Riesgos de acceso no autorizado: los beneficios de una solución IAM

Cómo una empresa puede reducir sus riesgos de TI ocasionados por los derechos de acceso de los usuarios

_betasystems

Libro blanco

Introducción

Casi cada día, los medios de comunicación informan sobre incidentes referentes a la seguridad de los datos, desde el acceso no autorizado a datos de empresas hasta la pérdida de los mismos y el robo de identidades. Contra esta situación, los analistas más destacados (Gartner, KuppingerCole…) enfatizan cada vez más la importancia de llevar a cabo una gestión basada en riesgos. Sin embargo, ¿Cómo pueden las empresas reducir el riesgo empresarial causado por procesos de gestión de acceso inadecuados? ¿Y qué funciones debe proporcionar un sistema moderno de Identity Access Management (IAM) para que las empresas puedan cumplir al mismo tiempo sus requisitos crecientes de cumplimiento?

Beta Systems Software, la empresa de software con base en Berlín, subraya la importancia de llevar a cabo un método basado en el riesgo que implique a los departamentos de negocio así como a los equipos de seguridad de información y de TI en seis puntos de beneficios de reducción de riesgo.

1. Crear y mantener la visibilidad

Es crucial que las empresas tengan conocimiento sobre qué cuentas de usuario pertenecen a qué empleados y que dicha información se mantenga actualizada. Necesitan información instantánea referente a los derechos de acceso a sistemas esenciales como Active Directory, Lotus Notes, o SAP. Las funciones de Access Intelligence, integradas en la mayoría de soluciones IAM sofisticadas, permiten garantizar que se capturan y documentan todos los datos relacionados con el acceso (usuarios, roles, permisos del sistema, etc.). Estas funciones de supervisión, en los casos más extremos, pueden requerir que el historial de datos se grabe de manera continua, de modo que cualquier cambio que se realice, en el pasado o en tiempo real, se pueda identificar, rastrear y consultar fácilmente. De esta manera, las empresas pueden contestar a la pregunta “quién da acceso a qué recurso y cuándo” en cualquier momento. Por eso, las mejores soluciones contienen sistemas de flujo de trabajo para automatizar y rastrear las solicitudes de acceso y hacer que las auditorías sean más fáciles.

Los derechos de acceso también se deberían volver a certificar de forma regular para garantizar que los empleados tienen los permisos adecuados para su trabajo y que los que ya no trabajan en la empresa ya no tienen acceso a ningún sistema. En este contexto, es vital que la solución disponga de una interfaz gráfica para mejorar la facilidad de uso y el tiempo de familiarización.

2. Implicar a los departamentos de negocio

Las soluciones IAM actuales reconocen la importancia de que el personal de TI, los equipos de seguridad y los departamentos de negocio compartan la responsabilidad en la gestión de los derechos de acceso para reducir el riesgo de forma más eficaz. Los sistemas IAM avanzados unen las funciones de negocio y de TI – son fáciles de utilizar, están muy alineados con las necesidades de la empresa e integrados en estructuras de organización complejas. Al compartir estas tareas se facilita la administración y se reducen costes.

3. Aplicar segregación obligatoria de tareas

Para evitar infracciones de gobernanza, las empresas deberían asegurarse que ningún empleado tiene una acumulación de derechos de acceso que van más allá de lo que necesita para realizar su trabajo. Un elemento de riesgo en muchas compañías es que las funciones exclusivas no siempre resultan en derechos de acceso exclusivo recíprocamente. Las soluciones IAM avanzadas incluyen una segregación estricta de tareas (SOD) para minimizar estos riesgos.

4. Implementar una administración basada en roles y reglas

Agrupar las autorizaciones de acceso en base a los roles (RBAC - Role-Based Access Control) disminuye el riesgo inherente en la autorización manual. Cada decisión de acceso está basada en el rol vinculado al usuario. Los usuarios que tengan actividades similares se agruparán bajo el mismo rol. También puede formar una parte integral de las definiciones de rol de una empresa. Las soluciones IAM actuales incluyen permisos basados en roles y reglas que enlazan información técnica y de usuario de la empresa y tienen la flexibilidad para crear roles dinámicos y estáticos. Además, para fortalecer la seguridad, se contrastarán de forma automática los permisos de acceso al sistema y roles.

5. Facilitar el cumplimiento

Asegurar el cumplimiento de sistemas de información para cumplir obligaciones reglamentarias es un proceso complejo pero necesario. Para realizarlo correctamente, las organizaciones tienen que dar prioridad a los sistemas de gestión de acceso diseñados para adaptarse perfectamente a los estándares relevantes y estructuras y así facilitar las auditorías a la vez que se proporciona un nivel máximo de seguridad. En concreto, para cumplir más fácilmente con el estándar ISO 2700X, las organizaciones deberán utilizar una solución que incorpore pruebas de seguridad y procedimientos de auditoría dinámicos que sean acordes con los requisitos estándar. También se pueden definir procedimientos de comprobación y auditorías personalizadas para aplicar procedimientos y políticas internas de una empresa.

6. Apoyar procesos de gobernanza

Las empresas necesitan información sobre posibles riesgos de usuario para maximizar la eficacia de gobernanza. A través de informes dinámicos y una interfaz gráfica optimizada para permitir la manipulación de datos, el análisis inteligente de acceso de usuario hace posible identificar posibles puntos débiles y el nivel de riesgo asociado. Se debe incluir un gran número de informes estándar. Estos paneles también se pueden personalizar para proporcionar el nivel de detalle necesario, en base al uso que hacen de ellos los auditores internos y externos, los gestores de seguridad de TI o los altos directivos. Además, las organizaciones lo verán todo más fácil a la hora de asegurar que el acceso de sistemas se cumple si la solución permite que gestores que no son especialistas de TI (como auditores o altos directivos) realicen auditorías descentralizadas. Estas herramientas de análisis permiten una corrección rápida de errores de autorización, una mejor gobernanza y un riesgo reducido.

“Utilizar un método basado en riesgo en IAM ayuda a las empresas a analizar y solucionar áreas de posibles problemas de forma más rápida” comenta Niels von der Hude, Director de desarrollo de mercado de IAM en Beta Systems Software AG. “Las herramientas de IAM sofisticadas como SAM Enterprise Identity Manager y Garancy Access Intelligence Manager de Beta Systems facilitan la tarea de los gestores, auditores, personal TI y usuarios a contribuir a minimizar el riesgo en la empresa”.

Beta Systems ofrece apoyo y orientación a más de 1.300 clientes por todo el mundo para proporcionar seguridad para sus procesos de TI y por lo tanto, cumplir la gobernanza, los requisitos de cumplimiento (GRC) y la gestión de riesgo. Basándose en sus 20 años de experiencia en el campo de IAM, Beta Systems ofrece un grupo de software exhaustivo que trata la gestión de acceso a recursos de TI en base a las identidades de usuario y los roles.

Garancy Access Intelligence Manager es un sistema de inteligencia empresarial que proporciona análisis de auditoria y apoyo que se puede utilizar para ver el cumplimiento de los derechos de acceso otorgados a los usuarios y para evaluar los riesgos de acceso a través de informes estándar y personalizados.

SAM Business Process Workflow facilita la gestión del flujo de trabajo mediante la automatización de la certificación y recertificación de los usuarios y sus derechos de acceso. Esta solución, por lo tanto, hace posible aplicar reglas de gobernanza de TI.

SAM Enterprise Identity Manager es un sistema de aprovisionamiento potente que ofrece conexiones a más de 50 sistemas de destino y se puede utilizar para gestionar identidades y acceso a los recursos por todas las plataformas y aplicaciones.

Beta 88 Access Management ofrece administración, funciones de comprobación de cumplimiento y auditoria a través de interfaz web o de Windows y una supervisión en tiempo real de sucesos RACF a través del registro y análisis de datos SMF.

Beta 96 Compliance Auditor proporciona una auditoria dinámica de sistemas de información entre las diferentes plataformas para detectar y analizar sucesos críticos y ofrece comprobaciones en la seguridad de sistemas TI. La solución incluye pruebas de seguridad y procedimientos de auditoria que cumplen el estándar ISO 2700x.

Acerca de Beta Systems

Beta Systems fue fundada en 1983, cotiza en bolsa desde 1997 y cuenta con alrededor de 240 trabajadores. La sede de la compañía se encuentra en Berlín, Alemania.

La compañía, junto con sus 14 filiales, tiene un fuerte enfoque doméstico e internacional. Más de 1.300 clientes, en más de 30 países, ejecutan unas 3.200 soluciones para ayudarles a optimizar sus procesos TI. Beta Systems es uno de los principales proveedores de soluciones de software europeos independientes de tamaño medio que genera alrededor del 40% del volumen total de negocio en el mercado internacional.

Si desea obtener más información, consulte la página www.betasystems.es.

Contact us

marketing-f@betasystems.com

+34 9 13 07 76 75

Libro blanco - Marzo de 2016
Beta Systems Software España, S.L.