Informatica

White paper

Seguridad centrada en los datos para un mundo híbrido

Cumplimiento del Reglamento General de Protección de Datos en entornos locales y cloud

Acerca de Informatica

La transformación digital modifica las expectativas: mejor servicio, entrega más rápida, menores costes. Los negocios deben transformarse para seguir siendo relevantes y los datos tienen la respuesta.

Como líder mundial en gestión de datos de cloud empresariales, le brindamos ayuda para que encabece la marcha de forma inteligente, en cualquier sector, categoría o nicho. Informatica le aporta perspectiva para que aumente su agilidad, concrete nuevas oportunidades de crecimiento o incluso invente cosas nuevas. Al estar completamente centrados en todo lo relacionado con los datos, ofrecemos la versatilidad necesaria para alcanzar el éxito.

Le invitamos a explorar todo lo que puede ofrecerle Informatica y a desatar el poder de los datos para impulsar su próxima disrupción inteligente.

Contenidos

Resumen ejecutivo

La mayoría de las organizaciones actuales almacenan información confidencial de los clientes, productos y otros aspectos en un número cada vez mayor de plataformas y ubicaciones físicas en todo el mundo. Estos datos críticos para el negocio suelen encontrarse en un cloud público, de manera local y en aplicaciones de software como servicio (SaaS). Con Informatica Intelligent Cloud Services™, por ejemplo, Informatica brinda una infraestructura de seguridad en forma de centros de datos de failover, autenticación de usuarios y control de acceso, protocolos de seguridad de red, cifrado y capas de seguridad en el sistema operativo, en la base de datos y en la aplicación.[1]

Los entornos híbridos plantean nuevos retos a los equipos de seguridad y cumplimiento de datos. La naturaleza dinámica de los datos, los usuarios y las aplicaciones requiere medidas adicionales para garantizar constantemente el registro, la legibilidad y la protección de los datos críticos de la organización. Los riesgos no son hipotéticos, tal como demuestran las filtraciones locales y en cloud de alto perfil y las sanciones impuestas por el Reglamento General de Protección de Datos.

En estos entornos híbridos dinámicos, necesita inteligencia y automatización para garantizar constantemente el cumplimiento y la protección de los datos, así como la capacidad de responder preguntas como las siguientes:

- ¿Dónde se encuentran los datos que necesitan protección?
- ¿Quién está accediendo a los datos y con qué aplicaciones?
- ¿Se ajustan el acceso y el uso actuales a los reglamentos y a las políticas de uso de los datos?
- ¿Es apropiada la protección de los datos? ¿Se mantiene el riesgo de los datos dentro de unos niveles aceptables? ¿Existen condiciones de riesgo que puedan solucionarse?

Los resultados de la detección y la clasificación de datos sensibles son la base para tomar decisiones relacionadas con el riesgo de los datos, la seguridad y el cumplimiento en un ecosistema de datos híbrido. Este documento brinda una serie de consideraciones en materia de seguridad y estrategias para entornos híbridos con un enfoque centrado en los datos que permita lo siguiente:

- Aplicar análisis, automatización e inteligencia artificial (IA) para identificar y proteger datos sensibles procedentes de todas las fuentes en un entorno híbrido utilizando una única interfaz para los cuadros de mando e informes.
- Cumplir con los nuevos reglamentos de seguridad y gobierno de datos.
- Preparar la infraestructura para una auditoría.
- Avisar a los usuarios clave en caso de que se produzca un comportamiento anómalo.

Informatica Data Masking e Informatica Secure@Source® proporcionan capacidades excepcionales para desempeñar estas funciones e incorporan una capa de seguridad centrada en los datos integrada para todas las fuentes de datos sensibles en un ecosistema híbrido.

[1] Monahan, David, "Información general sobre la arquitectura de seguridad en cloud de Informatica", Enterprise Management Associates (EMA), marzo de 2016.

Seguridad de los datos para su realidad híbrida

Según la empresa de investigación IDC, se prevé que el mundo generará 180 zettabytes de datos en 2025, una cantidad mucho mayor que los 10 zettabytes generados en 2015.[2] Organizaciones de todos los sectores confían en la precisión, la disponibilidad y la seguridad de sus datos para generar ingresos, atender a los clientes, aumentar la productividad y respaldar otros procesos empresariales de misión crítica.

El continuo crecimiento exponencial del volumen de datos y su uso también incluye datos sensibles en varios silos, tanto en entornos locales como en el cloud, y en diversos formatos. Estas condiciones han hecho que los métodos tradicionales de protección de los datos sean obsoletos, lo que exige un nuevo enfoque para la seguridad de los datos en toda la organización.[3]

También existe una fuerte tendencia en la que un gran porcentaje de los datos que utiliza una organización procede de fuentes externas. Es fundamental comprender la sensibilidad de estos datos en el momento en el que se integran en la organización y antes de transferirlos a los diversos sistemas y de usarlos en análisis. Sin embargo, la mayoría de las empresas no pueden identificar con exactitud el lugar donde se encuentran los datos sensibles, sobre todo si emplean formatos no estructurados o varias aplicaciones locales y en cloud, bases de datos relacionales, dispositivos de data warehouse y fuentes de big data. Este desconocimiento aumenta el riesgo de la organización y, por estas razones, las filtraciones de datos constituyen en la actualidad el principal riesgo de seguridad de IT.[4]

Con un panorama en el que las filtraciones de datos son cada vez más frecuentes y ante la proliferación de los datos sensibles, las organizaciones deben desarrollar una estrategia de mitigación de riesgos que incluya un producto de seguridad centrado en los datos con estas características clave:

- Visibilidad de todas las fuentes de datos para localizar y clasificar datos sensibles de toda la organización.
- Capacidad para implementar los mecanismos de protección de los datos sensibles para mitigar las filtraciones.
- Cumplimiento de los reglamentos vigentes en materia de privacidad y seguridad de los datos, así como el uso de la automatización y la inteligencia artificial para supervisar el comportamiento de los usuarios y comunicar anomalías prácticamente en tiempo real.
- Exhaustivas herramientas de visualización analítica para la gestión de datos sensibles.
- Capacidades transparentes y sólidas de generación de informes para prepararse ante una auditoría.

Gartner prevé que, para 2020, los productos de protección y auditoría centrados en los datos reemplazarán las diversas herramientas de seguridad de datos en silos en un 40 % de las grandes empresas, mucho más que el 5 % actual.[5] Estas soluciones de protección centradas en los datos, como Informatica Data Masking e Informatica Secure@Source, ofrecen una vista centralizada de datos en riesgo para que todos los usuarios clave de la organización puedan controlar el movimiento de los datos sensibles y aplicar mecanismos de protección según lo estipulado en los reglamentos y políticas de gobierno.

[2] "2016 IoT Midyear Review – The Report Card for Everyone", IDC, 4 de agosto de 2016.
[3] "Market Guide for Data-Centric Audit and Protection", Gartner, 21 de marzo de 2017.
[4] "Data Breaches and Sensitive Data Risk", Ponemon Institute, febrero de 2016.
[5] "Market Guide for Data-Centric Audit and Protection", Gartner, 21 de marzo de 2017.

Estrategia basada en cuatro puntos para proteger los datos sensibles

El riesgo de los datos sensibles hace referencia a las consecuencias que tiene la pérdida de los datos sensibles. La causa principal de esta pérdida es una filtración de datos. Existe la creencia equivocada de que este riesgo se mitiga solamente determinando la ubicación de los datos sensibles. Sin embargo, la localización y la clasificación de estos datos es solo el primer paso de una exhaustiva estrategia para mitigar el riesgo.

Otros pasos son la evaluación del riesgo de la organización en función de los resultados del análisis de la localización y la clasificación, y la determinación de una estrategia para reducir el riesgo que implique a todos los usuarios clave y no solo a la organización de IT; esta estrategia debe contemplar controles automatizados que apliquen políticas de gobierno de datos. La estrategia debe incluir también la adquisición e implementación de un producto de seguridad robusto centrado en los datos que proporcione capacidades para el cumplimiento de las normativas, visualización analítica completa de datos sensibles para cuadros de mando e informes de auditoría, y protección para todo tipo de datos sensibles de la organización. El producto de seguridad centrado en los datos elegido debe proteger también los datos sensibles de todas las fuentes del entorno híbrido: cloud público, aplicaciones SaaS, bases de datos y aplicaciones locales, datos no estructurados y dispositivos de data warehouse.

1. Detección y clasificación

Una estrategia común para la detección consiste en revisar las fuentes existentes y enviar cuestionarios. Sin embargo, este enfoque es demasiado manual e inadecuado, ya que consume mucho tiempo y muchos recursos valiosos, y suele resultar impreciso y obsoleto. Se basa en informes propios en lugar de supervisar el comportamiento real de los usuarios.

Las organizaciones deben plantearse estas cuestiones:

- ¿Qué datos almacenamos? ¿Quién tiene acceso a los datos? ¿Con qué objetivo acceden?
- ¿Cómo podemos administrar los privilegios de usuario y los derechos sobre los datos?
- ¿Cómo vamos a proteger los datos sensibles y a garantizar la aplicación de unos controles apropiados?

Otras consideraciones relacionadas con el cumplimiento de la detección y la clasificación son:

- Definir y comprender el panorama de los datos (incluidos los datos no estructurados, las aplicaciones y las bases de datos en entornos locales y en cloud).
- Elaborar un plan para gestionar externamente los datos obtenidos.
- Determinar los sistemas en los que se usarán datos sensibles.
- Adquirir una solución que puede determinar el movimiento de los datos por el ecosistema a la vez que se mantiene una vista casi en tiempo real con análisis y herramientas de elaboración de informes.

2. Cumplimiento

Las organizaciones se esfuerzan por identificar, supervisar y mitigar los riesgos relacionados con los reglamentos de seguridad y privacidad de datos. Además, deben supervisar, analizar y avisar sobre el acceso o el movimiento de los datos que puedan poner en peligro el cumplimiento.

El Reglamento General de Protección de Datos, en vigor desde el 25 de mayo de 2018, se adoptó con el objetivo de reforzar y unificar la protección de los datos de todos los habitantes de la Unión Europea. De esta forma, se simplificaría el entorno normativo para el entorno empresarial internacional. Muchas empresas aún no se han preparado para este reglamento y no lo cumplen de manera eficaz. No obstante, su incumplimiento acarrea importantes sanciones y el desprestigio de la entidad. Por otro lado, el cumplimiento puede marcar la diferencia en la seguridad y la privacidad de los datos sensibles, lo cual puede suponer una ventaja competitiva. También puede mejorar los resultados de la transformación digital basada en datos.

Las organizaciones deben desarrollar políticas inteligentes que identifiquen los almacenes de datos que contengan dominios de datos relevantes para el Reglamento General de Protección de Datos. Estas políticas atienden a varios factores y su lógica determina las combinaciones que suponen una amenaza para la privacidad.

3. Protección

En 2017, se produjeron 1120 filtraciones de datos que pusieron en riesgo aproximadamente 171 millones de registros.[6] Es evidente que, a pesar de las importantes inversiones en seguridad a nivel infraestructural, los datos críticos siguen siendo vulnerables. Las organizaciones necesitan proteger constantemente los datos de alto riesgo, identificar comportamientos sospechosos y el uso o el movimiento no autorizado de datos críticos, y automatizar y organizar las correcciones.

Las organizaciones deben identificar los riesgos de los datos críticos y corregirlos con controles centrados en los datos (en lugar de recurrir a las herramientas clásicas de ciberseguridad). Estos controles incluyen, por ejemplo, soluciones de cifrado y de enmascaramiento de datos. Además, las organizaciones deben controlar el acceso y el comportamiento de los usuarios. Un acceso excesivo a los datos o un comportamiento atípico pueden indicar que los usuarios no están respetando las políticas de privacidad o que se ha producido un robo de credenciales.

4. Preparación para una auditoría y respuesta

Ahora, las empresas se someten a muchas más auditorías y evaluaciones de datos sensibles que antes. Se afanan por demostrar a los auditores de que tienen visibilidad sobre los datos críticos y que los protegen.

Las organizaciones deben ser capaces de responder de forma inmediata a los auditores y de demostrar que saben dónde se encuentran los datos, los riesgos a los que están expuestos los datos, cómo se protegen los datos y cómo se están utilizando. Deben considerar que los auditores pueden requerir informes y vistas resumidas de departamentos o ubicaciones y que permitan examinar dominios de datos específicos.

[6] "2016 Data Breach Category Summary", Identity Theft Resource Center, 31 de diciembre de 2016.

Conclusión

Se necesitan protocolos de seguridad infraestructural de alto nivel para proteger cualquier entorno híbrido que transmita datos confidenciales a usuarios, servidores de centros de datos de todo el mundo y aplicaciones en cloud. La constante arremetida de las filtraciones de datos y el aumento de los requisitos de cumplimiento obligan a las organizaciones a implementar unas herramientas y unos procesos adecuados para identificar, analizar y proteger datos sensibles.

Ante el panorama actual en el que existe un mayor riesgo para la seguridad y donde las filtraciones de datos son frecuentes, las empresas deben desarrollar una estrategia de seguridad digital robusta para supervisar, analizar y corregir constantemente los riesgos a los que se exponen los datos sensibles. Deben supervisar los datos casi en tiempo real para detectar indicios de uso indebido o filtración, un número excesivo de accesos, un comportamiento atípico o transferencias internacionales. Con las soluciones de seguridad centradas en los datos, como Informatica Data Masking e Informatica Secure@Source, las organizaciones pueden mejorar su postura ante los riesgos para mitigar el impacto de las filtraciones de datos o del uso indebido interno, así como para satisfacer los requisitos cada vez más exigentes de los reglamentos industriales y regionales.

Recomendaciones

1. Realice una evaluación de riesgos para conocer exactamente dónde se encuentran los datos sensibles, hasta dónde se propagan en su ecosistema de datos y que conjuntos de datos sensibles son más vulnerables.
2. Atendiendo a los resultados de la evaluación, otorgue prioridad a las diez fuentes más importantes de la organización con los datos más sensibles; determine una estrategia y un producto para protegerlos; y aplique la estrategia para la seguridad de los datos.
3. Defina, documente y distribuya las políticas de cumplimiento de la organización y los usuarios clave responsables del cumplimiento del Reglamento General de Protección de Datos. Elabore un plan estratégico para mayo de 2018 y de cara al futuro.

Más información

Para obtener más información acerca de los riesgos de seguridad de los datos sensibles y las consideraciones acerca de la protección, consulte las siguientes publicaciones:

- "Detect and Protect: A Data-Centric Approach to Security", Informatica, abril de 2017.
- "Data Breaches and Sensitive Data Risk", Ponemon Institute, febrero de 2016.

Informatica

Informatica en España José Echegaray 8, edif. 3, PB 3, 28232 Las Rozas, Madrid Teléfono: +34 91 787 61 40, +34 91 787 61 40

IN09_0418_03429