Delinea

Guía profesional para una gestión de accesos con privilegios (PAM) exitosa

WHITEPAPER

| Introducción

El 80%

de las vulneraciones están relacionadas con credenciales comprometidas, lo que hace que la gestión de accesos con privilegios (PAM) sea una prioridad de seguridad para organizaciones de todo tipo. Sin embargo, las ciberamenazas son cada vez más persistentes, y los entornos empresariales y técnicos resultan más complejos e interdependientes. Por tanto, las empresas proactivas y las organizaciones en rápido crecimiento están yendo más allá de los controles básicos de seguridad PAM para fortalecer y ampliar sus programas de protección de privilegios.

Este marco de mejores prácticas está diseñado para ayudar a los CISO, a las operaciones del departamento de IT y a los profesionales de la ciberseguridad a planificar y ejecutar un programa PAM avanzado, empleando las personas, los procesos y las tecnologías adecuadas. Además, refleja la experiencia de Delinea con más de 15.000 clientes en todo el mundo, incluyendo la mitad de las empresas de la lista Fortune 500.

A lo largo de esta guía, expertos en soluciones PAM de algunas de las organizaciones más concienciadas con la seguridad comparten sus experiencias en torno a la implementación de controles avanzados de seguridad en cuentas con privilegios y en la evolución de sus estrategias de PAM.

Ser un experto en soluciones PAM no consiste simplemente en convertirse en un genio en el uso del software. También es necesario desarrollar una estrategia coherente y un programa continuo que funcione para todas las partes interesadas, tales como los ejecutivos, los equipos de seguridad y de IT, los desarrolladores, los usuarios de la empresa y otras terceras partes implicadas. Así pues, los expertos en PAM gestionan la colaboración entre los diferentes departamentos para reducir eficazmente el riesgo en toda la organización. Esto implica adoptar un enfoque que otorgue prioridad a la actividad de la empresa y que permita a los empleados seguir siendo productivos al tiempo que se reducen los riesgos.

Esta guía muestra los pasos necesarios para convertirse en un experto en soluciones PAM y ayuda a equilibrar los objetivos de protección del acceso a las credenciales con privilegios y a los end points, mejorando la productividad y minimizando los costes.

CAPÍTULO 1
Definición de solución PAM «avanzada»

Pongamos en contexto la solución PAM «avanzada» para ver cómo la mayoría de las organizaciones implementan controles de seguridad de las cuentas con privilegios a medida que progresan.

En comparación con las organizaciones que acaban de empezar con una solución PAM, las que tienen experiencia han pasado de una estrategia de seguridad de los privilegios reactiva a una proactiva. Para ellas, la solución PAM es una prioridad máxima de ciberseguridad, apostando por un compromiso de mejora continua en las prácticas de seguridad que hay en torno a los privilegios, empleando para ello un programa de PAM permanente.

Las organizaciones avanzadas llevan la mejora continua a un nivel superior, integrando tecnologías punteras como la inteligencia frente a amenazas, los marcos de confianza, el aprendizaje automático y la automatización avanzada con el fin de recopilar información y adaptar las reglas del sistema. Estas organizaciones automatizan y gestionan completamente todo el ciclo de vida del acceso con privilegios, desde el aprovisionamiento hasta la generación de informes, pasando por la rotación y el desaprovisionamiento.

¿Qué privilegios contempla su programa de PAM?

Las identidades con privilegios pueden ser humanas o no humanas. Algunas cuentas con privilegios están asociadas a entidades como usuarios empresariales, máquinas locales o administradores de dominio y de red, mientras que otras son cuentas de servicio utilizadas para proporcionar acceso a redes, bases de datos y aplicaciones, como los sistemas de IoT y las cadenas de herramientas de DevOps.

En la figura 3 que aparece a continuación se incluyen varios tipos de cuentas con privilegios, y se indica por qué y cómo se utilizan, así como quién las utiliza y cómo deben protegerse.

Fig. 3: Matriz de gestión de accesos con privilegios: por qué, quién, dónde y cómo

¿Por qué son necesarias?	¿Tipos de cuentas con privilegios?	¿Quién las utiliza?	¿Dónde se encuentran?	¿Cómo se utilizan?	¿Cómo se protegen?	¿Riesgos si se ven comprometidas?
• Cambios en la configuración • Tareas administrativas • Crear/modificar/ eliminar usuarios • Instalar software • Acceder a datos • Realizar copias de seguridad de datos • Actualizar revisiones de forma interactiva	• Cuentas de dominio • Cuentas locales • Raíz • Usuarios con privilegios • Cuentas de emergencia • Administrador del sistema • Cuentas de servicio • Aplicaciones • Trabajos por lotes • Humano / no humano • Acceso de cuentas estándar a datos privilegiados	• Administradores de IT • Equipos de seguridad • Soporte técnico • Subcontratistas • Propietarios de aplicaciones • Administradores de bases de datos • Aplicaciones • Sistemas operativos • Desarrolladores • Hardware • IoT	• Servidores • Endpoints • Sistemas operativos • Virtual • Software • Nube • Bases de datos • Servicios • Programas	• Inicios de sesión interactivos • API • Servicios • Aplicaciones • Automatización • DevOps • SSH • RDP • VPN • Navegadores	• Contraseñas • 2FA • MFA • Claves • Acceso a flujos de trabajo • Grabación de sesiones • Lanzamiento • Análisis de comportamiento	• Malware • Fraude financiero • Ransomware • Falta de cumplimiento normativo • Vulneración de datos • Envenenamiento de datos • Amenazas internas • Tiempo de inactividad de servicio/aplicación • Pérdida de ingresos/marca

LISTA DE COMPROBACIÓN:

Los aspectos básicos, en primer lugar

Antes de tratar las fases más avanzadas que se describen en esta Guía Profesional, hay que asegurarse de haber establecido las bases.

Se debería poder responder «sí» a las siguientes preguntas.

- ☐ ¿Incluye las cuentas con privilegios en su política de ciberseguridad general?
- ☐ ¿Conoce y tiene en cuenta todas las cuentas con privilegios de la organización?
- ☐ ¿Las cuentas con privilegios utilizan contraseñas complejas generadas automáticamente que rotan con regularidad?
- ☐ ¿Se guardan todas las credenciales con privilegios en un almacén seguro?
- ☐ ¿Todas las contraseñas con privilegios están protegidas con varias verificaciones de credenciales?
- ☐ ¿Se aplican controles de seguridad, como la autenticación de dos factores, a las cuentas con privilegios?
- ☐ ¿Sabe qué mandatos de cumplimiento normativo precisa la organización?

Si una empresa todavía está trabajando en los aspectos básicos, la lista de comprobación de PAM puede ayudar.

CAPÍTULO 2
EL COMPONENTE HUMANO: establecimiento de funciones y responsabilidades de todas las partes interesadas

Por muy avanzados que sean los conocimientos técnicos en una organización, no se podrá crear un programa de PAM con éxito si no se cuenta con la participación de las principales partes interesadas. Es necesario coordinar las personas y la tecnología para que la solución PAM pueda desplegarse y adoptarse sin problemas.

Un programa integral de PAM debe involucrar diversas funciones de IT y de negocio, así como asignar a personas específicas para que asuman funciones y responsabilidades, desde la gestión ejecutiva hasta la administración del sistema. Las organizaciones, incluidas las pequeñas, deben identificar a una persona, un departamento o un equipo formal para que se haga cargo del programa, estableciendo las políticas de PAM y asegurándose de su aplicación. El equipo de gestión de identidades y acceso (IAM) suele ser el responsable, ya que existen fuertes vínculos con el personal de seguridad y de riesgos.

En una organización más pequeña, conseguir la aceptación de la solución PAM suele ser más rápido, pues a menudo es una de las numerosas responsabilidades de seguridad y operaciones asociadas a un único equipo de IT. En las más grandes, en cambio, la solución PAM puede ser una responsabilidad compartida entre diferentes equipos: seguridad de IT, riesgos de IT, gestión de identidades y acceso, operaciones de IT, desarrollo e ingeniería, etc. Estos equipos suelen informar a través del CISO o el CIO a la dirección ejecutiva, que a su vez se lo da a conocer al consejo de administración.

Para evitar fricciones entre los grupos, los expertos en soluciones PAM han de priorizar la colaboración, la transparencia y los objetivos conjuntos entre departamentos. Aunque los equipos de ciberseguridad puedan establecer los objetivos y la estrategia, dependen de sus homólogos de operaciones de IT para que les ayuden en las labores de implementación, gestión continua y presentación de informes.

Además, las políticas de PAM repercuten en el flujo de trabajo de otros equipos. Por ejemplo, si el equipo de PAM elimina los derechos de administrador local de las estaciones de trabajo para reducir los riesgos, tendrá que trabajar estrechamente con los equipos de soporte de IT para mantener el negocio en funcionamiento y evitar la posible reacción de usuarios enfadados.

En la figura 4 se ilustra la amplia gama de funciones y cargos de las partes interesadas en una organización, junto con sus responsabilidades y su participación en PAM.

Fig. 4: Funciones y responsabilidades de las principales partes interesadas en PAM

Enfoque y responsabilidad de la solución PAM	Funciones y cargos individuales	Qué hacen y cómo se puede ayudar
Supervisión	Ejecutivos de alto rango / Consejo de administración	Los clientes, auditores y reguladores consideran a la dirección ejecutiva responsable de la ciberseguridad. Su compromiso con un programa de PAM es esencial para aprobar los recursos, los plazos y el presupuesto adecuados. La mayoría de los ejecutivos y consejos de administración no son expertos en ciberseguridad, y probablemente no comprendan los requisitos de una solución PAM en comparación con otras estrategias cibernéticas. Para obtener el apoyo de este grupo clave, los expertos en PAM deben crear conciencia y facilitar la comprensión de la importancia de proteger las cuentas con privilegios, así como comunicar con regularidad el impacto de su programa de PAM. Es necesario alinear los informes con las prioridades de la empresa para mostrar cómo una solución PAM hace posible la innovación empresarial y reduce los riesgos cibernéticos.

Enfoque y responsabilidad de la solución PAM	Funciones y cargos individuales	Qué hacen y cómo se puede ayudar
Responsabilidad/ Dirección	Directores de seguridad de la información (CISO)	Los CISO actúan como el «pegamento» que une diversas disciplinas de seguridad, como la seguridad de las aplicaciones, la de la red y la respuesta ante incidentes, entre otras. Los CISO deben tener en cuenta cómo funciona la solución PAM en el marco de su estrategia global de seguridad y su conjunto de herramientas. Han de establecer objetivos y mediciones de alto nivel que posibiliten el éxito y que sean compartidos por todos los equipos. Además, tienen que reservar los recursos adecuados y aprobar los plazos. Si es necesario, pueden resolver conflictos y eliminar obstáculos para la adopción de PAM. Más allá de ser guardianes de la seguridad, los CISO buscan formas de convertirse en facilitadores del negocio, asegurando que las herramientas y políticas de seguridad también hagan más eficientes los procesos y aceleren los objetivos empresariales.
Gobernanza	Administradores de seguridad	Los administradores de seguridad gestionan todos los aspectos de la seguridad de la información y protegen los recursos virtuales de una organización. Son responsables de la seguridad de los ordenadores (desktop), los dispositivos móviles y la propia red. Una solución PAM puede formar parte de una funcionalidad más amplia de gestión de identidades y acceso (IAM) y gobernanza de identidades, que debe tenerla en cuenta en el contexto de Active Directory u otras soluciones y políticas de gestión de identidades. Los especialistas en PAM de este grupo son responsables de la instalación, administración y resolución de problemas de las soluciones de seguridad de PAM, incluyendo las políticas de privilegios mínimos, el control de aplicaciones y el Privileged Behavior Analytics. Las responsabilidades de gobernanza de la solución PAM de este grupo incluyen la definición, confirmación y organización de las reglas para secretos, permisos y flujos de trabajo. Se encargan de las convenciones de nomenclatura, la estructura de las carpetas y otros aspectos fundamentales de la gobernanza de identidades que mantienen el programa PAM organizado y en marcha.
Cumplimiento normativo	Auditores y responsables de cumplimiento normativo	Al igual que la mayoría de las funciones de ciberseguridad, las políticas de PAM se derivan en gran medida de los requisitos de cumplimiento normativo como PCI, NIST, ISO, SOX, HIPAA y el RGPD de la UE. Debido a las implicaciones legales, los equipos de cumplimiento normativo deben participar en la gobernanza de la solución PAM, incluyendo la creación de políticas, los registros y los requisitos de notificación.
Gestión de riesgos	Responsables de la gestión de riesgos	PAM también puede entrar dentro de la gestión de riesgos de IT, que es responsable de la clasificación de dichos riesgos y determina qué cuentas con privilegios y casos prácticos representan el mayor peligro y deben priorizarse en un programa de PAM.
Despliegue	Responsables de operaciones de IT/ nube	Los responsables de las operaciones de IT, así como los de la nube, son esenciales para garantizar el despliegue de la solución PAM en el contexto de la arquitectura de IT y las políticas de alojamiento de su organización.
Operaciones	Administradores de IT	Los administradores de IT, responsables de la configuración y gestión de aplicaciones, bases de datos, redes y otros recursos de IT, son los principales interesados en el éxito continuo de la solución PAM. Se encargan de la administración diaria del software PAM y si las políticas de seguridad afectan negativamente a su productividad o crean problemas a los usuarios de la empresa, podrían no adoptar la solución. Los administradores de dominio pueden estar acostumbrados a compartir credenciales con privilegios o a realizar su mantenimiento de otra manera. El cambio a una solución PAM centralizada requerirá su aceptación y su voluntad de cambiar los procesos existentes.

Enfoque y responsabilidad de PAM	Funciones y cargos individuales	Qué hacen y cómo puede usted ayudar
DevOps	Desarrolladores	Los desarrolladores pueden utilizar herramientas PAM de código abierto, crear sus propios métodos para proteger las credenciales en el proceso de desarrollo o no utilizar ningún control PAM para poder mantener la velocidad en su intenso calendario de lanzamientos. En las organizaciones que utilizan un modelo DevSecOps, la ciberseguridad está integrada en el proceso de desarrollo. Para incorporar a los desarrolladores en su programa PAM, especialmente en lo que respecta a la gestión de credenciales con privilegios a través de controles centralizados, los expertos en PAM necesitan integrar la PAM dentro de la cadena de herramientas de DevOps y cumplir con los requisitos de los desarrolladores en cuanto a velocidad y escalada.
Unidades de negocio	Directores de unidades de negocio	Los expertos en PAM necesitan entender de las unidades de negocio qué aplicaciones, sistemas y usuarios requieren acceso con privilegios y cuáles no. Los directores de las unidades de negocio ayudan a garantizar la adopción de PAM y la comprensión de las políticas entre los usuarios empresariales con privilegios. Se les puede pedir que aprueben las solicitudes de acceso o elevación, o que revisen la actividad de las cuentas de los integrantes de sus equipos. Muchas unidades de negocio conceden licencias de aplicaciones SaaS, con o sin permiso de la dirección de IT. Los directores de las unidades de negocio deben estar dispuestos a integrar estas herramientas en las políticas y los procesos de PAM de la organización.
Recursos Humanos	Directores de RR. HH.	La ayuda del departamento de Recursos Humanos es esencial para concienciar a los empleados sobre la seguridad. RR. HH. también puede participar en la determinación de las políticas de privacidad y otras relacionadas con los procedimientos de los empleados tras producirse una vulneración de credenciales con privilegios.
Área legal	Abogados	El personal jurídico puede participar no solo en la elaboración de políticas en materia de accesos con privilegios, sino también en el establecimiento de procedimientos para la gestión de una vulneración de credenciales con privilegios y de las personas implicadas. El personal jurídico que revise los contratos con subcontratistas y proveedores debe asegurarse de que los requisitos de PAM se incluyan en todos los acuerdos. Por ejemplo, las terceras partes deben aceptar determinados niveles de permisos, requisitos de aprobación y monitorización de sesiones antes de que se les conceda acceso a sistemas e información sensibles. Asimismo, todos los proveedores de software u otras tecnologías deben confirmar en sus acuerdos con los proveedores que siguen las prácticas recomendadas de PAM.
Servicios de seguridad gestionados	Consultores o equipos SOC de Cloud Partners	Los proveedores de servicios de seguridad gestionados (MSSP) requieren especial atención, con medidas de seguridad para los equipos SOC u otros consultores detalladas en los acuerdos de nivel de servicio.
Equipos de respuesta ante incidentes	CISO, administradores de seguridad, área legal, RR. HH., comunicaciones corporativas	El equipo de respuesta ante incidentes (RA) probablemente incluirá a muchas de las partes interesadas aquí descritas. Debe crearse un equipo formal de RA encabezado por el CISO, establecerse un plan y celebrarse reuniones periódicas para revisar y discutir los procedimientos de RA y la evolución de las amenazas.

Solución PAM centralizada para una estrategia holística e integrada

A medida que el programa de PAM avanza, se incorporarán más departamentos. En lugar de contar con varias soluciones PAM superpuestas que operen en silos departamentales, un programa avanzado centraliza todas las políticas y procesos de gestión de accesos privilegiados para una administración y supervisión exhaustivas y eficientes.

Así pues, hay que asegurarse de que las personas de los distintos departamentos participen en el proceso y reciban la formación necesaria para apoyar la solución PAM.

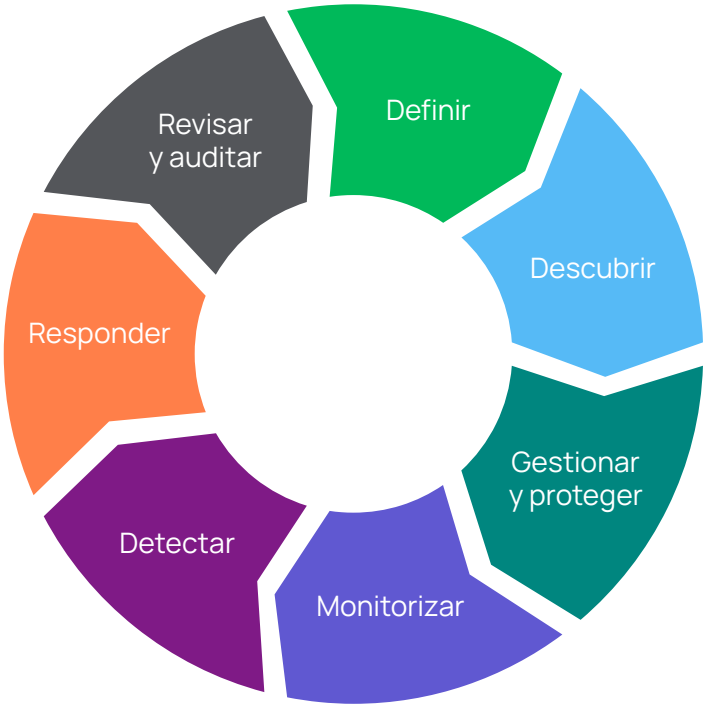
«Contar con un producto con el que todo el mundo esté de acuerdo hace que la gente sea mucho más productiva», señala Michael Somerville, de la Universidad de San Diego (Estados Unidos). Todo el personal debe compartir las mismas políticas, métricas y objetivos para conseguir el éxito».

CAPÍTULO 3

PROCESO: proceso y alcance del ciclo de vida de la solución PAM

Para ir más allá de lo básico, hay que planificar e implementar la solución PAM en el contexto de un programa continuo y en evolución.

La estrategia del ciclo de vida de la gestión de accesos con privilegios proporciona un marco para ayudar a los expertos a gestionar dicho acceso como un proceso continuo en lugar de como un proyecto único.



Definir

La fase de definición de un programa de PAM puede ser la que más tiempo consuma y en la que participen más partes interesadas, ya que en ella se sientan las bases de todo lo que viene a continuación. Es probable que no se disponga de los recursos necesarios para proteger todos los activos de datos, por lo que hay que priorizar dónde residen las llaves más importantes del reino, quién las utiliza, cuándo y con qué propósito. Esto no es estrictamente un ejercicio del departamento de seguridad o de IT, sino que debe involucrar a ejecutivos, responsables de unidades de negocio y propietarios de los datos de cara a entender perfectamente qué combinación de accesos con privilegios es la adecuada para una organización.

Es posible que ya se haya realizado una evaluación de riesgos básica. Sin embargo, para ser un experto en PAM, los procesos de evaluación han de ser continuos, integrados y automáticos.

Conviene comenzar por definir qué significa «acceso con privilegios», identificar qué es una cuenta con privilegios para la organización y definir las políticas de gobernanza. Estas decisiones son diferentes para cada empresa, por lo que es fundamental determinar qué funciones empresariales importantes dependen de los datos, los sistemas y el acceso. Comprender quién tiene acceso a las cuentas con privilegios y cuándo se utilizan es esencial para gestionar el alcance y la complejidad del programa de PAM.

Descubrir

Una vez identificadas las cuentas con privilegios, será necesaria una visión más detallada de los elementos de seguridad de los privilegios; por ejemplo, descubrir cuentas y dependencias de servicios, derechos de AWS, instancias de IT ocultas, así como usuarios y aplicaciones locales.

El descubrimiento no es un evento puntual. Se precisa continuidad para revelar la extensión de la superficie de ataque y su riesgo asociado. Lo ideal es que la detección se automatice y se revise semanalmente como mínimo.

Gestionar y proteger

Es necesario proteger el acceso a sistemas y servicios locales y en la nube, como IaaS, PaaS y SaaS. En el caso de los administradores de IT y los usuarios de cuentas con privilegios, se debe controlar el acceso a las estaciones de trabajo, los servidores, los contenedores y las consolas de la plataforma cloud a nivel detallado.

Los controles automatizados son la única manera de gestionar y proteger de forma práctica las cuentas con privilegios a escala.

Se ha de controlar el acceso a las cuentas con privilegios mediante requisitos de rotación de contraseñas y autenticación multifactor (MFA) en el inicio de sesión y en el aumento de privilegios.

También hay que implementar una gobernanza proactiva de las cuentas de servicio para evitar su proliferación.

Es recomendable implementar la gestión del aumento y la delegación de privilegios (PEDM) para evitar que los atacantes escalen esos privilegios, ejecuten aplicaciones maliciosas o herramientas de acceso remoto y comandos, y se desplacen lateralmente. La estrategia de aumento de privilegios tiene que basarse en la perspectiva del riesgo y el tipo de uso.

- En el caso de los usuarios que desean acceder a aplicaciones a través de estaciones de trabajo, en lugar de otorgar derechos de administrador local que aumenten el riesgo, se puede elevar el proceso a los privilegios de la aplicación, y no al usuario real. Esta estrategia de PEDM aumenta el número de pasos que debe dar un atacante para acceder a los

derechos administrativos. Las políticas de privilegios mínimos y las soluciones de control de aplicaciones permiten aumentar sin problemas las aplicaciones aprobadas y minimizar al mismo tiempo el riesgo de ejecución de las que no están autorizadas.

- Cuando existe un mayor riesgo, pero también una mayor confianza -cuando los usuarios administrativos necesitan acceder a los servidores- se puede optar por elevar al usuario.
- En el caso de que un tercero administre un firewall o una aplicación, es posible optar por conceder privilegios temporales que proporcionen derechos administrativos únicamente para una determinada aplicación, pero nada más.

Una vez establecidos los controles de seguridad, hay que monitorizar cómo se utilizan para asegurarse de que funcionan del modo esperado.

Monitorizar actividades

Hay que monitorizar y registrar toda la actividad de las cuentas con privilegios de forma muy detallada.

Al aumentar la supervisión, la monitorización puede imponer el comportamiento adecuado. También puede ayudar a determinar si una cuenta se ha visto comprometida. Si se produce una vulneración, esa monitorización ayuda a los forenses digitales a identificar las causas y a determinar los controles críticos que pueden mejorarse para reducir el riesgo de amenazas.

Específicamente se deben grabar las sesiones a nivel de almacén y/o a nivel de host, lo cual es útil si se pasa por alto el almacén.

Asimismo, conviene integrar la monitorización como parte de los inicios de sesión que los administradores utilizan para abrir conexiones remotas.

En el caso de una nube privada virtual, o de una plataforma en la nube como AWS, hay que asegurarse de que la dirección IP sea la única ruta de confianza hacia la red y confirmar que la conexión se origine a través del proxy.

Detectar

Con la monitorización en marcha, existe la oportunidad de detectar el abuso de privilegios y el compromiso de las cuentas. Sin embargo, nadie en el área de IT tiene tiempo para comprobar los registros de actividad de las cuentas con privilegios, pues es como buscar una aguja en un pajar.

¿Cómo se puede detectar a las personas que burlan los controles de seguridad? Las soluciones de análisis de comportamiento ayudan a entender los indicadores de compromiso. Determinan las líneas básicas para la actividad normal con privilegios, como la actividad de los usuarios, el acceso a las contraseñas, el comportamiento de usuarios similares y la hora de ese acceso.

Cuando se detecta una actividad inusual en las cuentas con privilegios, los sistemas de análisis de comportamiento pueden enviar alertas para así poder determinar las medidas a adoptar.

La forma de responder depende del nivel de compromiso y del nivel de riesgo.

Responder

Por ejemplo, si una cuenta de servicio se ve comprometida, puede bastar con rotar las contraseñas. También es posible que se desee investigar todas las actividades asociadas a una determinada cuenta. Podría cabe la posibilidad de que los hackers hubieran instalado malware e incluso creado sus propias cuentas con privilegios de puerta trasera mientras estaban dentro del sistema.

Sin embargo, si una cuenta de administrador de dominio se ve comprometida, la rotación no es suficiente. En ese caso, hay que asumir que todo el Active Directory está afectado y puede que sea necesario reconstruirlo para que un atacante no pueda volver fácilmente.

Revisar y auditar

Las alertas impulsadas por IA y los informes fáciles de comprender ayudan a rastrear la causa de los incidentes de seguridad, así como a demostrar el cumplimiento de las políticas y las regulaciones. La auditoría de las cuentas con privilegios también proporciona métricas que ofrecen a los ejecutivos información vital para tomar decisiones empresariales.

Prácticamente todas las normativas de ciberseguridad del mundo exigen controles de seguridad PAM como el control de acceso, la complejidad y rotación de contraseñas y las políticas de privilegios mínimos. Incluso las organizaciones que no están sujetas a requisitos del sector o de la ubicación en la que se encuentran se benefician de seguir los marcos de seguridad de las prácticas recomendadas, como los controles del NIST y el CIS.

Algunos reglamentos son muy prescriptivos, mientras que otros ofrecen directrices generales sin entrar en las decisiones detalladas. Para un experto en PAM su propio juicio es esencial para no abordar el cumplimiento normativo como un ejercicio puramente formal, sino como un proceso que permite fortalecer la postura de seguridad.

Las auditorías internas, planificadas y no planificadas, ayudan a los equipos a prepararse para las externas. Como parte de un proceso de auditoría, es necesario asignar las prácticas de PAM a los controles de seguridad indicados en las leyes aplicadas a la organización y asegurarse de conocer los plazos para el cumplimiento normativo.

CAPÍTULO 4
TECNOLOGÍA: implementación e integración de los controles de seguridad de la solución PAM

Una vez que se haya involucrado a las partes interesadas y se hayan creado los procesos PAM, el experto puede comenzar la implementación y el perfeccionamiento de las soluciones PAM que mejor se adapten al modelo de negocio específico y al sector. Una implementación con éxito de la solución PAM en toda la organización depende de la elección de las tecnologías adecuadas para automatizar y controlar el acceso con privilegios en diversos entornos y ecosistemas.

En la siguiente tabla se ofrece una guía práctica con recomendaciones técnicas prescriptivas para los expertos. Estos controles ayudan a establecer la seguridad de la solución PAM a lo largo del ciclo de vida de la misma y constituyen una base sólida con la que escalar a medida que madura el programa de PAM.

Fig. 6: Controles de seguridad de la solución PAM asignados al ciclo de vida

Etapa del ciclo de vida de la solución PAM	Control de la tecnología de seguridad	Cómo aplicar el control
Definir	Política y gobernanza	La gobernanza de la solución PAM incluye la instalación, organización e implementación del sistema en todas las unidades de negocio y áreas funcionales. Las organizaciones grandes o con suma diversidad pueden optar por incorporar primero algunas unidades de negocio o ubicaciones, y posteriormente desplegar la solución PAM en toda la estructura, segmento a segmento. En ese caso hay que decidir si se protegen primero los sistemas de alto impacto, ya que representan el mayor riesgo, o probar primero la solución PAM en sistemas de bajo impacto y con menos dependencias. Los requisitos de gobernanza guían la forma de configurar las identidades con privilegios, el flujo de trabajo, los permisos y los informes dentro de la solución PAM. Conviene tomarse el tiempo necesario para establecer políticas de convención de nombres, planificar la estructura de carpetas de permisos según los departamentos o equipos, establecer reglas para compartir secretos y definir una cadena de aprobaciones que se ajuste a la estructura de la organización. A continuación, hay que configurar la solución PAM en función de esos requisitos. Se debe decidir si gestionar y configurar la solución PAM internamente o trabajar con un proveedor para servicios gestionados o profesionales. A continuación hay que confirmar los requisitos del entorno de IT interno y las respectivas políticas, como las expectativas de alta disponibilidad y los acuerdos de nivel de servicio con otros departamentos. Esta información ayudará a definir la arquitectura subyacente y necesaria para una implementación local de la PAM, o bien se puede orientar la elección hacia una opción basada en la nube. Si se va a instalar un sistema PAM de forma interna, se ha de configurar y probar los motores distribuidos, las bases de datos, los firewalls, los enrutadores, la conmutación por error y los sitios de prueba. También hay que identificar a los administradores de SQL, AD, IIS y cualquier otra parte interesada que vaya a gestionar la solución PAM.
Descubrir	Descubrimiento y automatización	Se requiere la ejecución de procesos de descubrimiento para encontrar todas las cuentas que requieren privilegios, como las humanas, las de servicio, o las de administrador local en los endpoints y aplicaciones.

Etapa del ciclo de vida de la PAM	Control de la tecnología de seguridad	Cómo aplicar el control
Descubrir (continuación)	Descubrimiento y automatización	El descubrimiento debe incluir cuentas de Windows, Mac, Unix y VMware ESX/ESXi, así como plataformas en la nube como AWS y Azure. Para el descubrimiento adicional de tecnología heredada o personalizada, las secuencias de comandos de PowerShell pueden ayudar a garantizar la visibilidad de todos los posibles vectores de ataque. No hay que olvidar las cuentas con privilegios utilizadas por las tareas programadas y los grupos de aplicaciones, así como todas las dependencias entre sistemas. Es importante establecer procesos de descubrimiento continuo de modo que la información se mantenga actualizada a medida que las personas entran y salen y los sistemas cambian. Basándose en el descubrimiento exhaustivo, es posible determinar cuántas personas disponen actualmente de derechos de administrador de dominio en una organización e identificar oportunidades en las que se podrían reducir o compartir. Por ejemplo, es posible sustituir las cuentas individuales con nombre por cuentas compartidas y eliminar las cuentas con nombre del grupo de DA. O bien, se puede configurar la solución PAM para que pertenezca temporalmente al grupo DA únicamente cuando se utilice.
Gestionar y proteger	Seguridad del acceso	El núcleo de la solución PAM y la seguridad del acceso incluyen el almacenamiento, la delegación y el aumento de credenciales con privilegios de acuerdo con el principio de privilegios mínimos. Esto equilibra la protección de las cuentas con privilegios con la de las aplicaciones y los datos estratégicos que residen en estaciones de trabajo y servidores locales y en la nube. Las contraseñas, los certificados y las claves de las cuentas con privilegios se almacenan y gestionan en un repositorio seguro (un almacén cifrado), con permisos muy restrictivos, que idealmente requieren autenticación multifactor para acceder. Cuando los usuarios o los sistemas acceden a los secretos, la solución PAM establece los derechos de un solo usuario durante un período de tiempo específico. Es posible establecer automáticamente sesiones de inicio de sesión de administrador interactivo insertando credenciales en almacenes de forma transparente, sin exponer la contraseña al usuario. Una solución PAM avanzada puede servir como proxy a través del cual se realiza una sesión administrativa y así retransmitir automáticamente la contraseña de la cuenta con privilegios desde el almacén hasta el dispositivo o la aplicación de destino. Los programas PAM avanzados identifican y eliminan las contraseñas insertadas/codificadas y las sustituyen por llamadas a la API que insertan las contraseñas en las aplicaciones o los archivos de configuración. En lugar de residir en discos donde un atacante puede descubrirlas, se sustituyen por llamadas a la API para obtener las contraseñas del almacén en tiempo de ejecución. Además se pueden rotar las credenciales con regularidad, y bajo demanda, sin que ello afecte a las aplicaciones dependientes. También es factible aleatorizar y rotar las cuentas de servicio y las locales en los endpoints controlados. A medida que el programa se amplía a más sistemas y departamentos, se pueden configurar "cambiadores" de contraseña personalizados para cualquier credencial del sistema que no se conecte de entrada. También se pueden crear plantillas que den el máximo control sobre la complejidad de las contraseñas e incluir campos personalizados para las clasificaciones de impacto que pueden utilizarse de cara a determinar los niveles de acceso.

Etapa del ciclo de vida de la PAM	Control de la tecnologia de seguridad	Cómo aplicar el control
Gestionar y proteger	Protección de las sesiones	Los programas de PAM avanzados, especialmente importantes para las organizaciones que permiten el acceso de terceros a cuentas con privilegios, incluyen la monitorización y grabación de la actividad de las sesiones con privilegios, así como flujos de trabajo que permiten varios niveles de aprobación para conceder o denegar el acceso excepcional a datos sensibles o a sistemas críticos. Es recomendable añadir autenticación multifactor como garantía de identidad adicional, no solo en el inicio de sesión del almacén, el acceso a secretos y el establecimiento de la sesión, sino también en el servidor, durante el inicio de sesión y el aumento de privilegios.
Monitorizar	Auditoría/Monitorización	La monitorización de las sesiones incrementa el control sobre el uso de las cuentas con privilegios y permite un análisis en profundidad de la actividad de las sesiones en tiempo real o a posteriori. Con la capacidad «cuatro ojos» es posible conectarse en vivo para ver las sesiones, supervisar conexiones remotas, modificar privilegios o incluso finalizar conexiones.
Detectar	Análisis de comportamiento	Ciertas actividades, sistemas, aplicaciones, servicios en la nube, contenedores, etc. representan un riesgo relativamente bajo, mientras que otros son responsables de datos sensibles u operaciones críticas para el negocio y, por tanto, suponen un mayor riesgo. Los programas de PAM avanzados integran análisis de amenazas y clasificaciones de riesgo de sus soluciones SIEM u otros criterios de riesgo para ayudar a tomar decisiones. Además, el análisis de comportamiento puede rastrear la actividad de las cuentas con privilegios, reconocer patrones e identificar comportamientos sospechosos, denegando automáticamente el acceso o solicitando al usuario un segundo factor para demostrar su identidad.

TREND MICRO™

Trend Micro

El descubrimiento continuo permite al equipo de Trend Micro escanear la red y encontrar todas las cuentas de servicio, junto con los servicios, tareas y grupos de aplicaciones dependientes: determinar dónde se está utilizando cada una de esas cuentas, incluido el nuevo uso desde el último escaneo; e importar todas las cuentas de servicio a la herramienta PAM central para una gestión y auditoría continuas.

Su proceso elimina los errores manuales en la gestión, establece un rastro de auditoría y aumenta la rendición de cuentas. El equipo establece permisos y potentes funciones de control de seguridad, como Request Access, con el objetivo de monitorizar y aprobar a los usuarios que intentan acceder a las cuentas con privilegios. Asimismo, se graban las sesiones con privilegios que los usuarios inician utilizando las citadas cuentas de servicio y realizan un seguimiento de las pulsaciones de teclas durante dichas sesiones.

CUSTOMER SPOTLIGHT

Etapa del ciclo de vida de la PAM	Control de la tecnología de seguridad	Cómo aplicar el control
Responder	Respuesta ante eventos y recuperación	En función de los análisis que se configuren, se pueden activar alertas o respuestas automáticas. Por ejemplo, cuando se alerta de un comportamiento sospechoso, los administradores tienen la opción de rotar las credenciales inmediatamente, o bien finalizar o suspender las sesiones. Una vez que el evento es investigado y corregido o desestimado, los administradores pueden restablecer la línea de base. Cuando se configuran para la georredundancia y la alta disponibilidad, los sistemas PAM avanzados incorporan redundancia y conmutación por error.
Revisar y auditar	Auditoría/Monitorización	Los programas de PAM avanzados incluyen el registro de actividades con privilegios con un registro de auditoría inmutable que admite búsquedas guardadas, consultas ad-hoc, informes, reproducción para la investigación visual, auditoría y análisis forense de eventos. Hay que asegurar un registro que confirme que los empleados introducen un comentario explicando por qué necesitan acceder a una cuenta con privilegios. Esto puede ayudar a determinar si se puede delegar una tarea concreta. Se han de configurar alertas o correos electrónicos para responsables, jefes de equipo o InfoSec cuando se cambia el grupo de pertenencia del administrador del dominio u otros grupos con privilegios. Conviene reenviar el registro a un servidor SysLog o, si el registro se realiza en AD, utilizar el reenvío de eventos de Windows. Finalmente, se han de automatizar y compartir informes para aumentar la visibilidad y mejorar de forma continua el programa de PAM.

Poniendo la solución PAM en contexto: PAM multidimensional

La lista de controles destaca las principales actividades que deben implementarse durante el ciclo de vida de la solución PAM, pero hasta que se realice a escala el especialista no será un verdadero experto en PAM. Es importante tener en cuenta cómo un programa de PAM protege las credenciales con privilegios en diferentes estados, en toda su superficie de ataque y en el contexto de diferentes entornos.

- **Estado de las credenciales, sistemas y cargas de trabajo**
- **Dimensión de la superficie de ataque**
- **Contexto del entorno de IT**

A diferencia de los almacenes de contraseñas de los consumidores que guardan las credenciales en reposo, las credenciales empresariales se mueven por toda la organización, tanto en la memoria como en un token, y se utilizan para autenticar y autorizar la actividad con privilegios. Para hacerlo de forma segura, las credenciales con privilegios deben estar cifradas y utilizar autenticación multifactor (MFA).

También se pueden monitorizar las credenciales cuando están en uso, durante una sesión con privilegios o una llamada a la API.

Las empresas pueden tener miles o cientos de miles de cuentas con privilegios, como cuentas de servicio para servidores, bases de datos, aplicaciones y dispositivos de red (Windows, Mac, Linux/Unix y de propiedad). Muchas credenciales con privilegios se comparten entre personas y/o sistemas y pueden escapar fácilmente a su radar. A medida que un programa de PAM se amplía, especialmente a plataformas multinube, se descubrirán, incorporarán y gestionarán más plataformas.

¿Se utilizan credenciales con privilegios en la organización dentro de una cadena de herramientas DevOps, para conectar sistemas basados en la nube, archivos en scripts, o como parte de un entorno IoT integrado que pasa datos de un lado a otro? Estos entornos tienen un elevado nivel de dependencia y cambio. La interrupción de las conexiones en estos casos podría provocar el cierre de las operaciones y, por tanto, conlleva un mayor riesgo. Ampliar la solución PAM a estos tipos de entornos emergentes es un paso importante en el avance del programa.

Personalización de la solución PAM para que se adapte a una organización

Los programas de PAM suelen comenzar con el cambio de contraseñas por defecto o listas para usar en el caso de productos y dispositivos comunes. Sin embargo, cada organización es diferente y puede contar con sistemas y aplicaciones personalizados o heredados que también necesitan protección. Estas aplicaciones únicas requieren pruebas detalladas para identificar dónde podrían estar fallando los cambios de contraseña en el código. Los programas de PAM avanzados amplían la protección con privilegios a aplicaciones únicas con cambiadores de contraseña personalizados.

Del mismo modo, los programas de PAM comienzan por aprovechar fuentes de descubrimiento básicas como Active Directory, Unix y VMware. Una organización, sin embargo, puede necesitar ir más allá de estas fuentes con el fin de encontrar y gestionar cuentas con privilegios de bases de datos de Cisco, Oracle, SQL Server o MySQL. Un experto en PAM también puede descubrir y automatizar la gestión de esas credenciales, creando reglas para acceder a las cuentas, y convertir dichas credenciales en secretos que se puedan generar y cambiar automáticamente.

Las integraciones de expertos mejoran la colaboración y la eficiencia

Los equipos de operaciones de IT, seguridad y desarrollo deben formar un frente unido para protegerse de los ciberataques. Cuanto mejor coordinados estén, menos resquicios ofrecerá la superficie de ataque y más rápidamente se podrá responder ante un incidente.

Al igual que las operaciones de PAM no pueden existir aisladas, tampoco las herramientas que las respaldan. Los programas de PAM tienen más éxito cuando sus controles se integran con otras soluciones de IT y de seguridad. Con una integración sin fisuras, la información se mantiene actualizada, los informes tardan menos en generarse y las decisiones pueden tomarse con mayor rapidez. De este modo, un programa de PAM obtiene más visibilidad en toda la organización y para los ejecutivos y miembros del consejo de administración.

Las soluciones PAM pueden ofrecer una integración inmediata con herramientas de terceros y proporcionar acceso a las API y los scripts, que se pueden personalizar para adaptarlos a su propia solución y flujo de trabajo.

CUSTOMER SPOTLIGHT

IPC Subway

Con el objetivo de reforzar miles de servidores, IPC Subway confía en su solución PAM para garantizar la autenticación de dos factores y cambia las contraseñas semanalmente, con alertas que aseguran que los cambios se realizan correctamente. De cara a garantizar la disponibilidad y mitigar el riesgo, cada servicio de cada servidor tiene una contraseña única.

Mejora de la gobernanza durante todo el ciclo de vida de la solución PAM

PAM + IAM/IGA

Mientras que la solución PAM protege el acceso a las cuentas clave del sistema y de los administradores, la gestión de identidades y acceso (IAM) se aplica a cada cuenta de usuario de una organización. De hecho, la IAM posibilita que las personas adecuadas accedan a los recursos adecuados en el momento adecuado y por las razones adecuadas. Por ejemplo, la IAM permite proporcionar a un vendedor acceso a su cuenta y proporciona un acceso de mayor nivel para que determinadas personas inicien sesión en sistemas sensibles, como finanzas y recursos humanos, es decir, aquellos que requieran privilegios superiores.

Un sistema IAM/PAM integrado ayudará a realizar un seguimiento de la propiedad de las cuentas de usuario, marcar las que no se utilizan, automatizar el aprovisionamiento de nuevas cuentas, simplificar la asignación de cuentas con privilegios y permitir restricciones periódicas del acceso. La integración permitirá cumplir con los requisitos de cumplimiento normativo y presentación de informes de manera eficiente y con una carga mínima.

Algunas soluciones de IAM, como Identity Governance and Administration (IGA), proporcionan capacidades de monitorización y elaboración de informes que son necesarias para un programa de cumplimiento normativo. Estas soluciones son útiles para garantizar un amplio cumplimiento de las políticas de seguridad e identificar los valores atípicos. Asimismo, ayudan a segregar funciones, gestionar solicitudes de acceso y recertificar el acceso (recertificación continua o basada en activadores a lo largo de todo el ciclo de vida, en lugar de requerir una revisión periódica manual). Cuando se ajustan los derechos mediante una solución IGA como SailPoint IdentityIQ, el flujo de trabajo IGA integrado con PAM puede aplicar los cambios automáticamente, lo que hace que la solución PAM aprovisione nuevos roles y desaprovisione los existentes.

CUSTOMER SPOTLIGHT

Estado de Indiana (EE. UU.)

El Estado de Indiana ha desarrollado un despliegue de soluciòn PAM muy avanzado. Al integrarla con Active Directory, se asegura de que las cuentas de servicio se configuren correctamente, con los privilegios adecuados, y se gestionen de forma segura desde el primer día.

«Hemos eliminado todo tipo de errores al centralizar y automatizar la solución PAM, y al eliminar la creación manual de cuentas en Active Directory por parte de seis personas diferentes, con los consiguientes posibles errores».

Indiana ha ampliado el uso de la solución PAM desde la gestión de cuentas de servicio hasta la protección de aplicaciones utilizadas por terceros y desarrolladores de software. Según el experto en PAM del Estado de Indiana, «solíamos tener sesiones ocultas activas que podían durar cuatro o cinco horas. Había momentos en los que, en mitad de la noche, teníamos que levantarnos y compartir nuestra pantalla con un desarrollador para que pudiera solucionar un problema en producción. Ahora puedo entrar y elevar las aplicaciones utilizando su grupo de usuarios y simplemente se automatiza el proceso».

Ahorro de tiempo con la autenticación controlada

PAM + Active Directory

Las cuentas de usuarios con privilegios suelen estar ubicadas en un sistema central de autenticación que se ejecuta en Active Directory (Windows) -o en otro sistema central de identidad y autenticación que gestione cuentas, grupos y permisos para los empleados-. Los cambios de contraseñas pueden suponer un reto en un solo sistema; pero cuando se intenta mantener varios sincronizados, hay muchas posibilidades de que se produzcan errores.

Es importante que un proceso de gestión de cuentas, desde la creación hasta la rotación y el desaprovisionamiento, se mantenga coordinado en todo momento.

Además, una integración PAM puede aprovechar Active Directory como motor de políticas central para las políticas PAM y MFA en los sistemas Windows, Linux y Unix.

Una integración avanzada, como el puente de Active Directory, también puede ir más allá al ampliar muchas de las capacidades de AD a plataformas diferentes a Windows, como el inicio de sesión único basado en Kerberos, las políticas de grupo y la compatibilidad con tarjetas inteligentes para el inicio de sesión en Linux.

PAM + gestión de conexiones

Las credenciales con privilegios que se utilizan al realizar conexiones de escritorio remoto iniciadas por almacén, como el inicio de sesión en sistemas y cargas de trabajo directamente, así como la elevación de privilegios proporcionan acceso a infraestructuras, datos y aplicaciones críticas. Al configurar las sesiones remotas, los equipos de IT deben navegar por redes complejas, servicios cloud y las propias necesidades de los usuarios. Esto provoca que suelan tener varias sesiones activas a la vez, utilizando diferentes protocolos de conexión y diversas cuentas con privilegios.

Las soluciones de gestión de conexiones integradas proporcionan un entorno unificado para gestionar varias sesiones remotas e interactuar con ellas tanto para el protocolo de escritorio remoto (RDP) como para Secure Shell (SSH).

Como resultado de ello, los equipos de IT ahorran tiempo y reducen el riesgo. Los administradores pueden iniciar conexiones remotas utilizando varios protocolos, autenticar y obtener acceso a recursos críticos con los permisos adecuados. Además, pueden monitorizar y grabar varias sesiones remotas simultáneas de cara a aumentar la rendición de cuentas y proporcionar un rastro de auditoría para demostrar el cumplimiento normativo.

Mejora de la visibilidad y el flujo de trabajo entre la seguridad y las operaciones de IT

PAM + gestión de servicios de IT

Se deben cotejar los numerosos sistemas de gestión de servicios que una organización tiene en marcha para respaldar el flujo de trabajo y los procesos de IT. Un programa de PAM se implementará de forma más rápida y completa (y será más sostenible en el tiempo) si comparte información de forma bidireccional con los sistemas que conforman la base de las operaciones de IT para realizar su trabajo.

Por ejemplo, los sistemas de gestión de activos realizan un seguimiento de las estaciones de trabajo y aplicaciones aprobadas que se emplean en la organización. A medida que se despliegen las políticas de control de aplicaciones y de privilegios mínimos, la conexión con estos sistemas mejorará el proceso de descubrimiento y ayudará a mantener el inventario actualizado. Será posible entonces establecer rápidamente una política de privilegios mínimos para las nuevas estaciones de trabajo mediante la integración con las soluciones que el departamento de IT utiliza para la configuración y el despliegue de nuevos dispositivos. Además, se puede integrar el control de aplicaciones con los sistemas de creación de tickets del servicio de asistencia técnica utilizado por el área de operaciones de IT para atender las solicitudes de los usuarios en materia de aplicaciones y asistencia.

Las solicitudes de elevación de aplicaciones pueden gestionarse directamente en el sistema, por lo que existe una comunicación continua y un seguimiento de los eventos. Por último, la integración con ServiceNow y otras herramientas de gestión de operaciones de IT (ITOM) evita la configuración de contraseñas de cuentas codificadas, permitiendo que las aplicaciones de ITOM obtengan las credenciales mediante programación y desde el almacén como proveedor de credenciales externo.

Identificar los fallos de diseño con mayor rapidez y precisión

PAM + escaneo de vulnerabilidades

La integración de la solución PAM con las herramientas de gestión y comprobación de vulnerabilidades proporciona credenciales para escanear los sistemas en busca de revisiones que faltan y asegurarse de que estén instaladas correctamente.

Este escaneo profundo de credenciales permite una evaluación de vulnerabilidad más completa de lo que se podría lograr con las pruebas de penetración solamente.

Incorporación automática del malware conocido a las políticas de control de aplicaciones

PAM + análisis de amenazas

La integración de las soluciones PAM con el análisis de amenazas ayuda a seguir la actividad de los ciberdelincuentes a medida que desarrollan nuevos programas maliciosos y estrategias de ataque avanzadas.

Las bases de datos de inteligencia frente a amenazas, como VirusTotal, forman listas de denegación que se pueden incorporar a las soluciones PAM para bloquear la ejecución de aplicaciones maliciosas conocidas. La inteligencia artificial y el aprendizaje automático de soluciones como Cylance ayudan a anticiparse y detectar la actividad maliciosa.

IT'S HOW WE CONNECT

Telstra

La plataforma CI/CD de Telstra se conecta a su herramienta de PAM a través de la API para obtener credenciales con privilegios en tiempo de ejecución, reduciendo a la vez el impacto cuando hace falta cambiar contraseñas. Por ejemplo, Telstra almacena los certificados SSL como secretos en su almacén de PAM, estableciendo la caducidad y las alertas para garantizar la gobernanza adecuada.

CUSTOMER SPOTLIGHT

Registro de eventos, incorporación de datos de ciberseguridad y activación de alertas

PAM + SIEM

Muchos equipos de IT y de seguridad confían en las soluciones de gestión de eventos e información de seguridad (SIEM) y de gestión de registros, como ArcSight, Splunk y LogLogic, para la elaboración de informes centralizados y la respuesta coordinada ante incidentes. Como parte de una estrategia basada en el riesgo, conviene utilizar estas soluciones para clasificar y evaluar una amplia gama de eventos con el fin de priorizar el riesgo empresarial y técnico.

CAPÍTULO 5
CONCLUSIÓN Y SIGUIENTES PASOS: El proceso continuo de la solución PAM

Incluso los despliegues de PAM más maduros se encuentran en un proceso de mejora continua.

A medida que el privilegio se reconoce como nuevo perímetro, todos en la organización deben convertirse en «expertos» en PAM en cierto modo. Esto precisa una formación continua.

Una organización crecerá y evolucionará, lo que significa que los requisitos empresariales y técnicos cambiarán. Por ejemplo, los nuevos procesos de desarrollo o las políticas Cloud First pueden generar nuevos tipos de cuentas con privilegios que precisan protección. O bien puede que se adquiera o se fusionen dos empresas y sea necesario integrar nuevas personas y sistemas de forma rápida y segura.

Una empresa puede estar preparada para estas nuevas situaciones eligiendo una solución escalable que pueda adaptarse a nuevas situaciones.

No hay duda de que los ciberdelincuentes se volverán más sofisticados y desarrollarán nuevas estrategias para conseguir sus objetivos. Con los fundamentos bien aplicados, será posible construir desde una posición de fuerza para mantener el ritmo frente a las amenazas cambiantes, disminuir la superficie de ataque y reducir el riesgo para la organización.

CUSTOMER SPOTLIGHT

AMERICA FIRST CREDIT UNION

America First

La integración de PAM con las herramientas de vulnerabilidad de America First proporcionó una comprensión más precisa de la seguridad de la red de la organización.

Por ejemplo, con el escaneo no autenticado en un sistema de prueba de PC, QualysGuard no encontró vulnerabilidades en la red. Sin embargo, tras agregar el escaneo autenticado usando la solución PAM, QualysGuard arrojó 33 vulnerabilidades, y el equipo de InfoSec adoptó medidas para solucionarlas.

Delinea

Defining the boundaries of access

Delinea es un proveedor líder de soluciones de gestión de accesos con privilegios (PAM) que proporciona una seguridad sin fisuras para la empresa moderna e híbrida. Delinea Platform amplía sin problemas PAM proporcionando autorización para todas las identidades, controlando el acceso a la infraestructura de nube híbrida más crítica de una organización y a los datos sensibles para ayudar a reducir el riesgo, garantizar el cumplimiento y simplificar la seguridad. Delinea pone fin a la complejidad y define las limitaciones de acceso para miles de clientes en todo el mundo. Nuestros clientes comprenden desde pequeñas empresas hasta las mayores instituciones financieras del mundo, agencias de inteligencia y empresas de infraestructuras críticas. **delinea.com/es/**