BeyondTrust

WHITE PAPER

Gestión de Contraseñas Privilegiadas - Explicación

Este White Paper aborda los fundamentos de la administración de contraseñas privilegiadas, incluyendo algunas definiciones, retos, amenazas, buenas prácticas, beneficios y soluciones importantes.

ÍNDICE

Capítulo 1: ¿Qué es y por qué lo necesita?

La gestión de contraseñas privilegiadas, algunas veces denominada de gestión de contraseñas corporativas, se refiere a las prácticas y a las técnicas de controlar con seguridad las credenciales para cuentas privilegiadas, servicios, sistemas, aplicaciones y mucho más. La meta definitiva de la gestión de contraseñas es reducir los riesgos por medio de la identificación, almacenamiento seguro y gestión central de todas las credenciales que permite acceso elevado. La gestión de contraseñas privilegiadas trabaja juntamente con la implementación de privilegios mínimos, y debe ser un elemento básico de todas las iniciativas de gestión de Accesos Privilegiados (PAM) de una organización.

Aunque en décadas pasadas una empresa entera podía gestionarse de forma suficiente con tan solo algunas credenciales, la complejidad actual de los ambientes requiere que sean necesarias credenciales privilegiadas para diversos tipos de cuentas privilegiadas diferentes (de administrador de dominio y de administrador de sistemas hasta estaciones de trabajo con derechos de administrador), sistemas operativos (Windows, Unix, Linux, etc.), servicios de directorio, bases de datos, aplicaciones, instancias en la nube, hardware de redes, internet de las cosas (IoT), redes sociales y más.

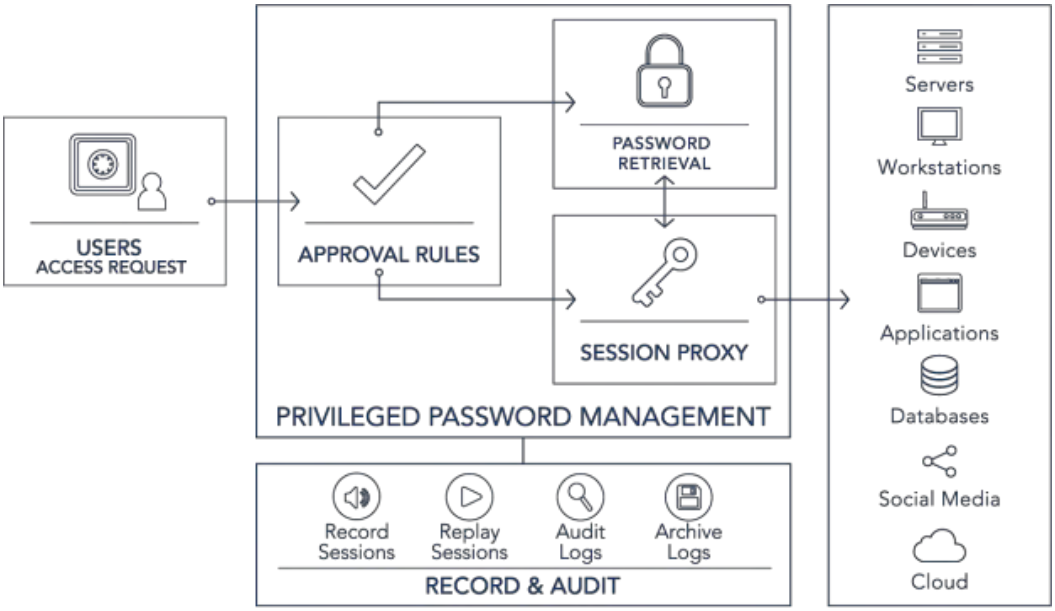

Figura 1: Representación del flujo de trabajo en la gestión de contraseñas privilegiadas.

La mayoría de las organizaciones depende de alguna variación de una“solución” para la gestión de contraseñas privilegiadas. Podría ser simplemente (pero esperamos que no lo sea) una planilla de Excel para el simple rastreo de las contraseñas o podría ser una solución avanzada para la gestión de contraseñas corporativas que automatice cuentas con privilegio y descubrimiento de credenciales, integración, control de acceso, protección y almacenamiento centralizados, rotación, alertas, generación de informes y supervisión de todas las credenciales corporativas que proporcionan derechos elevados de acceso privilegiado.

Aunque esté fuera del alcance de este Tech Paper, merece la pena mencionar que las organizaciones también pueden beneficiarse con herramientas de contraseñas personales que administran las informaciones de login de los empleados para usuarios estándar. Esos gestores de contraseñas personales generan contraseñas aleatorias protegidas por una única contraseña maestra que el usuario tiene que recordar y pueden realizar el login automático del usuario en los recursos que él utiliza.

En este artículo abordaremos los fundamentos de la gestión de contraseñas privilegiadas, incluyendo algunas definiciones, desafíos, amenazas, buenas prácticas, beneficios y soluciones importantes.

¿Qué Es Una Contraseña Privilegiada?

Una definición básica de contraseña *es que se trata de una palabra o frase destinada a diferenciar a un usuario o proceso autorizado (con la finalidad de permitir el acceso) de un usuario no autorizado*. Las contraseñas privilegiadas son un subconjunto de credenciales que proporcionan acceso elevado y permisiones en cuentas, aplicaciones y sistemas. Contraseñas de cuentas privilegiadas — tales como la cuenta Raíz en Linux y Unix, y de Administrador en Windows—suelen denominarse como "las llaves para el Reino de TI," puesto que ellas pueden proporcionar al usuario autenticado derechos de acceso privilegiado prácticamente ilimitados a los sistemas y datos más críticos de una organización. Esos privilegios con tanto poder inherente están "preparados" para ser mal utilizados por empleados de la organización y son altamente codiciados por los hackers.

De hecho, el estudio Investigación de Violaciones de Datos – 2016 de Verizon mencionó que contraseñas débiles, estándar o robadas constituyen el 63% de las violaciones de datos confirmadas, mientras que Forrester estima que el 80% de las violaciones de seguridad envuelven credenciales privilegiadas.

¿Qué Es Lo Que Hace Que Una Contraseña Sea Robusta?

Antes de que nos profundicemos en la gestión de privilegios específicos, presentamos aquí algunas buenas prácticas de gestión de contraseñas que son comunes a todos los tipos:

- Tamaño de la contraseña de al menos 12 caracteres
- Las contraseñas deben ser exclusivas, complejas, sin sentido, compuestas de una mezcla de letras no repetidas (mezclando mayúsculas y minúsculas), números y símbolos que no contengan palabras que consten en el diccionario de cualquier idioma o que tengan cualquier otro contexto previsible (ID del empleado, fechas etc.), o una secuencia de teclas del teclado, tales como'qwerty'o'zxcvb'
- Cambiar frecuentemente las contraseñas—un proceso denominado de rotación de contraseñas. La frecuencia de la rotación debe variar en función de la antigüedad de la contraseña, su uso e importancia para la seguridad. Por ejemplo, una contraseña de una

cuenta de usuario estándar puede exigir solamente rotación en intervalos de 60 días, un proceso que puede forzarse por medio de la expiración de la contraseña. Por otro lado, es necesario considerar la rotación de la cuenta de súper-usuario (p. ej.: raíz, administrador de dominio etc.) y de otras contraseñas altamente privilegiadas, con intervalos más frecuentes, incluyéndose hacerlo después de cada uso—conocidas como contraseñas de uso único (o por la sigla OTPs)—para sus cuentas más sensibles.

- Prohibición de la reutilización de contraseñas. Debe prohibirse que los empleados utilicen las mismas contraseñas en sus cuentas personales y de trabajo.
- Si en algún momento Ud. necesitara compartir una contraseña, cámbiela inmediatamente después de que la otra persona la haya utilizado.

Desafíos Y Trampas De Las Contraseñas Administradas Por Humanos

Aunque las buenas prácticas sobre contraseñas anteriormente citadas parecen ser suficientemente simples, ¿qué dificulta que esos principios se pongan en práctica?

Actualmente, la cantidad de contraseñas que un empleado debe recordar para tener acceso a diversas cuentas, sistemas y aplicaciones puede variar de casi una docena a más de un centenar. Cuando se trata de las credenciales privilegiadas de una organización, la cantidad de contraseñas que hay que administrar puede llegar fácilmente a decenas de millares, o incluso sobrepasar el millón.

La carga de tener que recordar manualmente tantas contraseñas diferentes (cambiándolas constantemente) lleva invariablemente a que los empleados sigan caminos que aumentan el riesgo y causan tiempo ocioso. Los empleados tienden a olvidarse de las contraseñas de vez en cuando, lo que los deja potencialmente fuera de los sistemas. Para compensar, ellos pueden utilizar las mismas contraseñas en diversas cuentas, elegir contraseñas fáciles de adivinar o recurrir a escribir las contraseñas en un papel o dentro de documentos electrónicos. En consecuencia, parte del peligro que eso representa es que los hackers pueden relacionar la contraseña, juntamente con direcciones de email y nombres de usuario, a partir de una cuenta comprometida para otros servicios que puedan utilizar la misma contraseña. Por lo tanto, por ejemplo, la utilización de la misma credencial privilegiada en un servidor, aplicación, switch y cuenta de redes sociales significa que una cuenta comprometida también puede perjudicar otras cuentas.

Aunque la automatización de la gestión de contraseñas esté avanzando, la mayoría de las organizaciones todavía dependen, hasta cierto punto, de prácticas manuales/humanas de gestión de las contraseñas. En consecuencia, la rotación de las contraseñas se realiza de forma inadecuada y sin auditoría en la práctica, dejando a las organizaciones susceptibles a violaciones de credenciales privilegiadas.

Capítulo 2: Desafíos para la gestión de contraseñas privilegiadas

Ahora, examinaremos algunos de los desafíos más específicos de las credenciales privilegiadas de una corporación.

La falta de visibilidad y de toma de conciencia de todas las cuentas y credenciales privilegiadas de una compañía representan un grand reto —especialmente para las compañías que dependen de procesos y herramientas manuales. Hay cuentas privilegiadas, olvidadas desde hace mucho tiempo, diseminadas por la mayoría de las organizaciones. Diferentes equipos pueden realizar una gestión separada—si es que la hacen—de su propio conjunto de credenciales, dificultando el rastreo de todas las contraseñas, por no hablar de quién tiene acceso a ellas o las utiliza. Un administrador puede tener acceso a más de 100 sistemas, posiblemente descartándolos para utilizar atajos al hacer el mantenimiento de las credenciales. Además, conforme se detalla en las secciones a continuación, algunos tipos de credenciales son prácticamente imposibles de localizar, qué diremos de administrar, sin el uso de herramientas de terceros.

Falta de supervisión y auditoría de credenciales privilegiadas: Aunque TI consiga identificar de forma satisfactoria todas las credenciales privilegiadas diseminadas dentro de la organización, eso no se traduce, de forma estándar, en que se sepa cuáles son las actividades específicas que se realizan durante una sesión privilegiada (es decir, el período durante el cual una cuenta, servicio o proceso tienen privilegios elevados). El acceso privilegiado a una cuenta de súper-usuarios no debe significar dar *carta blanca* a ese usuario. Además, las normas de PCI, HIPAA y de otras entidades exigen que las organizaciones no solo protejan y guarden los datos, sino que sean capaces también de comprobar la eficacia de tales medidas. Por lo tanto, por razones de conformidad y seguridad, TI tiene que tener visibilidad de las actividades realizadas durante la sesión privilegiada.

Idealmente, TI también debe tener la capacidad de asumir el control de una sesión, caso haya un uso inadecuado de las credenciales. Pero, con un potencial de centenares de sesiones privilegiadas operando paralelamente en una organización, ¿cómo TI puede detectar e interrumpir una actividad maliciosa? Mientras que algunas aplicaciones y servicios (como el Directorio Activo) pueden realizar las acciones de los usuarios y aunque los servidores de Windows utilicen eventos de login dentro de datos de Event Log puedan revelar algunas anomalías comportamentales, hay que esperar tener cobertura completa sobre el uso de cuentas privilegiadas para solicitar una solución de terceros.

Compartición de cuentas privilegiadas por conveniencia: Por lo general, los equipos de TI comparten contraseñas de raíz, Administrador del Window y muchas otras contraseñas privilegiadas para que las cargas de trabajo y las responsabilidades puedan compartirse de forma transparente sea cuando necesario. Sin embargo, con diversas personas compartiendo una contraseña de una cuenta, puede resultar imposible rastrear las acciones realizadas en una cuenta por un individuo específico, afectando las cuestiones de auditoría y responsabilidad.

Credenciales reforzadas por códigos/ insertadas: Son necesarias credenciales privilegiadas para facilitar la autenticación de aplicación para aplicación (A2A) y la comunicación y el acceso de aplicaciones para la base de datos (A2D). Aplicaciones, sistemas y dispositivos de

IoT son normalmente embarcados e implementados, por lo general, con credenciales estándar insertadas que son fácilmente adivinables y que representan un riesgo considerable hasta que se pongan bajo gestión. Esas credenciales privilegiadas suelen almacenarse frecuentemente en texto común, por lo general dentro de un script, código o archivo. Desafortunadamente, no hay una forma manual para que la detecte o gestione de forma centralizada las contraseñas almacenadas dentro de aplicaciones o scripts. La protección de contraseñas insertadas requiere la separación de la contraseña del códigofuente para que cuando no estén siendo usadas permanezcan almacenadas con seguridad en una caja fuerte centralizada de contraseñas y no constantemente expuestas como cuando están en texto común.

Claves SSH: Por lo general, los equipos de TI confían en claves SSH para automatizar el acceso seguro a servidores, evitando la necesidad de digitar manualmente las credenciales de login. La diseminación de claves SSH presenta un riesgo considerable para millares de organizaciones que pueden tener más de un millón de claves SSH—muchas de ellas inactivas y olvidadas desde hace mucho tiempo, aunque todavía viables como puerta de entrada para permitir la infiltración de hackers en servidores críticos. Las claves SSH son estándar y predominan más en ambientes Unix y Linux, pero también se utilizan en Windows. Los administradores utilizan claves SSH para la gestión de sistemas operativos, redes, transferencia de archivos, canalización de datos y mucho más. De la misma forma que con otras credenciales privilegiadas, las claves SSH no están necesariamente vinculadas a un único usuario—diversas personas pueden compartir una clave privada y pasar la frase de contraseña a un servidor que tiene la clave pública. De la misma forma que con otras credenciales privilegiadas, cuando las organizaciones dependen de procesos manuales, hay una tendencia pronunciada a reutilizar una frase de contraseña en muchas claves SSH o de reutilizar la misma clave SSJ pública. Eso significa que una clave comprometida puede entonces ser aprovechada para infiltrarse en múltiples servidores.

Credenciales privilegiadas y la nube: Los desafíos de la visibilidad y de la capacidad de auditoría suelen verse exacerbados en ambientes de nube y virtualizados. Las consolas de administrador de la nube y de virtualización (como sucede con AWS, Office 365 etc.) proporcionan amplios recursos de súper-usuario, habilitando a los usuarios para disponer, configurar y excluir servidores en gran escala. Dentro de esas consolas, los usuarios pueden accionar y administrar millares de máquinas virtuales (cada una con su propio conjunto de privilegios y cuentas privilegiadas) tan solo haciendo algunos clicks. Surge así la dificultad sobre cómo integrar y administrar todas esas cuentas y credenciales privilegiadas recién creadas. Por si fuera poco, con frecuencia las plataformas en la nube no tienen capacidad nativa para auditar la actividad del usuario. E, incluso para organizaciones que implementaron algún grado de automatización en su gestión de contraseñas (sea con soluciones internas o de terceros) si no se han proyectado teniendo en mente la nube, no hay garantía de que una solución de gestión de contraseñas sea capaz de administrar adecuadamente las credenciales en la nube.

Cuentas de proveedor subcontratado/ Soluciones para acceso remoto: Finalmente, otra situación difícil para las organizaciones es cómo hacer llegar las buenas prácticas de gestión de accesos privilegiados y de credenciales privilegiadas a usuarios subcontratados tales como consultores y otros proveedores que pueden realizar una variedad de actividades. ¿Cómo puede Ud. asegurar que una autorización suministrada vía acceso remoto o para un subcontratado se

utilice correctamente? ¿Cómo puede Ud. asegurar que una empresa subcontratada no comparta las credenciales o realice una mala gestión de las contraseñas como, por ejemplo, no cancelando las credenciales de autorización cuando un empleado sale de la empresa?

Capítulo 3: Algunas técnicas comunes de ataque a contraseñas

Los ataques a las contraseñas vienen de todos los lados. Algunos programas, tales como John the Ripper y LOphtCrack, son capaces de descifrar incluso contraseñas complejas, mientras que el conjunto de herramientas Pass-the-Hash puede llegar a ser fatídico sin ni siquiera descifrar la contraseña.

Veamos aquí algunas de las tácticas comunes de violación de credenciales:

- **Ataques de fuerza bruta** envuelven probar repetidamente una contraseña generando potencialmente millones de estimativas por segundo, con la combinación de caracteres (números, letras y símbolos) hasta encontrar una que coincida. Cuanto más compleja sea una contraseña matemáticamente, más difícil será descifrarla.
- **Ataques por diccionario**: Al contrario del método de fuerza bruta que computa combinaciones aleatorias de caracteres, el ataque del tipo diccionario trata de adivinar las contraseñas con base en palabras de un diccionario en cualquier idioma.
- **Los ataques del tipo Pass-the-Hash (PtH)** pueden suceder en Linux, Unix y otras plataformas, pero predominan en los sistemas Windows. En Windows, PtH viola el Single Sign On (SSO) por medio de los protocolos NTLM, Kerberos y de otros protocolos de autenticación. Cuando se crea una contraseña en Windows, se le aplica un hash y se almacena en el Administrador de Cuentas de Seguridad (SAM), en la memoria de proceso LSASS (Subsistema de Autoridad de Seguridad Local), en el The Credential Manager (CredMan), una base de datos ntds.dit en el Directorio Activo o en cualquier otra parte. Por eso, cuando un usuario hace el login en una estación de trabajo o en un servidor de Window, deja para atrás básicamente sus credenciales de contraseña. En los ataques de PtH, un atacante no necesita decodificar la contraseña con hash para obtener una contraseña en texto común, puesto que una vez captada, la contraseña con hash puede pasarse adelante para realizar el acceso a sistemas laterales. Un hacker podría elevar privilegios simplemente robando las credenciales RDP de un usuario privilegiado durante una sesión RDP.
- **Ataques del tipo Pass-the-Ticket (PtT) y Golden Ticket** son similares al PtH, pero envuelven copiar tickets Kerberos y pasarlos para acceso lateral en los sistemas. Un ataque Golden Ticket es una variación del Pass-the-Ticket, envolviendo el robo de la cuenta krbtgt en un controlador de dominio que codifica los tickets que garantizan tickets (TGT). Con este valioso punto de apoyo, un hacker podría crear libremente su propio ticket de acceso para cualquier nivel y duración de acceso. La rotación de contraseñas de cuentas privilegiadas después de cada uso y la aplicación de privilegios mínimos (tal como separar los diferentes tipos de cuentas privilegiadas y no privilegiadas, y lo que es aún mejor, retirar los derechos de administrador de los puntos finales) son importantes controles de seguridad para evitar ataques del tipo PtH, PtT y Golden Ticket.

- **Ataques a contraseñas con Ingeniería Social**, tales como phishing y spear phishing, implican engañar a las personas para que revelen informaciones que pueden utilizarse para conseguir acceso. Entre las víctimas recientes y con alta visibilidad de un ataque de spear phishing está el Comité Nacional Democrático (DNC), John Podesta, y otros por el grupo de hackers Fancy Bear. En el caso de Podesta, él aparentemente recibió un e-mail del Gmail falsificado, alertando que un impostor había intentado utilizar su contraseña, pero que Google había detectado la actividad ilícita y la había interrumpido. A lo que parece, Podesta después hizo click en un link ilegal para alterar su contraseña y de esa forma sus credenciales fueron robadas y después utilizadas para robar y colocar e-mails comprometedores en WikiLeaks.

Capítulo 4: Buenas prácticas y beneficios

En última instancia, el resultado de gestión de contraseñas privilegiadas es administrar eficazmente el ciclo de vida de las credenciales privilegiadas, para facilitar la autenticación segura para los usuarios, aplicaciones y recursos y para realizar procesos especiales. La mayoría de las organizaciones está en algún punto entre los procesos manuales y los automatizados en su abordaje de la gestión de contraseñas corporativas. Con amenazas constituidas por personas dentro de las empresas que perfeccionaron sus conocimientos de los sistemas y recursos internos y por atacantes armados con conjuntos de herramientas automatizadas para la invasión, las organizaciones que dependen de procesos manuales para administrar las contraseñas están en una situación considerablemente desventajosa.

En esta sección, Ud. conocerá ocho áreas centrales de enfoque para mejorar su gestión de cuentas y credenciales privilegiadas. Probablemente, conseguir una gestión holística de contraseñas corporativas deberá seguir el curso de un abordaje gradual. A medida que avance en la lectura, Ud. descubrirá insights sobre cómo comenzar y continuar.

Por otro lado, aunque sea posible resolver cada una de las ocho áreas aplicando una combinación de soluciones manuales y automatizadas, si estuviera realmente interesado en un abordaje totalmente automatizado, no se preocupe: Ud. no necesitará ocho soluciones diferentes. En realidad, algunas soluciones de gestión de contraseñas privilegiadas proporcionarán recursos automatizados y un flujo de trabajo agilizado durante todo el ciclo de vida de la gestión de contraseñas.

Para una gestión holística de cuentas y credenciales privilegiadas, concéntrese en estas ocho áreas:

1. **Descubra todas las cuentas compartidas** de administrador, usuarios, aplicaciones y cuentas de servicio, claves SSH, cuentas de base de datos, cuentas en la nube y en las redes sociales y otras credenciales privilegiadas, incluyendo las utilizadas por terceros/proveedores, en sus instalaciones y en la infraestructura en la nube. El descubrimiento debe incluir todas las plataformas (Windows, Unix, Linux, Cloud, en las instalaciones de la empresa etc.), directorios, dispositivos de hardware, aplicaciones, servicios / daemons, firewalls, routers etc. Este proceso también debe incluir la recolección de detalles de la cuenta de usuario que ayudarán a evaluar el riesgo, tal como nivel de privilegio, antigüedad de la contraseña, fecha

del login y fecha de expiración de la contraseña y asociación y servicios con dependencias de la cuenta. El descubrimiento debe subrayar dónde y cómo las contraseñas privilegiadas se utilizan y ayudar a mostrar puntos ciegos en la seguridad y también prácticas indebidas, tales como:

- Cuentas huérfanas olvidadas hace mucho tiempo que podrían proporcionar una puerta de entrada para un ataque a su infraestructura crítica,
- Contraseñas sin fecha de expiración
- Uso inadecuado de contraseñas privilegiadas, tal como utilizar la misma cuenta de Administrador en múltiples cuentas de servicios
- Claves SSH reutilizadas en diversos servidores

Los hallazgos del proceso de descubrimiento permitirán que Ud. reconsidere sus políticas y perfeccione los permisos de acceso a las cuentas. Como nuevos sistemas y aplicaciones corporativas pueden surgir en cualquier momento, Ud. tendrá que realizar descubrimientos periódicos para asegurar que cada credencial privilegiada esté protegida, centralizada y bajo gestión.

➢ **Soluciones de descubrimiento con abordaje manual x automatizado**: Cuando no haya automatización, un descubrimiento amplio probablemente será una tarea desordenada y demorada que dependerá de planillas para registro y exigirá múltiples lenguajes de script, APIs etc. Aún así, este abordaje resultará frecuentemente en credenciales perdidas y brechas de seguridad (vea más detalles en gestión de contraseñas y aplicaciones a continuación). Con soluciones de terceros, Ud. puede automatizar el escaneado de direcciones IP, puertos, sistemas, aplicaciones, la nube e incluso cuentas de redes sociales. Un proceso que puede tardar una eternidad (contando en años humanos) utilizando un abordaje manual, puede condensarse en pocos minutos con una solución automatizada.

2. **Coloque las cuentas y credenciales privilegiadas bajo una gestión centralizada**: Idealmente, el proceso de integración ocurre en el momento de creación de la contraseña o, de otra forma, inmediatamente después durante un scan de descubrimiento de rutina. Silos de individuos o de equipos que administran independientemente sus propias contraseñas son una receta para la diseminación de contraseñas y errores humanos. Todas las credenciales privilegiadas deben protegerse, controlarse y almacenarse centralmente. Idealmente, su almacenamiento de contraseñas debe estar en conformidad con algoritmos de criptografía estándares del sector, tales como AES 256 y Triple DES.

➢ Solución de abordaje manual x automatizado: Ud. puede centralizar el almacenamiento de credenciales privilegiadas en una base de datos codificada y también registrar los valores en una planilla Excel. Una solución automatizada de caja fuerte digital de contraseñas corporativas proporcionará una base de datos codificada a partir de la cual Ud. puede administrar el ciclo de vida de las contraseñas. Una solución automatizada de caja fuerte digital de contraseñas corporativas puede implementar automáticamente

su política de gestión de contraseñas privilegiadas, tal como complejidad de la contraseña, exclusividad (diferentes contraseñas por activo, cuenta etc.) expiración, rotación, verificación de entrada y salida, eliminación de contraseñas estándar y otras reglas. Una solución de caja fuerte digital de contraseñas corporativas simplifica extraordinariamente el descubrimiento e integración de credenciales para nuevas cuentas privilegiadas a medida que se crean.

3. **Implementar rotación** de contraseñas en cada cuenta, sistema, componentes y dispositivos de IoT en red, aplicación, servicio etc. Conforme mencionado anteriormente, las contraseñas deben ser exclusivas, nunca reutilizadas o repetidas y randomizadas de manera programada, en la verificación inicial o en respuesta a una amenaza o vulnerabilidad específica.

   - **Rotación de contraseñas manual x automatizada**: Ud. puede hacer la rotación de los valores de las credenciales privilegiadas en una planilla Excel y después realizar el login manualmente en las cuentas y sistemas asociados. Aunque no es altamente escalable, esto puede proporcionar una cierta cobertura para la gestión de contraseñas en ambientes simples; no obstante, la gestión y la rotación de algunos tipos de credenciales (por ejemplo, contraseñas y claves reforzadas por código) probablemente serán imposibles. Un abordaje automatizado de terceros, con base en una caja fuerte digital para contraseñas corporativas le permitirá tener la tranquilidad de que todas sus credenciales privilegiadas (de millares a millones) pasarán por una rotación realizada regularmente en intervalos determinados por la política de su empresa. Además, con una caja fuerte digital de contraseñas corporativas, Ud. puede sincronizar de forma transparente las alteraciones de contraseñas en el directorio en donde la cuenta reside con alteraciones en el sistema/dispositivo/ aplicación/ servicio en donde la contraseña se utiliza, para evitar tiempo ocioso.

4. C**oloque las contraseñas de aplicaciones bajo gestión**: En resumen, esto requiere la implementación de una solución subcontratada de gestión de contraseñas de aplicaciones que fuerce las aplicaciones y los scripts a pedir (o solicitar) el uso de la contraseña a partir de una caja fuerte digital de contraseñas centralizada. Al implementar llamadas API Ud. puede obtener control sobre scripts, archivos, código y claves insertadas, eliminando credenciales insertadas y codificadas. Una vez conseguido esto, Ud. puede automatizar la rotación de las contraseñas con la frecuencia determinada por la política. Y, al colocar las contraseñas de las aplicaciones bajo gestión y codificarlas en una caja fuerte digital de contraseñas a prueba de violaciones, las credenciales y las aplicaciones básicas estarán mucho más seguras que cuando permanecen estáticas y mezcladas dentro del código.

5. **Coloque las claves de SSH bajo gestión**: la NIST IR 7966 ofrece orientación para empresas, organizaciones gubernamentales y auditores sobre gobernanza de seguridad adecuada para implementaciones SSH que incluye recomendaciones sobre el descubrimiento, rotación, uso y monitoreo de clave SSH. El abordaje a las claves SSH debe ser igual al de cualquier otra contraseña, aunque acompañado de un par de claves que también se debe

administrar. Realice la rotación regular de las claves privadas y frases de contraseña y asegúrese de que cada sistema tenga un par de claves exclusivo.

- **Gestión manual x automatizada de claves SSH**: Para identificar cuentas configuradas para el uso de claves SSH, Ud. puede recuperar manualmente el archivo de claves autorizadas de la carpeta de usuario .SSH oculta, pero eso no ayudaría a identificar quién tiene la clave privada que coincide con cualquiera de las claves públicas en el archivo. Aunque la gestión manual de la clave SSH es mejor que la ausencia total de gestión, incluso en ambientes poco complejos, la rotación manual de las claves SSH es una estrategia no sostenible. Si este fuera el caso, busque una solución de terceros para generar pares de claves exclusivos para cada sistema y haga una rotación frecuente. Soluciones de terceros para la gestión automatizada de claves SSH simplificarán significativamente el proceso de creación y rotación de las claves SSH, eliminando su diseminación y asegurando que las claves SSH permitan la productividad sin perjudicar la seguridad.

6. **Implemente la gestión de sesión privilegiada** para mejorar la supervisión y la responsabilidad en relación a cuentas y credenciales privilegiadas. La gestión de sesión privilegiada se refiere al monitoreo, registro y control de sesiones privilegiadas. TI debe ser capaz de auditar actividades privilegiadas tanto para la seguridad como para cumplir lo determinado por las normas SOX, HIPAA, GLBA, PCI DSS, FDCC, FISMA y otras más. Las actividades de auditoría también pueden incluir la captura de toques en teclados y pantallas (permitiendo visualización en vivo y reproducción).
7.

- Solución de gestión manual x de terceros de sesiones privilegiadas: Aunque Ud. pueda, ciertamente, implementar algunos procesos manualmente, tales como registro de pantalla, las soluciones automatizadas le permiten hacerlo de forma transparente y con una escala de centenas o millares de sesiones simultáneas. Además, algunas soluciones de terceros pueden ofrecer flujos de trabajo automatizados que proporcionan a TI el control granular de las sesiones privilegiadas, tales como permitirles detectar una sesión irregular y parar, bloquear o terminar la sesión hasta que se realice una confirmación de que la actividad es adecuada.

8. **Análisis de amenazas**: Para mitigar el riesgo y desarrollar su política conforme sea necesario, Ud. debe analizar continuamente las contraseñas privilegiadas, los usuarios y el comportamiento de las cuentas y ser capaz de identificar anomalías y amenazas potenciales. Cuanto más integrada y centralizada sea su gestión de contraseñas, más facilidad tendrá Ud. para generar informes relacionados a cuentas, claves y sistemas expuestos al riesgo. Un mayor grado de automatización puede acelerar su toma de conciencia y una respuesta orquestada a las amenazas, así como proporcionarle la capacidad de bloquear inmediatamente una cuenta o una sesión, o cambiar una contraseña, como en el caso en que contraseñas incorrectas (como sucede durante un ataque del tipo fuerza bruta o diccionario) se utilizan repetidamente para conseguir acceso a un activo sensible.

9. **Automatice la gestión del flujo de trabajo**: Aunque Ud. pueda determinar su propio conjunto de reglas internas para disparar alertas y aplicar algunas políticas sobre la gestión de contraseñas, las soluciones de terceros proporcionan recursos robustos que pueden agilizar y optimizar el ciclo de vida completo de la gestión de contraseñas. Soluciones de terceros para gestión de contraseñas privilegiadas también pueden ayudar en la automatización:

   - Agrupación y gestión de activos de acuerdo con reglas inteligentes.
   - Flujos de trabajo para acceso a dispositivos, incluyendo un proceso de aprobación para cuando se necesite acceso administrativo. En lo que se refiere al acceso privilegiado mínimo, Ud. puede desear implementar contexto a solicitudes de flujo de trabajo considerando, y potencialmente limitando el acceso dependiendo de la cuenta, día, fecha, hora, intervalo de tiempo y localización (direcciones IP) cuando un usuario realiza el acceso a los recursos.
   - Flujos de trabajo para atender solicitudes del tipo "alarma de incendio/ruptura de vidrio" para asegurar el acceso a los sistemas administrados por contraseña después del horario comercial, en fines de semana o en otras situaciones de emergencia.
   - Verificación de entrada y salida de las contraseñas de la caja fuerte digital y autenticación automatizada / Single Sign On (SSO) para el usuario sin ninguna exigencia de login manual. Esto significa que las credenciales privilegiadas, incluyendo las de consolas administrativas en la nube, nunca se revelan al usuario.
   - Login de usuarios para sesiones RDP y SSH sin revelar las contraseñas.
   - Dispara la solicitud de aprobación de un supervisor para verificar credenciales altamente sensibles.
   - Inicio del monitoreo de sesión privilegiada y alerta sobre cualquier actividad crítica o sospechosa.

Capítulo 5: Cómo implementar la gestión de contraseñas privilegiadas y por dónde comenzar

De la misma forma que con cualquier proyecto de seguridad y gobernanza de TI, comience determinando el alcance. Una vez que haya descubierto totalmente todas sus credenciales privilegiadas y tenga una base de referencia de ellas y del riesgo patrimonial, Ud. puede establecer prioridades y detallar una política de contraseñas privilegiadas. Implementa gradualmente la automatización en el ciclo de vida de su gestión de contraseñas privilegiadas para aumentar sus esfuerzos en la aplicación de buenas prácticas con relación a las contraseñas.

Como Ud. ya sabe, tratar de la gestión de contraseñas privilegiadas no es algo aislado, Ud. debe tener un buen dominio del principio de privilegios mínimos, y tendrá que implementarlo dentro de una estructura de gestión de accesos privilegiados de amplio alcance. Para continuar aprendiendo, examine algunos de los recursos educativos proporcionados que se mencionan a continuación.

Recursos

- The Forrester Wave™: Privileged Identity Management, Q4 2018
- Gartner Magic Quadrant for Privileged Access Management, Q4 2018
- Modernizando La Seguridad De Sus Contraseñas Privilegiadas (Blog)