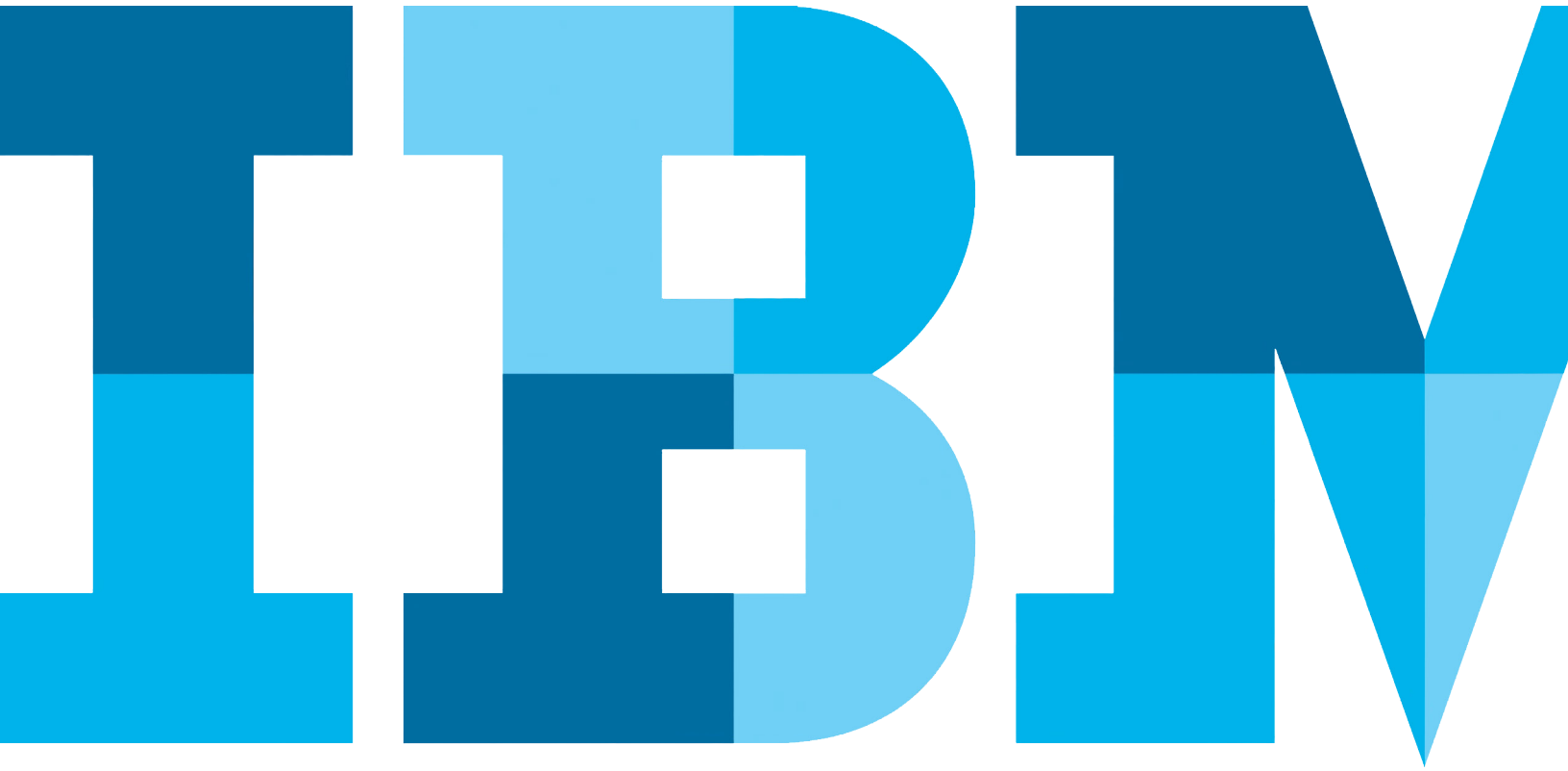
TechTarget Custom Media

July 2015

Thought-Leadership-Artikel

Compliance in heterogenen IT-Umgebungen gewährleisten

Autor: Oliver Schonschek



IBM

Die fortschreitende Digitalisierung der Geschäftsprozesse und die Einführung neuer IT-Technologien wie Cloud Computing und Big Data Analytics stellen IT-Manager und Compliance-Verantwortliche vor große Herausforderungen. Compliance-Vorgaben wie zum Beispiel SOX, PCI DSS und Datenschutzrichtlinien müssen erfüllt und die Einhaltung nachgewiesen werden, ganz gleich, in welcher der zahlreichen Datenbanken oder Anwendungen die zu schützenden Daten gespeichert, verarbeitet und genutzt werden.

Viele Unternehmen sind sich unsicher, wie sie die Compliance in einer zunehmend heterogenen IT-Landschaft noch gewährleisten sollen. So haben laut einer BITKOM-Umfrage fast 60 Prozent der Unternehmen die Sorge, dass Cloud Computing die Einhaltung von Compliance-Anforderungen gefährdet und schwerlich mit regulativen Rahmenbedingungen in Einklang zu bringen ist.

Tatsächlich aber ist die Vielfalt an Anwendungen und Datenbanken in der heutigen IT kein Hindernis für eine umfassende, revisionssichere Auditierung oder ein vollständiges Reporting, wie es die Compliance-Vorgaben vorschreiben. Die Enterprise-Security-Plattform IBM InfoSphere Guardium wurde speziell für die übergreifende Kontrolle, Überwachung und Auditierung aller in Unternehmenssystemen gespeicherten Daten entwickelt.

Compliance-Regeln zentral definieren und durchsetzen

Sicherheits- und Compliance-Richtlinien müssen nicht für jede einzelne Applikation oder Datenbank einzeln konfiguriert und überprüft werden. Diesen Aufwand ersparen sich Datenbank-Manager und IT-Manager, wenn sie eine zentrale Lösung wie IBM InfoSphere Guardium einsetzen, die die Einhaltung von Compliance-Vorgaben system- und plattformübergreifend prüft und automatisch dokumentiert.

Sämtliche Datenbanktransaktionen werden manipulationssicher und lückenlos protokolliert. Die Prüfprotokolle sind auch gegen Zugriffe von Administratoren geschützt. Diesem Schutz gegen Zugriffe privilegierter Nutzer kommt eine hohe Bedeutung zu. Rund die Hälfte aller Cyberattacken auf Unternehmen kommt aus den eigenen Reihen, so der neue IBM 2015 Cyber Security Intelligence Index.

Manipulationen der Compliance-relevanten Prüfprotokolle durch mögliche Innentäter müssen verhindert werden. Hier greift die klare Aufgabentrennung zwischen Datenbank-Administratoren und internen Auditoren, die bei IBM InfoSphere Guardium im Standard vorgesehen ist. Die Auswertung der Prüfprotokolle bleibt den internen oder externen Auditoren vorbehalten, die dadurch auch die Tätigkeit der Administratoren im Blick haben.

Automatisierung des gesamten Compliance- und Auditprozesses

Für die Compliance in heterogenen, zunehmend komplexen IT-Landschaften ist es wichtig, sämtliche Datenbanken und Anwendungen zentral und manipulationssicher überwachen zu können. Zusätzlich müssen die Auditierung und Prüfprotokolle für die zahlreichen Datenbanken in den Unternehmen vom Aufwand her beherrschbar bleiben.

Protokolle und Berichte bringen wenig, wenn sie nicht zeitnah ausgewertet werden können und die zuständige Stelle nicht unmittelbar erreichen. IBM InfoSphere Guardium sieht einen automatisierten Compliance- und Auditprozess vor. Die Auditberichte werden automatisch erstellt und der jeweils zuständigen Stelle wie zum Beispiel dem Compliance-Beauftragten als E-Mail-Anhang oder als Link zugestellt. Die Empfänger können die Berichte prüfen und freigeben sowie erkannte Abweichungen von den Compliance-Vorgaben eskalieren. Zusätzlich besteht die Möglichkeit, die Auditberichte in geeigneten Formaten an weitere IT-Sicherheitssysteme zu übertragen, zum Beispiel an ein SIEM-System (Security Information and Event Management).

Die Auditoren werden bei der Auswertung der Berichte unterstützt, indem durch InfoSphere Guardium automatisch alle überwachten Aktivitäten entsprechend der jeweils gültigen Compliance-Vorgaben auf Auffälligkeiten und mögliche Verstöße hin untersucht werden. Der Auditor kann sich so auf die tatsächlich relevanten Ereignisse konzentrieren und verliert sich nicht in der Durchsicht unkritischer Systemmeldungen.

Passgenaue Berichte für die branchenspezifische Compliance

Auditberichte müssen genauen Vorgaben entsprechen, damit ein Unternehmen die Ansprüche an die geforderte Compliance auch wirklich erfüllt. Die Vielfalt an Compliance-Vorgaben und die verschiedenen Branchenspezifika machen es nicht einfach, konforme Auditberichte zur Hand zu haben, wenn eine externe Auditierung ansteht. Hier unterstützt eine Lösung wie IBM InfoSphere Guardium mit passenden Audit- und Berichtsvorlagen, die automatisch befüllt werden. So erhalten die Auditoren die gewünschten Informationen, der Aufwand für die Auditierung sinkt und damit auch die Auditkosten.

Mehr als 100 vorkonfigurierte Berichte und Auditregeln helfen Unternehmen dabei, den Audit- und Berichtsprozess ohne aufwändige Vorarbeiten aufzusetzen. Die Berichte umfassen neben dem Compliance-Reporting auch Untersuchungen und Auswertungen zur System-Performance sowie die Möglichkeit, mittels forensischer Untersuchungen Verdachtsmomente zu überprüfen und digitale Spuren zu sichern.

Bei Bedarf können auch individuelle Berichte definiert werden. Dazu bietet IBM InfoSphere Guardium eine grafische Benutzeroberfläche, mit der sich neue Berichte erstellen oder vorhandene Berichtsvorlagen anpassen lassen.

Heterogene IT-Landschaften lassen sich somit zentral, automatisiert und den spezifischen Compliance-Vorgaben entsprechend auditieren. Eine Lösung wie IBM InfoSphere Guardium unterstützt die Compliance-gerechte Nutzung der vielfältigen Möglichkeiten der modernen IT, vereinfacht das Datenbank-Management und senkt die Aufwände für die Auditierung.