LIBRO BLANCO | JUNIO DE 2017

Gestión de accesos con privilegios: una planificación para calcular el coste total de propiedad

Descubra las ventajas y costes ocultos de su planteamiento de implementación de PAM

ca technologies

Tabla de contenido

Sección 1 3
Introducción

Sección 2 3
Cuentas con privilegios vinculadas a infracciones de gran repercusión

Sección 3 4
Protección frente a infracciones de cuentas con privilegios con PAM

Sección 4 5
Estrategia de implementación de la PAM: un gran impacto en el TCO

Sección 5 6
Componentes básicos de una solución de PAM completa

Sección 6 6
Evaluación del impacto empresarial de la solución de PAM completa en la organización

Sección 7 9
Visualización en conjunto

Sección 8 10
Conclusión: Perspectiva largoplacista del TCO

Sección 1

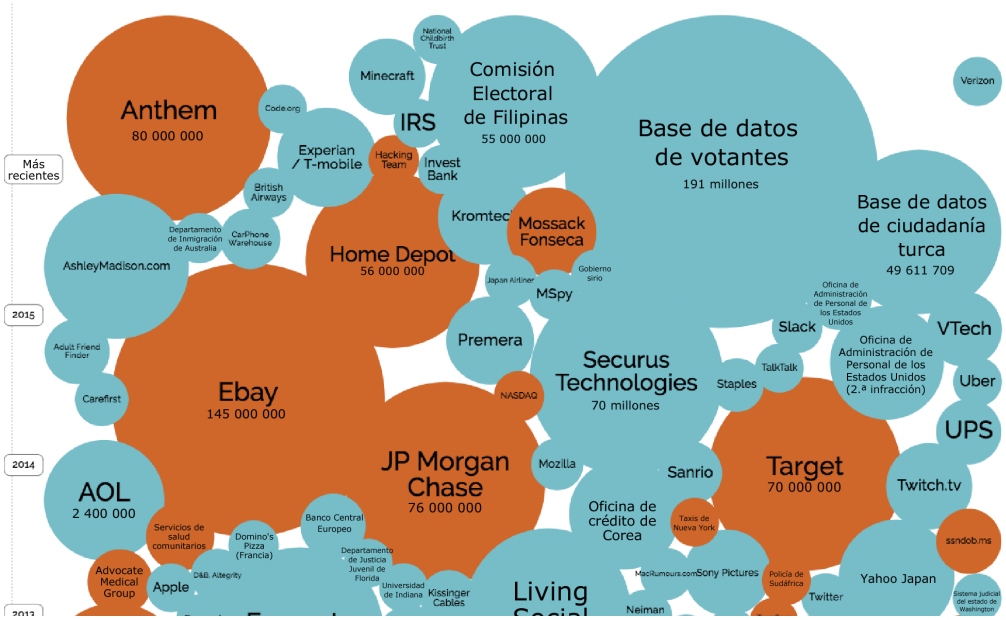
Introducción

Las cuentas de usuario con privilegios, ya se usurpen, sean objeto de abuso o, simplemente, se usen de forma incorrecta, se encuentran en el corazón de la mayoría de las infracciones relativas a datos. Los equipos de seguridad evalúan, cada vez más, soluciones de gestión de accesos con privilegios (PAM) completas para evitar el perjuicio que podría provocar un usuario malintencionado con privilegios altos o un usuario con privilegios que está cansado, estresado o que, sencillamente, comete un error. La presión que ejercen los ejecutivos y los equipos de auditoría para reducir la exposición de la empresa aseguran el esfuerzo, pero las soluciones de PAM completas pueden acarrear costes ocultos, según la estrategia de implementación adoptada. Dado que una solución de PAM ofrece varias capacidades, incluidos los almacenes de contraseñas, la gestión y la monitorización de sesiones y, a menudo, el análisis del comportamiento de los usuarios y la inteligencia de amenazas, la forma en la que se implementa puede tener un gran impacto en el coste y las ventajas. En este informe, se proporciona una fórmula para determinar los costes directos e indirectos, así como los ocultos, de un despliegue de PAM a lo largo del tiempo.

Sección 2

Cuentas con privilegios vinculadas a infracciones de gran repercusión

Las infracciones de seguridad de gran repercusión se han convertido en una noticia constante, y los expertos afirman que, en entre el 80 y el 100 % de ellas, se ve involucrado el uso de cuentas con privilegios. Cada vez más ataques implican cuentas de administradores de TI, desarrolladores de aplicaciones, gestores empresariales, partners y proveedores, así como ejecutivos de la cúpula directiva. Una vez que el infractor se encuentra dentro del sistema, puede moverse de forma horizontal y vertical para acceder a información confidencial e instalar malware con el fin de provocar daños futuros. Sin embargo, para un administrador de TI no es fácil determinar si existe un problema cuando los usuarios con privilegios acceden a zonas con información confidencial, ya que puede tratarse de actividad diaria habitual.



En resumen: la función del usuario con privilegios puede ser el eslabón más débil de la cadena de seguridad de cualquier organización, sin importar su tamaño ni su ubicación en el mundo. Si se aborda de forma adecuada, puede resultar rentable durante años.

Sección 3

Protección frente a infracciones de cuentas con privilegios con PAM

Existen numerosos aspectos de la seguridad de la información; la gestión de accesos con privilegios es solo uno de ellos. En general, las organizaciones estudian delicadamente la gestión de accesos con privilegios por uno de estos dos motivos:

- Se enfrentan a problemas graves (por ejemplo, han sufrido infracciones o no han cumplido los requisitos de conformidad).
- Están preparadas para implementar prácticas recomendadas.

Independientemente del motivo, no es extraño conjeturar sobre la implementación de una solución de PAM. Puede resultar tentador adoptar una perspectiva cortoplacista si se parte del supuesto de que se puede empezar por un conjunto limitado de funcionalidades y aumentar el alcance y la escala de la implementación a lo largo del tiempo. Si bien este podría ser un punto de vista razonable con otras medidas de seguridad, la experiencia demuestra que, con la PAM, no resulta práctico desde una perspectiva técnica ni económica. De hecho, se trata de un área en la que resulta extremadamente importante adoptar un planteamiento a largo plazo: se deben proteger dispositivos, terminales, usuarios y cuentas, así como contemplar problemas de conformidad, además de la planificación de la empresa. Todos estos factores influirán en el coste total de propiedad.

Dispositivos

Ya no solo tenemos que encargarnos de proteger los terminales tradicionales. En la actualidad, el alcance se ha ampliado para incluir entornos virtualizados, contenedores y sistemas basados en la nube. La infraestructura de TI híbrida, las consolas de gestión, las grandes cantidades de recursos y los cambios constantes pueden ampliar la superficie de ataque disponible. Una protección adecuada requiere defensas que incorporen entornos completos desde el principio para que pueda proporcionar un alcance y una profundidad acordes a las amenazas. Las necesidades futuras como estas deben tenerse en cuenta al planificar la implementación de la PAM.

Usuarios

En la actualidad, la suplantación de identidades y la ingeniería social son métodos habituales para obtener credenciales de usuarios con privilegios. La amenaza externa (y, cada vez más, la interna) exige obtener información contextual completa: debemos entender el comportamiento normal del usuario con privilegios para poder aislar las anomalías. El propio concepto de usuario con privilegios cambia con la adopción de metodologías de entornos en la nube, híbridas y ágiles. Por ejemplo, a los propietarios de la empresa se les puede asignar privilegios administrativos para soluciones de CRM basadas en la nube. Si damos una vuelta más de tuerca, el comportamiento de los usuarios cambia a lo largo del tiempo y los ataques dirigidos se transforman, de manera que se dificulta la labor de afirmar con certeza si una cuenta se ha visto comprometida. Las soluciones de gestión de usuarios con privilegios deben aprender y mejorar de forma continua para poder identificar posibles infracciones.

Conformidad

El mantenimiento de un requisito constante para organizaciones de todos los tamaños, además de la conformidad (y su demostración), puede provocar rápidamente lo que se conoce como “fatiga legislativa” debido al gran volumen y alcance del cambio de la normativa.

Las tecnologías de PAM deben ser compatibles con las normativas que rigen los controles y los procesos utilizados para garantizar la ciberseguridad. Esto podría incluir la documentación del acceso a parámetros de configuración y datos privados, la imposición de ITIL® y la presentación de pistas de auditoría para el cumplimiento de la ley Health Insurance Portability and Accountability Act (HIPAA) de 1996, la norma de seguridad de datos de la industria de tarjetas de pago (PCI-DSS) y otras normativas. Las pruebas de conformidad se deben crear desde el principio, no incorporar a posteriori.

Sección 4

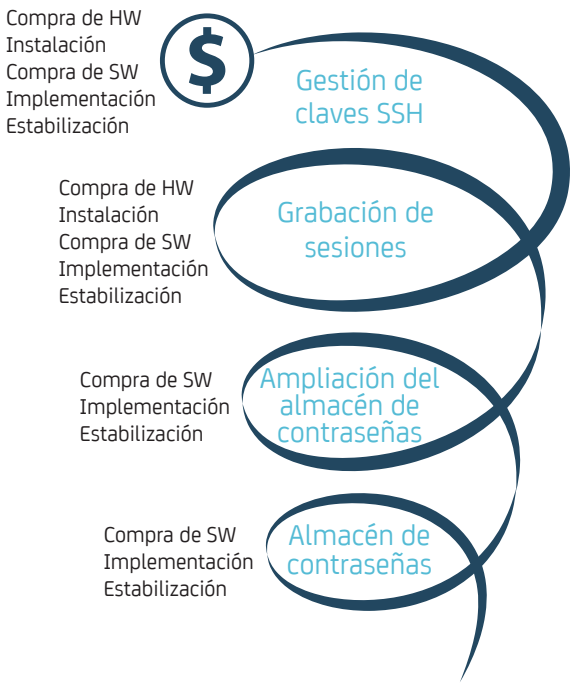
Estrategia de implementación de la PAM: un gran impacto en el TCO

El método de implementación elegido para una solución de PAM tendrá un gran impacto en el coste total de la propiedad. Resulta fundamental entender los dos métodos de implementación de una solución de PAM.

El primero, lo llamaremos "completo", se centra en crear una planificación de los requisitos clave, obtener un producto que proporcione todas las capacidades (incluidos los requisitos futuros) por adelantado y, después, aumentar la escala y el alcance de dichas capacidades a lo largo del tiempo y por fases. Por ejemplo, si necesita almacenar contraseñas, grabar sesiones y gestionar claves del protocolo Secure Shell (SSH), puede adquirir un producto que incorpore todas estas capacidades y las active según corresponda. Todas están integradas y no se requiere un periodo de estabilización prolongado.

El segundo, que llamaremos "fragmentado", también empieza por una planificación, pero los productos se obtienen a medida que se necesitan. Por ejemplo, si la planificación incluye las tres capacidades indicadas en el ejemplo anterior, puede comprar primero un almacén de contraseñas y, después de implementarlo y estabilizarlo durante unos meses, puede recurrir otra vez al distribuidor para comprar una grabación de sesiones (además de cualquier hardware adicional que necesite), implementarla y estabilizarla durante seis meses. A continuación, solo tiene que repetir el proceso con la gestión de claves SSH.

El método elegido puede influir tanto en el coste total de propiedad como en el tiempo de recuperación de la inversión. La implementación de una solución de PAM integrada y completa que se crea a partir de características de almacenamiento inteligente puede proporcionar un tiempo de recuperación de la inversión más rápido y un coste total de propiedad más bajo, ya que se conocen los costes y son predecibles. Por el contrario, si la implementación es fragmentada, el despliegue inicial puede ser sencillo: un almacén de contraseñas para, únicamente, unas pocas cuentas que crece con el paso del tiempo mediante el aumento de la cantidad de cuentas incluidas en el almacén y, después, mediante la incorporación de la grabación de sesiones. Sin embargo, los costes se vuelven impredecibles porque los costes de infraestructura pueden variar con cada módulo añadido. Además, el cliente se ve atado al distribuidor, lo que puede no resultarle óptimo. Los cálculos del coste total de propiedad deben contemplar el coste, el tiempo y la exposición resultantes del aumento de la escala y el alcance en una implementación fragmentada. Se incluyen tanto los costes tangibles (de licencias, de infraestructura y elementos similares) como los intangibles, que engloban el tiempo de recuperación de la inversión, la exposición prolongada al riesgo, los costes de integración y mantenimiento, y otros aspectos. En última instancia, la generación de scripts y el mantenimiento para incorporar terminales adicionales para el almacén de contraseñas pueden diferenciarse en gran medida de lo que resulta necesario para la gestión de claves SSH.



Con el fin de hacerse una mejor idea de qué cuestiones hay que plantearse y qué capacidades se deben evaluar, la comprensión de los elementos que forman una solución de PAM completa y de cómo se determinan tanto las ventajas cualitativas como las cuantitativas frente al coste financiero puede ser de utilidad.

Sección 5

Componentes básicos de una solución de PAM completa

Una solución de PAM completa dispone de varios componentes principales, como la capacidad de controlar los accesos con privilegios en todos los recursos, proteger el almacenamiento de credenciales con privilegios, monitorizar y registrar la actividad, proteger las consolas de nube híbrida y gestionar API, además de analizar el comportamiento de los usuarios para detectar anomalías que podrían indicar un peligro. Algunos aspectos específicos que se deben tener en cuenta al evaluar la gestión de accesos con privilegios son los siguientes:

Almacén de contraseñas. Un almacén de contraseñas reforzado y cifrado (o caja) para almacenar credenciales gestiona contraseñas y otras credenciales o tokens cambiándolas en intervalos configurables, según una política. De este modo, se ayuda a proteger cuentas administrativas, compartidas y de servicios, así como cuentas de aplicación a aplicación y entornos de nube híbrida. Sin embargo, el almacenamiento de contraseñas en sí mismo no es suficiente.

Monitorización de contraseñas. Con frecuencia, este componente primordial se encuentra desaparecido en combate en un despliegue inicial fragmentado. La capacidad para iniciar automáticamente una sesión remota que registre, analice y monitorice una sesión de usuario con privilegios permite monitorizar en tiempo real y analizar la sesión una vez finalizada. Esta capacidad no se debe añadir después del hecho: si un usuario con privilegios infringe una política o, de otro modo, exhibe un comportamiento anómalo, querrá empezar a monitorizar de inmediato, no dentro de seis meses.

Entornos híbridos. Una solución de PAM completa puede controlar los accesos con privilegios a recursos en la nube, máquinas virtuales e hipervisores, además de a los entornos de centros de datos físicos tradicionales. La detección automática es clave, ya que los recursos nuevos pueden añadirse al entorno en cuestión de minutos.

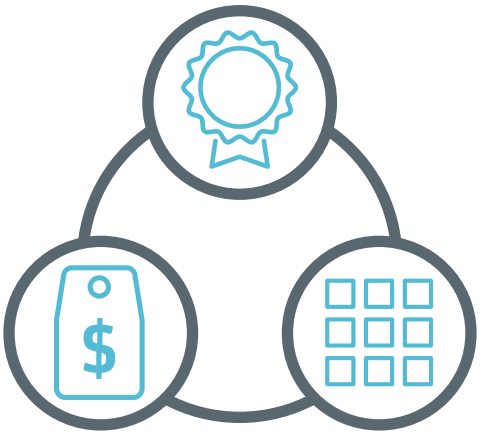
Análisis del comportamiento de los usuarios. Una solución de PAM completa puede distinguir el comportamiento de usuarios con privilegios normal y anómalo, así como activar mecanismos de protección adicionales cuando se detectan anomalías. Recopila datos específicos de dominios, así como contextuales, y realiza análisis avanzados para crear modelos de riesgo en función de los patrones de comportamiento anteriores. Si detecta un comportamiento inusual, puede activar automáticamente sistemas de autenticación adicionales (como Radius, TACACS+ o CA Advanced Authentication) o una grabación de sesiones.

Una solución de PAM completa, además de proporcionar estas capacidades, se implementa rápidamente, ofrece capacidades de detección e información listas para usar, y requiere habilidades especiales mínimas para obtener ventajas inmediatas. Debe permitir que los administradores investiguen las incidencias con facilidad, así como la forma en la que se utilizan sus cuentas con privilegios.

Sección 6

Evaluación del impacto empresarial de la solución de PAM completa en la organización

¿Cuáles son los factores que intervienen en la determinación de los costes y las ventajas habida cuenta de los requisitos anteriores? En términos generales, se deben evaluar tres tipos de factores: los costes financieros, las ventajas cualitativas y las ventajas cuantitativas. Estas últimas se pueden determinar con relativa facilidad, en función de las medias del sector y las prácticas específicas de la organización. La medición de las ventajas cualitativas resulta un poco más complicada, pero problemas como el tiempo de detección, la facilidad de uso y similares pueden tener una importante repercusión. En las siguientes secciones, se le guiará para saber cómo plantear cada uno de estos factores.



Factores del cálculo de costes financieros

En general, el cálculo de costes financieros es un ejercicio simple que incluye los siguientes elementos:

- Los costes de licencia del producto (una vez o suscripción)
- Los costes de mantenimiento del producto (segunda fase y posteriores, además de costes de compatibilidad interna)
- Los costes de implementación del producto (servicios profesionales, despliegue y configuración)
- Los costes de formación (formación interna del cliente, así como formación del usuario final)

Al calcular los costes financieros, se deben contemplar varios aspectos. En primer lugar, el coste de la implementación de una solución completa frente a una implementación fragmentada. En el caso de una solución completa, entran en juego el coste inicial (incluida la adquisición de licencias, el despliegue y la formación) y cualquier mantenimiento posterior. Sin embargo, con una implementación fragmentada, el cálculo también debe incluir el coste de integración, que puede ser directamente proporcional al número de sistemas que se van a integrar, así como a su tamaño. Si se va a adquirir una solución de PAM en fases, en lugar de todo a la vez, existirán costes graduales de aprovisionamiento, formación y despliegue más allá de los costes básicos mencionados en líneas anteriores. Asimismo, el coste de los gastos operativos (OPEX) influyen a la hora de decantarse por una implementación fragmentada: con frecuencia, las capacidades adicionales requieren hardware específico, que se deberá presupuestar, aprovisionar, configurar y mantener. Igualmente, el cálculo de costes debe contemplar las habilidades, los recursos y el tiempo requeridos si se elige un planteamiento de implementación fragmentada, que presenta un reto real para el proceso de elaboración del presupuesto dada la gran cantidad de aspectos desconocidos.

Factores de determinación de ventajas financieras cualitativas

En ocasiones, la evaluación de las ventajas financieras cualitativas resulta complicada, pero desempeñan una función principal a la hora de decidirse por una solución completa o una implementación fragmentada. En primer lugar, estudiaremos la implementación fragmentada: Empiece por un almacén de contraseñas para un número reducido de cuentas, agregue más cuentas con privilegios a lo largo del tiempo, posteriormente, incluya la grabación de sesiones y, por último, una vez que se ha instalado todo el sistema, contemple el uso de análisis del comportamiento de los usuarios.

Ventajas:

- Pueden obtenerse ahorros de costes por adelantado.

Inconvenientes:

- El tiempo de recuperación de la inversión es mucho mayor: resulta imposible conseguir visibilidad suficiente para mitigar el riesgo de forma eficaz.
- Se aumenta en gran medida el riesgo de que se produzca una infracción: las capacidades como la grabación de sesiones requerirán semanas o meses de retraso para conseguir el hardware necesario.
- Se amplía la superficie de riesgo durante tiempos prolongados.
- Se puede requerir la codificación o generación de scripts para escalar la implementación.
- Supone un coste adicional para el hardware, las copias de seguridad y la redundancia: los costes a largo plazo probablemente sean mayores.
- Bloqueo de distribuidores: cada vez que se contemple un nuevo módulo, el proceso de aprovisionamiento se inicia de nuevo. Es posible que el reloj de los módulos implementados previamente se restablezca, es decir, aumentará el compromiso con el producto en cuanto a la planificación inicial.

Por otro lado, una solución completa, repleta de características e integrada que se puede implementar de una vez implica la selección de una solución con todas las capacidades necesarias desde el principio. Si bien es posible activar las capacidades según corresponda, todo está listo para cuando lo necesite. Este tipo de implementación, sobre todo, si se proporciona en forma de dispositivos, ofrece una mitigación lista para usar y no requiere habilidades especiales para obtener ventajas inmediatas. De este modo, se reduce la carga de trabajo a la vez que se evitan las infracciones.

Ventajas:

- Despliegue y tiempo de recuperación de la inversión rápidos.
- Protección inmediata en caso de que se sospeche que se ha producido una infracción: si se requiere la grabación de sesiones, tan solo hay que activarla.
- Capacidades adicionales, como los análisis, están a su disposición de inmediato para garantizar control y visibilidad en todo el entorno.
- Superficie de ataque reducida en gran medida.
- Coste total inferior: no se requiere codificación personalizada, generación de scripts ni hardware adicional.

Inconvenientes:

- Los costes por adelantado pueden ser mayores.

Asimismo, determinados factores tecnológicos pueden contribuir en las ventajas financieras cualitativas. Si la solución de PAM aprovecha el análisis del comportamiento de los usuarios y la integración completa con la inteligencia de amenazas, se refuerza considerablemente la capacidad de detectar actividad anómala y tomar acciones inmediatas. Si se incluye la agrupación de clústeres en varios sitios como característica, puede conseguirse una capacidad mayor y un tiempo de respuesta reducido. Si la solución se proporciona como dispositivo virtual o físico, la implementación durará mucho menos tiempo en comparación con una solución basada en software. Por último, resulta primordial contemplar los costes de mantenimiento, que pueden ser significativamente menores en el caso de un dispositivo frente a un conjunto de productos de software en el que cada uno requiere su propio hardware concreto.

En consecuencia, todos los factores cualitativos descritos pueden contribuir en la reducción del coste total de propiedad, así como del tiempo de recuperación de la inversión.

Factores de determinación de ventajas financieras cuantitativas

Cuando se trata de ventajas financieras cuantitativas, debe tener en cuenta tres factores clave: la reducción de los costes, las mejoras de la productividad y la protección de los ingresos.

Reducción de los costes

La reducción de los costes incluye la elusión de costes de infraestructura, costes relativos a infracciones, tasas de auditor y en materia de conformidad normativa, y costes de interrupciones imprevistas. Otro factor que no se puede desestimar es la reducción de los costes de implementación, mantenimiento y compatibilidad.

Puede evitar los costes de infraestructura eligiendo una solución de PAM completa y basada en dispositivos frente a una solución fragmentada o basada exclusivamente en software. Para calcularlo, se estima el número de servidores o dispositivos requeridos para las soluciones de PAM existentes o de la competencia, el coste por servidor, la cantidad de equilibradores de carga necesarios y el coste de cada uno, y el porcentaje de costes de infraestructura que se podría evitar con una solución basada en dispositivos.

Los costes relativos a infracciones incluyen impactos en los ingresos, costes de notificación al cliente, costes derivados de incidencias y de la aparición en prensa, además de honorarios jurídicos. El cálculo de estos costes requiere una estimación de la probabilidad de que se produzca una infracción (la estimación actual se encuentra en el 22 % en un periodo de dos años) y el volumen de grabaciones potencialmente expuestas junto con el coste por grabación, así como el coste de corrección y el porcentaje de dichos costes que se podría evitar con una solución de PAM completa. Dado que se estima que unas credenciales vulneradas causan más de un 80 % de las infracciones, esta ventaja puede ser importante.

Los costes derivados del auditor externo y de la conformidad normativa se pueden reducir a través del uso de una solución de PAM completa. Para calcular la posible reducción, debe estimar la cantidad de problemas en materia de conformidad normativa por año, el coste anual de infracciones por incumplimiento, el coste del auditor externo para corregir los problemas de los que se deba informar y el porcentaje de tasas de constatación por auditoría, la corrección y las penalizaciones relativas a la conformidad normativa que se podrían evitar a través del uso de una solución de PAM completa.

Otra ventaja financiera se obtiene de la probabilidad reducida de que se produzcan interrupciones del sistema imprevistas, que pueden provocar el descontento de los empleados, así como la carencia de productividad, y, posiblemente, la pérdida de clientes. Este cálculo incorpora una estimación de la cantidad de posibles interrupciones empresariales por año debidas a cuentas de usuarios con privilegios vulneradas, el tiempo de inactividad medio por interrupción del sistema, el coste por minuto y el impacto del aumento de disponibilidad.

Uno de los problemas clave de la implementación de la solución de PAM en modo fragmentado es que el coste de mantenimiento y despliegue asciende de manera drástica a medida que se adquiere, implementa y estabiliza cada módulo. Se requieren habilidades específicas de generación de scripts, pero ¿cuántos clientes están dispuestos a contratar a una persona a tiempo completo para que gestione, mantenga y despliegue la solución? Al adquirir una solución completa e implementar las capacidades según corresponda, se evita este coste.

Aumento de la productividad

La mejora de la productividad se obtiene de dos formas: una reducción de los costes de las tareas del administrador del sistema de TI y una reducción de los costes operativos de implementación y aplicación.

Una solución de PAM completa implica que el administrador dedique menos tiempo a la detección de infracciones, la imposición de políticas y la recuperación o regeneración de contraseñas, es decir, dispone de más tiempo para implementar soluciones innovadoras que harán avanzar a su empresa. Para calcular las reducciones de costes relativos a las tareas del administrador del sistema de TI, debe tener en cuenta la cantidad de recursos y de dispositivos que disponen de credenciales con accesos con privilegios y el número de cuentas por recurso, dispositivo o aplicación. Después, necesita la cantidad de minutos que el administrador de TI requiere para proporcionar o actualizar accesos con privilegios y el coste medio incluido por hora, así como la reducción prevista en el tiempo para actualizar credenciales de accesos con privilegios a través del uso de una solución de PAM completa.

Los costes operativos y de implementación se pueden reducir considerablemente a través del uso de una solución de PAM completa basada en dispositivos. Para calcular estos ahorros, debe tener en cuenta la cantidad de administradores del sistema de TI que deben implementar, alojar y gestionar una solución existente o de la competencia, así como el coste medio incluido por hora y por año, y, a continuación, aplicar la reducción de porcentaje en el coste que puede esperar si elige una solución de PAM completa basada en dispositivos.

Protección de los ingresos

Una solución de PAM completa puede contribuir en buena medida a mitigar la mayoría de las consecuencias financieras graves de una infracción de datos. Para calcular esta ventaja financiera, debe estimar el impacto que supondría en sus ingresos que su empresa se viese perjudicada por una infracción del sistema o de datos, así como el porcentaje de la protección de ingresos a través del riesgo reducido de credenciales vulneradas. Un informe reciente de Ponemon Institute demuestra que para las empresas de EE. UU. encuestadas en 2016, el impacto financiero en los ingresos debido a la debilitación del reconocimiento de la marca y al fondo de comercio fue de 3,97 millones de dólares por año, por lo que la gestión de accesos con privilegios puede crear un gran impacto financiero.

Sección 7

Visualización en conjunto

No cabe duda de la necesidad de una solución de PAM completa; el método para calcular el coste total de propiedad incluye varios factores que se deben contemplar. Los costes dependerán de si se decanta por implantar una solución de PAM completa, de manera que active las características según corresponda, u opta por una implementación fragmentada con el conocimiento total de los costes posteriores. No pierda de vista los costes y las ventajas del planteamiento completo:

- Los costes son predecibles y se presupuestan con facilidad, sin costes adicionales asociados al planteamiento fragmentado (aprovisionamiento, licencias, formación, despliegue, recursos e infraestructura adicional).
- Las ventajas cualitativas son sustanciales: una implementación y un tiempo de recuperación de la inversión rápidos, una protección inmediata en caso de infracción, una superficie de ataque reducida y un coste total de propiedad menor.
- Las ventajas cuantitativas son igualmente impresionantes: evita los costes de infraestructura, reduce los costes relativos a infracciones, así como los asociados a las auditorías y en materia de conformidad normativa, evita interrupciones imprevistas y reduce los costes de despliegue, mantenimiento y compatibilidad.

Por supuesto, los resultados de estos cálculos variarán en función de su situación y sus preferencias empresariales, pero sigue siendo indiscutible que el planteamiento de una implementación completa da lugar a un coste total de propiedad mucho más favorable comparado con el planteamiento de implementación de PAM fragmentada.

Sección 8

Conclusión: Perspectiva largoplacista del TCO

Diariamente, crece el número de superficies de ataque sin proteger, de manera que aumenta el riesgo para la organización. Una solución de PAM completa puede reducir la superficie de ataque y proporcionar un tiempo de recuperación de la inversión extremadamente rápido, que es la verdadera preocupación cuando una organización se encuentra en peligro de sufrir una infracción. Ofrece todas las capacidades necesarias, desde el primer día, y usted, a la vez, puede elegir inicialmente la activación de un subconjunto de capacidades: todo el potencial de la solución a su disposición al instante cuando sospecha que se está produciendo una infracción. Si estudia los cálculos, resulta evidente que la solución de PAM completa y basada en dispositivos tiene lógica desde un punto de vista financiero a largo plazo, empresarial y productivo.

Para obtener más información acerca de cómo pueden beneficiar las soluciones de gestión de accesos con privilegios de CA a su organización, visite **ca.com/pam**

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 núcleo de cada empresa, sea cual sea su sector. Desde la planificación hasta la gestión y la seguridad, pasando por el desarrollo, CA colabora 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 y entornos de mainframe y distribuidos. Para obtener más información, visite **ca.com/es**.

1 Thomson Reuters, “Cost of Compliance 2016”, https://risk.thomsonreuters.com/en/resources/special-report/cost-compliance-2016.html

2 Ponemon Institute, “2016 Cost of Data Breach Study: Global Analysis”, junio de 2016, https://securityintelligence.com/media/2016-cost-data-breach-study/

3 Ibíd.

CS200-282765_0617