologías de autenticación multifactorial y, dado el elevado nivel de riesgo asociado a los accesos con privilegios, incluso un rudimentario análisis de coste/beneficios será favorable a su implementación.

Además, la utilización de autenticación multifactorial también se ha convertido en un tema relevante para la conformidad y las auditorías. El Gobierno Federal de EE. UU. se pusieron en cabeza de esta tendencia con la creación de estándares que imponían el uso de tarjetas denominadas PIV/CAC para el acceso administrativo a los sistemas. Estas son las siglas de verificación de identidades con privilegios (privileged identity verification, PIV) para las agencias gubernamentales civiles y tarjetas de acceso común (common access card, CAD), un dispositivo similar empleado en las entidades militares. Estas tarjetas proporcionan identificación basada en la tecnología PKI (Public Key Infrastructure o infraestructura de clave pública) para una persona. Al combinarse con las comprobaciones de identidad, ofrecen un alto nivel de seguridad sobre la identidad del usuario. También se han añadido estándares similares a una variedad de normas de conformidad, incluida entre otras la revisión más reciente de los estándares de seguridad Payment Card Industry Data Security Standard (PCI-DSS).

Otras medidas de sentido común que se pueden aplicar para reducir el riesgo de accesos no autorizados son las restricciones de acceso a los sistemas basadas en la dirección IP de origen del inicio de sesión de un usuario o la hora del día. Estos tipos de controles se pueden implementar mediante una puerta de enlace de gestión de accesos con privilegios y también por medio de controles basados en agentes sobre servidores o recursos específicos. Si un usuario determinado inicia sesión de forma rutinaria durante un cierto período de tiempo desde un conjunto de ubicaciones concreto, no hay motivo para otorgarle acceso sin restricciones. Además, tal vez le convenga bloquear por completo los inicios de sesión desde un intervalo de direcciones, desde las cuales no sería previsible o deseable que se accediese al sistema.

Un segundo aspecto de este problema es proteger las credenciales utilizadas para acceder realmente a los sistemas gestionados. Como ya hemos descrito, con demasiada frecuencia esas credenciales cuentan con una protección muy pobre, se comparten de forma indiscriminada o se gestionan de forma ineficaz, lo que comporta riesgos obvios. Idealmente, un sistema de gestión de accesos con privilegios debe proporcionar una caja fuerte de credenciales para almacenar y cifrar los pares de contraseñas y claves, lejos de usuarios malintencionados y miradas curiosas. La caja fuerte de credenciales debe admitir capacidades de gestión activa real de las credenciales, interactuar con sistemas para cambiar las contraseñas basándose en estándares apropiados para una organización o el nivel de riesgo del recurso. Automatizar este proceso reduce tanto los riesgos de seguridad (dado que es posible actualizar de forma rutinaria las credenciales en miles e incluso cientos de miles de recursos al tiempo que se mantienen dichas credenciales protegidas) como los riesgos operativos, ya que las actualizaciones automáticas de contraseñas y claves son menos propensas a errores. Al combinar la automatización con el inicio de sesión único para usuarios con privilegios, es posible lograr un alto nivel de seguridad, ya que se puede proporcionar a un usuario acceso a un sistema sin necesidad de darle también acceso a las credenciales relevantes. Además, si un usuario carece de una credencial, no puede robarla, compartirla ni entregarla a un atacante tras haber sido engañado.

Segundo paso: Limitar la escalación de privilegios, el reconocimiento y los movimientos laterales

Este paso constituye una transición hacia el siguiente de cara a romper la cadena de ciberataque: limitar la capacidad que tiene un usuario para realizar un reconocimiento de la red y desplazarse por ella. Por desgracia, en muchas redes la autenticación acaba por convertirse, esencialmente, en la misma cosa que el control de accesos. Una vez que se ha iniciado sesión en la red, es frecuente ver que se tiene acceso a recursos de toda la red. Magníficas noticias si es usted un atacante: dispone del tiempo y a menudo de los medios para trasladarse de un sistema a otro, acercándose al objetivo.

Capacidades como el inicio único de sesión para los usuarios con privilegios ayudan a prevenir estos problemas. El enfoque se asienta fundamentalmente sobre un control de accesos con menos privilegios, denominado control de accesos "de confianza cero". Al separar la autenticación del acceso al sistema de gestión de accesos con privilegios y del acceso real a los recursos gestionados, los usuarios solamente ven aquellos sistemas y recursos que se hayan definido y autorizado mediante una política. Si las responsabilidades laborales de un usuario concreto exigen que acceda a un único servidor o tipo de recursos, eso es lo único que debería ver en la red. Al introducir sistemas proxy o agentes para las sesiones entre el sistema de gestión de accesos con privilegios y los recursos gestionados, es posible limitar la autoridad que detentan sobre un sistema y controlar los comandos que pueden emitir, lo que restringe aún más la capacidad de escalar privilegios o desplazarse lateralmente dentro de la red.

Por ejemplo: con una sesión a la que se ha accedido mediante proxy, es posible iniciar la sesión de un usuario en un sistema con una cuenta estándar, incluso una cuenta potente como la de usuario raíz. Dado que el sistema puede imponer filtros de comandos, es posible limitar a esa persona para que utilice solamente comandos específicos o prohibir otros sin autorización. Por ejemplo, se puede asignar a un usuario la tarea de actualizar el software de un conjunto de servidores y tal vez sea necesario iniciar sesión como usuario raíz para llevarlo a cabo. Con los filtros de comandos es posible que el usuario inicie sesión permitiéndole únicamente emplear los comandos necesarios para realizar la tarea. Se puede impedir que ejecute otros comandos, como para reiniciar el sistema o interrumpir un proceso.

Los controles adicionales permiten adoptar respuestas variables ante intentos de infringir las políticas. Supongamos que un usuario emite un comando sin autorización; tal vez sus políticas asuman que la acción ha sido el resultado de una necesidad inocente o sencillamente un error. En tal caso, se puede enviar un aviso al usuario e impedir la ejecución del comando. La repetición de los intentos u otras infracciones más graves pueden desencadenar el fin de la sesión e incluso desactivar la cuenta del usuario hasta que un administrador tenga la oportunidad de revisar el incidente a fondo.

La adición de agentes basados en host permite disfrutar de capacidades similares, pero a menudo con controles mucho más exhaustivos, como la posibilidad de restringir estrictamente el acceso a archivos y directorios o supervisar los archivos para detectar modificaciones. También es posible impedir los intentos de moverse lateralmente dentro de la red. Por ejemplo, tras conseguir acceder al sistema, un atacante podría intentar emitir un comando SSH o TELNET, o bien abrir una sesión RDP remota para llegar a un sistema objetivo. Una vez más, el sistema de gestión de accesos con privilegios puede examinar las políticas y determinar si la actividad está permitida. Si no lo está, se impide la ejecución del comando y se registra el intento de infracción.

Tercer paso: Vigilar, registrar y auditar la actividad

Idealmente, nuestro atacante no llegará nunca al punto donde es capaz de alcanzar su objetivo final. La larga serie de controles y comprobaciones establecidos e impuestos por un sistema de gestión de accesos con privilegios proporciona muchas oportunidades para interrumpir la cadena de ciberataque. El paso final de vigilar, registrar y auditar la actividad actúa como elemento disuasorio adicional frente a intentos de violación, además de rendir notables ventajas cuando finalmente se produce una violación.

Como hemos subrayado, saber que sus actividades se registran y someten a análisis puede tener un fuerte efecto disuasorio ante comportamientos incorrectos o aparentemente inocentes pero potencialmente peligrosos, como la exploración y el examen de los sistemas. Las amplias capacidades de registro, grabación, creación de alertas y generación de informes representan un "sistema de alerta temprana" que advierte a otros administradores, gestores y auditores acerca de comportamientos sospechosos o inusuales. Las alertas y los eventos proporcionan advertencias inmediatas sobre las infracciones de las políticas y los intentos de violación, lo que permite responder rápidamente. Los registros se pueden analizar, de forma individual o mediante un sistema de gestión de registros o gestión de eventos e información de seguridad (SIEM) dentro del contexto de las demás actividades del sistema, para obtener información adicional sobre eventos sospechosos. Así se puede iniciar la investigación incluso antes de que se produzca una violación.

Dado que las cuentas administrativas compartidas son de uso muy frecuente, la capacidad de atribuir las acciones ejecutadas con una de estas cuentas a una persona concreta es imprescindible para cumplir los requisitos de conformidad.

Por último, la grabación de sesiones aporta una serie de ventajas. A veces, los administradores cometen errores. Las grabaciones de sesiones pueden ser útiles en tales casos, ya que permiten revisar la actividad y determinar con precisión qué acciones se llevaron a cabo durante una interacción. Eso puede acelerar la solución de problemas; por ejemplo, cuando se detecta un problema con un sistema. Si se ejecutó una actualización o se realizó un cambio de configuración durante el turno anterior, determinar lo que ocurrió con exactitud puede ser una tarea difícil y larga. Las grabaciones de sesiones permiten reproducir el contenido de inmediato, lo que agiliza la recuperación. También se pueden utilizar para formación; facilitan la labor de señalar dónde se cometió un error y cuál sería el modo de actuar preferible.

Naturalmente, en el peor de los casos, si el intento de violación de la seguridad tuviese éxito, estas grabaciones y registros pueden ser cruciales para determinar exactamente qué se hizo en el sistema, qué información se sustrajo y cómo se vulneró la seguridad del recurso. Todos estos detalles agilizan la investigación forense, ayudan a evaluar los daños y proporcionan información valiosa que se puede utilizar para mitigar el riesgo de futuras violaciones.

Ventajas

Por desgracia, los ataques de violación de datos son un hecho, con todos los costes y perjuicios que llevan aparejados. Sin embargo, como hemos demostrado aquí, los delincuentes suelen seguir una línea de acción definida y previsible para tratar de ejecutar estos ataques. La gestión de accesos con privilegios otorga una serie de capacidades y controles que impiden activamente que los atacantes puedan dar pasos clave para sus ataques. Así se interrumpe la cadena de ciberataque, además de conseguir más apoyo para reducir los riesgos, limitar al mínimo los daños y acelerar la recuperación en caso de que un ataque tenga éxito. Implementar una solución de gestión de accesos con privilegios completa estos beneficios:

- **Reducir el riesgo.** Impedir los accesos no autorizados y limitar el acceso a recursos tras haber concedido la entrada a la red. Proteger contraseñas y otras credenciales frente a usos sin autorización y vulneraciones. Limitar las acciones que los usuarios pueden realizar sobre los sistemas, impedir que se ejecuten comandos sin autorización y prevenir los movimientos laterales dentro de la red.
- **Incrementar la responsabilidad.** Observar la atribución completa de la actividad de los usuarios, aunque se utilicen cuentas compartidas. Funciones completas de registro, grabación de sesiones y advertencias para los usuarios, que capturan la actividad desarrollada y sirven como elementos disuasorios frente a comportamientos no autorizados.
- **Mejorar las auditorías y simplificar la conformidad.** Simplificar la conformidad al proporcionar soporte para sistemas autenticación emergentes y requisitos de control de accesos y limitar el alcance de los requisitos de conformidad por medio de la segmentación lógica de la red.
- **Reducir la complejidad y potenciar la productividad de los operadores.** El inicio único de sesión no solo contribuye a limitar los riesgos, sino que también puede impulsar la productividad de los administradores individuales, ya hace más fácil y rápido que accedan a los sistemas y recursos que necesitan gestionar. La definición e imposición centralizadas de políticas simplifican la creación e imposición de controles de seguridad.

Conclusiones

- Las identidades, cuentas y credenciales con privilegios constituyen activos fundamentales e imprescindibles para las empresas, que deben protegerse a través de una combinación de tecnología y procesos que habilita la gestión de accesos con privilegios.
- Proporcionar esa protección es algo básico para interrumpir la cadena de ciberataque puesta en marcha para efectuar una violación de datos, lo que contribuye a impedir los ataques y reduce el impacto de los que finalmente sí se producen.
- Un modelo de control de accesos de "confianza cero" resulta esencial para todos los tipos de acceso con privilegios, tanto humanos como de programas.
- Aunque los enfoques de la seguridad basada en perímetro han demostrado que tienen graves limitaciones, la defensa en profundidad continúa siendo una estrategia clave para proteger los recursos. La gestión de accesos con privilegios es capaz de proporcionar varias capas de defensa adicionales a los usuarios, las cuentas y las credenciales con privilegios, tanto en los niveles de redes como de host.
- Dada la preponderancia de las violaciones y la sofisticación de los atacantes resulta muy, muy tentador (a menudo se nos anima a ellos) centrarnos exclusivamente en la detección de las violaciones y su respuesta. Se trata de un error. Es cierto que son actividades muy importantes, pero es crucial recordar que la gestión de accesos con privilegios puede ayudar a que las organizaciones mejoren sustancialmente su capacidad para prevenir que se produzcan las propias violaciones.

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 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.

Comuníquese con CA Technologies en ca.com/es

CA Technologies (NASDAQ: CA) crea software que impulsa la transformación de las empresas y les permite aprovechar las oportunidades que brinda la economía de las aplicaciones. El software se encuentra en el corazón de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA trabaja con empresas de todo el mundo para cambiar la forma en que vivimos, realizamos transacciones y nos comunicamos, ya sea a través de la nube pública, la nube privada, plataformas móviles, entornos de mainframe o entornos distribuidos. Para obtener más información, visite **ca.com/es**.

1 Intel Security y el Center for Strategic and International Issues (Centro de estudios estratégicos e internacionales), "Net Losses: Estimating the Global Loss of Cybercrime, Economic Impact of Cybercrime II", junio de 2014, http://www.mcafee.com/es/resources/reports/rp-economic-impact-cybercrime2.pdf

2 Foro Económico Mundial y McKinsey & Company, "Risk and Responsibility in a Hyper-connected World", enero de 2014, http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

3 Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D., Lockheed Martin Corporation, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

4 Andras Cser, Forrester Research, "Critical Questions to Ask Your Privileged Identity Management Solution Provider", 10 de septiembre de 2014.

5 Ars Technica, "AWS console breach leads to demise of service with 'proven' backup plan", 18 de junio, 2014, http://arstechnica.com/security/2014/06/aws-console-breach-leads-to-demise-of-service-with-proven-backup-plan/

6 Brian Krebs, "China To Blame in Anthem Hack?", 15 de febrero de 2015, http://krebsonsecurity.com/2015/02/china-to-blame-in-anthem-hack/

7 Anmol Singh y Felix Gaehtgens, "Twelve Best Practices for Privileged Access Management, Gartner", 8 de octubre de 2015, G00277332

CS200-162063_1115