

Daten gehören zum wichtigsten Kapital eines Unternehmens!

Checkliste: Datensicherheitskonzept

Die Entwicklung eines Datensicherheitskonzepts ist essenziell, um den **Überblick** über alle **Unternehmensdaten** gewährleisten zu können. Dieses sollte dabei folgende Schutzziele beinhalten:

✓ Vertraulichkeit

- Schutz der Daten und Informationen vor unberechtigten Zugriffen und unbefugten Personen

Folgende Maßnahmen erhöhen die Vertraulichkeit von Daten:

Zutrittskontrollen, Objektsicherungen, Sicherheitszonen, Regelungen der Zutrittsberechtigten, zusätzliche Maßnahmen bei Fernzugriffen

✓ Integrität

- Korrektheit und Vollständigkeit aller Daten und Informationen auch während der Verarbeitung

Folgende Maßnahmen erhöhen die Integrität von Daten:

Wiedergabeprotokolle und Übertragungskontrollen führen, Regelungen bei elektronischer Übertragung, Regelungen bei Speicherungen und Wechseldatenträgern sowie dem Transport von Daten

✓ Verfügbarkeit

- Daten und Informationen stehen für die Verarbeitung jederzeit zur Verfügung

Folgende Maßnahmen erhöhen die Verfügbarkeit von Daten:

Erstellung von Sicherheitskopien, Gewährleistung des laufenden Betriebs, Ausfallsicherheit, unterbrechungsfreie Stromversorgung, redundante Internetverbindung

Um den Datenschutz zu gewährleisten reichen manuelle Methoden nicht aus, verdächtige Aktivitäten in Echtzeit zu identifizieren. Compliance-Vorgaben und potenzielle Audits erhöhen die Komplexität. Daher ist eine automatisierte Lösung gefragt, mit der Sie alle Datenaktivitäten im Blick haben.



Effektiver Schutz von unstrukturierten Daten mit IBM Security Guardium

Mit dieser Plattform können Sie Ihre Informationsressourcen plattformübergreifend mit einem minimalen Aufwand schützen.

Erhalten Sie mit IBM Security Guardium wichtige verwertbare Erkenntnisse, Echtzeitkontrollen und eine automatisierte Compliance-Unterstützung:

Vollständiger datenzentrierter Sicherheitsansatz

Erkennung interner und externer Risiken

- Erkennt und klassifiziert sensible Daten in Dateien und überwacht und prüft kontinuierlich alle Datenaktivitäten

Durchsetzung von Sicherheitsrichtlinien in Echtzeit

- Sicherheitsrichtlinien werden in Echtzeit umgesetzt, unter anderem wird der Zugriff auf sämtliche Daten geregelt. Automatische Identifikation von autorisierten Benutzern sowie Unterbindung nicht-autorisierter User

Erstellung eines zentralisierten Repositorys

- Zeigt detaillierte Berichte zu allen Datenaktivitäten in einer einzigen, zentralen Managementkonsole an

Wichtige Leistungsmerkmale von IBM Guardium Data Protection for Files

- Überwachung und Prüfung aller Datenaktivitäten
- Durchsetzung von Sicherheitsrichtlinien für Dateizugriff und Änderungsmanagement
- Schnellere Compliance-Workflows und Prüfaktivitäten
- Schutz sensibler Daten in heterogenen Umgebungen
- Erkennung und Klassifizierung von Daten in Dateien und Dateisystemen



Einblick

Erhalten Sie einen Einblick, welche Ihrer Daten kritisch sind und machen Sie sich ein umfassendes Bild von den Zugriffen auf diese



Transparenz

Erstellung und Anwendung detaillierter Richtlinien für eine kontinuierliche Transparenz



Sicherheit

Kontrollieren Sie den Zugriff auf wichtige Daten, indem Sie Warnungen erhalten und Blockierungen für diese durchführen



Compliance

Beschleunigung Ihrer Compliance, durch vorkonfigurierte, zentralisierte Berichte und Richtlinien für verschiedene Vorschriften

Tipp: Wenn Sie Fragen zum Thema intelligenter Datenschutz oder zu IBM® Security Guardium® haben sollten, können Sie sich gerne bei unserem Experten melden:

Peter.Siegmann@blue-consult.de