Testdaten als Risikofaktor

Eine klare Testdatenrichtlinie reduziert die Gefahr eines Missbrauchs sensibler Daten

von Klaus Haller

Welcher Tester will schon vor Gericht stehen, nur weil er seinen Job gemacht hat? Sicher keiner! Doch was gestern Standard war, ist heute ein Risiko. Ein professionelles Testdaten-Management verringert die Gefahr, dass sensible Daten im Testprozess missbraucht werden. Um Gesetzesverstöße und Datenverluste bei Outsourcing und Offshoring von Testverfahren zu vermeiden, benötigen Unternehmen klare Richtlinien für Testdaten und müssen ihre Umsetzung konsequent überwachen.

Ein Tester braucht passende Testdaten in der Datenbank, um eine Datenbankapplikation zu testen. Die einfachste Lösung ist, Datenbanken aus der Produktion in die Testumgebung zu kopieren. Dieses Vorgehen war bis vor kurzem Standard. Doch Compliance- und IT-Risk-Abteilungen werden zunehmend nervös, weil sich die Sourcing-Modelle ändern. Viele Unternehmen lassen Dienstleister und/oder Tester im Ausland testen. Das führt zu regulatorischen Risiken und gefährdet den Schutz des geistigen Eigentums. Schließlich speichern viele Applikationen sensible Daten. Gelangen Konstruktionszeichnungen aus CAD-Systemen von Maschinenbaufirmen oder Forschungsdaten aus der Pharmaindustrie an Konkurrenten, ist der Schaden groß. Daher setzen die meisten Unternehmen in Produktionsumgebungen das Need-to-know-Prinzip durch. Anwender sehen nur Daten, die sie für ihre Arbeit benötigen.

Testumgebung als Risikofaktor für das Unternehmen

Testumgebungen sind dagegen weniger abgesichert. Tester können sich meist ohne Authentifizierung in Applikationen und Datenbanken einloggen und auf alle Daten zugreifen. Enthalten Testumgebungen Produktionsdaten, kann eine SQL-Query reichen und ein Tester kennt die Herstell-

kosten aller Produkte. Dazu kommen Auswirkungen von Outsourcing und Offshoring. Die Loyalität der Mitarbeiter kann leiden. Wer tatsächlich am Testungsprozess beteiligt ist kann nicht immer nachvollzogen werden. Strikte Kontrollen werden schwierig. Das Risiko steigt, dass sensible Firmendaten fahrlässig oder kriminell aus Testumgebungen abfließen, beispielsweise per Email oder FTP. Im deutschsprachigen Raum sind die gesetzlichen Bestimmungen zum Datenschutz streng. Das gilt für Kundendaten, Daten bei öffentlichen Einrichtungen, für Bankkundendaten etc. Bereits die reine Existenz solcher Daten in Offshore-(Test-)Umgebungen oder bei Outsourcing-Partnern kann gegen Gesetze verstoßen, egal ob manuell erfasst oder aus der Produktion kopiert. Es drohen Reputationsverlust, Eingriffe von Aufsichtsbehörden und Strafen. Für Tester persönlich bestehen rechtliche Risiken, wenn sie gegen Gesetze verstoßen – auch wenn sie auf Anweisung ihrer Vorgesetzten handeln. Deshalb heißt es in Unternehmen oft: „Keine sensiblen Daten in Testumgebungen kopieren! Keine vertraulichen Daten aus Testumgebungen verlassen die Firma!“ Solche Vorgaben mögen sensibilisieren, zuallererst aber verwirren sie. Einerseits ist unklar, was genau verboten ist. „Sensible Daten“ ist ein weiter Begriff. Andererseits fragen sich die Tester, wie sie sonst zu ihren Testdaten kommen, wenn sie nicht mehr unverändert aus der Produktion kopiert werden

Richtlinien für ein professionelles Testdatenmanagement

Drei Schritte sind für die Vorbereitung eines professionellen Testdatenmanagements notwendig. Im ersten Schritt müssen sich die Legal & Compliance-Abteilung – sie wacht über das Einhalten rechtlicher Bestimmungen und das ethisch korrekte Verhalten im Unternehmen – und das IT-Risiko-Management über mögliche Risiken verständigen. Welche Daten sind sensibel und wo sind sie überall gespeichert? Welche regulatorischen Vorgaben gibt es? Wo werden sie potentiell verletzt? Im zweiten Schritt wird eine verbindliche Testdatenrichtlinie erarbeitet. Das Management entscheidet, welche Risiken es akzeptieren kann und will. Die Testdatenrichtlinie definiert, welche Daten sensibel sind, in welche Länder sie übermittelt werden können und ob Dienstleister sie sehen dürfen. Dazu kommen Vorgaben zum Anonymisieren. Reicht es zum Beispiel aus, die Kundennamen zu löschen oder sind auch Adressen und Buchungstexte unkenntlich zu machen?

Die Testdatenrichtlinie schränkt den Tester in seiner Arbeit ein. Deshalb ist es im dritten Schritt wichtig, Alternativen aufzuzeigen. Synthetisch erzeugte Testdaten oder (sehr gut!) anonymisierte Daten aus der Produktion können die bisherigen Datenkopien aus der Produktion ablösen. Das erfordert oft neue Tools. Dadurch ändern sich Arbeitsprozesse und die Teamorganisation in der Das alles bindet Ressourcen und kostet Zeit.

Erst wenn alle drei vorbereitenden Schritte abgeschlossen sind kommuniziert das Management die Testdatenrichtlinie und gleichzeitig das neue Vorgehen bei Testdaten. Danach setzen die Tester die Vorgaben in der Praxisum. Doch Vorsicht: Testumgebungen sind wie Kinderzimmer! Einmal aufräumen reicht nicht. Regelmäßiges Überprüfen ist erforderlich. ■

Klaus Haller arbeitet bei Swisscom IT Services in Zürich im Consulting mit Schwerpunkt Testorganisationen, Testdaten, IT-Risk und Data Loss Prevention.