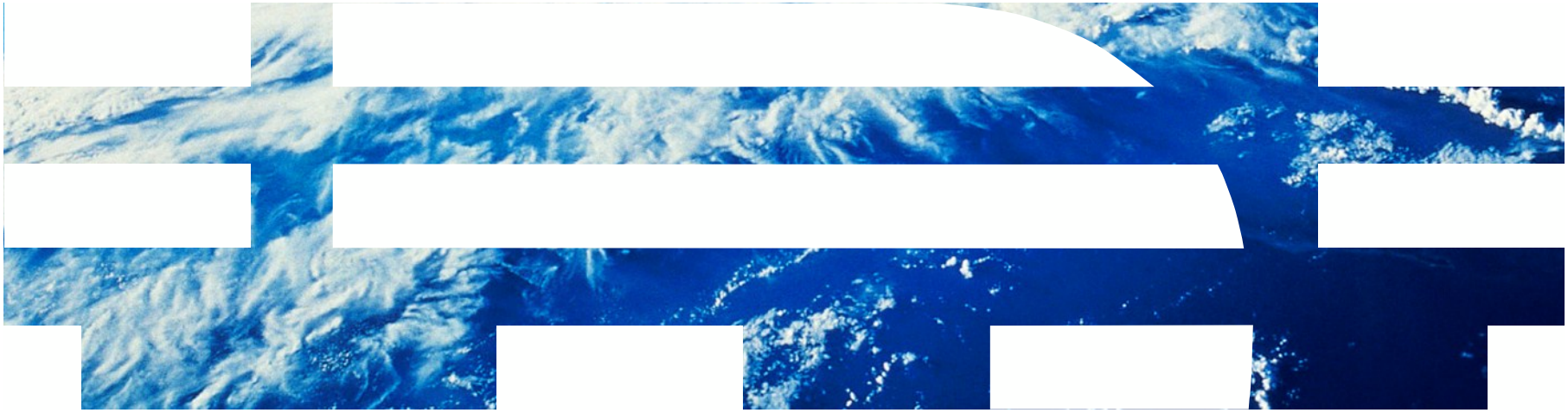
Service Modul DB2 Security HealthCheck



Was ist DB2 Security Health Check?

- Der DB2 Security Health Check wurde erstellt um den Zustand der Sicherheit der Datenbank und Daten abzuschätzen und zu verbessern, um somit zukünftigen kostenintensiven – Security - Engpässen vorzugreifen.
- In der Zeit, in der Phishing, Datenklau, sowie der räuberische Missbrauch der Daten an der Tagesordnung sind, ist eine Überprüfung des eingesetzten Sicherheitskonzeptes eine immer wichtiger werdende Aufgabe.
- Dabei werden Fragen wie:
  - Wie sicher ist mein System und die darin enthaltenen Daten?
  - Entspricht das verwendete Konzept noch den heutigen Anforderungen?
- DB2 Administratoren sind oft mit sehr vielen Aufgaben betraut, so daß oftmals eine ausführliche Analyse bzw. Einarbeitung in die neuen Security-Konzepte und -Möglichkeiten nicht möglich ist.

Wer ist daran beteiligt?

- Wenn Sie einen IBM Consultant mit der Analyse beauftragen, erhalten Sie zusätzlich zu dem DB2 Experten auch noch das geballte Wissen eines führenden Datenbank Herstellers.
- Der Security HealthCheck ist mehr als nur eine Überprüfung, es ist auch eine Möglichkeit Ihre DBA‘s auf den aktuellen Stand der securityspezifischen Eigenschaften der DB2 Datenbank zu bringen.

In folgenden Bereichen bieten wir Unterstützung an:

- Service 1/3: Analyse und Auswertung
  - Analyse und Auswertung des aktuellen Sicherheitsstatus, zugeschnitten auf Ihre konkreten Anforderungen
  - Handlungsempfehlungen zur DB- und Serverhärtung anhand öffentlicher Schwachstellen-Datenbanken sowie anhand von IBM-Best Practices
  - (Option) Automatisierte Schwachstellenanalyse mit InfoSphere Guardium

- Service 2/3: Unterstützung bei der Umsetzung
  - Erstellung des Nutzer-/Rechte-/Rollen-Konzeptes
  - Einrichtung der Userverwaltung und Zugriffskontrollen
  - Einrichtung von Verschlüsselung für „data in motion“ und „data at rest“

- Service 3/3: Weitere Serviceleistungen
  - Neuaufbau von Datenbanken anhand Sicherheitskonzept
  - Migrationen von Datenbanken auf das neue DB2-Rechtekonzept
  - Implementierung und ggf. Anpassung einer automatisierten Schwachstellenanalyse

Service 1/3: Analyse und Auswertung

- Individuelle Analyse
  - Review Ihres Sicherheitskonzeptes
  - Aufnahme Ihrer Erwartungen/Wünsche
  - Überprüfung der sicherheitsrelevanten Datenbank-Konfigurationsparameter anhand Best Practices und für Ihre konkrete Situation
  - Überprüfen aller Nutzer/Gruppen/Rollen und deren Rechte auf der Datenbank
    - auf Systemebene (SYSADM, SYSMON, SYSCTRL, ...), inklusive Auswirkungen auf die Sicherheit, wenn Ausführung mittels Sticky Bit oder „sudo“
    - auf Datenbankebene (DBADM, LOAD, CONNECT, ...)
    - auf Ebene von Tablespaces, Schemata, Objekten (Views, Tables - IUD) sowie Stored Procedures (SP, UDF, Rechte zur Ausführung, fenced user)
- Auswertung der Analyse und Abschätzen Aufwand für sicherheitsrelevante Policies, Regeln und Verfahren
- Unterbreitung von Empfehlungen basierend auf Industriestandards und IBM Best Practices

Service 1/3: Automatisierte Schwachstellenanalyse und –auswertung (Option)

- Automatisierte Schwachstellenanalyse mit InfoSphere Guardium Vulnerability Assessment
  - Mehr als 500 DB-spezifische Tests anhand Best Practices und bereits entdeckter Schwachstellen
  - Quellen: DoD STIG (Security Technical Implementation Guides), CIS (Center for Internet Security), CVE (Common Vulnerabilities and Exposures), IBM X-Force research team
  - Immer aktuell dank Database Protection Knowledgebase
  - Auch plattformübergreifend nutzbar
- Übersichtlicher Bericht mit durchgeführten Tests, Ergebnis sowie ggf. Handlungsempfehlungen
- Auch als regelmäßiger Service buchbar, inklusive Fortschritt / Regression über mehrere Tests

Service 2/3: Unterstützung bei der Umsetzung

- Userverwaltung
  - System, LDAP, Einrichten der Zugriffskontrollen
- Rollen/Gruppenkonzept
  - Trennung zwischen System Admin / Einführung des SECADM
  - Festlegung von Gruppen/Rollen zum Zugriff auf die Datenbank und deren Objekte,
  - Verhindern Zugriff des DBA's auf Tabelleninhalte
  - Zuweisung der minimal erforderlichen Rechte
  - LBAC (Label Based Access Control)
  - Trusted Context and Connection
- Einrichtung von Verschlüsselung (Encryption)
  - Data Encryption: Column-Level, Database Encryption Expert. (“data at rest”)
  - Dataflow Encryption (z. B. SSL), um Sicherheit und Integrität der Datenbank-Kommunikation zu gewährleisten. („data in motion“)

Service 3/3: Weiteres

- Migration
  - bei Verwendung DB2 <10.5, Unterstützung zur erfolgreichen Überführung zum mindestens DB2 9.7 Rechtemodell
- Einrichtung einer automatisierten Schwachstellenanalyse
  - Einrichtung des Guardium Vulnerability Assessments zur regelmäßigen, automatisierten Schwachstellenanalyse
  - Entwicklung und Implementierung individueller Prüfroutinen anhand Ihres Sicherheitskonzeptes
- Wartung
  - Unterstützung bei Erstellung Skripte zur Verwaltung / Bereinigung des Berechtigungskonzeptes

Was wird benötigt?

- Bisherige Sicherheitskonzepte
- Instanz/Datenbank-Konfiguration
- Inhalt der Authentication-Tabellen
- Systemgruppen / -User
- Rechtekonzept/Umsetzung von externen Anwendungen
- Java für automatisiserte Tests mit Guardium

Aufwand

DB2 Security HealthCheck Service	7	
Sichtung existierendes Sicherheitskonzept	1,5 - 2	
Analyse/Sammlung	2	
Auswertung und Workshop zur Auswertung	2,5 – 3	
Unterstützung bei Migrationskonzept, ...	Nach Aufwand	
Durchführung der automatisierten Schwachstellenanalyse mit Guardium	Nach Aufwand	
Einrichtung einer individuellen, automatisierten Schwachstellenanalyse mit Guardium	Nach Aufwand	