Informatica

Informe de la solución

Caso práctico: Análisis del comportamiento de SaaS para empresas

Ventajas principales

- Activar los procesos de negocio con una rápida y ágil gestión de los accesos
- Mejorar la seguridad de las vías de acceso a los datos sensibles y las autorizaciones relacionadas
- Eliminar la incertidumbre en torno a amenazas internas y concesiones de credenciales
- Centrar las respuestas y los esfuerzos de gobierno en reaccionar ante amenazas reales

Aumente la velocidad y la agilidad empresariales y refuerce al mismo tiempo la seguridad.

En el competitivo mercado actual, la velocidad, la agilidad, el acceso a la información y la disponibilidad de datos fiables para poder tomar decisiones rápidas pueden marcar la diferencia entre una empresa de éxito y una derrotada por la competencia. El tradicional modelo de compromiso de seguridad se centra en la implementación de sistemas seguros que satisfacen los requisitos de negocio. Sin embargo, las rápidas iteraciones de la demanda del mercado tras la puesta en marcha, ponen a prueba incluso al más ágil de los equipos de seguridad y crean tensiones entre la seguridad y el negocio.

Pero, entonces, ¿cómo puede un equipo de seguridad seguir el ritmo de los cambios naturales en los negocios sin perder de vista el respeto al principio de privilegio mínimo y el objetivo del control de acceso basado en funciones (RBAC)?

Con la funcionalidad de análisis de comportamiento de los usuarios (UBA) de Informatica Secure@Source, es posible aplicar los modelos de cumplimiento de acceso tradicionalmente utilizados por los administradores de TI, unos modelos que proporcionan a los propietarios de datos información y garantías sobre quién utiliza sus datos y cómo lo hace. Combinado con funciones de alertas y respuesta, el análisis UBA permite a los gestores y propietarios de datos gestionar y mitigar los riesgos inherentes a la concesión de credenciales y el abuso de privilegios.

Debido al uso de modelos familiares para los equipos de auditoría y cumplimiento, el análisis UBA permite que incluso los entornos altamente regulados se beneficien de un acceso rápido a la información que necesitan para mantener su competitividad, sin un impacto negativo sobre su postura respecto a la seguridad.

Cuantifique con precisión los riesgos asociados a los usuarios autorizados

Situación y oportunidad

Cuando el cambio empresarial es rápido, las preocupaciones sobre seguridad y accesos pueden ralentizar el cambio e impedir la habilitación de negocios. Esto puede llevar a la empresa a adoptar soluciones y realizar actividades de análisis o gestión de datos fuera del sistema de control principal.

Esto conlleva la dispersión del control de accesos, que es muy difícil de gestionar, impide saber quién tiene acceso a qué conjuntos de datos e imposibilita la detección de usos indebidos o abusos. Comprender cómo los procesos de negocio utilizan y exponen los datos es fundamental para mejorar los controles sin interrumpir las transacciones comerciales.

De la confluencia de los requisitos de velocidad y agilidad de la empresa, los requisitos normativos alrededor del acceso a datos y la necesidad de una posición conservadora por parte de los indicadores de cumplimiento, surge una oportunidad para las funcionalidades que pueden ofrecer garantías no solo relativas a los datos a los que pueden acceder los usuarios, sino también a lo que hacen con ellos.

Acerca de Informatica

La transformación digital está cambiando nuestro mundo. Como líderes en gestión de datos de cloud empresariales, le brindamos ayuda para que encabece la marcha de forma inteligente y aportamos perspectiva para que aumente su agilidad, concrete nuevas oportunidades de crecimiento o incluso invente cosas nuevas. Le invitamos a explorar todo lo que puede ofrecerle Informatica y a desatar el poder de los datos para impulsar su próxima revolución inteligente. Y no una vez, sino una tras otra.

Planteamiento y solución

Hemos descubierto que el análisis UBA proporciona seguridad relativa al acceso a los datos y mantiene la velocidad y la flexibilidad empresariales. En nuestro ejemplo interno, hemos examinado en primer lugar algunos procesos de negocio clave y luego hemos pasado al conjunto de datos, que cambió de una salida de fuente fidedigna al componente de informes y análisis. La evaluación de la actividad en el dominio de datos, y no exclusivamente en una aplicación, proporciona un contexto más amplio sobre las actividades del conjunto de datos y una mayor seguridad sobre los límites de uso de los datos. No definimos de antemano los casos de acceso de usuarios. En su lugar, mantuvimos la protección y la responsabilidad mediante la supervisión de las acciones de usuario facilitada por la detección de anomalías y las funcionalidades de elaboración de informes.

La detección y las alertas, por sí solas, no pueden reducir los riesgos sin una acción rápida por parte de los usuarios, los propietarios de datos y la administración. Es necesario incluir en el proceso, cuanto antes, a los propietarios de datos y los jefes de equipo. Tienen que asumir la responsabilidad de las consecuencias de los riesgos del acceso a sus datos, y la mejor manera de lograrlo pasa por demostrar los riesgos (o posibles riesgos) desde el punto de vista de los datos. En la mayoría de los casos, los propietarios y administradores de datos no disponen de información sencilla y accesible sobre el acceso a los datos y los patrones de uso. Un bucle de aprendizaje entre los usuarios, la administración y los propietarios de los datos destaca los patrones de uso y los comportamientos aceptables, además de alentar la adopción de patrones responsables.

Hay muchas similitudes entre este modelo y el modelo de acceso “romper el cristal” que utilizan normalmente los administradores de sistemas confidenciales que necesitan infringir la separación de controles de tareas durante el mantenimiento y la solución de problemas. El administrador tiene los permisos adecuados para completar las atribuciones de su función. Los accesos con privilegios elevados generan una revisión para garantizar que todas las acciones han sido autorizadas. La utilización del aprendizaje automático permite que este modelo, que cuenta con la aprobación de los auditores, escale y cubra a toda la organización.

Un programa exitoso debe centrarse, en primer lugar, en optimizar el modelo de respuesta orientado a la acción, a fin de reaccionar ante comportamientos de los usuarios y anomalías. A continuación, debe ampliarse para incluir los procesos de negocio críticos, que requieren velocidad/agilidad o que presentan riesgos significativos para los objetivos de la organización.

Conclusión

Las funcionalidades de aprendizaje automatizado de Secure@Source proporcionan un nivel de fiabilidad inalcanzable a través de la revisión manual, y el resultado es una mayor coordinación entre las concesiones de acceso y el uso de datos.

UBA se integra naturalmente con los modelos de propiedad de datos para establecer un factor formal e impulsar la protección y gestión de los datos por parte de sus propietarios. A través de programas de sensibilización, de la formación específica y de la corrección de procesos, el análisis UBA puede impulsar mejoras y cambios en los procesos para que la organización se mantenga en consonancia con los objetivos de cumplimiento por muy rápido que sea su crecimiento.

Dado que el análisis UBA no está sujeto a una aplicación o plataforma específicas, se puede utilizar en distintas aplicaciones para proteger un ecosistema de datos en su totalidad, en lugar de centrarse exclusivamente en un sistema de origen y dejar de lado los sistemas de elaboración de informes.

El análisis UBA de Informatica Secure@Source impulsa la velocidad y la agilidad de la empresa, además de apoyar los objetivos de seguridad y cumplimiento al incluir a los propietarios de datos y a la administración en el proceso de respuesta.

Informatica

Informatica en España: José Echegaray 8, edif. 3, PB 3, 28232 Las Rozas, Madrid. Teléfono: +34 91 787 61 40 Fax: 933 714 895.
www.informatica.com/es linkedin.com/company/informatica twitter.com/Informatica

IN17_0617_3339