WALLIX
CYBERSECURITY SIMPLIFIED

Guía de Seguridad de Accesos para principiantes

Guía de Seguridad de Accesos
para principiantes

ÍNDICE DE CONTENIDOS

RESUMEN EJECUTIVO

En esta guía se abordan los conceptos básicos sobre Seguridad de Accesos.

La seguridad de los accesos es un marco de políticas y tecnologías que se combinan para gestionar el acceso que tienen los usuarios a los activos de IT más sensibles de una organización. Una seguridad de accesos robusta ofrece grandes beneficios, entre ellos, una ciberseguridad más fuerte, un mejor cumplimiento de las regulaciones, y un mayor control sobre los dispositivos externos que acceden a la red y los datos de la organización.

Las empresas actuales necesitan protegerse de las amenazas que existen tanto dentro como fuera de sus paredes. La seguridad de accesos ofrece a los negocios las herramientas que necesitan para saber exactamente quién está accediendo a sus recursos y así controlar los niveles de privilegios de esos usuarios. Tres son los procesos clave para ello: identificación, autenticación y autorización.

El Modelo Zero Trust y el Principio del Menor Privilegio son dos conceptos vitales para una robusta seguridad de accesos. Hay varios sistemas específicos que las empresas pueden emplear para aplicar estos conceptos en su infraestructura de TI: Gestión de Identidad, Gestión de Accesos Privilegiados y Gestión de Privilegios en los 'Endpoint'.

Seguridad de Accesos

Introducción a la Seguridad de Accesos

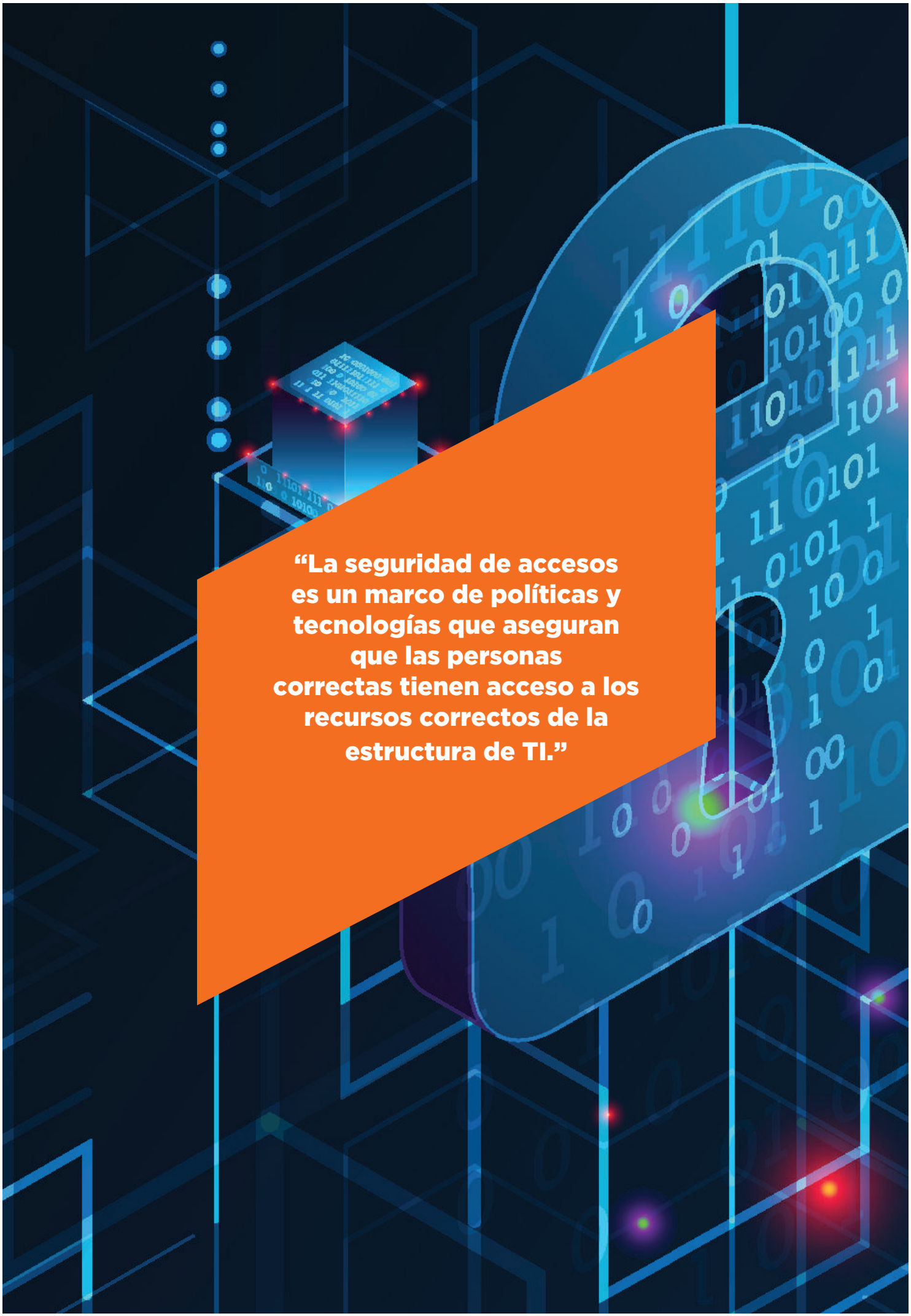
¿En qué consiste la Seguridad de Accesos?

Las empresas tienen procedimientos de seguridad físicos para asegurar que las personas externas no pueden entrar en sus edificios cuando ellos quieran. Los controles y estructuras de acceso permiten asegurar diariamente que solo las personas adecuadas pueden acceder a las áreas donde está la información más sensible. Estos controles físicos pueden ser pases de acceso, puntos de control de acceso o checkpoints, códigos clave, o tecnologías de reconocimiento facial. Hoy en día la información sensible y los datos de los clientes se encuentran alojados en infraestructuras de TI. Por lo tanto, que las empresas se preocupen por aplicar el mismo nivel de escrutinio en sus redes tecnológicas e informáticas parece tener sentido ¿verdad?

Todos tenemos una identidad física, y ahora también tenemos identidades digitales. Puede ser fácil detectar a un intruso basándonos en su identidad física, pero las identidades digitales son más difíciles de rastrear. En todo momento, las organizaciones necesitan saber quiénes son los usuarios y qué nivel de acceso deberían tener dentro de una red de TI. Deben asegurarse de que sus empleados y socios comerciales tengan los niveles adecuados de acceso a sus activos de TI y, por el contrario, de que no tengan acceso a los recursos que no necesitan. No tendría sentido permitir que las personas tengan acceso físico sin restricciones dentro del edificio de una organización, y ocurre lo mismo con las redes de TI.

Las empresas deben tener una identidad digital (ID) por cada persona individual que use su sistema. Estas identidades deben mantenerse, modificarse y monitorearse durante el "ciclo de vida" de cada usuario. Por ejemplo, el rol de un empleado puede cambiar, o pueden abandonar la empresa, lo que significa que su nivel de acceso digital debe modificarse o anularse por completo.

La seguridad de accesos es un marco de políticas y tecnologías que aseguran que las personas correctas tienen acceso a los recursos correctos de la estructura de TI. Establece 'derechos' y 'restricciones' a cada una de las personas que necesitan usar la red. Cuando cientos de usuarios están activos en una red, es vital saber quién es quién, qué han hecho, y cuándo. Para dar respuesta a ello existen tres procesos: **identificación, autenticación y autorización.**



“La seguridad de accesos es un marco de políticas y tecnologías que aseguran que las personas correctas tienen acceso a los recursos correctos de la estructura de TI.”

Identificación, autenticación, autorización

Estos procesos funcionan al unísono para verificar quiénes son los usuarios y qué nivel de privilegios de acceso tienen dentro de una red. A primera vista, el significado de estas tres palabras parece similar. Sin embargo, existen algunas diferencias importantes entre estos aspectos clave de la seguridad de accesos.

Identificación

La seguridad de accesos comienza con la identidad. Para controlar lo que los usuarios pueden o no pueden hacer dentro de una red de TI, primero necesitamos saber quién es quién. Cada usuario dentro de una red tiene una identidad digital asociada a un nombre de usuario o dirección de correo electrónico únicos. Estas identidades virtuales tienen una relación específica con la correspondiente única persona en el mundo real.

El acceso y los privilegios dentro de la red de TI se otorgan de acuerdo con estas identidades únicas, lo que garantiza que las personas tengan acceso a las aplicaciones que necesitan para realizar su trabajo. Cuando las organizaciones implementan un proceso o sistema de gestión de identidad, su motivación principal es otorgar los privilegios apropiados a los usuarios a través de sus identidades.

Sin embargo, no podemos basarnos únicamente en la identidad de un usuario para dar por hecho que quien está detrás es el usuario en cuestión. Las ID de usuario únicas no están lo suficientemente 'cercanas' como para verificar a los usuarios en un entorno de TI moderno. Después de todo, alguien podría simplemente escribir el nombre de usuario de otra persona y comenzar a acceder a los archivos de su cuenta. Por eso es importante autenticar.

Autenticación

Es necesario que haya una forma de demostrar o autenticar que un usuario realmente coincide con su identidad digital. Esto viene en forma de información confidencial separada, generalmente algo que sabes, algo posees o algo que es parte de tí.

- **Algo que sabes:** el ejemplo más común sería una contraseña. Si su nombre de usuario es tu identificador, tu contraseña es tu forma de autenticación. Una contraseña es la forma más básica de seguridad de acceso, una que está abierta a riesgos como el uso compartido de contraseñas o el robo.

- **Algo que posees:** puede ser un elemento físico, como una tarjeta de acceso o un token fob / RSA que genera un código de acceso temporal.

- **Algo que eres:** estos son factores de autenticación biométricos. Autentican tu identidad mediante el uso de parte del cuerpo del usuario, como un escáner de iris, reconocimiento facial o escaneo de huellas digitales. La biometría conductual también se puede utilizar, como el reconocimiento de mecanografía, voz o firma.

Emparejar una identidad de usuario con un método de autenticación crea un conjunto de credenciales de usuario: sus claves para el reino de TI.

Requerir formas adicionales de autenticación sobre una contraseña aumenta en gran medida la probabilidad de una identificación precisa. Es más difícil para un pirata informático robar dos (o más) de los factores anteriores, lo que otorga mayor credibilidad a los inicios de sesión en los activos de TI sensibles. El uso de dos o más de estos métodos de autenticación se conoce como autenticación multifactor (MFA).

Autorización

La autorización es el proceso de dar permiso a alguien para tener o hacer algo. En un sistema informático con cientos de usuarios, este es un paso de seguridad vital. Un usuario puede tener las credenciales para iniciar sesión en una red, pero ¿qué se le permite hacer allí? La autorización otorga niveles de privilegio y protege los activos corporativos sensibles al garantizar que solo ciertas personas aprobadas puedan acceder a ellos. Una vez que podamos identificar de manera única a cada usuario y verificar que son quienes dicen ser a través de la autenticación, los administradores de TI pueden otorgar los niveles correctos de acceso privilegiado a los recursos para cada uno de los roles y las necesidades de cada usuario.

Este paso es importante, ya que no todos los usuarios necesitan tener el mismo nivel de acceso. Es posible que un usuario solo necesite usar Internet y una pequeña cantidad de aplicaciones, mientras que otro puede necesitar acceder y modificar servidores y bases de datos importantes. No tendría sentido que esos dos usuarios tengan el mismo nivel de acceso a los sistemas.

Un marco de seguridad de accesos sólido se basa en que la empresa pueda identificar a los usuarios, autenticarlos y autorizarlos para los niveles de acceso adecuados. Las empresas que implementan esto de manera efectiva pueden disfrutar de la gran cantidad de beneficios que brinda una seguridad de acceso robusta.

Los beneficios de una seguridad de accesos robusta

Gestionar niveles de privilegio

Nunca es bueno que un actor malicioso robe las credenciales de usuario. Sin embargo, la cantidad de daño que se puede hacer depende del nivel de acceso otorgado a esa identidad específica, y se puede mitigar. Una seguridad de accesos fuerte permite a las organizaciones administrar niveles de privilegios y controlar la visibilidad que tienen los usuarios.

No todos los usuarios necesitan los mismos privilegios para hacer su trabajo. Tener un marco de seguridad de acceso para administrar los niveles de privilegios ayuda a las empresas a evitar que los usuarios con privilegios excesivos tengan acceso a demasiados recursos confidenciales dentro de sus redes de TI. Esto reduce el riesgo de que las credenciales privilegiadas caigan en las manos equivocadas y produzcan una brecha de seguridad al negocio.

Las soluciones de seguridad de acceso también ayudan a optimizar la gestión real de los privilegios. Permiten a los administradores de TI otorgar o revocar privilegios a todos los recursos desde un 'hub' centralizado. Esto hace que el proceso sea más ordenado y manejable para el administrador de TI, y permite una supervisión simplificada.

Protección contra amenazas de ciberseguridad

Gartner predice que el gasto mundial en ciberseguridad alcanzará los 133.7 mil millones de dólares en 2022. Organizaciones de todas las formas y tamaños están tomando importantes medidas para protegerse de los ciberataques, y la seguridad de accesos es una parte integral de esto. La Gestión de Accesos Privilegiados (PAM) fue nombrada por Gartner como prioridad número uno de ciberseguridad en 2019.

Dado que las amenazas pueden venir tanto de dentro como de fuera de la organización, nunca ha sido más importante saber:

- ¿Quiénes están accediendo al sistema?
- ¿Qué privilegios tienen?
- ¿Qué están haciendo durante ese acceso?
- ¿En qué momento han accedido?

Esto es relevante para las personas internas de la compañía, como pueden ser los empleados en el edificio de la compañía, pero también para los externos, como las terceras partes, contratistas o los trabajadores remotos. Las credenciales de usuario comprometidas son habitualmente la puerta de entrada a la red para actividades maliciosas como ramsonware, malware o phishing, por lo que la seguridad de accesos se convierte en la máxima prioridad.

Asegurando el perímetro

En el pasado, el perímetro de seguridad de TI de una empresa terminaba dentro de sus paredes. Ahora las empresas tienen 'endpoints' o terminales en todo el mundo, ya que tanto los empleados como los proveedores pueden acceder a las redes de forma remota desde sus propios dispositivos. El Internet de las cosas (IoT) se está expandiendo, abriendo más caminos que nunca de acceso a las redes. También está creando rutas hacia industrias que anteriormente estaban aislados del amplio mundo conectado.

Estos factores hacen que los endpoints o terminales externos a la red de la corporación no estén protegidos por la seguridad perimetral tradicional. Los negocios necesitan una capa adicional de seguridad para los dispositivos que acceden a la información sensible desde cualquier lugar. Una solución de gestión de accesos puede autenticar a los usuarios desde múltiples endpoints, lo que significa que esos usuarios pueden verificar sus identidades de forma remota sin ningún impacto en su productividad.

Cumplimiento de las regulaciones

Saber exactamente quién está entrando y saliendo de una red, y qué privilegios tiene, es una política sensata. Pero no debe quedarse en una recomendación. Se trata de una obligación. Esto se refleja así en las diferentes regulaciones y

normativas, como la ISO 27001 y el RGPD, que requieren a las empresas tener un fuerte control, transparencia y realizar auditorías de las sesiones de los usuarios privilegiados. Contar con un marco de seguridad de accesos robusto es la mejor manera de adaptarse correctamente a las regulaciones, así como de evitar cualquier penalización por no respetar los estándares regulatorios.

Las empresas no deberían esperar a sufrir un robo de datos para protegerse con una seguridad de accesos sólida. Las soluciones adecuadas permiten a los equipos de TI mantener el cumplimiento de las regulaciones sin sobrecargar los recursos de ciberseguridad ni complicar demasiado la actividad de la empresa. Una solución de seguridad de accesos bien administrada puede ayudar a optimizar y acelerar la implementación de las normas de cumplimiento en toda la organización.

La seguridad de accesos ofrece muchos beneficios a la organización. Pero antes de explorar los sistemas específicos que pongan en funcionamiento la seguridad de accesos, es importante entender algunos conceptos que hay tras ellos; conceptos tales como "amenazas Internas', Confianza Cero (Zero Trust) y El Principio del Menor Privilegio son elementos críticos para mantener la seguridad de las redes.

Entendiendo la seguridad de accesos

Amenazas internas ('Insider Threat')

Un usuario interno (Insider) hace referencia a cualquier persona que tenga acceso legítimo a los datos sensibles de una empresa. Estos son, por ejemplo, los empleados a tiempo completo, los empleados a tiempo parcial, y los empleados de contratistas terceros, porque todos tienen derechos de acceso a la infraestructura de la organización en diferentes momentos. En la era del cibercrimen, esto hace que este tipo de usuarios sean una potencial enorme puerta de entrada para los hackers.

Puede parecer extraño considerar a empleados fiables y valiosos como amenazas, pero la realidad es que una alta cantidad de ataques están vinculados a credenciales de acceso de los usuarios internos. Esto no quiere decir que se tenga que tratar a cada uno de los usuarios como si ellos mismos fueran cometer algún acto malicioso, pero en términos de seguridad de accesos, cada conjunto de credenciales de acceso, sin importar cuán fiable sea el usuario, representa un nuevo punto de vulnerabilidad. Aunque la mayor parte de los empleados nunca pondrían deliberadamente en riesgo la seguridad de su compañía, podrían perder sus credenciales, podrían robárselas o podrían compartirlas inadvertidamente con alguien de menor confianza.

¿Cómo de importante es la amenaza interna?

La amenaza interna es la principal causa de ciberataques. Según un informe presentado en 2020 por The Ponemon Institute, el número de incidentes de ciberseguridad causados por usuarios internos se ha incrementado un 47% desde 2018. El informe también establece que el 62% de los incidentes fueron causados por negligencia, en oposición a las acciones criminales.

La amenaza interna es un riesgo porque incluso los empleados de confianza pueden causar una infracción o violación grave de datos sin darse cuenta a través de estafas de phishing de correo electrónico, compartiendo las credenciales de su cuenta y las contraseñas, o simplemente accediendo a los activos críticos desde terminales fuera de la red corporativa. El estudio del Instituto Ponemon, establece que las organizaciones están invirtiendo hasta un 60% más en amenazas internas hoy que hace tres años. Muchas más compañías están tomando medidas para protegerse de estas vulnerabilidades.

¿Cómo nos protegemos contra ello?

Las personas siempre necesitarán acceso a recursos de TI para hacer su trabajo. Las organizaciones deben proteger sus activos de usos indebidos accidentales que originen vulnerabilidades. Cuanta más exposición y vulnerabilidades se originen, más probabilidades de ataques maliciosos hay.

Aquí vamos a explorar dos principios que las empresas pueden aplicar para protegerse de estas violaciones de seguridad. Primero, aplicando el Modelo Zero Trust (Confianza Cero) en los procesos de identificación y autenticación para garantizar que se conoce a todos los que están entrando en la red. Y, en segundo lugar, autorizando a los usuarios internos con los menores privilegios necesarios para realizar su trabajo.

El modelo Zero Trust (Confianza Cero)

Es una verdad desafortunada que cualquier usuario puede ser considerado como una amenaza cuando se trata de la seguridad de los accesos, incluso los usuarios internos de mayor confianza de la organización. Es por ello por lo que tiene sentido implementar un enfoque 'Zero Trust' o 'Confianza Cero' sobre los usuarios que acceden a nuestra red corporativa. Esto no quiere decir que se deba tratar a todo el mundo como sospechoso o como si hubiera siempre un problema latente a punto de ocurrir.

Según un informe presentado en 2020 por The Ponemon Institute, el número de incidentes de ciberseguridad causados por usuarios internos se ha incrementado un 47% desde 2018. El informe también establece que el 62% de los incidentes fueron causados por negligencia, en oposición a las acciones criminales.

Simplemente significa que no se confía implícitamente en nadie cuando se trata de acceder a los datos confidenciales de una organización. En lugar de suponer que toda actividad es legítima hasta que se demuestre lo contrario, un modelo de seguridad Zero Trust requiere proactivamente prueba de identidad antes de permitir el acceso. Los usuarios deben demostrar que tienen tanto la necesidad como la autorización para acceder a un recurso de la red antes de que se otorgue la entrada.

¿Cómo podemos confiar en los usuarios?

Usar un enfoque Zero Trust para la gestión de los

accesos no elimina la amenaza interna, pero ayuda a mitigarla. Otorgar nuestra confianza a un usuario basándonos únicamente en que tiene un usuario y una contraseña no es suficiente protección.

Aquí es donde la autenticación multifactor (MFA) entra en juego. Como se detalla anteriormente, MFA requiere más de una forma de verificación para probar que un supuesto usuario es quien dice ser. Es mucho menos probable (aunque no imposible) que un hacker obtenga dos formas de verificación que solo una. Un hacker necesitaría, por ejemplo, robar tanto la contraseña de un usuario como su token de seguridad, en lugar de únicamente la contraseña. Cuantos más factores de autenticación entren en juego, mayor confianza se puede otorgar a la identidad del usuario.

Es suficiente con
la autenticación multifactor

Los empleados son confiables, lo que es bueno. Sin embargo, cuando se trata de seguridad de accesos, la confianza por defecto es una política peligrosa. Nadie debería ser implícitamente confiable cuando están en riesgo importantes brechas de seguridad de los datos

El Modelo Zero Trust es la primera línea de defensa para prevenir que los hackers roben las credenciales. Un aspecto importante en la implementación de este modelo es el Principio del Menor Privilegio que asegura que, si las credenciales acaban siendo robadas, el impacto que el hacker puede tener será el mínimo.

El Principio del Menor Privilegio

El Principio del Menor Privilegio significa dar a los usuarios la posibilidad de acceder solamente al menor número de archivos y aplicaciones necesarias para realizar su trabajo. Limitar los derechos de acceso a los mínimos que se requieren, ni más, ni menos, elimina los usuarios con privilegios excesivos y los riesgos que conllevan. Un hacker puede hacer más daño con el gran alcance de los privilegios de usuario administrador que con unos privilegios reducidos de cualquier usuario comprometido. El Menor Privilegio también se puede extender a los 'momentos' y a los 'lugares' en los que las diferentes personas necesitan acceder a los recursos. Por ejemplo, se puede permitir a los empleados acceder a los archivos solamente durante las horas de trabajo y desde ubicaciones concretas.

Con la política del menor privilegio implementada, la potencial 'superficie de ataque' sobre la que un hacker puede actuar se reduce. Considera esta analogía: sería como visitar un hotel y que te ofrezcan una tarjeta de acceso que desbloquea cualquier puerta del edificio por el tiempo que quisieras usarla. En lugar de ello, lo que le estamos dando es una tarjeta que funciona solamente para entrar en las áreas comunes y en tu propia habitación, y únicamente por el tiempo de estancia.

¿Por qué es el principio
del Menor Privilegio tan importante?

El Menor Privilegio limita la visibilidad de los usuarios sobre los recursos que no necesitan o que no están autorizados a ver. Por lo tanto, si un hacker

roba las credenciales de un usuario, únicamente tendría acceso a un limitado número de recursos y el daño que puede infligir será menor. No será capaz de alcanzar otros recursos, aunque quisiera. Limitando el acceso que tienen los usuarios, limitamos la exposición en el caso de que sus credenciales se vean comprometidas.

Por ejemplo, un proveedor contratado para llevar a cabo el mantenimiento administrativo de un equipo específico no necesita el mismo nivel de acceso y permisos que podría tener el director de TI. Sólo necesitaría acceso a los activos requiera para hacer su trabajo. Solo sería necesario que un contratista con privilegios elevados pinche un link con phishing para descargar el malware, y entonces tenemos un hacker con privilegios de administrador para los activos más sensibles de la organización. Si un usuario interno necesitara tener permisos elevados de acceso a un área sensible de la red, esto siempre puede solicitarse -y otorgarse- para cada tarea concreta.

Cómo puedo implementar el Principio del Menor Privilegio?

El principio del menor privilegio es en teoría simple. No obstante, podría ser necesario aplicarlo sobre cientos o miles de trabajadores de una organización, cada uno de los cuales va teniendo diferentes roles y necesidades de acceso según pasa el tiempo. También podría haber muchas nuevas incorporaciones y bajas que tener en cuenta. Para poder implementar el Principio del Menor Privilegio con éxito y de forma sostenible, es importar entender bien lo siguiente:

- ¿Cuáles son los recursos considerados sensibles?
- ¿Quién debe necesariamente acceder a estos recursos?
- ¿Cuáles son las regulaciones que debe cumplir el negocio?

El Menor Privilegio aplicado junto con un enfoque Zero Trust es una potente metodología de seguridad de accesos. Identificar los usuarios y administrar sus derechos de privilegio es mucho más fácil cuando se gestiona desde una solución centralizada. A continuación, puedes conocer los sistemas de gestión que permiten aplicar estos dos modelos.

Gestionando la Seguridad de Accesos

Gestión Accesos e Identidades (IAM)

Los entornos en la nube, el trabajo en remoto, las políticas de 'bring your own device' (BYOD), y el Internet de las Cosas en el mundo Industrial (IIoT), han hecho que las redes de TI sean más complejas que nunca. Esto puede dificultar aún más la gestión de las identidades digitales. Sin un sistema centralizado capaz de monitorizar y administrar el acceso de los usuarios las organizaciones quedan expuestas a riesgos innecesarios.

Ya hemos visto cómo verificar el ID de los usuarios de una red es una parte integral de la seguridad de acceso. La Gestión de Accesos e Identidades (IAM) es un conjunto de soluciones que identifican y autentican a cualquier usuario que necesita acceso al sistema de una organización. Estos sistemas permiten a los negocios definir quién es cada usuario y qué puede hacer dentro de la red.

¿Cuáles son las prestaciones clave del IAM?

Los sistemas IAM incluyen una variedad de herramientas que facilitan los tres pilares clave: identificación, autenticación y autorización. Con la correcta selección de soluciones, una organización puede establecer una defensa fuerte para proteger identidades, accesos y datos corporativos.

¿Qué se requiere de las soluciones que integran el ecosistema IAM? Una solución de gestión de identidades debe ser capaz de verificar usuarios, preferiblemente mediante la autenticación MFA. Esto permite a las organizaciones reforzar una política Zero Trust siempre que alguien intenta acceder a la red.

Las identidades digitales de una infraestructura pueden cambiar con el tiempo, por lo tanto, deben administrarse de manera flexible a medida que los usuarios avanzan a través de su "ciclo de vida", permitiendo que las identidades sean fácilmente añadidas, eliminadas o modificadas. Una gestión de accesos efectiva permite a los 'super-administradores' habilitar y deshabilitar cuentas, dar y revocar permisos de acceso y almacenar la información de los usuarios en una base de datos. El sistema debe ser fácil de manejar por los administradores de TI. Si la administración del sistema es complicada o está distribuida en múltiples recursos, no será tan efectiva.

Asimismo, las soluciones de seguridad más efectivas son las que proveen de una mejor experiencia de usuario. Si conectarse a los recursos es complicado, los usuarios buscaran escapatorias que anulan el propósito de las soluciones y ponen a las empresas aún más en riesgo. Simplificar la autenticación través de un Inicio de Sesión Único (SSO) y centralizar el acceso a través de una única plataforma, mejora la experiencia del usuario y le anima a adoptar los procesos de seguridad adecuados.

IAM es un término general para gestión de todas las Identidades, y los accesos asociados, dentro de una organización. Por ello, un sistema IAM potente debe incluir también soluciones de Gestión de Accesos Privilegiados (PAM). Las soluciones PAM ofrecen una robusta capa de seguridad facilitando la implementación de Menor Privilegio y Zero Trust a los derechos de acceso de usuario elevados.

Gestión de Accesos Privilegiados

La Gestión de Accesos Privilegiados (PAM), es una solución que ayuda a las empresas a monitorizar y auditar todas las acciones que realizan los usuarios con privilegios. Las soluciones de gestión de identidad y MFA atentican y autorizan a los usuarios que necesitan entrar al sistema y, tras ello, los sistemas PAM se centran en agilizar la administración y supervisión de los derechos de acceso de los usuarios con privilegios elevados, manteniendo a las organizaciones a salvo del uso incorrecto de los privilegios de acceso, ya sea accidental o deliberado.

Los peligros de confiar incondicionalmente en cualquier usuario son evidentes dadas las amenazas internas, y la metodología Zero Trust requiere que cada intento de acceso privilegiado sea validado y monitorizado. Es arriesgado hasta otorgar a los

administradores privilegios como los de cambiar la configuración del sistema, instalar softwares o acceder a datos seguros. Las credenciales privilegiadas se pueden perder, compartir o robar. Un usuario malintencionado con derechos de administrador no solo puede realizar cambios de gran alcance en un sistema, sino que también podría estar en la posición de poder esconder sus acciones. Por no mencionar las posibles negligencias o errores a través de los que, de forma accidental, pudiera hacerse un mal uso de esos derechos privilegiados.

Una solución PAM mitiga esta amenaza, facilitando un control preciso sobre exactamente quien tiene privilegios de administrador, para que recursos y cuando. Monitoriza las acciones del usuario, permitiendo su rastreo, trazabilidad que puede ser utilizada en caso de que ocurra una brecha de seguridad. Los sistemas PAM más efectivos validan los intentos de los usuarios privilegiados para acceder a los recursos contra los siguientes criterios:

1. ¿Puede ese usuario probar quién es?
2. ¿Tiene ese usuario los privilegios necesarios para acceder a ese recurso en cuestión?
3. ¿Se dan las circunstancias apropiadas para ese acceso privilegiado?
4. ¿Se está registrando, grabando y monitorizando la actividad de este usuario con fines de trazabilidad y auditoría?
5. ¿Puede la sesión terminarse (ya sea automática o manualmente) si la actividad del usuario no está autorizada o es sospechosa?

Las soluciones PAM pueden variar en su arquitectura, pero la mayoría presentan estos tres componentes:

- **Un gestor de accesos**
- **Un gestor de contraseñas**
- **Un gestor de sesiones**

Estos módulos trabajan de forma conjunta para asegurar que las cuestiones arriba mencionadas tienen siempre una respuesta afirmativa antes de otorgar el acceso privilegiado al usuario.

Gestor de Accesos

El Gestor de Accesos gobierna el acceso a las cuentas privilegiadas. Permite al equipo de seguridad de TI de la organización mapear los roles de sus usuarios y su acceso, permitiendo, denegando y modificando los privilegios de usuario a todos y cada uno de los activos desde una única consola. Proporciona las herramientas necesarias para proporcionar a todos los usuarios (internos, externos y terceras partes) el acceso que necesitan para hacer su trabajo, y ofrece una vía los administradores para gestionar las autorizaciones y rastrear a los usuarios.

El gestor de accesos centraliza el acceso y gestiona todos los recursos desde una única plataforma, sin inicios de sesión diferentes, y sin tener que usar distintas de herramientas. Los usuarios solamente pueden ver los recursos a los que tienen derechos de acceso, ni más, ni menos. No pueden ver ningún otro activo de la red, aunque puedan presuponer que están ahí.

Usar un Gestor de accesos permite a los administradores hacerse una idea clara de quién está usando y accediendo a los recursos de la organización. Y simplifica la conexión de los usuarios internos y externos a los recursos, agilizando el acceso a todos los recursos autorizados a través de una única plataforma. El Gestor de accesos es especialmente importante para las grandes organizaciones que necesitan proporcionar acceso desde el exterior a contratistas, proveedores de servicios y empleados remotos, ya que ofrece una capa adicional de seguridad para estos usuarios que se conectan desde fuera de la red corporativa.

Gestor de Contraseñas

El objetivo de una solución PAM efectiva es evitar que los usuarios privilegiados conozcan las contraseñas reales de los sistemas más importantes y críticos de la compañía. El administrador de contraseñas almacena todas las claves SSH de contraseña dentro de una caja fuerte, lo que significa que los usuarios no necesitan saber nunca las contraseñas originales, ni compartirlas. El empleo de una herramienta avanzada de gestion de contraseñas en una solución PAM reduce significativamente el riesgo de que las contraseñas de una organización caigan en las manos equivocadas. Las contraseñas se aplican por complejidad y se van rotando automáticamente, lo que significa que las credenciales ya usadas se invalidan incluso si son robadas.

Un gestor de contraseñas es más que simplemente una caja fuerte. Si bien almacena y encripta de forma segura las contraseñas, también ayuda a aplicar políticas de contraseña robustas y a implementar las mejores prácticas dentro de una organización. El administrador de contraseñas es una parte clave de la solución PAM, que permite a las organizaciones reducir la exposición al riesgo y alcanzar una gran variedad de requisitos de cumplimiento.

Gestor de Sesiones

El gestor de sesiones es el núcleo de una solución PAM robusta, pues supervisa el acceso privilegiado en tiempo real y verifica si las acciones realizadas en la sesión privilegiada son legítimas y están autorizadas. También crea una trazabilidad inalterable de todas las sesiones, con unos registros a los que se puede acceder, lo que facilita el cumplimiento de las normativas. Y si se intenta acceder a recursos sensibles sin autorización, la sesión se puede finalizar automáticamente. Es el principio de Zero Trust en acción: "más vale prevenir que curar".

El gestor de sesiones proporciona completa visibilidad sobre las acciones de los usuarios privilegiados, lo que reduce el riesgo de incurrir en un abuso de privilegios de forma deliberada o accidental. Registra los clics, la pulsación de teclas y demás acciones del usuario privilegiado para permitir que las organizaciones vean exactamente lo que hizo durante una determinada sesión. Esto incluye aquellas acciones que el usuario pueda estar intentando ocultar, ya sea usando otra pantalla o a través de comandos de teclado. La grabación de las sesiones también puede ayudar a detectar errores en tiempo real y posibilitar que se reviertan. Estas

grabaciones son particularmente útiles en caso de que la información deba revisarse durante una auditoría o formación futuros.

Una solución PAM integral es la mejor manera posible de optimizar la seguridad ante los potenciales riesgos que plantean los usuarios privilegiados.

Gestión de Privilegios en los Endpoint

Junto a la Gestión de Accesos Privilegiados (PAM), la Gestión de Privilegios en los Endpoint (EPM) es un componente critico dentro de una estrategia IAM efectiva, de cara a proteger los dispositivos desde los que los usuarios acceden a la red de la organización y otros equipos terminales. EPM aplica el principio del Menor Privilegio a estos terminales, lo que permite a las organizaciones definir privilegios más allá del nivel del usuario, para aceptar o bloquear el uso de las aplicaciones y procesos. Así se protege la red de amenazas como el *ransomware* o el *malware*. Ya sea un teléfono, un ordenador o un terminal en el punto de venta, todos los dispositivos deberán cumplir con criterios específicos antes de obtener acceso a los recursos de la red.

¿Por qué hay que proteger los terminales?

Esos días en los que los empleados solo accedían a la red de TI desde sus estaciones de trabajo fijas han desaparecido. Las organizaciones modernas pueden tener cientos o miles de terminales, y el número aumenta al ritmo que avanza el Internet de las Cosas en el mundo Industrial, donde cada vez hay más dispositivos. La mayoría de los empleados pueden acceder a la organización a través de PC de sobremesa, portátil, teléfono móvil o desde sus dispositivos personales, y desde cualquier parte. Cuantos más *endpoints*, más caminos para que los hackers puedan infiltrarse a la infraestructura TI.

Es importante que se apliquen las medidas de seguridad correctas para prevenir que dispositivos no autorizados entren a la red. Sin embargo, no sería práctico aplicar estas medidas a cada dispositivo individualmente. La Gestión de Privilegios de los Endpoint permite este control, así como poder alcanzar el cumplimiento de regulaciones como GDPR, NIS, y PCI-DDS, sin sacrificar productividad.

¿Cómo funciona la gestión de privilegios en los endpoints?

EPM ofrece un software centralizado que permite a los administradores identificar y gestionar el acceso de los dispositivos de los usuarios a la red corporativa. EPM elimina los riesgos asociados a los usuarios con privilegios excesivos, aplicando los privilegios a nivel de procesos y aplicaciones, en vez de a nivel de usuario. Los administradores pueden establecer permisos de acceso para que incluso los dispositivos personales fuera del perímetro de la red no puedan suponer un riesgo para los activos corporativos. Pueden incluso reforzar el Principio del Menor Privilegio estableciendo políticas que otorguen a los terminales permisos de acceso precisos y granulares, para asegurar que la infraestructura de TI está protegida, sin impactar en la productividad.

Con los controles establecidos a nivel de procesos, TI puede generar listas blancas, listas negras, o listas

grises para uso de aplicaciones o acciones específicas. Así, las tareas diarias no se interrumpen (no necesitan llamar al equipo informático para solicitar permisos concretos para descargarse una determinada herramienta cada vez que la necesita), sino que se mantiene la seguridad de los terminales con restricciones impuestas sobre los procesos que esas aplicaciones pueden o no llevar a cabo, incluso en el caso de un usuario con privilegios elevados.

Resumen final

Analicemos un caso. Un contratista necesita acceder a la base de datos de una organización para realizar un determinado trabajo, de modo que intenta iniciar sesión en la red corporativa a través de su Tablet personal. El procedimiento IAM de la organización asegura que la persona autentifica su identidad usando MFA: una contraseña temporal que se le ha proporcionado, así como el código de un token RSA.

El sistema PAM autoriza su acceso al servidor al que necesita entrar y, entonces, empieza a monitorizar y grabar la sesión mientras está activa. Si necesitase acceder a otros recursos puede solicitar elevación de privilegios y el equipo de TI se los otorga por un determinado periodo. Al finalizar sus tareas, una vez que completa su trabajo, el sistema PAM lo registra automáticamente, rota la contraseña de los recursos utilizados y revoca sus privilegios elevados. El sistema PAM elimina sus privilegios de acceso a la red de la empresa cuando la necesidad de uso de esos derechos desaparece. El sistema EPM asegura que el dispositivo que se ha usado para modificar la base de datos cuenta con la configuración de seguridad adecuada, y le permite descargar las apps incluidas en la lista blanca y trabajar con ellas.

Este escenario muestra cómo una organización con una fuerte seguridad de acceso puede usar PAM y EPM de forma conjunta para mantener seguros los sistemas y los datos más críticos de la compañía, como parte de una estrategia IAM global.

SOBRE WALLIX

WALLIX Group, una compañía de software que brinda soluciones de ciberseguridad, es el especialista europeo en cuentas privilegiadas gubernamentales. En respuesta a los recientes cambios regulatorios y las amenazas a la seguridad cibernética que afectan a todas las compañías hoy en día, las soluciones de WALLIX ayudan a los usuarios a defenderse contra ataques cibernéticos, robos y fugas de datos vinculados a credenciales robadas y abusos de privilegios.

WWW.WALLIX.COM

WALLIX
CYBERSECURITY SIMPLIFIED