Proteja la privacidad de los datos confidenciales en entornos externos a la producción

IBM Information Management Software

IBM Optim Data Privacy Solution for Siebel Customer Relationship Management

Aspectos destacados

- ***Proteja la privacidad mediante la desidentificación de los datos confidenciales en entornos externos a la producción***
- ***Sustituya los datos confidenciales por valores ficticios y genere resultados precisos en las pruebas***
- ***Aplique técnicas de enmascaramiento de datos compatibles con las aplicaciones que conserven la integridad de los datos***
- ***Aproveche las rutinas de serie para enmascarar números de tarjetas de crédito, identificadores y direcciones de correo electrónico***
- ***Compatibilidad con las normativas de conformidad y los estándares de dirección corporativa***

Asegure la conformidad de la privacidad: cumpla la ley

La opción de proteger la privacidad de los datos de identificación personal no es una cuestión voluntaria, es un aspecto regulado por la ley. Como en todas las empresas, las instalaciones de Siebel® en todo el mundo están sujetas a normativas gubernamentales promulgadas para evitar el uso indebido de la información personal. Por ejemplo, la Unión Europea ha establecido la Directiva de protección de datos personales como marco de regulación de la protección de la privacidad en sus países miembros. En Canadá, las organizaciones siguen las directrices de la Ley de protección de la información personal y los documentos electrónicos (PIPEDA - *Personal Information Protection and Electronic Documents Act*), mientras que las empresas australianas están sujetas a la Enmienda a la Privacidad (*Privacy Amendment Act*). En los Estados Unidos, se aplican múltiples normativas a nivel nacional y estatal, y existen estatutos y leyes similares en todo el mundo.

Además, algunas alianzas empresariales están desarrollando estándares de dirección específicos por sectores. Por ejemplo, el estándar de seguridad de los datos del sector de las tarjetas de crédito (PCI DSS – *Payment Card Industry Data Security Standard*), iniciado por Visa® y MasterCard®, está siendo adoptado por otras empresas de tarjetas de crédito como respuesta a la creciente presencia de casos de fraude y robo de datos. El estándar requiere que los miembros, los comerciantes y los proveedores de servicios apliquen 12 criterios de salvaguarda de la seguridad para la protección de los datos de los propietarios de las tarjetas. En particular, el requisito 6.3.4 del estándar PCI indica que las bases de datos de prueba no deben contener números de cuenta personales (PAN) que provengan de datos de producción.

Las infracciones de la privacidad aumentan el riesgo y los costes

Las instalaciones de Siebel procesan muchos tipos de datos confidenciales durante las operaciones diarias. Por ejemplo, además de los números de identificación del cliente, los nombres, las direcciones y los números de teléfono, otro tipo de información de identificación personal puede incluir fechas de nacimiento, números de documentos de identidad, (DNI, pasaporte, seguridad social), números de

cuentas bancarias, números de tarjetas de crédito y direcciones de correo electrónico.

Las sanciones derivadas de la no protección de la información de identificación personal pueden ser muy elevadas. Las empresas y sus directivos deberían afrontar no sólo penas de cárcel, sino multas que en los Estados Unidos podrían superar los 100.000 dólares por incidencia. En este mismo país, por ejemplo, la Comisión de comercio federal (*Federal Trade Commission*) multó a ChoicePoint con 15 millones de dólares por vender datos confidenciales de sus clientes a terceros. De forma similar, en el Reino Unido la empresa Capital Financial Administrators (CFA) recibió una multa de 300.000 libras esterlinas por parte de la Autoridad de los servicios financieros (FSA - *Financial Services Authority*) por los errores de sus controles y sistemas antifraude que permitieron la realización de solicitudes de pago fraudulentas en cuentas de sus clientes.

La protección de la privacidad de los clientes genera confianza pública y sencillamente aporta un sentido empresarial correcto. Una única infracción de las normas de privacidad puede ser suficiente para que un cliente deje de hacer negocios con su empresa. Sin unos controles correctos para proteger la privacidad, el riesgo de una intromisión en sus datos aumenta de forma significativa.

Entre las consecuencias se incluyen, entre otras cosas, la pérdida de cuota de mercado, daños en la percepción de la marca, erosión de la fidelidad del cliente y pérdidas de ingresos; aspectos que en definitiva pueden hacer que sus operaciones queden fuera del mercado.

Las instalaciones de Siebel reconocen que la protección de la privacidad de los datos a lo largo de todo el parque de sistemas es esencial para obtener la confianza de los clientes y los Business Partners. Pero deben afrontar muchos retos en sus esfuerzos para gestionar con éxito la información de identificación personal, especialmente debido al hecho de que traspasa los límites del sistema de procesamiento de transacciones seguras.

La protección de los datos personales presenta retos importantes

La mayoría de instalaciones gestionan diversas instancias de producción de sus aplicaciones Siebel CRM. Una empresa que ejecute Siebel Contact Center and Service, por ejemplo, puede desplegar diversas instancias para conseguir la compatibilidad con sus operaciones en Norteamérica, EMEA y Asia-Pacífico. Para dar soporte al desarrollo de aplicaciones, las pruebas, la formación, la copia de seguridad y otras actividades, una instalación puede gestionar en cualquier lugar entre 3 y 30 clones de cada instancia, que contengan una réplica exacta de los datos confidenciales del sistema de origen.

Las instalaciones de Siebel protegen la información privada en sus sistemas de procesamiento de transacciones de producción, asegurando y restringiendo el acceso a los datos subyacentes mediante el uso de autorizaciones. Unos controles estrictos y unas interfaces diseñadas cuidadosamente presentan una vista gestionada.

Desgraciadamente, no resulta tan sencillo proteger los datos privados una vez han sido copiados en entornos externos a la producción (desarrollo, pruebas y formación), en los cuales los controles de acceso están menos restringidos.

De hecho, los expertos en privacidad mantienen que tanto el personal, como los desarrolladores de aplicaciones o los verificadores de productos, no deberían tener ningún tipo de acceso a la información de identificación personal. Por otro lado, los desarrolladores y los verificadores necesitan unos requisitos exclusivos para interactuar con los datos de Siebel. Específicamente requieren disponer de un acceso a los datos válidos para poder probar y desplegar de forma precisa sus aplicaciones Siebel.

Por todo ello, los métodos de control de acceso y las vistas gestionadas utilizadas para proteger los datos de producción simplemente no funcionan para el desarrollo y las pruebas. Pero el uso de datos reales podría comportar violaciones de la privacidad o intrusiones en los datos. Para resolver esta paradoja, las instalaciones de Siebel necesitan un enfoque alternativo.

Técnicas eficaces para el enmascaramiento de los datos

La desidentificación de los datos es el proceso de enmascaramiento o transformación de los datos confidenciales, de tal modo que puedan utilizarse con seguridad para el desarrollo de aplicaciones, las pruebas y la formación. La información de identificación personal se elimina de la base de datos. Se aplican algoritmos de transformación para crear datos ficticios pero adecuados al contexto, y esta información sirve para sustituir los datos originales

Como práctica recomendable reconocida, la desidentificación de los datos proporciona la forma más eficaz de proteger la privacidad y buscar la compatibilidad con las iniciativas de conformidad.

Los datos enmascarados o transformados son válidos y pueden utilizarse para las pruebas o la formación.

IBM® Optim™ Data Privacy Solution for Siebel® Customer Relationship Management ofrece unas capacidades integrales comprobadas para la desidentificación de los datos de prueba, adecuando los datos a las necesidades de las pruebas, pero a la vez evitando que puedan ser identificados por posibles delincuentes o piratas informáticos. Las capacidades de Optim de enmascaramiento de los datos compatible con las aplicaciones reconoce, captura y procesa los elementos de datos de Siebel de tal manera que los datos enmascarados no infringen la lógica de la aplicación. Los valores enmascarados mantienen la percepción y el aspecto de la información original.

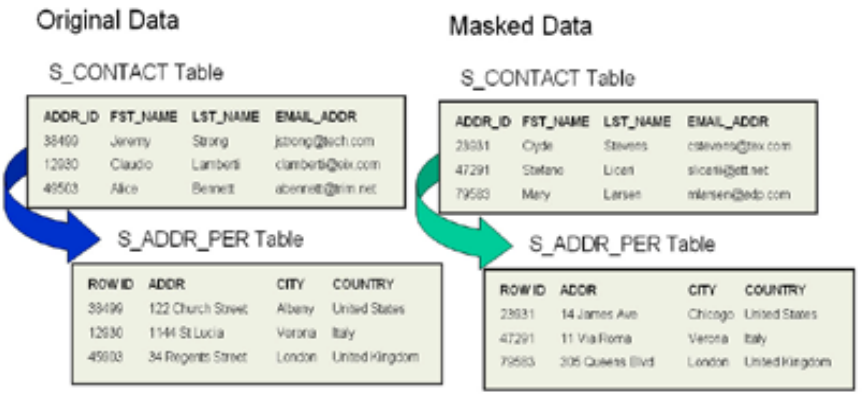

Figura 1. La capacidad de propagación de claves de Optim ayuda a conservar la integridad referencial, incluso cuando los datos están enmascarados.

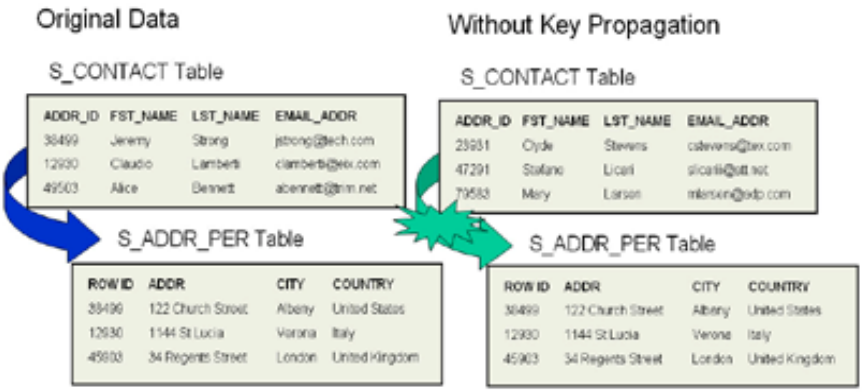

Figura 2. Sin una capacidad de propagación de claves, las relaciones entre los datos fundamentales se romperían

Por ejemplo, los apellidos específicos de una cultura determinada se sustituyen por apellidos similares seleccionados en bases de datos de búsqueda propias, no por series de texto sin sentido. Los campos numéricos mantienen su patrón y su estructura adecuados.

Las sumas de comprobación siguen siendo válidas, de tal forma que las pruebas funcionales pasan todas las comprobaciones de validez. Y lo que es más importante, Optim propaga todos los elementos de datos enmascarados de forma precisa y coherente a lo largo de las bases de datos de prueba de Siebel, y a otras aplicaciones y bases de datos relacionadas.

Optim proporciona unas capacidades sofisticadas, incluyendo unas tablas de búsqueda incorporadas para enmascarar nombres y direcciones. Las rutinas de serie permiten una transformación precisa de elementos de datos complejos, como números de la seguridad social, números de tarjetas de crédito y direcciones de correo electrónico.

Puede incorporar también rutinas de transformación específicas de cada ubicación, integrando la lógica de procesamiento de múltiples bases de datos y aplicaciones relacionadas.

Optim proporciona una solución de gestión centralizada de los datos que permite la redimensión para cubrir las necesidades empresariales, compatible con las aplicaciones comerciales estándar y las personalizadas. Es compatible también con todos los sistemas operativos y las bases de datos principales: IBM DB2®, Oracle®, Sybase®, Microsoft® SQL Server®, IBM Informix®, IBM IMS™, IBM VSAM®, Microsoft Windows®, UNIX®, Linux® e IBM z/OS®.

Acerca de IBM Optim

La solución de gestión de datos empresariales IBM® Optim™ se centra en los problemas más importantes para las empresas, como la gestión del crecimiento de los datos, la privacidad de los datos, la conformidad, la gestión de los datos de prueba, el e-discovery, las actualizaciones de las aplicaciones, la migración y las retiradas de productos.

Optim pone al mismo nivel la gestión de los datos de las aplicaciones y los objetivos empresariales, para ayudarle a optimizar el rendimiento, a mitigar los riesgos y a controlar los costes, proporcionando a la vez unas capacidades que permiten la redimensión en las distintas plataformas, bases de datos y aplicaciones empresariales. En la actualidad, Optim ayuda a las empresas de todos los sectores a nivel mundial a capitalizar el valor empresarial de sus bases de datos y aplicaciones empresariales, con la capacidad de gestionar datos de estas aplicaciones a lo largo de cada fase de su ciclo de vida.

Información adicional

Para obtener más información acerca de las soluciones de gestión de datos empresariales IBM Optim, póngase en contacto con su representante de ventas de IBM o visite la dirección: **www.optimsolution.com.**

IBM Software Group
111 Campus Drive
Princeton, NJ 08540-6400
USA
www.optimsolution.com

Producido en EE.UU.
Mayo de 2005

ORACLE CERTIFIED ADVANTAGE PARTNER
SIEBEL CUSTOMER RELATIONSHIP MANAGEMENT

IMS14032-USEN-00