28/10/2025

Gestión de identidades: el nuevo perímetro de la ciberseguridad empresarial

La gestión de identidades es uno de los grandes ejes de la ciberseguridad. La realidad es la siguiente: la multiplicación de servicios en la nube, el auge del teletrabajo y la proliferación de identidades digitales están transformando por completo el perímetro de las organizaciones. Lo que se traduce en que los sistemas tradicionales de control de accesos, resultan insuficientes, y las compañías se ven obligadas a evolucionar hacia modelos más avanzados y centralizados.

Según Gartner, para 2026 más del 70% de las organizaciones habrán centralizado la gestión de accesos en soluciones IAM (Identity and Access Management), lo que refleja que el mercado está en plena transición hacia la madurez. Sin embargo, todavía tienen que enfrentarse al reto de la fragmentación de sistemas y a la complejidad de las infraestructuras digitales. En opinión de Ángel Núñez Simón, responsable de Identidad Digital de Accenture en España y Portugal, la estrategia actual "podría calificarse como en transición hacia la madurez", aunque aún existen carencias en la automatización del ciclo de vida de las identidades y en el control de credenciales no humanas.

Carla Roncato, vicepresidenta de Identidad de WatchGuard Technologies, coincide al afirmar que las compañías que se apoyan en Zero Trust avanzan más rápido. Roncato explica: "Las que han adoptado este enfoque reducen la superficie de ataque y habilitan experiencias seguras en cualquier lugar y momento, frente a aquellas que mantienen marcos de seguridad perimetral".

Por su parte, Álvaro Fernández, director de ventas en Iberia de Sophos, advierte de que todavía hay demasiados enfoques fragmentados. A su juicio, la mejora pasa por "consolidar la visibilidad y aplicar políticas consistentes en todo el ciclo de vida IAM, especialmente en entornos híbridos y multicloud".

En esta misma línea, Alfonso Ríos, Global Head of Digital Identity Solutions Business Development en Minsait, recuerda que muchas estrategias siguen a medio camino, "en general, las organizaciones cuentan con estrategias de gestión de identidades en desarrollo o implementadas parcialmente, lo que indica un nivel de madurez medio o bajo". El portavoz de Minsait señala que la automatización de altas y bajas de usuarios, la adopción generalizada de MFA y la simplificación de accesos mediante SSO siguen siendo grandes asignaturas pendientes.

Y es que, aunque las empresas reconocen la importancia estratégica de la gestión de identidades, «su estrategia actual es todavía reactiva y en una fase de transición compleja. Además, la fragmentación derivada de entornos multicloud dificulta la aplicación de políticas coherentes y rompe con el principio de mínimo privilegio", añade Ángel Serrano, Senior Manager en Palo Alto Networks.

La gestión de identidades como prioridad estratégica en ciberseguridad

La identidad digital se ha convertido en el nuevo perímetro de la seguridad empresarial. Un informe de Cybersecurity Ventures revela que los ataques basados en credenciales representan la principal vía de entrada en el 60% de las brechas de datos, lo que explica que cada vez más compañías consideren la gestión de identidades como un pilar estratégico.

Tal y como subraya Núñez, "para preservar la seguridad de una empresa es fundamental contar con un riguroso control de accesos", recordando además que normativas como NIS2, DORA o el propio RGPD han sido un motor clave en la adopción de soluciones IAM.

Por otro lado, Roncato recalca que "los ataques basados en credenciales representan el riesgo más grande, continuo y significativo

para las empresas en los últimos 15 años". A su juicio, resulta imprescindible que las organizaciones revisen de forma constante su postura de riesgo e incorporen monitorización continua.

Desde la visión de Fernández, "la gestión de identidades ya es uno de los pilares de la ciberseguridad. La rápida migración a la nube y la proliferación de APIs han multiplicado los permisos innecesarios o mal configurados, lo que obliga a las compañías a apoyarse en un marco sólido y coherente de gestión de accesos".

A esta valoración se suma Ríos, incidiendo en que "la mayoría de las brechas de seguridad actuales están relacionadas con identidades comprometidas". El directivo afirma que la transformación digital, la generalización del trabajo remoto, la presión normativa y la necesidad de garantizar experiencias seguras han situado la gestión de identidades como "una base imprescindible en cualquier estrategia moderna de ciberseguridad".

Por su parte, Serrano pone el acento en que la dispersión de datos y aplicaciones, junto con el auge del trabajo híbrido, ha hecho que IAM se consolide como una prioridad ineludible, "La identidad digital se ha convertido en el nuevo perímetro sobre el que se construyen tanto la seguridad moderna como la habilitación del negocio digital".

Robo de credenciales y suplantación de identidad: la primera causa de filtraciones

La suplantación de identidad continúa siendo la causa más frecuente de filtraciones de datos. Ante este panorama, las empresas han reforzado los mecanismos de autenticación y detección de amenazas. Desde Accenture, explican que "las compañías han adoptado medidas orientadas a reducir la dependencia de contraseñas tradicionales y aplicar controles adicionales de verificación". Entre ellas, mencionan mecanismos de MFA resistentes al phishing, tecnologías passwordless y planes de concienciación dirigidos a empleados.

Sin embargo, como advierten desde WatchGuard, la respuesta no siempre es proactiva: "En general, las empresas desconocen los factores de riesgo hasta que un enlace de phishing es clicado o se detecta un ataque de fuerza bruta".

Sophos apunta que MFA, SSO y detección de anomalías de inicio de sesión ya se están combinando con análisis de comportamiento en tiempo real, aplicando además el principio de privilegios mínimos.

Centralización y gobierno de identidades: del modelo fragmentado al descentralizado

La consultora Forrester señala que el 45% de los incidentes de acceso indebido se deben a duplicaciones e inconsistencias entre sistemas de identidad. Estos datos evidencian la necesidad de un gobierno unificado.

Sobre este punto, Núñez resalta la importancia de estándares como SAML, OAuth2 o OpenID Connect, que facilitan la federación de identidades, "la automatización del ciclo de vida y los modelos basados en roles han dotado de robustez al gobierno de identidades".

De forma complementaria, Roncato explica que los sistemas modernos tienden a ser descentralizados para minimizar el riesgo de un único punto de fallo, "la resolución de entidades es el proceso de eliminar duplicados y verificar qué identidad es la auténtica".

Para Javier San Juan, Blockchain Technology Sales Head de Var Group España, el futuro pasa por un esquema descentralizado (SSI), "donde cada persona disponga de una identidad única y verificable". San Juan cita como ejemplo proyectos en Ceuta o Andorra que ya permiten a los ciudadanos controlar sus credenciales y revocarlas cuando lo deseen.

En palabras de Fernández, los conectores nativos hacia aplicaciones SaaS y los directorios unificados han permitido "una mayor estandarización y reducción de silos, avanzando hacia un gobierno más coherente".

Automatización del ciclo de vida de las identidades: del aprovisionamiento al Just-In-Time

Un informe de Deloitte estima que el 60% de las brechas de seguridad ligadas a identidades están relacionadas con errores en la gestión manual de permisos y cuentas. La automatización del ciclo de vida de las identidades (ILM) se consolida así, como un requisito indispensable.

Para Ángel Núñez Simón de Accenture, la clave es integrar estas plataformas con RR. HH. y directorios corporativos para aprovisionar y desaprovisionar cuentas de manera automática, reduciendo riesgos de error humano. “El acceso Just-In-Time ha supuesto un avance significativo, ya que permite accesos temporales, limitados y bajo demanda, solo cuando son necesarios y por el tiempo estrictamente requerido”, sentencia.

En palabras de Carla Roncato, el acceso Just-In-Time y el modelo Just Enough Access son ya los dos principios clave en la gobernanza moderna, eliminando privilegios permanentes. Álvaro Fernández coincide y recalca que estos modelos “aportan un valor crítico al permitir accesos temporales, auditables y limitados en alcance”.

También Ángel Serrano recuerda que la automatización ha pasado de ser aspiración a capacidad esencial, “el aprovisionamiento y desprovisionamiento mediante estándares como SCIM y APIs garantiza que los accesos se actualicen de forma sincronizada en todas las aplicaciones, evitando cuentas huérfanas”.

Alfonso Ríos, Global Head of Digital Identity Solutions Business Development en Minsait, alerta de que muchas estrategias aún carecen de automatización plena en provisión y revocación, lo que “genera errores humanos y ralentiza procesos”.

Identidades no humanas: un reto que ya supera a las humanas

Según Gartner, para 2026 las identidades máquina (APIs, bots, certificados, servicios en la nube) superarán en más del doble a las humanas. Esta proliferación plantea un reto urgente en seguridad y gobierno. Desde Accenture, advierten: “Uno de los grandes riesgos es que persistan credenciales estáticas embebidas en código, tokens sin caducidad o contraseñas por defecto”.

Por otro lado, en WatchGuard, Roncato señala que muchas empresas aún confían en herramientas pensadas para usuarios humanos, que no sirven para identidades dinámicas y efímeras.

Siguiendo este esquema, en opinión de la compañía Sophos, la estrategia adecuada pasa por aplicar los mismos principios Zero Trust a identidades máquina, con vaults de secretos y rotación automática de claves.

En Minsait Cyber, coinciden en que “la clave de todo está en inventariar las identidades no humanas, aplicar gobernanza unificada, automatizar la gestión y aplicar principios de Zero Trust”.

Desde Palo Alto Networks añaden que la gestión de accesos privilegiados (PAM) será el gran diferencial, “IAM establece las bases, pero PAM garantiza el control real de accesos sensibles, especialmente en agentes de IA y entornos multicloud”.

Seguridad y experiencia de usuario: un equilibrio posible

Datos de McKinsey muestran que el 70% de los usuarios abandona un servicio digital si el proceso de autenticación es demasiado complejo. El desafío está en equilibrar seguridad robusta con accesos ágiles.

Para Núñez, el futuro se basa en que haya “una seguridad contextual, automatizada y transparente, donde el usuario apenas note que está siendo protegido”. En esta misma línea, Roncato defiende el uso de passkeys: “Son resistentes al phishing y preservan la privacidad, simplificando el inicio de sesión en múltiples plataformas”.

San Juan pone ejemplos prácticos de cómo en Ceuta y Andorra se eliminan contraseñas, validando identidad con un simple QR. Ríos añade que MFA adaptativo, SSO y autenticación biométrica son claves para ofrecer accesos intuitivos y fluidos sin renunciar a la seguridad. Mientras que Serrano subraya que el equilibrio se logra convirtiendo la seguridad en “un facilitador dinámico e inteligente, no en una barrera estática”.

Inteligencia artificial y analítica: la nueva guardia de la identidad

El auge de la IA está transformando la gestión de identidades. Según IDC, el 80% de las empresas planea usar IA para monitorizar accesos y detectar anomalías antes de 2026.

Núñez resalta que la IA analiza patrones en tiempo real y puede bloquear cuentas o generar alertas ante actividades sospechosas. Por su parte, Roncato observa que técnicas de machine learning ya ayudan en ITDR y en la evaluación de riesgos.

Además, Álvaro Fernández asegura que “la IA permite detectar accesos atípicos y ajustar políticas en tiempo real, reforzando la protección sin incrementar la carga administrativa”.

En palabras de Ríos, la IA convierte modelos estáticos en dinámicos, “pasa de un modelo reactivo a uno proactivo y adaptativo, detectando amenazas antes de que ocurran”. Lo mismo opina Serrano al resaltar que la IA es ya “aliado un indispensable”, capaz de aprender el comportamiento habitual de cada identidad y descubrir desviaciones que indicarían riesgo interno.

Cumplimiento normativo y privacidad: regulaciones que marcan el camino

El RGPD, la directiva NIS2 y la inminente eIDAS2 han elevado la exigencia en materia de identidades. Las organizaciones ya no solo deben asegurar accesos, sino también garantizar derechos y demostrar cumplimiento en auditorías.

Núñez apunta que “las organizaciones deben adaptarse a normativas que obligan a pedir consentimiento explícito y garantizar derechos como el de acceso o eliminación”.

Siguiendo este punto, Roncato recuerda que el enfoque debe ser “privacy & security by design”, con evidencias en tiempo real que permitan demostrar cumplimiento continuo.

Finalmente, Javier San Juan enfatiza que blockchain asegura “inmutabilidad y trazabilidad, facilitando la auditoría y reforzando la confianza”.

Fuente: https://revistabyte.es/

LINK DE LA NOTICIA