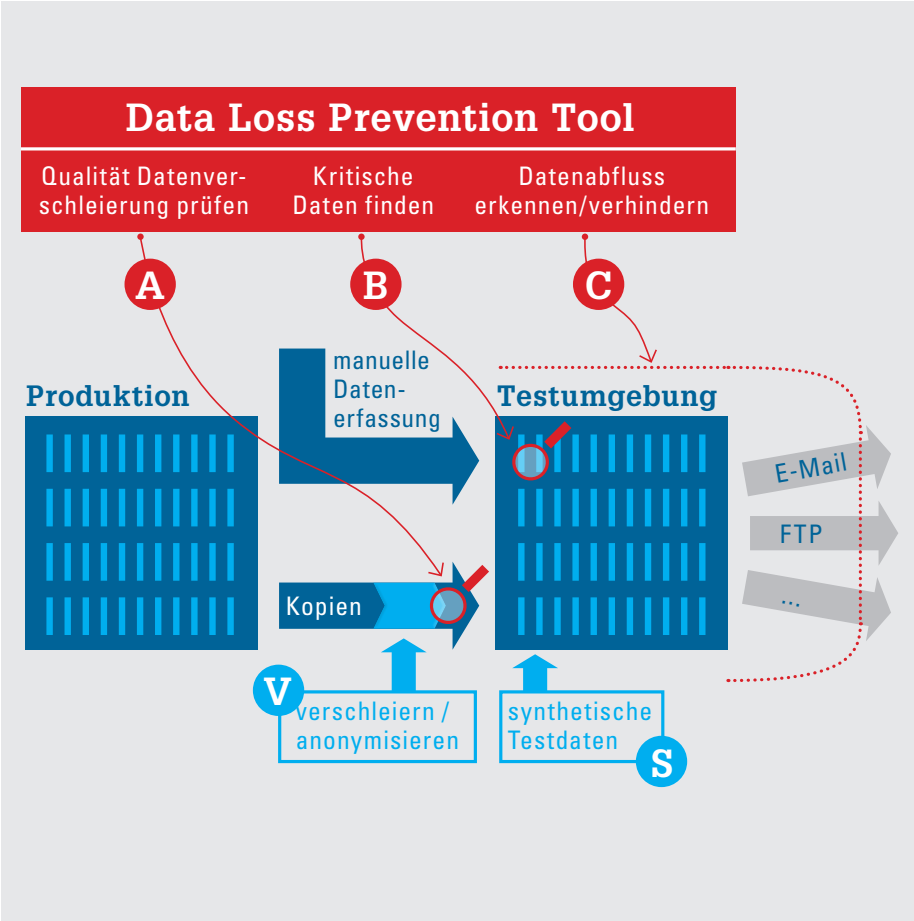

Abbildung 1: Schema des Data Loss Prevention-Tools (DLP)

Überblick zu TDM-Tools

Unabhängig davon, ob die Testdaten aus den Produktivdaten abgezogen oder synthetisch erzeugt werden, ist die Unterstützung durch ein geeignetes Tool erforderlich. Als Hilfestellung bei der Toolauswahl hat imbus auf der Plattform *www.testtoolreview.de* eine Übersicht am Markt befindlicher Testdatengeneratoren und anderer TDM-Tools zusammengestellt. Dort sind neben der Kategorie „Testdatenmanagement-Werkzeuge" auch andere Testtools zu finden. Die Übersicht soll helfen zu entscheiden, welches Tool für die eigene Situation in Frage kommen – inklusive der dazugehörigen Evaluierung und Beschaffung. ■

Dirk Reimann ist Senior Consultant für Software-Testsysteme bei der imbus AG.

Data-Loss-Prevention-Tools minimieren Sicherheitslücken in Testumgebungen

von Klaus Haller

Data Loss Prevention-Tools (DLP) unterstützen das regelmäßige Überprüfen der Testumgebung in Hinblick auf sicherheitsrelevante Risiken. Sie finden sensible Daten wie Kreditkartennummern, Kundennamen oder auch CAD-Files in Datenbanken, Files oder Emails etc. Sie können Datenabfluss blockieren und sensible Daten an sichere Orte verschieben. Doch bisher setzen nur IT-Security-Abteilungen DLP-Tools ein. Dabei können sie auch Testcentern helfen, Testdatenrisiken in Testumgebungen zu mindern:

>> Eingangskontrolle. Möchte ein Tester Testdaten in die Testumgebung einspielen, überprüft das DLP-Tool, dass die Testdaten keine sensible Daten enthalten. Das vermeidet präventiv Verstöße gegen die Testdatenrichtlinie (Abbildung 1, A).

Da DLP-Tools sind jedoch dahingehend optimiert sind, viele sensible Daten zu finden, ohne zu viele falsche Treffer zu generieren, finden sie nicht alle Daten dieser Art. DLP-Tools dürfen daher nicht verwendet werden, um eine Liste aller sensiblen, zu löschenden Daten zu erhalten, sondern nur zur Kontrolle von Bereinigungen.

>> Überwachen der Testumgebung. Trotz Eingangskontrolle können sensible Daten in Testumgebungen gelangen, beispielsweise durch manuelle Eingabe oder externe Feeds. DLP-Tools scannen Datenbanken und Files auf solche Verstöße gegen die Testdatenrichtlinie, die bereinigt werden müssen (Abbildung 1, B).

>> Datenabfluss erkennen und verhindern. DLP-Tools erkennen zum Beispiel, wenn Emails mit sensiblen Daten das Unternehmen drohen zu verlassen oder sensible Daten auf USB-Sticks kopiert werden. Dies können sie unterbinden (Abbildung 1, C). ■

Klaus Haller arbeitet bei Swisscom IT Services in Zürich im Consulting.