ManageEngine
PAM360

Proteger las cuentas de servicio de Windows con controles de gestión de acceso efectivos

Las cuentas de servicio son cuentas de dominio privilegiado, que son utilizadas por aplicaciones o servicios críticos para interactuar con sus sistemas operativos y para ejecutar archivos por lotes, tareas programadas y aplicaciones alojadas en bases de datos, sistemas de archivos y dispositivos. Estas cuentas son controladas por usuarios "no humanos", como sistemas, scripts, aplicaciones, y por lo general tienen privilegios elevados a aplicaciones críticas para el negocio, bases de datos, servicios web, API, etc.

Categorías de cuentas de servicio

Tipo de cuenta	Descripción
Compartida	Cuentas que son utilizadas por dos o más usuarios en un sistema. Las credenciales de la cuenta se comparten entre los usuarios.
Sistema	También conocidas como cuentas privilegiadas o de "superusuario". Estas cuentas administrativas se utilizan para habilitar las comunicaciones y los procesos dentro del sistema operativo (por ejemplo, root en UNIX).
No interactiva	Cuentas que se utilizan para ejecutar procesos y servicios del sistema, como ejecutar scripts automatizados, archivos por lotes y tareas programadas. Los usuarios finales no pueden iniciar sesión en estas cuentas.

Note: Podría haber más sub-clasificaciones de las cuentas que podrían entrar en las categorías de cuentas de servicio y SO.

Riesgos de seguridad asociados a las cuentas de servicio

Hay varias razones por las que la mala gestión de las cuentas de servicio puede suponer grandes riesgos de seguridad para las organizaciones.

Demasiado complejo para gestionarse manualmente

Las cuentas de servicio, aunque son fáciles de configurar y usar, están estrechamente interconectadas y compartidas con varias aplicaciones y servicios. Además, se hace referencia a ellas en múltiples instancias a través de múltiples activos y aplicaciones, lo que hace que gestionar estas cuentas sea tan complejo que incluso el más mínimo descuido con la cadena de dependencias podría causar fallos en el sistema masivos.

Puerta trasera a información privilegiada

Las cuentas de servicio están, la mayoría de las veces, vinculadas a aplicaciones críticas para el negocio y, por lo tanto, pueden requerir acceso privilegiado a servidores, bases de datos y otros activos. Con una sola cuenta comprometida, los atacantes pueden obtener un control total sobre los activos privilegiados, los endpoints y la información confidencial compartida.

Alto valor, objetivo fácil para los atacantes

Dado que las cuentas de servicio son utilizadas principalmente por entidades no humanas para realizar operaciones, no se pueden aplicar controles de seguridad como la autenticación de dos factores (TFA), ya que requiere interacción humana para fines de autenticación. Para complicar esto, las contraseñas de las cuentas de servicio se configuran para que sean permanentes, ya que rotarlas con frecuencia puede provocar bloqueos e interrupciones imprevistas. Como resultado, las cuentas de servicio se convierten en un objetivo fácil y lucrativo para los atacantes.

Ciclo de vida de la gestión de cuentas de servicio: Primeros pasos

A medida que las organizaciones crecen, gestionar manualmente las cuentas de servicio resulta abrumador y laborioso debido al número de aplicaciones y servicios a los que acceden. Debido a la omnipresencia y proliferación de las cuentas de servicio, y el creciente riesgo de que sean un objetivo fácil, es importante monitorear, administrar y auditar activamente el uso de estas cuentas. Para que las organizaciones identifiquen y frustren posibles explotaciones de las cuentas de servicio, tendrán que implementar un curso de acción que logre un fino equilibrio entre las operaciones y la seguridad.

- .[NcWOUSXMNBXU[XYUU[R(W
  RW[XYXR(WbXW[XUMNXMNUWJMNNRRX
- .WNNNUNW[X[WXMNUJURR(WYNR(MRWW[NYU
  MNR[UWJMNNRRXWNbUX\
  NRRXJURRXWNbX[WJMNNRRXUXW
  NJW[XWN[W
- NP-[NNMNXU[MNWRUNMNUWJMNNRRX
  NX[NWbURNW[NPU[WJNNWOWR(WMNUJ
  YXU[RWMN[XWJNJWM[
- NRNNUNJMXMNUWJMNNRRXRJ
  RW[RJNURRWWJNP-[NNMNXUWJMN
  NRRXNWRMWNURRWWJMNU[M

3. Proteja el acceso a las cuentas de servicio.

Para contrarrestar los riesgos de abuso de la cuenta de servicio, las organizaciones deben considerar firmemente invertir en soluciones de gestión de acceso privilegiado (PAM), que ayudan a racionalizar la gestión del ciclo de vida de la cuenta de servicio. Las herramientas PAM permiten a los administradores de TI desarrollar un control sólido sobre las cuentas de servicio distribuidas en toda la red corporativa mediante automatizaciones efectivas para descubrir, proteger y monitorear el acceso a estas cuentas. Una solución PAM sólida proporciona una bóveda segura para almacenar y rotar las credenciales de las cuentas de servicio, y permite compartir contraseñas a usuarios que no son administradores en función de requisitos específicos. Esto ayuda a evitar el acceso no autorizado a las cuentas de servicio y protege estas cuentas del abuso de privilegios.

Integrar las herramientas PAM con herramientas SIEM y herramientas de análisis de TI permite a los administradores de TI monitorear la actividad de los usuarios con estas cuentas, identificar y contener comportamientos anormales, y adherirse a las políticas de cumplimiento al generar informes en tiempo real.

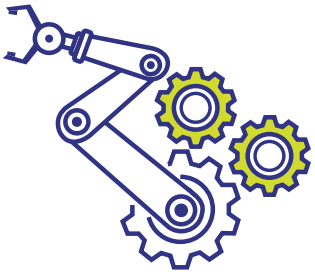
4. Establezca una buena gobernanza de las cuentas de servicio.

Es importante que las organizaciones garanticen la gobernanza sobre las cuentas de servicio y las contraseñas estableciendo controles de seguridad específicos basados en las políticas y estándares existentes. Esto incluye asignar propiedades, roles y responsabilidades para usuarios privilegiados, y delegar la propiedad con un sistema de uso compartido basado en roles para usuarios, propietarios, administradores y superadministradores (aprobadores). Además de la capacitación y educación de los usuarios, las organizaciones necesitan establecer un flujo de trabajo bien definido para los procesos de creación, revisión y asignación de cuentas de servicio para obtener una visibilidad completa de estas cuentas.

El flujo de trabajo de la cuenta de servicio debe abordar estas preguntas:

- ¿Quién debería crear cuentas de servicio y quién debería aprobar el acceso a ellas?
- ¿Quién será el propietario predeterminado de las cuentas de servicio?
- ¿Con qué frecuencia se revisarán estas cuentas? ¿El proceso de revisión estará alineado con la política interna y/o los requisitos de cumplimiento?
- ¿Cuál será la política de contraseñas para las cuentas de servicio?
- Si una cuenta de servicio tiene que ser renovada, ¿tiene que pasar por un proceso de aprobación que es similar a la creación de la cuenta?
- ¿Existe alguna disposición para revocar automáticamente las cuentas de servicio caducadas/inactivas?

5. Adopte la automatización.



Establecer un flujo de trabajo tangible puede agilizar la gestión de las cuentas de servicio, pero es casi imposible gestionar todo el ciclo de vida de cada cuenta en un entorno a gran escala. Aquí es donde entra en juego la automatización.

Una vez que se establece un flujo de trabajo bien definido, las organizaciones pueden aprovechar las herramientas de automatización que pueden centralizar la gestión de las cuentas de servicio. Estas herramientas ayudan a los administradores de TI a obtener un control granular sobre las cuentas de servicio y ayudan a gestionar todo el ciclo de vida de la cuenta, desde la detección automática, hasta la creación de plantillas de flujo de trabajo que cumplan con las políticas internas y la provisión de informes de cumplimiento para cumplir los objetivos de seguridad.

Automatizar la gestión de cuentas de servicio permite a los administradores privilegiados crear y revisar los usuarios, grupos y roles designados, así como el acceso seguro a las cuentas de servicio. Algunas herramientas de automatización permiten a los administradores aprovisionar y desaprovisionar cuentas de servicio automáticamente, y proporcionan a los administradores opciones para personalizar sus flujos de trabajo en función de los requisitos empresariales específicos y el tipo de solicitud de cuenta de servicio.

To proactively prevent misuse, automation tools provide real-time status reports for service accounts, and help admins decommission expired or inactive accounts without disruptions in operations. In addition, these tools notify admins whenever service accounts are created, approved, renewed, and deleted.

ManageEngine PAM360

ManageEngine PAM360 is a unified privileged access management solution for enterprises. It enables IT administrators and privileged users to gain granular and complete control over critical IT resources, such as passwords, digital signatures and certificates, license keys, documents, images, service accounts, and more.

Recognized by Gartner and Forrester as one of the top PAM vendors of 2020, ManageEngine PAM360 includes contextual integrations with SIEM, ticketing and analytics solutions to help IT teams build user behaviour models to identify and terminate anomalous activities, generate comprehensive audit and compliance reports, and take data-driven security decisions.

www.manageengine.com/pam360

4141 Hacienda Drive Pleasanton,
CA 94588, USA
US +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898
www.manageengine.com/pam360

ManageEngine
PAM360