Administración de Cuenta No Humana (v3)

Por Graham Williamson, André Koot, Gloria Lee

Tabla de contenidos

Resumen

Las cuentas no humanas son el "talón de Aquiles" de un entorno IAM robusto. Mientras que los profesionales IAM se preocupan con la administración de identidades, autenticación, RBAC, ABAC, gobernanza y auditoría de cuentas de usuario, otra parte del equipo TI se dedica a implementar servicios y dispositivos que reciben acceso a recursos protegidos a través de cuentas cableadas, servicios expuestos y API.

La gestión del control de cuentas no humanas debe ser coherente con la gestión de cuentas basada en usuarios, y los controles aplicados al acceso de las cuentas de los usuarios a aplicaciones de alta seguridad también deben aplicarse a las cuentas no humanas.

No existe una solución única para lidiar con cuentas no humanas. Algunos profesionales de IAM sugieren que todas las cuentas deben administrarse mediante los mismos procesos y la misma infraestructura para garantizar una implementación de políticas coherente. Argumentan que esta coherencia debería garantizar que las cuentas no humanas no queden "excluidas" cuando

se produzcan implementaciones de IAM. Otros consideran que esto no es práctico y recomiendan que se implementen procesos con fines específicos para cuentas no humanas. Pero independientemente del mecanismo utilizado para gestionar las cuentas no humanas, garantizar su gestión es primordial. De lo contrario, las cuentas no humanas seguirán siendo un vector de ataques de ciberseguridad usadas por piratas informáticos que quieran acceder a las instalaciones corporativas.

Introducción

Una identidad no humana está asociada con un servicio o dispositivo en lugar de con un usuario humano. La identidad en este contexto está definida por los identificadores del dispositivo. Un dispositivo debe ser identificable para que pueda interactuar con los sistemas corporativos. Por ejemplo, es posible que un sistema de gestión de edificios necesite iniciar sesión periódicamente en otro sistema para escribir datos ambientales en una base de datos del sistema de monitoreo corporativo.

En este documento, las "cuentas no humanas" incluyen cuentas de sistemas informáticos que no están asociadas con una persona, como una rutina de respaldo que se ejecuta fuera del horario comercial para crear una copia fuera de línea de los datos de producción. Dichas cuentas deben limitarse al propósito específico para el que fueron creadas y suspenderse si se utilizan de forma interactiva.

Si bien los profesionales de IAM suelen centrarse en las cuentas de usuarios, estas cuentas no humanas representan un vector de ataque potencial para las organizaciones. Estas cuentas deben considerarse al formular políticas de acceso a los sistemas informáticos. A continuación, se muestra una comparación entre las características de estas cuentas:

	Identidad humana	*Identidad no-humana*
Uso	Multifacético, debe adaptarse a múltiples requisitos de acceso a muchas aplicaciones o recursos protegidos.	Propósito específico, requisito único para cada implementación
Ciclo de vida	Creado durante el proceso de "ingreso", modificado cuando ocurren "movimientos", monitoreado continuamente para verificar el cumplimiento, deshabilitado y luego eliminado de acuerdo con el proceso de "salida".[1]	Creado durante la implementación del dispositivo/servicio, eliminado tras su terminación.
Control de acceso	Dinámica: autenticación continúa con evaluación de riesgos que coincide con los requisitos de nivel de seguridad de la aplicación solicitada o recurso protegido. La Autenticación de Múltiples Factores (MFA, por sus	Estático: determinado en el momento de la creación de la cuenta. Sin requisito de MFA.

[1] Cameron, Andrew y Olaf Grewe, "Una descripción general del ciclo de vida de la identidad digital", Cuerpo de Conocimientos de IDPro, 30 de octubre de 2020, https://bok.idpro.org/article/id/31/.

	siglas en inglés) se utiliza para la elevación de autenticación.	
Puntos finales de acceso	Los usuarios suelen acceder a los servicios informáticos desde teléfonos inteligentes, PC y computadoras portátiles de forma interactiva.	Los puntos finales suelen ser dispositivos o controladores de dispositivos. También pueden ser aplicaciones informáticas, rutinas de servicio o *bots* de Internet.

Tabla 1 - Características según el tipo de cuenta

Hay dos categorías amplias de cuentas no humanas que los profesionales de IAM deben diferenciar:

- cuentas utilizadas por dispositivos o servicios para realizar una función específica; estas cuentas deben ser monitoreadas y alertar sobre cualquier incidente que suponga una anomalía en la operación esperada;
- cuentas que tienen acceso a funciones del sistema pero que no están asignadas a una persona específica, incluidas cuentas administrativas con privilegios elevados.

Terminología

- *Bot*: a veces llamado robot de Internet, abreviatura de "robot", pero que se refiere a una rutina de software que realiza tareas automatizadas a través de Internet, un robot web que se refiere a una aplicación de red autónoma o simplemente un "bot" que se refiere a una tarea automatizada, generalmente repetitiva, utilizada para un propósito específico.
- Identidad: define atributos para un usuario humano que pueden variar según los dominios; por ejemplo, la identidad digital de un usuario tendrá una definición diferente en un entorno de trabajo y en el de su banco. A veces se hace referencia a un identificador de dispositivo como su identidad.
- Tríada de la CIA: los conceptos fundamentales de seguridad de la información de clasificación de riesgos de recursos desde las perspectivas de confidencialidad, integridad y disponibilidad.
- Cuenta no humana: cualquier cuenta que no es utilizada por una persona, incluidas las cuentas utilizadas para dispositivos, servicios y servidores.
- Cuenta de servidor: una cuenta con derechos de acceso privilegiados a la operación de un servidor que normalmente se utiliza con fines de configuración.
- Cuenta de servicio: una cuenta utilizada por una aplicación informática para acceder a otra aplicación o servicio para un propósito específico.
- Cuenta del sistema: término genérico para una cuenta privilegiada que tiene amplios permisos que permiten cambios en la configuración del sistema.

Control de acceso no humano

Una preocupación importante para el profesional de IAM es cómo gestionar el control de acceso hacia y desde los dispositivos, particularmente con servicios que los humanos no utilizan de forma interactiva. Esto incluye *bots* que se utilizan cada vez más para procesos automatizados.

Dispositivos de IoT

Los dispositivos del Internet de las Cosas (IoT, por sus siglas en inglés) pueden ser un sensor o un actuador. En algunos casos, los sensores proporcionan un flujo continuo de datos que se muestran en tiempo real o lecturas discretas que se escriben en una base de datos para su análisis periódico. Los actuadores son dispositivos que normalmente se utilizan para controlar un proceso, activando o desactivando algo. Se pueden utilizar para abrir o cerrar una válvula

pulsando un servomotor un número suficiente de veces hasta alcanzar la apertura deseada. En muchos casos, los dispositivos están ubicados de forma remota y conectados a través de un controlador al sistema de supervisión situado en una ubicación central.

En una configuración típica de IoT hay tres zonas:

1. Dispositivos IoT (sensores y actuadores). La gestión del acceso hacia y desde los dispositivos debe regirse por una política que imponga requisitos de cifrado del canal de comunicaciones, como DNP3, MQTT y/o tecnología de firma digital (por ejemplo, PKI), para adaptarse al nivel de seguridad requerido. En entornos de baja seguridad, se pueden utilizar contraseñas estáticas que permanecen en servicio hasta que se desmantela el equipo. En aplicaciones de mayor sensibilidad, las credenciales de seguridad (contraseñas, certificados, etc.) rotan periódicamente. El requisito de seguridad seleccionado debe coincidir con la capacidad de los dispositivos, pero las limitaciones técnicas a menudo restringen los dispositivos de IoT. La "Terminología para redes de nodos restringidos" (RFC 7228) nombra tres clases de dispositivos:[2]
    a. Clase 0: sin capacidad para admitir autenticación configurable
    b. Clase 1: capacidad limitada para gestión de claves, soporte de *tokens*, etc.
    c. Clase 2: totalmente configurable y capaz de admitir mecanismos de autenticación dinámica.
2. El Controlador (al que están conectados los dispositivos). Si los datos del dispositivo sensor son agregados por un controlador de dispositivo que asigna cada sensor o actuador a su lógica de control, se requiere proporcionar control de acceso a los actuadores y protección al escribir los datos recopilados en una base de datos (consulte Cuentas de servicio, a continuación).
3. Aplicación de Interfaz Hombre-Máquina (HMI, por sus siglas en inglés), como una aplicación de controlador o una aplicación SCADA que monitorea o controla los dispositivos IoT. En algunos casos, los sensores escribirán datos directamente en una base de datos que es leída por otra aplicación, como una aplicación SCADA o una HMI similar. El acceso a estas aplicaciones será por parte de humanos y deberá gestionarse a través del entorno de Administrador de Identidades (IDM, por sus siglas en inglés).

Históricamente, los entornos de IoT han sido gestionados por un equipo responsable de la tecnología operativa (OT, por sus siglas en inglés) y han tenido poco que ver con el entorno de tecnología de la información (TI) dentro de una organización. La naturaleza especializada de la tecnología IoT ha justificado esta estructura organizacional y, a menudo, es política corporativa aislar la OT de posibles compromisos a través del entorno de TI. Pero la necesidad de aislamiento está disminuyendo a medida que mejora la tecnología de seguridad. La integración de los sistemas de IoT con el entorno IAM mejorará las capacidades de control de acceso y proporcionará una mejor gobernanza corporativa sobre las implementaciones de tecnología operativa para la mayoría de las aplicaciones industriales.

Si los controles regulatorios lo permiten, la mejor práctica es integrar el entorno de OT con el entorno de IAM de TI. Esto permite que la OT establezca derechos del sistema a través del sistema IAM y que el personal de OT use sus credenciales corporativas para la autorización, potencialmente a través de un sistema de gestión de acceso privilegiado.

Existe una preocupación cada vez mayor con respecto a la procedencia de los dispositivos de IoT y los dispositivos de seguimiento a lo largo de la cadena de suministro para garantizar que

[2]Bormann, C., Ersue, M. y A. Keranen, "Terminología para redes de nodos restringidos", RFC 7228, DOI 10.17487/RFC7228, mayo de 2014, <https://www.rfc-editor.org/info/ rfc7228>.

no se hayan realizado modificaciones que potencialmente podrían implementar un acceso de "puerta trasera". Es posible que el profesional de IAM desee asegurarse de que la política corporativa defina los procesos de certificación que se emplearán para los dispositivos de IoT.

Tan importante como proteger el dispositivo en sí es proteger los datos del dispositivo IoT. En muchos casos, las bases de datos con dispositivos IoT no están adecuadamente protegidas. Se debe emplear un enfoque de gestión de riesgos para determinar la idoneidad de la protección; los datos de los dispositivos del entorno del edificio pueden ser de bajo riesgo, pero los datos de producción de la planta que no están adecuadamente protegidos contra el espionaje industrial pueden considerarse críticos. El profesional de IAM debe garantizar que se establezcan controles de acceso adecuados en los almacenes de datos industriales. Es una buena práctica asignar una función de controlador de datos a una base de datos industrial.

Mitigación de vulnerabilidad
No existe una "respuesta correcta" cuando se trata de decidir la participación de los profesionales de IAM en la gestión de dispositivos IoT. En un extremo del espectro está el caso de uso en el que todas las implementaciones y gestión de IoT son dominio del personal de OT. En este caso, la participación de IAM estará restringida a las cuentas humanas que acceden a los sistemas OT. La gestión grupal de derechos de cuentas que pueden configurar sistemas de IoT aumentará el nivel de seguridad.

En el punto medio del espectro, una identidad humana es responsable de los dispositivos de IoT. El flujo de trabajo de aprovisionamiento de IAM enviará las solicitudes de configuración y, potencialmente, las solicitudes de rotación de contraseñas, a la persona responsable. Los dispositivos IoT participarán tanto en los informes de certificación al administrador responsable como en la gestión de cumplimiento con integración al centro de operaciones de seguridad (SOC, por sus siglas en inglés) y posiblemente al sistema de gestión de eventos e información de seguridad (SIEM, por sus siglas en inglés).

En el otro extremo del espectro, el aprovisionamiento de dispositivos se incluye en la infraestructura de gestión de identidad. Los dispositivos de IoT reciben el mismo trato que los individuos, aplicando una "identidad digital" a los dispositivos. Sus derechos se pueden configurar a través de los flujos de trabajo normales de aprovisionamiento de cuentas y su control de acceso puede utilizar los mismos protocolos. La mayoría de los sistemas API modernos, incluidas las puertas de enlace, utilizan OAuth para comunicaciones de máquina a máquina, mientras que *OpenID Connect* puede ser apropiado para la autenticación del controlador de dispositivos IoT.[3]

Cuentas de servicio

Existe una amplia variedad de cuentas de servicios. Por lo general, se utilizan en procesos que se ejecutan periódicamente de forma automatizada, por ejemplo, a través de un trabajo cron de UNIX o el Programador de tareas de Windows. Los auditores a menudo pasan por alto las cuentas utilizadas por estos procesos porque los usuarios no acceden a ellas de forma interactiva. Dado que los usuarios no inician sesión en ellas, suelen ser cuentas bastante básicas y de un solo propósito con privilegios restringidos.

Algunos ejemplos:

- Una cuenta utilizada para realizar una copia de seguridad de datos todas las noches.

[3] Consulte la sección 'La innovación móvil y API nos dio OAuth y marcos de autorización delegada' en Dingle, Pamela, “Introducción a la identidad - Parte 2: Gestión de acceso”, Cuerpo de Conocimiento de IDPro, 17 de junio de 2020, https://bok.idpro.org /artículo/id/45/.

- Una cuenta que proporciona acceso al sistema de Calefacción, Ventilación y Aire Acondicionado (HVAC, por sus siglas en inglés) con fines de monitoreo.
- Una cuenta utilizada para la replicación de datos entre instancias de directorio.

El término "cuenta por lotes" se utiliza a veces para una cuenta de servicio. A menudo se refieren a una o más operaciones de servicios públicos que se ejecutan periódicamente durante las horas de no producción para realizar una función del sistema. Varios procesos por lotes pueden utilizar una única cuenta por lotes.

Mitigación de vulnerabilidad
Las cuentas de servicio son una fuente importante de preocupación para muchas organizaciones porque a menudo se establecen con una contraseña estática que, si no está cifrada, puede ser leída por cualquier administrador del sistema. Luego, un actor malintencionado puede utilizar estas cuentas de forma interactiva y posiblemente utilizarlas para el movimiento lateral a otros servidores de la organización. Incluir cuentas de servicio en las herramientas corporativas de protección contra pérdida de datos, como el monitoreo de autenticación para detectar anomalías, puede proteger contra tales vulnerabilidades. Una mejor práctica es migrar cuentas de servicios estáticas a API que normalmente imponen un estricto régimen de seguridad y monitoreo.

Nota: el término "cuenta de servicio" (una cuenta no humana) a veces se utiliza incorrectamente para describir una cuenta a la que accede periódicamente una persona de servicio, por ejemplo, un técnico de HVAC. Dichas cuentas son cuentas de usuario y no se tratan en este documento. Tenga en cuenta que debido a que este personal suele ser externo a una empresa y, por lo tanto, no está en el almacén de datos de IAM, a veces se establece una "cuenta genérica" para que la utilice cualquier persona de la empresa de servicios. Este enfoque conveniente es un problema para el entorno IAM. No hay lugar para cuentas genéricas en las organizaciones modernas y no deberían utilizarse.

Algunas opciones:
- Autenticación federada con la empresa de servicios.
- Gestión de contraseñas de autoservicio con flujo de trabajo de aprobación.
- Emisión del dispositivo MFA a la empresa de servicios.
- Despliegue de una API para gestionar y monitorear el acceso de las empresas de servicios.

Bots

El término "*bot*" proviene del sector de la automatización robótica de procesos (RPA, por sus siglas en inglés) que tuvo su génesis en la automatización de plantas, donde se implementan rutinas de software para procesos repetitivos. Los *bots* ahora se utilizan para todo, desde rastreadores de sitios web para recuperar información de uso hasta programa maligno de denegación de servicio. Las organizaciones los utilizan cada vez más para automatizar tareas repetitivas, como la recuperación de datos de gestión de información de edificios o la consolidación de datos de transacciones de clientes. En estos casos, el acceso de los *bots* estará restringido a un propósito específico.

Los *bots* suelen utilizar Internet para acceder a servicios o recursos remotos. Un sitio web disponible públicamente debe aplicar mecanismos para limitar la actividad de los *bots* y evitar el acceso malicioso. Estos mecanismos pueden incluir la aplicación de controles de eliminación de pantalla, comprobaciones de verificación humana y protección DDOS. Una forma común de actividad maliciosa es el "relleno de credenciales", mediante el cual un pirata informático altera las credenciales de inicio de sesión para tomar el control de una sesión.

Las organizaciones deben prepararse para el uso externo de *bots*. Los *bots* exhibirán características diferentes en comparación con el acceso no humano "normal" a un proceso o servicio. Para el profesional de IAM, el análisis del comportamiento del usuario se puede utilizar para identificar anomalías de acceso.
Se debe establecer un proceso para revisar el uso de los *bots*, probar su funcionalidad antes de su implementación y analizar sus patrones de uso. El monitoreo es una tarea continua ya que la corrupción maliciosa de los *bots* es una preocupación constante.

Mitigación de vulnerabilidad
Para la aplicación corporativa de la tecnología *bot*, la tarea del profesional de IAM es garantizar que se observen los controles adecuados sobre las credenciales y que las firmas y el cifrado PKI se utilicen según corresponda. Sólo se deben permitir actividades autorizadas.

Por ejemplo, un *bot* que accede a los datos de un sitio web normalmente se autenticará a través de HTTPS utilizando un *token* de sesión asignado. Es una buena práctica hacer caducar los *tokens* de sesión periódicamente. El período de tiempo de validez de un *token* debe depender de la sensibilidad del servicio o de los recursos a los que se accede.

Dispositivos cliente

Tradicionalmente las identidades son personas; tienen identificadores almacenados en un almacén de datos de identidad y luego se utilizan para autenticar a los usuarios en recursos protegidos. Es cada vez más necesario realizar un seguimiento también de los dispositivos finales que los usuarios emplean para acceder a recursos corporativos, como ordenadores portátiles, tabletas o teléfonos inteligentes. Para rastrear esos dispositivos, se crea un objeto en el directorio de la organización u otros almacenes de datos que registran los detalles de cada dispositivo. Estos datos nos permiten otorgar acceso a un recurso según el dispositivo que se utiliza para acceder a él.

Existen varios beneficios al registrar dispositivos cliente:

- Puede proporcionar un segundo factor durante un evento de autenticación humana, reduciendo así la puntuación de riesgo asociada con la autenticación.
- Se puede utilizar para personalizar la presentación y mejorar la experiencia del usuario pasando los detalles del dispositivo de un usuario a una aplicación.
- Puede habilitar la autenticación de dispositivos desatendida para admitir eventos programados, como actualizaciones de dispositivos o recuperación de datos.
- Puede eliminar una vulnerabilidad y mejorar las opciones de gobernanza cuando los objetos del dispositivo cliente del almacén de datos se deshabilitan o eliminan cuando se excede el período de tiempo de *LastLogonTimestamp*.

Ya sea que su entorno sea local, de nube híbrida o de múltiples nubes, administrar el ciclo de vida de la identidad del dispositivo del cliente es clave para reducir la superficie de ataque de la organización y mantener el cumplimiento de la política corporativa.

Mitigación de vulnerabilidad
Con la ubicuidad de los dispositivos de los clientes hoy en día, la gestión de los dispositivos de los clientes puede mejorar el perfil de ciberseguridad de una organización. Por ejemplo, un teléfono inteligente puede ser un dispositivo valioso para la autenticación multifactor (MFA). Puede proporcionar un factor de "posesión", por ejemplo, si el usuario está utilizando su teléfono móvil registrado. También se puede utilizar para proporcionar una verificación biométrica de un factor de "inherencia".

Algunas organizaciones utilizan una herramienta de administración de dispositivos móviles (MDM, por sus siglas en inglés) para administrar los dispositivos de los clientes. MDM facilita el seguimiento y la gestión de dispositivos y normalmente incluirá un módulo de autoservicio para permitir a los usuarios registrar y cancelar el registro de sus dispositivos a medida que se adquieren nuevos dispositivos o se pierden o retiran dispositivos antiguos.

Seleccionar e implementar la solución adecuada para gestionar las "identidades" de los dispositivos del cliente es una capacidad fundamental para permitir el control de acceso no humano.

Control de acceso a la cuenta del sistema

Las cuentas del sistema brindan a los humanos acceso a sistemas o servidores físicos o virtuales y otorgan derechos a la funcionalidad privilegiada del sistema. Si bien no son cuentas estrictamente no humanas, las cuentas del sistema se incluyen aquí porque no tienen un único individuo a quien asignarlas. Las cuentas del sistema generalmente se refieren a cuentas de administración que se establecen cuando se pone en funcionamiento un sistema/servidor. Dado que este tipo de cuenta no está asociada directamente con una sola persona, generalmente no se administran a través de los procesos de recursos humanos de una organización. Los profesionales de IAM deben preocuparse por la gestión de estas cuentas.

Cuenta de administrador o *root*

La cuenta de administrador o *root* de servidores Windows y Linux o Unix es una cuenta altamente privilegiada que cuenta con acceso a operaciones a nivel de sistema en la plataforma respectiva:

- Está autorizado al más alto nivel.
- Tiene acceso a todos los archivos y procesos que se ejecutan en una plataforma.
- Tiene permisos para configurar el funcionamiento del sistema y con ello influir en el comportamiento de la plataforma.
- Los registros de un sistema normalmente mostrarán los comandos ejecutados y las respuestas vistas.
- El uso operativo de la cuenta debe ser monitoreado continuamente.

Nota: las plataformas de virtualización e hipervisor (VMware, Citrix, Xen) y las plataformas de contenedores (Docker, Openshift, DCOS, Kubernetes) tienen cuentas administrativas que proporcionan un vector de ataque si no se administran adecuadamente.

Cuenta de superusuario

El término superusuario se aplica a un sistema de información empresarial o cuenta de aplicación que tiene privilegios elevados sobre las cuentas de usuario estándar. Se genera como parte del proceso de puesta en servicio del sistema cuando se implementa el mismo. La cuenta de Superusuario tiene permiso para modificar una configuración, lo que la convierte en una cuenta de misión crítica en un sistema de información.

Cuenta de servidor

Las cuentas para procesos de *middleware* como DBMS, ESB u otros componentes de TIC que se ejecutan en entornos de sistemas operativos Windows o Linux a veces se denominan cuentas de servidor. Estas son cuentas privilegiadas en una aplicación como un DBMS para otorgar acceso administrativo al propietario de un recurso.

Dispositivos cliente

Existe una creciente preocupación por la vulnerabilidad de los dispositivos de consumo que tienen conexión a Internet. Los incidentes recientes incluyen:

- Violaciones de privacidad por parte de dispositivos que tienen capacidades de captura de audio o video y que envían datos confidenciales a una agencia de monitoreo.
- Los incidentes de seguridad, como los ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés), son comunes y se utilizan contraseñas administrativas publicadas, lo que brinda a los piratas informáticos acceso a dispositivos de consumo que luego se utilizan para realizar dichos ataques.

La mayoría de las jurisdicciones ahora exigen que los productos cumplan con un conjunto apropiado de estándares entre los cuales se encuentran generalmente:[4]

- Poner fin al uso de contraseñas predeterminadas. Todos los dispositivos se envían con una contraseña única que no se puede restablecer a una configuración predeterminada común.
- Habilitación del soporte para actualizaciones de software. Los dispositivos se envían con *firmware* que se puede actualizar fácilmente en caso de que se detecte una vulnerabilidad.
- Apoyar el almacenamiento seguro de credenciales. Todas las credenciales deben almacenarse de forma segura con protección de cifrado y/o un mecanismo de almacenamiento confiable.
- Envío con una configuración predeterminada más segura. Las superficies de ataque se minimizan cerrando los puertos no utilizados, restringiendo los servicios expuestos solo a los funcionalmente necesarios y ejecutando software con el nivel más bajo de privilegios necesarios para el funcionamiento del sistema.
- Restringir el almacenamiento de información de identificación personal (PII, por sus siglas en inglés). La PII nunca se almacena en el dispositivo, según los requisitos de la normativa de privacidad en las zonas geográficas de destino.

Características de la cuenta del sistema

Dado que las cuentas del sistema no están asignadas a una única identidad, no pueden ser administradas en su totalidad por una solución IAM; por ejemplo, cuando la persona con privilegios administrativos abandona una organización, no es apropiado eliminar dicha cuenta. Una práctica común es proporcionar acceso a cuentas privilegiadas a través de un grupo administrado para que todos los usuarios del grupo tengan acceso a la cuenta. Pero todavía se requiere una gestión fuera del entorno IAM. Las buenas prácticas incluyen:

- Utilizar una base de datos de gestión de configuración en la que se registra el servidor/servicio como atributo de la identidad a la que pertenece.
- Asignar un propietario de cuenta para que sea responsable del uso de la cuenta, normalmente el propietario del sistema/servicio al que pertenece. Si no se ha definido ningún propietario del sistema, una persona responsable en el departamento de TI debe ser la parte responsable.
- Las cuentas interactivas solo deben usarse para cambios en la infraestructura o calamidades. Los privilegios de administrador deben otorgarse a través de la cuenta de un usuario, por ejemplo, mediante membresía en el grupo de administración apropiado.

---

[4] Por ejemplo, consulte Fernández, Ángel, "Nuevas regulaciones de seguridad de IoT: lo que necesita saber", blog de Allot, 30 de enero de 2020, https://www.allot.com/blog/new-iot-security-regulations-what-you-need-to-know/#.

- Las contraseñas para las cuentas de administrador/*root* deben administrarse de cerca. Se pueden proteger mediante un procedimiento manual, una bóveda de contraseñas o un sistema de gestión de cuentas privilegiadas.

Mitigación de vulnerabilidad
Los profesionales de IAM deben ayudar en la protección del acceso a todas las cuentas del sistema. En un entorno UNIX, esto podría realizarse mediante la eliminación del archivo "*etc/passwd*" y el uso de SUDO para escalar privilegios. En un entorno de Microsoft Windows, un sistema de gestión de acceso privilegiado (PAM, por sus siglas en inglés) es una solución común. En este caso, las contraseñas del sistema son específicamente complejas y se rotan según corresponda. El acceso a dicha cuenta se realiza a través de un sistema PAM, que restringe el acceso a personas específicas con los derechos adecuados y registra todos los eventos de acceso.

Si no se utiliza un PAM, Windows admite la elevación de privilegios de cuenta por tiempo limitado, con notificación a la administración. La intervención manual que garantice el uso y la gestión adecuados de las cuentas del sistema y del servidor también es una buena práctica, al igual que incluir cuentas de servidor en las auditorías corporativas. Este nivel de gestión requerirá que se establezca una política corporativa para las cuentas de servidor que aumentará la visibilidad de las prácticas de gestión de cuentas.

Cada vez más, las aplicaciones se implementan en servicios en la nube que requieren un entorno de control de acceso que se adapte a cada implementación. Este tipo de implementación podría significar configurar un administrador de recursos para proteger los privilegios de la cuenta maestra o establecer políticas que garanticen que las aplicaciones no utilicen la cuenta maestra para acceder a la base de datos.

El futuro

La ubicuidad de los dispositivos IoT será cada vez más frecuente. Los dispositivos abarcarán tanto el mundo corporativo como el de consumo, y la integración de dispositivos y flujos de datos de IoT será un nuevo riesgo corporativo. La automatización se implementará cada vez más con aprendizaje automático e inteligencia artificial, lo que aumentará la complejidad del entorno de control de acceso. Se debe considerar la integración con el entorno IAM mediante el uso de puertas de enlace API, puertas de enlace de bases de datos, mallas de servicios y soluciones de control de acceso basado en políticas.

Las API se utilizan cada vez más para la comunicación de máquina a máquina (M2M, por sus siglas en inglés). Las API brindan la capacidad de aplicar controles de seguridad consistentes en un canal de comunicación y también de monitorearlo con fines de administración. Las empresas que adoptan un enfoque de puerta de enlace tienen la capacidad de brindar coherencia en las comunicaciones M2M, lo que es prácticamente imposible si cada instancia de servicio se implementa individualmente.

A medida que la adopción de servicios en la nube continúe acelerándose, el uso de microservicios y la contenedorización se volverán prevalentes. El profesional de IAM debe garantizar que se implementen las soluciones de seguridad de la información adecuadas para proteger las comunicaciones entre servicios que comunican datos de identidad.

El uso de *bots* también seguirá acelerándose; se debe considerar la implementación de análisis de comportamiento y tecnología de puerta de enlace. El Departamento de Seguridad Nacional de EE. UU. aconseja lo siguiente:

- Los desarrolladores de *bots* maliciosos buscarán vulnerabilidades en los nuevos dispositivos IoT a medida que se lancen al mercado y competirán entre sí para implementar programa maligno.
- El tamaño del código del *bot* será más pequeño y sofisticado para evitar la detección y frustrar las defensas.
- Las *botnets* se ampliarán y se monetizarán mejor, probablemente a través de interfaces con plataformas de redes sociales.
- Los operadores de *botnets* operarán cada vez más globalmente, aprovechando las vulnerabilidades regionales. Aumentarán los ataques de operadores de Estados-nación extranjeros.

El control de acceso para entidades no humanas es una competencia crítica para las organizaciones con aversión al riesgo. Es cada vez más importante asegurarse de que los dispositivos y *bots* se identifiquen adecuadamente, migrar a API con controles de seguridad y monitoreo consistentes e implementar tecnologías de prevención de pérdida de datos, como herramientas de análisis de comportamiento.

Conclusión

Con demasiada frecuencia, los profesionales de IAM están aislados de la gestión de cuentas no humanas y solo se centran en el aprovisionamiento y el control de acceso asociados con las cuentas de usuario. Esto es desafortunado porque fragmenta el enfoque de gestión de riesgos de la organización anfitriona en materia de ciberseguridad y frustra la tarea de gobernanza. Como mínimo, el profesional de IAM debe hacer las preguntas apropiadas sobre cómo se protegen los dispositivos de IoT, cómo se administran las cuentas de servidor y qué defensas existen para frustrar los *robots* maliciosos. Es preferible que los equipos de IAM e InfoSec dentro de una organización trabajen juntos para garantizar la aplicación consistente de controles de ciberseguridad que estén alineados con la política corporativa.

Biografía de los autores

 Graham Williamson

Graham Williamson es un consultor de IAM que trabaja con organizaciones comerciales y gubernamentales desde hace más de 20 años con experiencia en gestión de identidades y control de acceso, arquitectura empresarial y arquitectura orientada a servicios, comercio electrónico e infraestructura de clave pública, así como desarrollo de estrategias de TIC y gestión de proyectos. Graham ha llevado a cabo importantes proyectos para organizaciones comerciales como Cathay Pacific en Hong Kong y Sensis en Melbourne, instituciones académicas en Australia como la Universidad Monash y la Universidad Griffith, y agencias gubernamentales como la oficina del CIO del Gobierno de Queensland y el Gobierno del Territorio del Norte en Australia y el Ministerio del Interior de Singapur.

Graham tiene una licenciatura en ingeniería eléctrica de la Universidad de Toronto y una maestría en administración de empresas de la Universidad Bond. Como miembro del Comité del Cuerpo de Conocimientos de IDPro, espera ayudar a crear el conjunto definitivo de conocimientos para el sector IAM.

 André Koot

André Koot es estratega de IAM y director de éxito del cliente en Sonic Bee. Su experiencia en IAM proviene de su experiencia en contabilidad y auditoría financiera. Estos antecedentes de procesos comerciales de detección y prevención de fraude lo llevaron a la investigación en el área de los principios de autorización.

 Gloria Lee

Gloria Lee es gerente sénior de programas en el equipo de ingeniería de Azure AD en Microsoft. Como parte del equipo de experiencia del cliente para Identidad y Acceso a la Red, su función es impulsar el éxito del cliente en la división de Identidad de Azure. Gloria se centra en ayudar a los

clientes a aumentar la postura de seguridad con la implementación de *Azure Active Directory*, soluciones híbridas basadas en la nube de Azure para proporcionar gestión de identidades.

Antes de unirse a Microsoft, Gloria era una ingeniera y arquitecta experimentada con más de 18 años de experiencia en las áreas de identidad, seguridad, implementación de servicios Microsoft O365, así como mensajería y colaboración. Anteriormente fue ponente en varios eventos, como la Conferencia *Microsoft Identity Driven Airlift* para socios, *GrayHat 2020* y la Cumbre de Seguridad de Texas. Además de la tecnología, le gusta pasar tiempo con sus hijos y su familia y viajar e ir a la caza de oportunidades.

Registro de cambios

Fecha	Cambio
28-02-2022	Se agregó una sección sobre dispositivos cliente; se agregó Gloria Lee como autora
19-04-2021	Cambio en la afiliación del autor
30-10-2020	V1 publicada