IBM Optim Data Privacy Solution for SAP

Highlights

- ***Effizienter Datenschutz durch Deidentifizierung vertraulicher Daten auch außerhalb von Produktionsumgebungen***
- ***Austausch gültiger fiktionalisierter Werte für vertrauliche Daten und Generierung präziser Testergebnisse***
- ***Anwendungsorientierte Datenmaskierungstechniken für hohe Anwendungsintegrität***
- ***Vordefinierte Routinen zur Maskierung von Kreditkartennummern, Kennungen und E-Mail-Adressen***
- ***Einhaltung von Datenschutzrichtlinien und unternehmensweiten Governancestandards***

Einhaltung der vom Gesetzgeber vorgegebenen Datenschutzrichtlinien

Der Schutz von personenbezogenen Daten ist keine Option, sondern wird vom Gesetzgeber vorgeschrieben. Wie viele andere Unternehmen unterliegen auch die Standorte von SAP-Kunden weltweit den gesetzlichen Bestimmungen zum Schutz solcher Daten. Die Europäische Union beispielsweise hat mit seiner Personal Data Protection Directive für alle Mitgliedsländer ein umfassendes Gerüst für den Datenschutz geschaffen. In Kanada gelten für Unternehmen die Richtlinien des PIPEDA (Personal Information Protection and Electronic Documents Act) und in Australien die des Privacy Amendment Act. In den USA wiederum finden verschiedene Regelungen auf nationaler und bundesstaatlicher Ebene Anwendung. Weltweit gibt es also diesbezüglich durchaus vergleichbare Gesetzgebungen.

Hinzu kommen branchenspezifische Governancestandards, die von qualifizierten Gremien in den jeweiligen Branchen ausgearbeitet wurden. Der Payment Card Industry Data Security Standard (PCI DSS) beispielsweise, der von Visa und MasterCard initiiert wurde, wird auch von anderen Zahlungskartenunternehmen übernommen, um den zunehmenden Delikten wie Datendiebstahl und Betrug vorzubeugen. Bei diesem Standard müssen die Mitglieder, Händler und Serviceanbieter zwölf Sicherheitsrichtlinien zum Schutz der Karteninhaberdaten anwenden. So besagt PCI-Anforderung 6.3.4, dass Testdatenbanken keine PANs (persönliche Kontennummern) aus den Produktionsdaten enthalten dürfen.

An SAP-Kundenstandorten werden im täglichen Betrieb die unterschiedlichsten vertraulichen Daten verarbeitet. Zum Beispiel werden Mitarbeiterdaten im Zusammenhang mit Arbeitgeberleistungen und Lohnbuchhaltung über SAP Human Capital Management (HCM) verarbeitet. Neben den Kennungen, Namen, Adressen und Telefonnummern von Mitarbeitern gehören auch Angaben wie Geburtsdatum, Sozialversicherungsnummer, Bankkontonummer, Arbeitgeberleistungen, Krankenversicherungsnummer usw. zu den personenbezogenen Daten.

Hohe Risiken und Kosten durch Datenschutzverletzungen

Die Strafen bei Nichteinhaltung der Datenschutzrichtlinien für personenbezogene Daten können sehr gravierend sein. Für Unternehmen und deren Führungskräfte kann dies neben Haftstrafen auch hohe Geldstrafen nach sich ziehen. In den USA beispielsweise verurteilte die Federal Trade Commission das Unternehmen ChoicePoint zu einer Zahlung von 15 Mio. US-Dollar wegen des Verkaufs von vertraulichen Kundendaten an Dritte. In Großbritannien wurden CFAs (Capital Financial Administrator) von der britischen Financial Services Authority (FSA) zu einer Strafe in Höhe von £ 300.000 verurteilt, weil Fehler in deren Antibetrugssystemen und Kontrollmechanismen aufgetreten waren, wodurch es zu unzulässigen Zahlungsvorgängen auf Kundenkonten kam.

Der Schutz von vertraulichen Kundendaten schafft in der Öffentlichkeit ein hohes Maß an Vertrauen und ist auch aus Unternehmenssicht sinnvoll. Eine einzige Datenschutzverletzung reicht schon aus, dass der Kunde die Geschäftsbeziehung zu Ihrem Unternehmen abbricht. Ohne geeignete Datenschutzkontrollmechanismen gehen Sie daher hohe Risiken ein. Die Folgen können fatal sein: Verlust von Marktanteilen, Imageschäden, deutlicher Rückgang bei der Kundenloyalität und Umsatzeinbußen – Folgen, die Ihr Unternehmen schnell in die Knie zwingen können.

SAP-Kunden haben mittlerweile erkannt, dass ein systemweiter Datenschutz für die Schaffung von Vertrauen bei Kunden und Geschäftspartnern gleichermaßen von ausschlaggebender Bedeutung ist. Beim Management der personenbezogenen Daten stoßen jedoch viele Unternehmen auf Hindernisse, insbesondere wenn dies über die Grenzen des sicheren Produktionssystems hinausgeht.

Die Herausforderungen beim Datenschutz

Die meisten SAP-Kunden verwalten mehrere Produktionsinstanzen ihrer SAP-Anwendungen. Das folgende Beispiel soll dies verdeutlichen: Ein Unternehmen, das mit SAP HCM arbeitet, implementiert mehrere Instanzen für seine Niederlassungen in Nordamerika, im Raum Europa, Naher/Mittlerer Osten und Afrika (EMEA) sowie im asiatisch/pazifischen Raum. Zur Unterstützung von Prozessen wie Anwendungsentwicklung, Test, Schulung, Backup und anderen Aktivitäten können an einem Standort zwischen drei und 30 Klone für jede Instanz verwaltet werden, die eine exakte Replik der vertraulichen Daten aus dem Quellensystem enthalten.

Die SAP-Kunden schützen ihre persönlichen Informationen in ihren produktionsspezifischen Transaktionsverarbeitungssystemen, indem sie den Zugriff auf diese Daten mit Hilfe von Berechtigungen sichern und einschränken. Strenge Kontrollmechanismen und sorgfältig entwickelte Schnittstellen bieten dabei eine gut verwaltete Sicht. Leider ist es aber nicht so einfach, persönliche Daten zu schützen, wenn diese in Umgebungen außerhalb der Produktionsumgebung (z. B. Entwicklung, Test und Schulung) kopiert werden, in denen der Zugriff weniger stark eingeschränkt ist. Datenschutzexperten sind der Meinung, dass Mitarbeiter, die in diesen Umgebungen arbeiten, wie Anwendungsentwickler und Tester, überhaupt keinen Zugriff auf personenbezogene Daten haben sollten. Andererseits benötigen diese Entwickler und Tester aber Zugriff auf diese SAP-Daten. Vor allem müssen sie aber auf verwertbare Daten zugreifen können, um ihre SAP-Anwendungen präzise testen und implementieren zu können.

Die Zugriffssteuerung für den Schutz der Produktionsdaten ist somit für Entwicklungs- und Testumgebungen ungeeignet. Die Verwendung realer Daten kann jedoch schnell zu einer Datenschutzverletzung führen. Um dieses Paradoxon aufzulösen, benötigen SAP-Kunden einen anderen Ansatz.

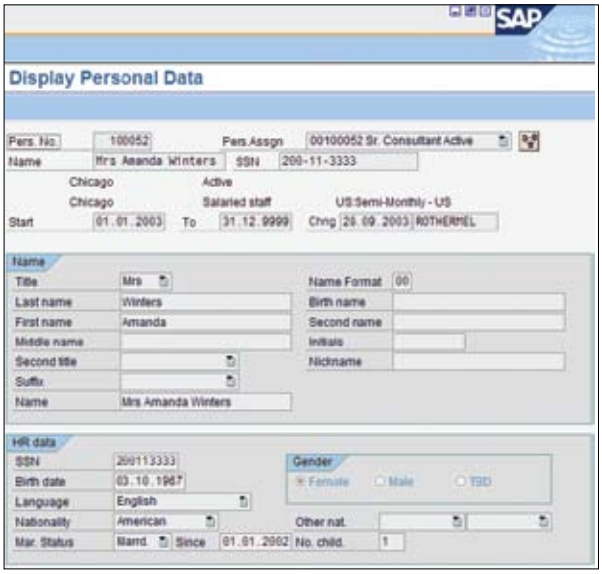
Effiziente Verfahren für die Datenmaskierung

Die Deidentifizierung von Daten ist ein Prozess, bei dem vertrauliche Daten maskiert oder transformiert werden, so dass diese ohne Sicherheitsbedenken in der Anwendungsentwicklung, beim Testen und in Schulungen eingesetzt werden können. Identifizierbare persönliche Daten werden aus der Datenbank entfernt. Über Transformationsalgorithmen werden fiktionale, aber kontextspezifisch korrekte Daten erzeugt, die dann anstelle der ursprünglichen Quellendaten verwendet werden.

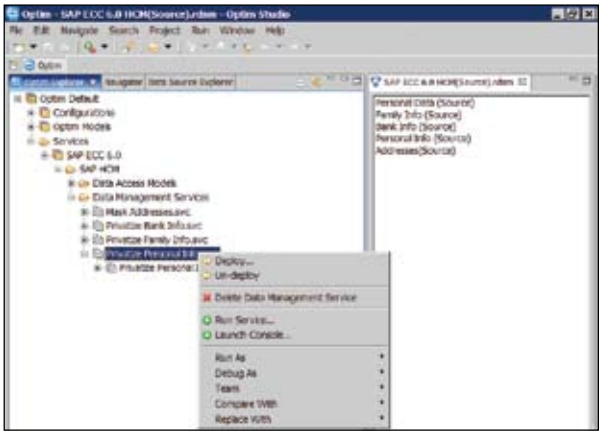
Die Deidentifizierung von Daten, die als Best Practice-Methode anerkannt ist, ist wohl die effizienteste Art für mehr Datenschutz und wirksame Complianceinitiativen. Daten, die maskiert oder transformiert wurden, können problemlos für Test- oder Schulungszwecke eingesetzt werden. Die Optim Data Privacy Solution for SAP von IBM bietet ein umfassendes und bewährtes Funktionsspektrum für die Deidentifizierung von Testdaten, wodurch diese Daten zwar für Testzwecke bestens geeignet, jedoch für Diebe und Hacker wertlos sind.

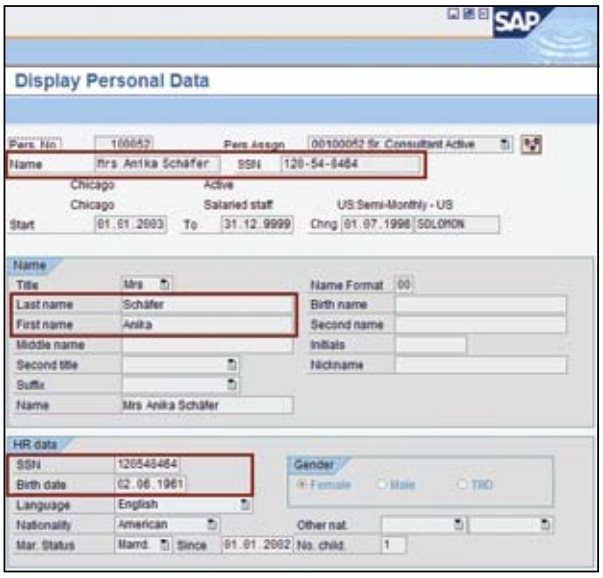
Die anwendungsorientierten Optim-Funktionen für die Maskierung von Daten erkennen, erfassen und verarbeiten SAP-Datenelemente mit höchster Präzision, so dass die maskierten Daten die Anwendungslogik nicht negativ beeinflussen. Maskierte Werte sind in Darstellung und Funktionsweise durchaus mit den ursprünglichen Informationen vergleichbar. Länderspezifische Nachnamen beispielsweise werden durch beliebige andere Nachnamen ersetzt, die aus proprietären Suchdatenbanken ausgewählt werden, und nicht durch bedeutungslose Textzeichenfolgen. Numerische Felder behalten ihre ihnen eigene Strukturen und Muster. Prüfsummen bleiben weiterhin gültig, so dass Funktionstests alle Gültigkeitsprüfungen für Anwendungen bestehen. Der wichtigste Punkt kommt zum Schluss: Optim verteilt alle maskierten Datenelemente präzise und konsistent an alle SAP-Testdatenbanken und an andere zusammengehörige Anwendungen und Datenbanken.

Optim verfügt über ein Spektrum an ausgereiften Funktionen wie integrierte Suchtabellen für die Maskierung von Namen und Adressen. Vordefinierte Routinen erlauben eine genaue Transformation von komplexen Datenelementen wie Sozialversicherungsnummern, Kreditkartennummern und E-Mail-Adressen. Sie können auch standortspezifische Datenkonvertierungsroutinen einsetzen, durch die die Verarbeitungslogik aus verschiedenen zusammengehörigen Anwendungen und Datenbanken integriert wird.



SAP-Daten vor der Maskierung.


IBM Optim Data Privacy Solution for SAP.



SAP-Daten nach der Maskierung.

Optim ist als zentrale Datenmanagementlösung zu sehen, die sich exakt an die Anforderungen des Unternehmens anpassen lässt und sowohl Ihre eigenen Anwendungen als auch Ihre Standardsoftware unterstützt. Optim unterstützt alle führenden Unternehmensdatenbanken und Betriebssysteme: IBM DB2, Oracle, Sybase, Microsoft® SQL Server, IBM Informix, IBM IMS, IBM VSAM, Microsoft Windows®, UNIX®, Linux® und IBM z/OS.

Informationen zu IBM Optim

IBM Optim Enterprise Data Management Solutions gehen gezielt auf kritische geschäftliche Problemstellungen ein wie Management der wachsenden Datenmengen im Unternehmen, Einhaltung von Datenschutzvorschriften, Management von Testdaten, E-Discovery, Anwendungsupgrades, Migrationen und Anwendungsstilllegung. Die Optim-Lösungen berücksichtigen dabei die Ausrichtung des Anwendungsdatenmanagements an den Geschäftszielen des Unternehmens und bieten somit Vorteile wie Leistungsoptimierung, Risikominimierung und Kostenkontrolle. Gleichzeitig stellen diese Lösungen ein Funktionsspektrum bereit, das sich gezielt an die Anwendungen, Datenbanken und Plattformen im Unternehmen anpassen lässt. Optim unterstützt weltweit Unternehmen aus allen Branchen bei der bestmöglichen Nutzung ihrer Unternehmensanwendungen und -datenbanken, indem Anwendungsdaten während ihres gesamten Lebenszyklus optimal verwaltet werden.

Weitere Informationen

Weitere Informationen zu IBM Optim Enterprise Data Management Solutions erhalten Sie von Ihrem IBM Vertriebsbeauftragten oder unter:

www.optimsolution.com

IBM Deutschland GmbH
70548 Stuttgart
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation.

DB2, IMS, Informix, Optim, VSAM und z/OS sind Marken der IBM Corporation in den USA und/oder anderen Ländern.

Linux ist eine Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

UNIX ist eine eingetragene Marke von The Open Group in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern. Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

Jeder Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen selbst verantwortlich. Es obliegt allein dem Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Einhaltung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die sich auf seine Geschäftstätigkeit und alle Maßnahmen des Kunden auswirken können, die dieser im Hinblick auf die Einhaltung solcher Bestimmungen durchführen muss. IBM erteilt keine Rechtsberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit jeglichen relevanten Gesetzen und Verordnungen.

© Copyright IBM Corporation 2008
Alle Rechte vorbehalten.

TAKE BACK CONTROL WITH **Information Management**

IMS14023-DEDE-00