¿Qué es una política de Administración de Acceso Privilegiado (PAM)?

TABLA DE CONTENIDO

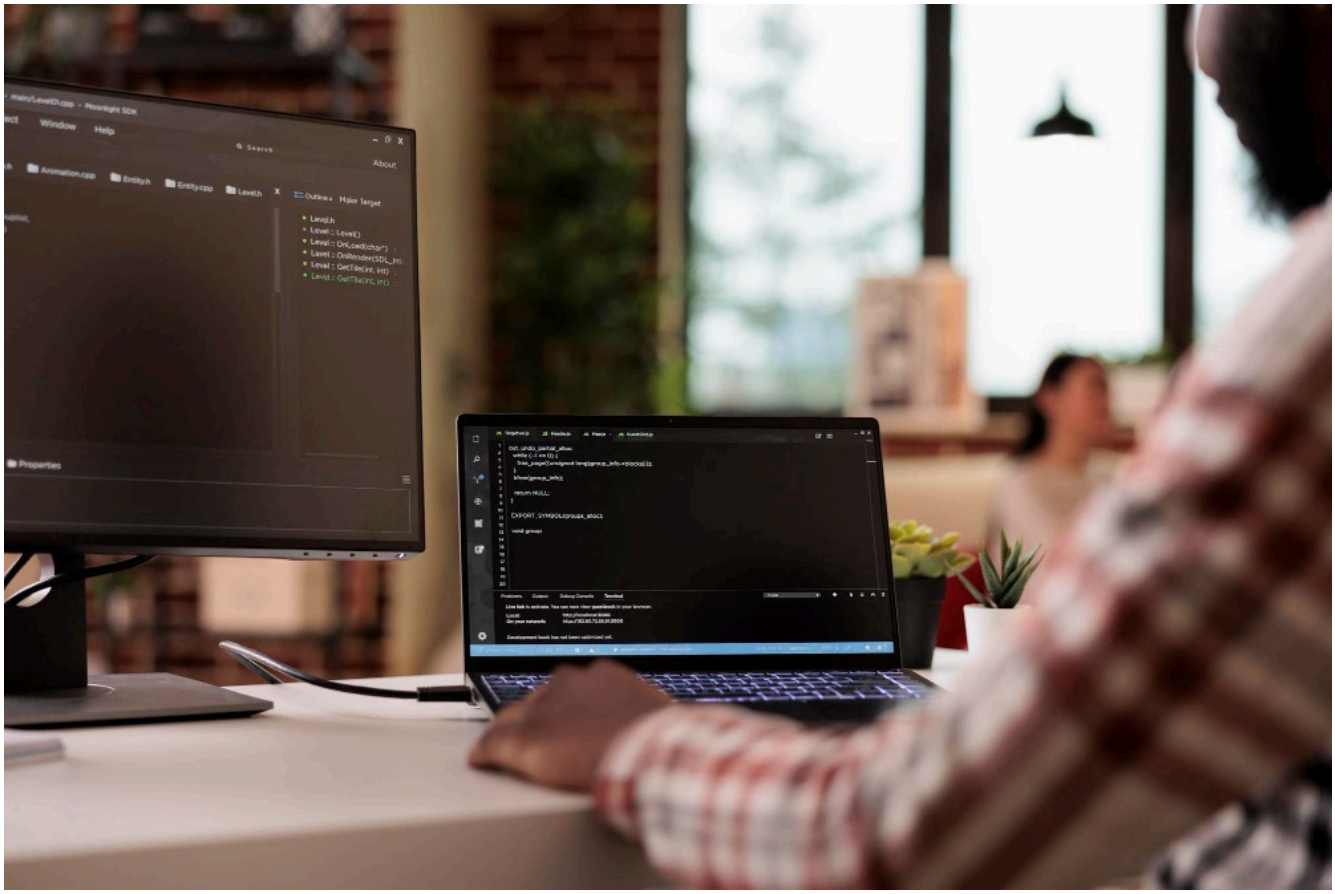
¿Qué es una política de administración de acceso privilegiado?

Beneficios de una política de gestión de acceso privilegiado

Cómo crear una política de administración de acceso privilegiado

¿Cómo hacer cumplir una política de PAM?

¿Cómo puede ayudar Heimdal?



La tecnología de ciberseguridad va de la mano con la gobernanza basada en políticas, pero no basta con desarrollar una política de contraseñas para proteger los datos y la información de la empresa. Uno de los primeros pasos para implementar con éxito una solución de administración de acceso privilegiado (PAM) es definir políticas claras y consistentes que todos los que usan y administran cuentas privilegiadas entiendan y acepten.

Veamos qué es una política de Administración de acceso Privilegiado o privileged access management (PAM) y por qué las organizaciones la necesitan.

¿Qué es una política de administración de acceso privilegiado?

Las políticas, o reglas, determinan cómo los equipos involucrados deben implementar la tecnología de seguridad. Un firewall puede evitar el acceso no autorizado, pero si no hay reglas que establezcan claramente quién puede modificar su configuración, se vuelve inútil.

Una política PAM es un conjunto de procedimientos y controles que restringen el acceso a los sistemas, datos y otros recursos a los usuarios autorizados. El objetivo de una política de administración de acceso privilegiado es proteger la información confidencial y evitar el acceso no autorizado. Escribir una política formal para cuentas privilegiadas, definir roles dentro de su organización y delinear los privilegios y derechos de acceso requeridos para cada rol es solo una de las mejores prácticas de PAM de las que hablamos en un artículo anterior.

Puede personalizar fácilmente la política de PAM para que coincida con las necesidades de su entorno de TI, los requisitos reglamentarios y la estructura organizativa, y luego finalizar y compartir el documento con todos los miembros del equipo de TI, ejecutivos y auditores.

Las políticas de administración de acceso privilegiado suelen incluir los siguientes componentes:

- Listas de control de acceso que especifican qué usuarios están autorizados a acceder a qué recursos.

- Mecanismos de autenticación que verifican la identidad de los usuarios antes de que se les conceda acceso.
- Reglas de autorización que dictan lo que los usuarios pueden hacer con los recursos a los que se les ha otorgado acceso.
- Pistas de auditoría que rastrean la actividad del usuario e identifican cualquier intento de acceso no autorizado.
- Medidas de seguridad que restringen el acceso físico a sistemas y datos.

Beneficios de una política de gestión de acceso privilegiado

Una política de administración de acceso privilegiado es un conjunto de reglas que rigen cómo los usuarios privilegiados (por ejemplo, aquellos con permisos elevados) acceden y usan sistemas y datos confidenciales. Al implementar una política de este tipo, las organizaciones pueden protegerse mejor de las amenazas internas, los actores maliciosos y las fugas de datos accidentales.

Existen muchos beneficios al implementar una política de administración de acceso privilegiado, que incluyen:

- Menor riesgo de violaciones de datos: al restringir el acceso solo a quienes lo necesitan, puede reducir las posibilidades de que los datos confidenciales caigan en manos equivocadas.
- Cumplimiento mejorado: una política bien definida puede ayudar a su organización a cumplir varios requisitos de cumplimiento, como los relacionados con la privacidad y la seguridad de los datos.
- Seguridad mejorada: al dificultar el acceso de usuarios no autorizados a datos y sistemas confidenciales, puede mejorar aún más la postura de seguridad general de su organización.
- Mayor eficiencia: al agilizar el proceso de aprobación y administración de cuentas privilegiadas, puede ahorrarle tiempo y dinero a su organización.

Cómo crear una política de administración de acceso privilegiado

Las políticas de ciberseguridad suelen estar plasmadas en un documento escrito. Las reglas controlan qué empleados y usuarios tienen acceso a la tecnología y los activos de información de una organización.

Al crear una política de administración de acceso privilegiado, hay algunos aspectos clave que debe tener en cuenta.

1. Primero, identifique qué usuarios requerirán acceso a qué sistemas y datos. Para comenzar, haga una lista de todos los sistemas y datos que requieren acceso privilegiado. Una vez que tenga una lista completa, comience a asignar usuarios a cada elemento de la lista. Tenga en cuenta lo que cada usuario necesita hacer con el sistema o los datos en cuestión al realizar sus asignaciones.
2. Una vez que haya determinado qué usuarios necesitan acceso a qué sistemas y datos, es hora de establecer qué nivel de acceso necesitará cada usuario. ¿Requerirán plenos derechos administrativos o será suficiente un conjunto más limitado de privilegios? Establecer esto con anticipación lo ayudará a evitar otorgar demasiado acceso y minimizar el riesgo de abuso.
3. Finalmente, deberá reunir algunas reglas y procedimientos para otorgar y revocar el acceso según sea necesario. ¿Quién será responsable de administrar las cuentas de los usuarios? ¿Qué procesos se implementarán para agregar nuevos usuarios o revocar privilegios? Tener estos procedimientos implementados con anticipación ayudará a garantizar que solo aquellos con el nivel adecuado de acceso lo tengan cuando lo necesiten.

¿Cómo hacer cumplir una política de PAM?

Una vez definidas, las políticas de seguridad cibernética deben aplicarse, ya que la definición y la aplicación de políticas son dos actividades separadas. Si la definición de la política PAM cubre aspectos tales como quién puede acceder a qué sistema, la aplicación de la política PAM es donde la solución pone en práctica estas políticas definidas.

Deben integrarse los mecanismos de aplicación y definición de políticas de PAM. De lo contrario, existe el riesgo de que las definiciones de las políticas se vuelvan obsoletas y se ignoren mientras la aplicación pierde su conexión con las políticas reales. Una solución PAM debería poder proporcionar a los administradores de seguridad medios simples y eficientes para definir y hacer cumplir las políticas PAM.

¿Cómo puede ayudar Heimdal?

Nuestra solución de Gestión de Acceso Privilegiado destaca por sus características:

- Cuando se usa junto con nuestro Antivirus Nex-Gen, se convierte en el único software que reduce automáticamente los derechos de los usuarios, en caso de que se detecten amenazas.
- Interfaz liviana e impresionante que le brinda un control completo sobre la sesión elevada del usuario. Apruebe o rechace desde el tablero o sobre la marcha directamente desde su dispositivo móvil.
- Tiene la pantalla Protección de ejecución de confianza cero en la vista Privilegios y control de aplicaciones: Administración de acceso privilegiado, que incluye muchos detalles como los procesos (archivos ejecutables no firmados) que interceptó el motor de protección de ejecución de confianza cero, con datos sobre el nombre de host, Nombre de usuario, nombre del proceso, hash MD5, marca de tiempo y estado.
- Análisis de datos avanzados que ayudarán a investigar incidentes y realizar controles de seguridad periódicos. Obtenga informes ricos en gráficos sobre los detalles del nombre de host, la duración promedio de la escalada, los usuarios o archivos escalados, los archivos o procesos ejecutados durante la escalada y más.

Además, puede agregar nuestro módulo de control de aplicaciones a la combinación y podrá realizar la aprobación o denegación de la ejecución de la aplicación o la personalización de la sesión en vivo para garantizar aún más la seguridad comercial.

La gestión de privilegios es un aspecto fundamental de cualquier estrategia de ciberseguridad. ¡Asegúrese de tener la herramienta PAM adecuada y esté un paso por delante de los piratas informáticos!

Puede leer el artículo original siguiendo este enlace.