Data Masking schützt vertrauliche Informationen

Big Data ist für viele Manager ein Traum, für Datenschützer dagegen häufig ein Albtraum: Allein in Deutschland sind zurzeit etwa zwei Drittel der für IT-Tests verwendeten Daten unverschlüsselt. Doch die seit April dieses Jahres gültige EU-Datenschutz-Grundverordnung (EU-DSGVO) zwingt Unternehmen, besonders im Testmanagement umzudenken. Freiwillige Verpflichtungen, wie beispielsweise der Code of Conduct der Versicherungswirtschaft, reichen nun nicht mehr aus. Doch mit den richtigen Tools und intelligenten Prozessen lässt sich nicht nur dem Datenschutz gerecht werden, sondern auch das Business Develop-ment vorantreiben.

Für IT-Abteilungen besteht mit der EU-DSGVO im kommenden Jahr akuter Handlungsbedarf, denn ab 2018 können Verstöße teuer wer-den. Die Strafe für Missachtung der Datenschutzregeln kann Firmen bis zu vier Prozent ihres weltweiten Um-satzes kosten oder mindestens 20 Mill. Euro. Neben dem finanziellen Risiko ist auch der Reputationsscha-den bei einem Datendiebstahl im-mens, wie das aktuelle Beispiel von Yahoo zeigt.

Sicherheit durch Tarnung

Neben Verschlüsselungen und dem Einsatz von Token ist Data Mas-king eine effiziente Methode, die vie-le Möglichkeiten für eine sichere Datennutzung bereithält. Beim Data Masking werden vertrauliche und persönliche Daten der Nutzer so an-onymisiert, dass sie sich am Ende nicht mehr einer bestimmten Person zuordnen lassen. Daten verwandeln sich in Pseudonyme – ähnlich wie Menschen, die ihre wahre Identität hinter einer Maske verstecken. Auch im Falle eines Diebstahls bleiben so individuelle Daten geschützt.

Bei der Maskierung werden Daten entweder durch frei definierbare Zeichenketten, einen Algorithmus oder die Trennung von Daten so geschützt, dass sensible Angaben verwendet werden können, ohne dass ein Rückschluss auf reale Identitäten möglich ist. Beispielsweise werden persönliche Angaben wie Name, Vorname oder Geburtsort verfremdet, ebenso wie Telefon- und Kontonummern. Unverändert bleiben beispielsweise Angaben zum Geschlecht, Familienstand oder Ort. So können Tests und Analysen mit realistischen, aber nicht realen Daten durchgeführt werden. Grundsätzlich lassen Daten sich entweder dynamisch maskieren, also erst bei einer Abfrage aus dem operativen System verschlüsseln, oder die Daten werden dauerhaft maskiert und später in eine Testumgebung verschoben.

Auch nach der Maskierung lassen sich die Daten in den Testumgebungen weiter verwenden. Dies ist beispielsweise für Ratings in der Versicherungswirtschaft wichtig. Denn intelligente Regeln bei der Verschlüsselung sorgen dafür, dass die maskierten Daten gleiche Rating-Ergebnisse liefern wie unverschlüsselte Daten. Insgesamt sind Testdaten, die aus einer maskierten Umgebung stammen, damit schneller, günstiger und vor allem sicherer zur Hand.

Jeanette Wygoda

Geschäftsführerin Compliance, Strategie, Kommunikation, Hamburg

Marc Böning

Geschäftsführer productive-data GmbH, Hamburg

Für das Data Masking bieten Hersteller wie IBM, Informatica oder Oracle Werkzeuge an, die sich ohne große Hürden implementieren lassen. Die Tools aller Anbieter lassen sich an operative Systeme anknüpfen und können Daten ohne Vorbereitung in Testumgebungen schreiben. Die Daten werden während der Verarbeitung maskiert und können in passende Häppchen in den Testumgebungen konfektioniert werden. Da sich die Testdaten viel einfacher erzeugen lassen, können nicht nur Abschlusstests vor Produktivsetzungen schneller durchgeführt werden. Insgesamt ist die Dauer der „Time to Market" deutlich geringer.

Um das volle Potenzial aus Data-Masking-Anwendungen herauszuholen, bieten spezialisierte Beratungsunternehmen umfassende Kenntnisse zu Technik, Prozessen, Change Management und Compliance. Der breite Ansatz macht sich für den Auftraggeber bezahlt: Unternehmen, bei denen zur Einführung der Datenschutz-Tools nicht nur IT- und Compliance-Kollegen miteinander sprechen, sondern auch die Fachbereiche mit am Tisch sitzen, erreichen erfahrungsgemäß den größten betriebswirtschaftlichen Nutzen. Denn neben dem Change Management spielt bei der Einführung der Pseudonymisierung auch die Optimierung der bestehenden Prozesse eine wichtige Rolle. Damit erhalten IT-Projekte so zwar einen größeren Fokus, der auch bestehende Strukturen auf den Prüfstand stellen kann, doch sind die Kosten-Nutzen-Vorteile am Ende ungleich größer.

Ausweg aus Dilemma

Die Begleiterscheinungen beim Einsatz von Data-Masking-Tools machen deutlich, dass intelligenter Datenschutz nicht nur für IT und Compliance relevant ist, sondern auch für das Business Development und die Produktentwicklung großes Potenzial besitzt. Bisher stehen die Bedenken der Datenschützer noch im Kontrast zu den Bedürfnissen der Fachabteilungen, die mit Self-Service-Tools für Business-Intelligence-Anwendungen besseren Zugang und mehr Agilität bei der Datenabfrage fordern. Data Masking bietet hier einen eleganten Ausweg aus dem Dilemma. Die Zeit bis 2018 können Unternehmen also noch gewinnbringend nutzen, um über Datenschutz Big Data einen großen Schritt näher zu kommen.