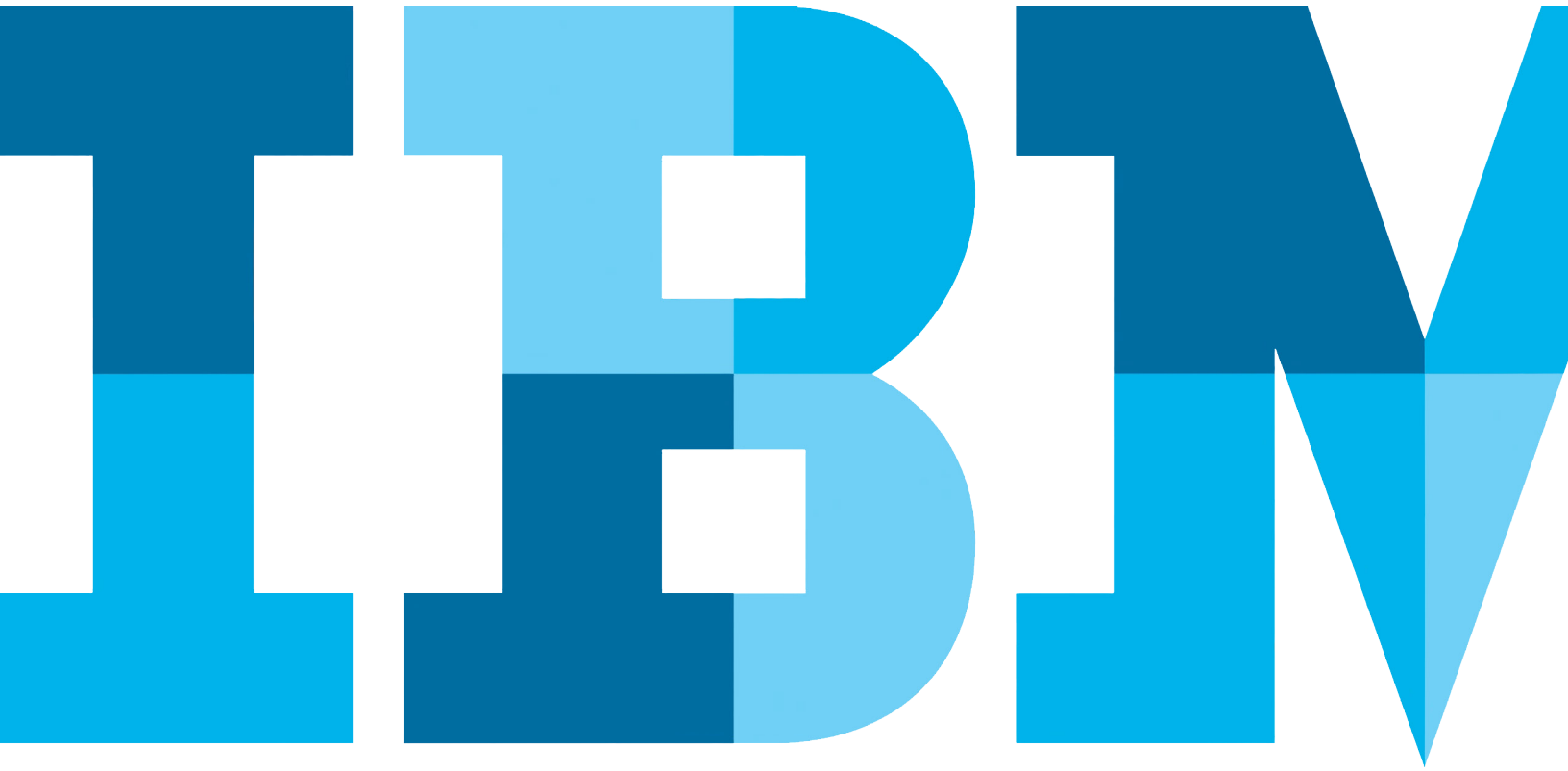
TechTarget Custom Media

July 2015

Thought-Leadership-Artikel

Intelligente Datensicherheit für den Schutz von Big Data

Autor: Oliver Schonschek



IBM

Big Data, das Sammeln, Speichern und Auswerten großer Datenmengen, ist kein Zukunftstrend, sondern bereits Realität im Unternehmensalltag. Laut einer BITKOM-Umfrage stellten 91 Prozent der befragten Unternehmen fest, dass das Datenvolumen bei ihnen innerhalb eines Jahres im Durchschnitt um 22 Prozent zugenommen hat. Ein Drittel der Unternehmen gab an, dass die Datenmenge sogar um 30 Prozent oder mehr gewachsen ist.

Während die Datenmengen stetig anwachsen, müssen für die sichere Nutzung von Big Data in vielen Unternehmen erst noch die Voraussetzungen geschaffen werden: Als Hindernisse für die Nutzung von Big Data sehen viele Unternehmen die Anforderungen an die technische Sicherheit (61 Prozent) und an den Datenschutz (48 Prozent).

Mit einer Lösung wie IBM InfoSphere Guardium lassen sich große und verteilte Datenmengen absichern, indem die vertraulichen Daten gleich mehrfach geschützt werden. Die Lösung erkennt automatisch die zu schützenden Daten auch innerhalb von großen Datenmengen (Big Data), maskiert die vertraulichen Informationen und verschlüsselt die Daten entsprechend ihres Schutzbedarfs. Zusätzlich werden die Zugriffe auf die zu schützenden Daten automatisch überwacht und Verstöße gegen Zugriffsvorgaben gemeldet und abgewehrt. Dabei schützt die Lösung die Daten plattformübergreifend und unterstützt insbesondere auch Big-Data-Umgebungen wie Hadoop-basierte Systeme.

Mehrstufiger Schutz für große Datenmengen und verteilte Datenhaltung

Der Schutz von Big Data erfordert einen umfassenden, intelligenten und risikobasierten Ansatz. Gerade bei großen Datenmengen besteht sonst die Gefahr, dass vertrauliche Daten schlicht nicht berücksichtigt werden und ungeschützt bleiben. Zudem laufen Unternehmen bei der Absicherung von Big Data Gefahr, mit klassischen Sicherheitskonzepten schnell an ihre Grenzen zu kommen. Schutzlösungen für Big Data müssen die vertraulichen Daten vollständig aufspüren und so absichern, dass eine schnelle, performante Maskierung oder Verschlüsselung der Daten erfolgt. Sicherheitslösungen, die nur „Dateninseln“ schützen oder für den Unternehmensalltag viel zu langsam arbeiten, können keinen Big-Data-Schutz gewährleisten.

IBM InfoSphere Guardium sucht und klassifiziert sensible Informationen über die Grenzen von Datenumgebungen hinweg. Auf Basis der Klassifizierung der Daten und der Ermittlung ihrer Speicherorte ist es möglich, automatisch passende Zugriffsregeln festzulegen und deren Einhaltung zu überprüfen. Die Klassifizierungsregeln lassen sich auf interne Sicherheitsrichtlinien des Unternehmens anpassen. Zudem kann die Datensuche und Klassifizierung regelmäßig und zeitgesteuert wiederholt werden, um auf die meist dynamischen Änderungen in der Datenhaltung zu reagieren.

Big-Data-Schutz: Vertrauliche Daten maskieren oder verschlüsseln

Um die vertraulichen Daten entsprechend ihrer Klassifizierung zu schützen, kann IBM InfoSphere Guardium mit verschiedenen Funktionen aufwarten: IBM

InfoSphere Guardium Data Redaction kann vertrauliche Passagen in Dokumenten gegen unberechtigte Kenntnisnahme schwärzen. Dabei hängt die genaue Schwärzung individuell von den Berechtigungen des einzelnen Nutzers ab. Die Datenmaskierung läuft automatisch ab, unterstützt verschiedene Sprachen und lässt sich auf unterschiedliche Dateiformate anwenden, darunter PDF, DOC, XLS oder auch JPG-Bilder.

Der Datenmaskierung kommt eine zentrale Rolle zu, um dem Datenschutz bei der Nutzung von Big Data gerecht zu werden. So fordern sowohl das deutsche Bundesdatenschutzgesetz (BDSG) als auch die geplante EU-Datenschutzgrundverordnung (EU-DSGVO) die Anonymisierung von personenbezogenen Daten, soweit dies nach dem Verwendungszweck der Daten möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

IBM InfoSphere Guardium Data Encryption bietet eine leistungsstarke Verschlüsselung strukturierter und unstrukturierter Daten und führt die Verschlüsselungs- und Entschlüsselungsprozesse ohne nennenswerte Leistungsbeeinträchtigungen durch. Zudem ist die Verschlüsselung flexibel einsetzbar, denn sie erfordert keine Datenbank-, Anwendungs- oder Netzänderungen. Heterogene Datenumgebungen und Big-Data-Anwendungen lassen sich so rundum schützen.

Zugriffe auf Big Data überwachen

Neben der Klassifizierung, Maskierung und Verschlüsselung sensibler Daten auch innerhalb großer Datenmengen bietet die IBM-Lösung ein Monitoring der Datenzugriffe in Echtzeit an. Unerlaubte Datenzugriffe und Angriffsversuche werden aufgedeckt, indem die Zugriffsaktivitäten einer Vergleichsanalyse unterzogen werden. Verdächtige Zugriffe werden an die verantwortlichen Stellen gemeldet und entsprechend des Regelwerks auch blockiert.

Auf Basis der Zugriffsprotokolle und -analysen werden automatisch Berichte erstellt, wie sie von verschiedenen Compliance-Vorgaben gefordert werden. Die Berichte werden entsprechend eines Workflows zur Freigabe oder im Rahmen einer Eskalation verteilt. Damit kann die von Compliance-Regelwerken wie auch von den Datenschutzgesetzen geforderte Zugriffskontrolle auch bei Big-Data-Umgebungen umgesetzt werden. Big-Data-Schutz wird so möglich und damit die sichere Nutzung von Big Data für den Unternehmenserfolg.