LIBRO BLANCO | MAYO DE 2017

Un modelo de madurez de gestión de accesos con privilegios para la transformación y automatización digitales a escala

ca technologies

Índice

Resumen ejecutivo

Reto

Las organizaciones que se están sometiendo a transformaciones digitales se enfrentan a un hecho que no sorprende: mayores preocupaciones en torno al riesgo y la seguridad. Inevitablemente, las iniciativas de transformación digital dan lugar a más puntos de acceso a la infraestructura empresarial que se encuentran fuera de los controles existentes, a los que puede acceder un conjunto mayor y más diverso de identidades, y que proliferan por toda una infraestructura dinámica y distribuida.

Oportunidad

Si conoce los usuarios con privilegios, conoce los riesgos. Las propias herramientas de gestión de accesos con privilegios deben ser capaces de admitir la automatización en procesos de autorización, así como de permitir la escalabilidad a través de la compatibilidad con operaciones dinámicas e infraestructuras efímeras, como las cuentas administrativas de Amazon Web Services (AWS) para identidades humanas.

Ventajas

La detección de los ataques que aprovechan el robo de credenciales no se mejora simplemente acumulando más datos, sino que requiere incorporar datos de mayor calidad sobre el comportamiento de los usuarios con privilegios, de manera que se puedan identificar cambios significativos que representen un riesgo real. Este planteamiento se ve más reforzado mediante la integración con sistemas de gobernanza de accesos con privilegios para permitir el análisis del comportamiento de todos los usuarios con funciones comparables.

Sección 1

Introducción

En la actualidad, el software se encuentra en el núcleo de la metodología de las empresas para competir y funcionar de forma eficaz en el siglo XXI. Durante mucho tiempo, la tecnología ha desempeñado un papel decisivo en la estrategia empresarial. Sin embargo, la transformación digital ha ampliado las iniciativas de transformación y aceleración del ciclo de entrega de software, así como los procesos de desarrollo de aplicaciones, a un imperativo que se extiende por toda la empresa y se interseca cada vez más con la otra preocupación que acucia a los directivos: la ciberseguridad.

Por obligación, la transformación implica cambio y, por ende, riesgo. A medida que las empresas avanzan en su proceso de transformación digital, el riesgo se acentúa, excepto si cuentan con un plan para progresar en materia de seguridad y gobernanza de accesos en sintonía con sus iniciativas y que reproduzca las prioridades de muchos planes de transformación digital:

- Habilitación de la automatización con responsabilidad y visibilidad
- Aumento de la velocidad de entrega en conjunto con la protección de los activos de la empresa
- Garantía de escala con gobernanza de accesos y detección de amenazas integrados

Para garantizar la visibilidad y responsabilidad de cara a la conformidad normativa, la seguridad y la gobernanza y, al mismo tiempo, facilitar la flexibilidad para la transformación digital, hace falta un enfoque actual y más armonizado respecto a quién (y, ahora, respecto a qué —aplicaciones, servicios, máquinas y cosas—) se proporcionan las llaves del reino: el acceso con privilegios.

Del mismo modo en que muchas empresas se encuentran en la actualidad en plena definición de una planificación práctica para su proceso de transformación digital, los equipos de seguridad precisan de las herramientas y capacidades de integración adecuadas para automatizar, acelerar y escalar progresivamente la gestión de accesos y la mitigación de riesgos de acuerdo con las necesidades de la empresa (sin tener que llevar a cabo nuevas y considerables inversiones).

Sección 2

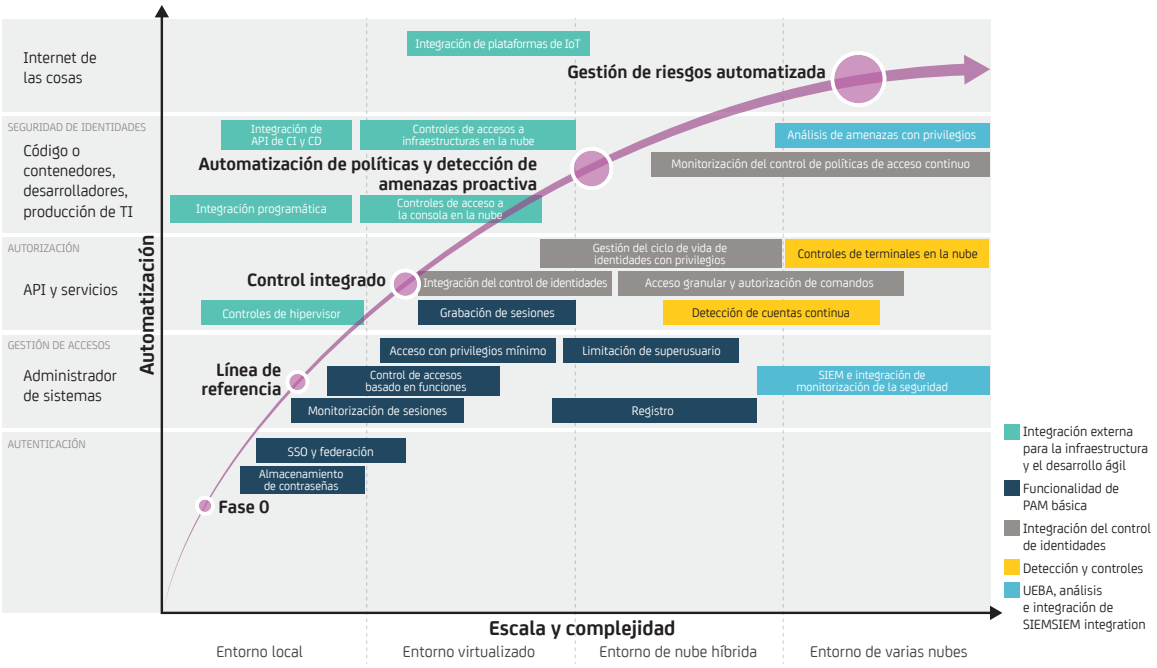
Aumento del riesgo relativo a los accesos con privilegios debido a la transformación digital

Por necesidad, la transformación digital cambia, acelera y automatiza la forma en la que interactúan las identidades humanas, las máquinas y el código. Las preocupaciones relativas al riesgo y la seguridad se magnifican porque las iniciativas de transformación digital dan lugar, de forma inevitable, a más puntos de accesos a la infraestructura empresarial que se encuentran fuera de los controles existentes, a los que puede acceder un conjunto mayor y más diverso de identidades que antes, y que proliferan por toda una infraestructura dinámica y distribuida (local, virtual y en la nube).

La determinación de qué identidades deben disponer de acceso a servicios y recursos específicos, la gestión de sus credenciales para los recursos y la garantía de que el acceso es adecuado con una intervención manual mínima y basada en políticas conforman un reto fundamental para posibilitar la automatización, la escala y la velocidad.

Asimismo, con el fin de asumir la revolución de la movilidad, las empresas deben prepararse para el modelo de Internet de las cosas (IoT), que incrementa exponencialmente el volumen de transacciones en toda la infraestructura. Como resultado de la adopción de herramientas de transformación digital, el elemento "quién" de la ecuación de la gestión de accesos experimenta un drástico cambio, incluso antes de que se introduzcan los dispositivos del IoT.

A fin de que la gestión de accesos con privilegios sirva como impulsor clave de la transformación digital y no se convierta en un cuello de botella, tanto la tecnología como las herramientas deben proporcionar una solución consolidada y ampliable para los riesgos derivados del proceso de transformación.



Gobernanza integrada

Los planteamientos manuales que dependen de un proceso de certificación humana no pueden escalar cuando la transformación digital amplía la cantidad de los usuarios que requieren acceso con privilegios más allá de las funciones de administrador de sistemas tradicionales y las entidades que pueden actuar como identidades con privilegios. Con el objetivo de equilibrar la agilidad y la seguridad para nuevas situaciones de acceso (independientemente de si se trata de desarrolladores con acceso a credenciales con privilegios en entornos de producción, contenedores virtualizados y hosts con autorización para acceder a orígenes de datos, o de administradores con acceso de superusuario a servicios en la nube), los requisitos de autorización y función se deben gestionar a través de un proceso de gobernanza integrada.

Automatización de políticas

Las arquitecturas de desarrollo e implementación de nubes híbridas que abarcan recursos locales, centros de datos virtualizados y entornos de nubes públicas pueden dar lugar a un planteamiento fragmentado y aislado en cuanto a las identidades con privilegios. Para garantizar la coherencia (y evitar la dependencia de ciertos distribuidores), se deben imponer de forma dinámica políticas centralizadas de gobernanza y control de accesos en cuentas con privilegios para entornos específicos (como las cuentas de superadministrador de AWS).

Detección de amenazas proactiva

Ahora, en lugar de gestionare el acceso a una contraseña compartida de una infraestructura estática (como un servidor de un centro de datos físico), las empresas deben gestionar cómo autorizar, monitorizar y registrar los accesos con credenciales con privilegios durante un periodo de una hora, un día o inclus, minutos, así como evaluar si las acciones realizadas o los cambios llevados a cabo con dichas credenciales son legítimos y no aumentan el riesgo. La adopción de un planteamiento basado en el contexto que aproveche el aprendizaje automatizado y los análisis del comportamiento puede impulsar la detección en tiempo real y activar los pasos de mitigación de riesgos, incluso en entornos dinámicos y efímeros.

Gestión de riesgos automatizada

La adopción del IoT no solo introduce un nuevo tipo de identidad de máquina con privilegios en forma de controladores de dispositivos de IoT; el uso de la tecnología también contribuye a obtener una cantidad quizás exponencialmente mayor de transacciones que se deben autorizar de forma explícita, así como monitorizar para detectar posibles ataques. Con el fin de hacer frente a la escala de identidades y el volumen de transacciones que realizan identidades con privilegios, se requiere un modelo automatizado que sea eficaz en materia de detección de amenazas y admita mecanismos para evaluar riesgos e implementar mitigaciones sin interrumpir de forma significativa los procesos empresariales.

Sección 3

Gobernanza integrada y automatización de políticas: cómo conseguirlas paso a paso

La gestión y la protección de accesos con privilegios en el marco de la transformación digital suponen un reto apremiante, pero no insuperable.

Sin embargo, dado que los atacantes aprovechan cada vez más (y con éxito) las credenciales de usuarios con privilegios para obtener acceso no autorizado, se requiere un modelo de madurez para limitar los puntos ciegos que presentan las políticas y la monitorización, además de para habilitar un modelo de detección proactiva a través de análisis basados en aprendizaje automatizado que puedan reforzar el valor de las inversiones actuales y mejorar la precisión.

A fin de facilitar la transformación digital, en lugar de lastrarla, el acceso con privilegios a la infraestructura, a los datos y a los sistemas con información confidencial se debe fundamentar en un conjunto de fases realistas y coordinadas en el contexto de un modelo de madurez. La acción más obvia consiste en reducir la cantidad de pasos manuales necesarios para proporcionar acceso a credenciales con privilegios y basar las decisiones de autorización en políticas claramente definidas.

A su vez, cuanto mejor integrados estén los procesos de gestión de accesos con privilegios y de gestión de ciclos de vida de identidades, de mayor alcance dispondrán los equipos de seguridad para habilitar la automatización a escala. Al aplicar comprobaciones automatizadas a las autorizaciones de funciones y accesos a los que se han asignado identidades con privilegios, se pueden detectar infracciones de forma proactiva, como el aprovisionamiento de acceso a credenciales a un desarrollador para que obtenga el código de producción.

La cuestión relevante en este caso gira en torno a la idea de que las propias herramientas de gestión de accesos con privilegios deben ser capaces de admitir la automatización en procesos de autorización, así como permitir la escalabilidad a través de la compatibilidad con operaciones dinámicas e infraestructuras efímeras, como las cuentas administrativas para identidades humanas de AWS.

Muchos planteamientos actuales en materia de gestión de accesos con privilegios se basan en la cobertura de un subconjunto de identidades con privilegios y no se diseñaron con la infraestructura moderna de TI en mente. Con el fin de avanzar por las fases del modelo de madurez, las empresas deben contemplar cómo los planteamientos de gestión de accesos con privilegios abordan la proliferación, la distribución y la transformación de identidades con privilegios, en función de su capacidad para realizar lo siguiente:

- Ampliar el control y la visibilidad de las identidades con privilegios desde centros de datos locales hasta centros de datos virtualizados, pasando por servicios en la nube.
- Automatizar la autorización de accesos con privilegios en función de los requisitos operativos a través de la integración con políticas de gestión de identidades basadas en funciones, en lugar de procesos de autorización manuales.
- Escalar e integrar los controles y la monitorización en infraestructuras dinámicas y efímeras.
- Facilitar tanto la monitorización como la gobernanza centralizadas y continuas para identificar cuándo se están otorgando inicialmente demasiados privilegios, así como para activar un flujo de trabajo de corrección.
- Incorporar la capacidad de detectar y corregir a medida que las nuevas amenazas evolucionan, a través de modelos de aprendizaje automatizado y basados en datos.

Sección 4

El riesgo en el contexto adecuado

Puesto que los programas de transformación digital dan lugar a redes distribuidas y elevados índices de cambios y volumen transaccional, así como a más identidades con privilegios, presentan un reto para los planteamientos tradicionales basados en reglas a la hora de detectar usos incorrectos o robos de credenciales con privilegios, cuya inadecuación ha quedado demostrada, incluso para las amenazas existentes.

Al adoptar un enfoque generalizado en materia de análisis de elementos con privilegios e introducir más datos en los sistemas de gestión de eventos e información de seguridad (SIEM), se pierde contexto importante que permite que los analistas de seguridad y las operaciones de TI realicen una distinción primordial entre una incoherencia, una anomalía grave y una actividad de alto riesgo que requiere corrección.

En lugar de ello se necesita un enfoque centrado en los dominios que aproveche tanto el contexto como el conocimiento sobre las funciones y el comportamiento de los usuarios con privilegios para reducir las posibilidades y encontrar la aguja en el pajar, acciones que representan pruebas tangibles de un ataque o peligro.

Un enfoque centrado en los dominios funcionará según los mismos principios de definición de modelos de comportamiento: qué acciones están llevando a cabo los usuarios con privilegios, cuáles han realizado en el pasado y el nivel o riesgo asociado a ellas (incluido el grado de confidencialidad del recurso objetivo), y cómo acceden a los sistemas. No obstante, el enfoque también debe incorporar una relación gráfica de entidades que ponga el comportamiento en contexto.

Sección 5

Conocimiento de los usuarios con privilegios: conocimiento de los riesgos

Una mejor localización de los ataques que aprovechan el robo de credenciales no se obtiene simplemente acumulando más datos, sino que implica la incorporación de mejores datos sobre el comportamiento de los usuarios con privilegios, de manera que se puedan identificar cambios significativos que representen un riesgo real.

Este planteamiento se ve más reforzado mediante la integración con sistemas de gobernanza de accesos con privilegios para habilitar análisis del comportamiento de todos los usuarios con funciones comparables. Cuando un usuario o máquina con privilegios accede a un sistema que no se corresponde con su función o con la de sus homólogos, o bien accede a un sistema desde una dirección IP diferente a la habitual y lleva a cabo acciones incoherentes en cuanto a patrones pasados, el sistema puede detectar con mayor precisión comportamientos acordes a un ataque y activar la corrección adecuada.

Sección 6

Conclusión

La transformación digital no se produce de la noche a la mañana, pero, inevitablemente, dependerá de la capacidad de automatización de, por un lado, la imposición de políticas de seguridad para las identidades que suponen un mayor riesgo y, por otro, la detección de posibles amenazas a partir del uso incorrecto de esas identidades con privilegios. La implementación de un planteamiento basado en riesgos se traduce en la garantía de que los controles y los análisis de seguridad pueden funcionar en sintonía con el proceso de transformación digital, así como habilitar de manera rentable la automatización, la escala y la velocidad sin crear riesgos. Este proceso requiere reflexionar sobre una planificación clara que abarque varios años, anticipar los requisitos a corto y largo plazo de una solución de gestión de accesos con privilegios, además de garantizar la satisfacción de las necesidades de alcance y escala a un coste de propiedad razonable durante todo el ciclo de vida.

La seguridad es obligatoria, pero su alcance, escala y coste no se pueden convertir en un impedimento para la transformación digital.

Para obtener más información sobre cómo CA PAM puede beneficiar a su negocio, 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**.

CS200-270334_0517