Auch Irrtümer sind Fehler

„Legale“ Fehler, die auf Irrtümer von Mitarbeitern zurückzuführen sind, können ebenso lästig sein wie irrtümliche Verstöße gegen gesetzliche Vorschriften. Beides kann aus unterschiedlichen Gründen teuer werden. Die Stuttgarter Libelle AG widmet sich mit ihren Lösungen auch diesen Themen.

Von Holm Landrock, Freier Journalist in Dresden

Es gibt eine Redewendung in der Informationstechnik, wonach sich der eigentliche Fehler zwischen Tastatur und Stuhl befände. Das ist nur natürlich: Computer sind von Menschen für Menschen gebaut und schon im Design liegen Herausforderungen für die Betreiber und die Benutzer. Moderne Entwicklungstrends wie DevOps, die zu schnell verfügbarer, aber erst nach einiger Zeit ausgereifter Software führen, sind nicht ganz unschuldig an der Fehleranfälligkeit vieler Systeme. Zusammen mit der fast vollständigen Durchdringung der Geschäftsprozesse mit Informationstechnik ergeben sich viele Gelegenheiten, Fehler zu machen – und oft sind diese allzu menschlich.

Während es gegen Hardware-Fehler mittlerweile recht brauchbare Schutzmechanismen gibt, wirken sich gerade menschliche Fehler immer dramatischer aus. Das liegt vor allem in der Abhängigkeit der Geschäftsprozesse von IT sowie am permanenten Datenaustausch zwischen den immer komplexeren Systemverbünden. Fehler, die bei einer völlig legalen, aber irrtümlichen Handhabung entstehen, haben hier die unangenehme Angewohnheit, sich in kürzester Zeit auf alle beteiligten Systeme und somit Geschäftsprozesse auszubreiten, mithilfe der Hardware-Schutzmechanismen außerdem auch bis in Backup-Systeme und -Medien.

Auch Irrtümer in der Handhabung von Daten sowie ungenaue organisatorische Abläufe können zu Fehlern bei der Einhaltung gesetzlicher Vorgaben führen. Diese wirken sich vielleicht nicht direkt auf die Leistungsfähigkeit des Unternehmens aus, können aber durch Strafen und Nacharbeiten hohe Kosten verursachen.

Um diesen Entwicklungen etwas entgegenzusetzen, haben sich einige Lösungen etabliert, die dazu geeignet sind, begangene Fehler rückgängig zu machen oder Fehler bei der Einhaltung von Regularien von vornherein auszuschließen. Solche Lösungen kommen unter anderem von der Libelle AG in Stuttgart.

„Legale“ Fehler rückgängig machen

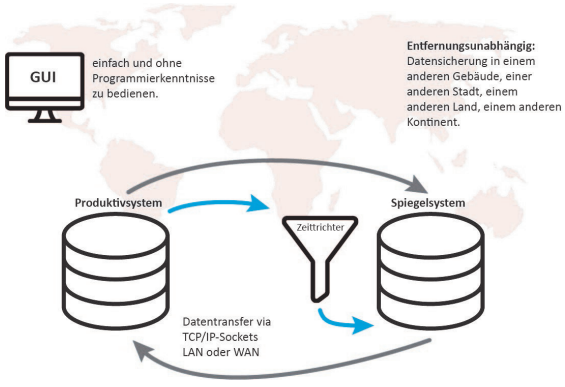
Unachtsamkeit und auch die mangelnde Widerstandsfähigkeit gegen Irrtümer sind immer noch die häufigsten Fehlerursachen. Gegen Irrtümer lässt sich eine IT-Landschaft allerdings auch nur schwer schützen: Der Irrtum ist in all seinen Spielarten ein harter Brocken für die IT. Denn häufig sind es Bedienfehler, die zu Datenverlusten oder kritischen fehlerhaften Veränderungen führen.

Lars Albrecht, Vorstand der Libelle AG, erinnert sich an solch eine kritische Situation bei einem Kunden: „Ein Datenbank-User wollte im Rahmen einer groß angelegten Datenpflege Tabellenstrukturen ändern. Statt jedoch den internen Support zu bemühen, bastelte der Anwender ein leider fehlerhaftes Skript, um Daten automatisch in die Tabellen zu schreiben. Da es sich um geschäftskritische Tabellen handelte, liefen diese Änderungen sofort durch alle Snapshots und anderen hardwareseitigen Sicherungsmechanismen. Das Ergebnis: Auf allen Instanzen enthielten einige Tabellen keine gültigen Daten mehr.“

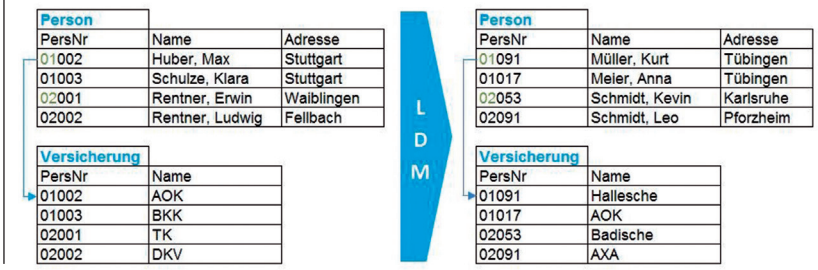
Solch ein Fehler ist maschinell schwer zu entdecken, da die Daten aus Datenbanksicht technisch korrekt und vermeintlich gültig scheinen. Der Anwender jedoch bemerkte schließlich seinen Fehler und suchte beim Support eine Lösung. Rollbacks anhand der Snapshots waren ebenso fruchtlos wie ein Blick auf die redundanten Speichersysteme. Die eingesetzte Hochverfügbarkeitstechnik hatte den logischen Fehler sorgfältig über alle physischen und virtuellen Instanzen dupliziert. Die Rekonstruktion der Tabellen aus einem vorhandenen Backup wäre möglich gewesen, hätte die Anwendungsumgebung allerdings für mehrere Stunden blockiert.

Zeitversetzte Datenspiegelung dreht Zeit zurück

In solchen Fällen entfaltet die asynchrone, zeitversetzte



Das Grundprinzip der patentierten zeitversetzten Datenspiegelung von BusinessShadow. (Bild: Libelle AG)



Person

PersNr	Name	Adresse
01002	Huber, Max	Stuttgart
01003	Schulze, Klara	Stuttgart
02001	Rentner, Erwin	Waiblingen
02002	Rentner, Ludwig	Fellbach

Versicherung

PersNr	Name
01002	AOK
01003	BKK
02001	TK
02002	DKV

Person

PersNr	Name	Adresse
01091	Müller, Kurt	Tübingen
01017	Meier, Anna	Tübingen
02053	Schmidt, Kevin	Karlsruhe
02091	Schmidt, Leo	Pforzheim

Versicherung

PersNr	Name
01091	Hallesche
01017	AOK
02053	Badische
02091	AXA

LDM erzeugt aus konkreten Produktivdaten konsistente und legale Daten für Test und Entwicklung. (Bild: Libelle AG)

Datenspiegelung des Libelle BusinessShadow ihre Stärke: Nach einer einmaligen initialen Kopie der Datenbank auf ein Spiegelsystem laufen alle Transaktionen in einen Zwischenspeicher auf der Spiegelseite, auch Zeittrichter genannt. Die Verweildauer der Daten im Trichter wird vom Anwender individuell festgelegt. Im Falle logischer Fehler wie im genannten Beispiel oder auch bei fehlerhaften Updates kann das Produktivsystem auf den Spiegel umgeschaltet werden. In wenigen Minuten werden dann alle gültigen Transaktionen, und zwar genau bis zum Zeitpunkt vor dem Fehler, aus dem Zeittrichter in die Schattendatenbank wiederhergestellt. Anschließend wird die Schattendatenbank als Produktivsystem online geschaltet.

Mit diesem Verfahren lassen sich auch Applikationsumgebungen mit enorm großen Datenbeständen in wenigen Minuten wiederherstellen. Die Wiederherstellungszeit ist dabei von der Anzahl und dem Volumen der Änderungen beziehungsweise der Archive-Dateien abhängig. Ein durchaus typisches Resultat ist die Wiederherstellung eines Zeittrichters von vier Stunden innerhalb von zehn Minuten. Ein klassisches Restore hätte einen Arbeitstag gedauert – und dabei personelle wie technische Ressourcen blockiert.

Irrtum schützt vor Strafe nicht

Menschliche Fehler entstehen hier nicht nur durch Unachtsamkeit, sondern liegen vielfach im Organisatorischen oder ganz einfach in der Natur der Prozesse. So wird die DSGVO im Mai 2020 zwei Jahre alt, doch noch immer ist die Verordnung für viele Unternehmen „Neuland".

Zum Beispiel wird für die Weiterentwicklung von Apps oft schnell und unkompliziert eine Datenquelle auf das Entwicklungssystem kopiert. In diesem Vorgang lauert jedoch ein dramatischer Fehler: Kopieren Entwickler dabei personenbezogene Daten, entsteht ein Verstoß gegen die Bestimmungen der DSGVO. Personenbezogene Daten dürfen in den typischen Fällen nur für den Zweck verwendet werden, für den eine Einwilligung vorliegt. Das Kopieren auf andere Systeme ist in den meisten Fällen nicht gestattet, weil die Einwilligung oder die Zweckbindung nicht gegeben sind. Die „Weiterentwicklung" der Services, für die eine Person die Einwilligung erteilt hat, genügt nicht für die Verarbeitung der Daten auf anderen Systemen oder die Nutzung als Testdaten. Zudem dürfen personenbezogene Daten ohne ausdrückliche Einwilligung nicht an die Unternehmen in der Supply-Chain weitergegeben werden.

Durch das „wilde" Kopieren ist auch die DSGVO-konforme Auskunftspflicht nicht mehr verlässlich und vollumfänglich möglich.

Hier gibt es zwei Lösungsansätze: Der Erwerb von Testdaten oder die Anonymisierung von Daten. Libelle-Vorstand Albrecht erläutert: „Testdaten von Dritten haben den großen Nachteil, dass sie in Inhalten und Strukturen nicht hundertprozentig zu der zu testenden Anwendung passen und dadurch die Integrität der Anwendung beeinträchtigen können." Das Ergebnis daraus kann in Abläufen resultieren, die mit Testdaten perfekt funktionieren, in den Echt-Umgebungen jedoch schnell in Fehlerfällen aufgrund unerwarteter Datenkonstellationen und Inkonsistenzen enden.

Automatische Anonymisierung über Datenstrukturen hinweg

Manche Anwender helfen sich mit einer Pseudonymisierung – ebenfalls ein allzu menschlicher Irrtum. Mit typischen Pseudonymisierungs-Verfahren, wie Löschen von Einzelwerten (gerne Namen) oder Hashing, sind die Daten für den Test oft ungeeignet.

Die Anonymisierung von Daten mit einem Tool wie Libelle DataMasking (LDM) verfolgt einen anderen Ansatz. LDM erzeugt für die Test- und Entwicklungssysteme realitätsnahe – aber vollständig anonymisierte – Daten. Diese sind nicht auf die Originaldaten rückführbar, weisen aber dieselbe logische Konsistenz und Struktur auf. Lars Abrecht: „Spätestens, wenn es um verteilte Datenbankstrukturen geht, steigt der Aufwand enorm und die Notwendigkeit eines Tools macht sich bemerkbar. LDM leistet den gleichartigen, logisch korrekten Austausch von Werten, auch in komplexen Umgebungen, über alle beteiligten Systeme hinweg."

Für Unternehmen, die komplexe Datenstrukturen mit personenbezogenen Daten verarbeiten und ihre Lösungen dafür ständig weiterentwickeln, ist eine automatische Anonymisierung von Datenstrukturen für Test- und Entwicklungssysteme im Grunde unerlässlich. Übrigens: Die DSGVO setzt die korrekte Anonymisierung von Daten mit deren Löschung gleich. ■