Access und SQL Server-Security

AEK 21

Nürnberg/Hannover - Oktober 2018

berndjungbluth.de

Zur Person

- Bernd Jungbluth
- Freiberuflicher Berater und Entwickler
  - Migration Access nach SQL Server
  - Administration SQL Server
  - Entwicklung und Optimierung von SQL Server-Datenbanken
  - Datawarehouse-Systeme
  - SQL Server Reporting Services
  - SQL Server Integration Services
  - SQL Server Sicherheitsanalysen
- Zertifizierter Datenschutzbeauftragter

Agenda

- Datenschutz
  - Sicherheit der Verarbeitung
  - Datenschutz durch Technikgestaltung
- Zugriffsschutz
  - Sicherheitsarchitektur des SQL Servers
  - Berechtigungskonzepte mit SQL Server
- Verschlüsselung
  - Verschlüsselungsmethoden
  - Verschlüsselung mit SQL Server
- Zusammenfassung und Fazit

- Sicherheit der Verarbeitung
  - Sicherheit der Verarbeitung personenbezogener Daten – Artikel 32 DSGVO
  - Treffen von technischen und organisatorischen Maßnahmen
    - Pseudonymisieren und Verschlüsseln
    - Sicherstellen der Vertraulichkeit und Integrität der Systeme und Dienste
    - Sicherstellen der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
    - Sicherstellen einer schnellen Wiederherstellung der Systeme und Dienste
    - Prüfen, Bewerten und Evaluieren der Wirksamkeit der Maßnahmen
- Technisch organisatorische Maßnahmen – TOM
  - Sinnvolle Präzisierung der Maßnahmen im BDSG neu § 64 Abs. 3
    - Zugriffskontrolle, Datenträgerkontrolle, Speicherkontrolle, Benutzerkontrolle, etc.

- Datenschutz durch Technikgestaltung
  - »privacy by design« – »data protection by design« – Artikel 25 DSGVO
  - Gewährleisten der Grundsätze des Datenschutzes durch den Einsatz von Technik
  - *„zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung“* (2)
  - Bei Planung und Beschaffung sowie beim Design neuer Produkte und Dienstleistungen
- Datenschutzfreundliche Voreinstellungen
  - »privacy by default« – »data protection by default« – Artikel 25 DSGVO
  - Begrenzen der Verarbeitung personenbezogener Daten durch Voreinstellung der Systeme
  - *„dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden“* (3)
  - Menge der Daten, Umfang der Verarbeitung, Speicherfrist, Zugangsmöglichkeiten

Datenschutzpannen, die technisch nicht möglich sind, passieren auch nicht! (3)

- Datenschutz
  - Betrifft die personenbezogenen Daten eines Unternehmens
  - Schutz natürlicher Personen vor dem willkürlichem Gebrauch ihrer Daten
  - Schutz des Rechts auf »informationelle Selbstbestimmung«
  - Urteil des Bundesverfassungsgericht vom 15.12.1983 zur Volkszählung
  - *„Freie Entfaltung der Persönlichkeit setzt unter modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.“* (4)
- Datensicherheit
  - Betrifft alle Daten eines Unternehmens
  - Technischer Schutz der Daten eines Unternehmens
  - Vor unbeabsichtigter Veröffentlichung, Verlust, Manipulation und andere Bedrohungen

Agenda

- Datenschutz
  - Sicherheit der Verarbeitung
  - Datenschutz durch Technikgestaltung
- Zugriffsschutz
  - Sicherheitsarchitektur des SQL Servers
  - Berechtigungskonzepte mit SQL Server
- Verschlüsselung
  - Verschlüsselungsmethoden
  - Verschlüsselung mit SQL Server
- Zusammenfassung und Fazit

Zugriffsschutz

- Access
  - Datenbankkennwort
  - Arbeitsgruppen-Informationsdatei – MDW
  - Eigene implementierte Logik – bspw. per Formularsteuerung
- SQL Server
  - Mehrstufige Sicherheitsarchitektur
  - Zugriffsschutz und Rechtevergabe auf Ebene der SQL Server-Instanz
    - Zugriff per Anmeldekonto – »Anmeldung«
  - Zugriffsschutz und Rechtevergabe auf Ebene der Datenbanken
    - Zugriff per Benutzerkonto – »Benutzer«
  - Zwei Authentifizierungsmethoden
    - Windows-Authentifizierung sowie Windows- und SQL Server-Authentifizierung

- Windows-Authentifizierung
  - Anmeldung am SQL Server mit aktueller Windows-Anmeldung
  - »Integrierte Sicherheit« – »trusted connection«
  - Zuordnung zu Windows-Benutzern wie auch zu Windows-Gruppen möglich
  - Empfohlene Authentifizierungsmethode
- SQL Server-Authentifizierung
  - Anmeldung am SQL Server mit Benutzername und Kennwort
  - Nicht empfohlene Authentifizierungsmethode
  - Notwendig u.a. in Umgebungen ohne Windows-Anmeldungen
  - Empfehlungen zur Konfiguration einer SQL Server-Anmeldung
    - Vergabe eines komplexen Kennworts
    - Erzwingen des Ablaufs vom Kennwort sowie der Kennwortrichtlinien

- Anmeldung *sa*
  - Administrationskonto vom SQL Server
  - Aktiviert im Gemischten Modus – Windows- und SQL Server-Authentifizierung
  - Deaktiviert bei reiner Windows-Authentifizierung
  - Aktivieren mit Vergabe eines neuen Kennworts möglich
- Empfehlungen
  - Verwenden nur in Ausnahmefällen
  - Umbenennen in einen unscheinbaren Anmeldenamen
  - Erzwingen des Ablaufs vom Kennwort sowie der Kennwortrichtlinien
  - Vergabe eines komplexen und nicht zu merkenden Kennworts
  - Verwahren des Kennwort an einem sicheren Ort unter 4-Augen-Prinzip
  - Beste Empfehlung: Deaktivieren der Anmeldung *sa*

- Demo
  - Anmeldung *sa* konfigurieren
  - Anmeldung *sa* deaktivieren

- Datenbanken
  - Zugang über Benutzerkonto – »Benutzer«
  - Standardverfahren über Anmeldung
  - Zuordnen einer Anmeldung zu einer oder mehrerer Datenbanken
  - Je Datenbank unterschiedliche Rechtevergabe möglich
  - Steuerung der Rechte
  - Benutzer
  - Datenbankrollen

- Datenbankrollen
  - Systemdatenbankrollen
  - Benutzerdefinierte Datenbankrollen
  - Anwendungsrollen

- Demo
  - Anmeldungen erstellen
  - Benutzer zuordnen

- Serverrolle *sysadmin*
  - Administrationsrechte an SQL Server-Instanz und allen dort enthaltenen Datenbanken
  - Lese- und Schreibrechte an allen Tabellen der SQL Server-Instanz
  - Überwiegt zugewiesenen `DENY`-Rechten innerhalb der Datenbanken
- Datenbankrolle *db_owner*
  - Administrationsrechte an allen Objekten und Eigenschaften der Datenbank
  - Lese- und Schreibrechte an allen Tabellen der Datenbank
  - Mit Ausnahme bei zugewiesenen `DENY`-Rechten an Tabellen
- Empfehlungen
  - Vermeiden von Rollenmitgliedern mit Zuordnung zu Windows-Gruppen
  - Reduzieren der Anzahl der Rollenmitglieder auf das notwendige Minimum

- Demo
  - Serverrolle *sysadmin* und die Rechte der Mitglieder

Agenda

- Datenschutz
  - Sicherheit der Verarbeitung
  - Datenschutz durch Technikgestaltung
- Zugriffsschutz
  - Sicherheitsarchitektur des SQL Servers
  - Berechtigungskonzepte mit SQL Server
- Verschlüsselung
  - Verschlüsselungsmethoden
  - Verschlüsselung mit SQL Server
- Zusammenfassung und Fazit

- Berechtigungskonzept
  - Prinzip der Aufgabentrennung – »Separation Of Duties«
    - Pro Benutzer ein Windows-Benutzerkonto
    - Trennen der Aufgaben einzelner Benutzer
- Umsetzung
  - Analyse und Definition von Prozessen bzw. der Aufgaben der Benutzer
  - Trennen der definierten Prozesse von den Benutzern
  - Zusammenfassen der Benutzer in Gruppen
  - Zusammenfassen der Prozesse in Rollen
  - Zuordnen der Gruppen zu den Rollen
  - Erteilen der Rechte der Rollen an den Objekten der Datenbank
    - Nur die zum Erfüllen der Aufgaben minimal notwendigen Rechte – »Least Privilege«

- Demo
  - Zugriffsberechtigungen mit Access

- Berechtigungskonzept mittels Datenbankrollen
  - Erstellen von Datenbankrollen je Prozess bzw. Aufgaben der Benutzer
  - Zuordnen der Datenbankobjekte zu den Datenbankrollen mit Vergabe der Rechte
    - `SELECT`, `INSERT`, `UPDATE`, `DELETE` und `EXECUTE`
  - Zuordnen der Datenbank-Benutzer zu den Datenbankrollen
- Bewertung
  - Hoher Aufwand bei der Konzepterstellung
  - Hoher Aufwand bei der Rechtevergabe
    - Vergabe der Rechte für jedes einzelne Datenbankobjekt einer Datenbankrolle
  - Gilt für jeden autorisierten Datenzugriff
    - Auch für Datenzugriffe über nicht gewünschte Applikationen

- Demo
  - Rechtevergabe per Datenbankrollen

- Berechtigungskonzept mittels Schemata
  - Erstellen von Schemata je Prozess bzw. Aufgaben der Benutzer
  - Zuordnen der Datenbankobjekte zu den jeweiligen Schemata
    - Fachliche Kategorisierung der Datenbankobjekte in Schemata
  - Zuordnen der Benutzer zu den Schemata mit Vergabe der Rechte
    - `SELECT`, `INSERT`, `UPDATE`, `DELETE` und `EXECUTE`

- Bewertung
  - Mittlerer bis hoher Aufwand bei der Konzepterstellung
  - Mittlerer Aufwand bei der Rechtevergabe
    - Vergabe der Rechte für alle Datenbankobjekte eines Schemas
  - Gilt für jeden autorisierten Datenzugriff
    - Auch für Datenzugriffe über nicht gewünschte Applikationen

- Demo
  - Rechtevergabe per Schemata

- Berechtigungskonzept mittels Schemata und Gespeicherte Prozeduren
  - Erstellen einzelner Schemata je Prozess bzw. Aufgaben der Benutzer
  - Erstellen einzelner Gespeicherter Prozeduren für jegliche Datenzugriffe
  - ➢ Fachliche Kategorisierung der Gespeicherten Prozeduren
  - Zuordnen der Schemata zu den Benutzern mit Vergabe des Rechts EXECUTE
  - Keine Berechtigungsvergabe für den Zugriff auf Tabellen und Sichten
- Bewertung
  - Geringer Aufwand bei der Konzepterstellung
  - Geringer Aufwand bei der Rechtevergabe
  - ➢ Vergabe des Rechts EXECUTE für alle Gespeicherte Prozeduren eines Schemas
  - Gilt für jeden autorisierten Datenzugriff
  - ➢ Jedoch ausschließlich über die Gespeicherten Prozeduren

- Demo
  - Rechtevergabe per Schemata und Gespeicherte Prozeduren

- SQL Server-Zugriffsrechte bei eingebundenen Tabellen
  - Prüfen der Zugriffsrechte beim Zugriff auf eingebundene Tabelle
  - Auswirkung der Zugriffsrechte abhängig von der Authentifizierungsmethode
- Windows-Authentifizierung
  - Zugriff mit den Rechten des angemeldeten Benutzers
    - Einmaliges Einbinden der Tabellen ausreichend
- SQL Server-Authentifizierung
  - Zugriff mit den Rechten der gespeicherten SQL Server-Anmeldung
    - Beim Einbinden der Tabellen verwendete SQL Server-Anmeldung
  - Bei Benutzerwechsel erneutes Einbinden der Tabellen erforderlich
  - Benutzerwechsel erst nach Neustart der Access-Applikation wirksam

- Demo
  - Access und SQL Server-Authentifizierung

Agenda

- Datenschutz
  - Sicherheit der Verarbeitung
  - Datenschutz durch Technikgestaltung
- Zugriffsschutz
  - Sicherheitsarchitektur des SQL Servers
  - Berechtigungskonzepte mit SQL Server
- Verschlüsselung
  - Verschlüsselungsmethoden
  - Verschlüsselung mit SQL Server
- Zusammenfassung und Fazit

- Symmetrische Schlüssel
  - Symmetrisches Verfahren mit einem Schlüssel
  - Gleicher Schlüssel zum Verschlüsseln und Entschlüsseln
- Asymmetrische Schlüssel
  - Asymmetrisches Verfahren mit öffentlichem und privatem Schlüssel
  - Verschlüsseln mit öffentlichem Schlüssel
  - Entschlüsseln mit privatem Schlüssel
- Zertifikat
  - Bestätigt den Eigentümer und die Eigenschaften eines öffentlichen Schlüssels
  - Enthält zusätzlich Name des Eigentümers, Betreff, Gültigkeitsdauer, u.a.
  - Enthält öffentlichen Schlüssel und optional auch den privaten Schlüssel

Agenda

- Datenschutz
  - Sicherheit der Verarbeitung
  - Datenschutz durch Technikgestaltung
- Zugriffsschutz
  - Sicherheitsarchitektur des SQL Servers
  - Berechtigungskonzepte mit SQL Server
- Verschlüsselung
  - Verschlüsselungsmethoden
  - Verschlüsselung mit SQL Server
- Zusammenfassung und Fazit

- SQL Server
  - Verschlüsselungsmethoden
    - Symmetrische Schlüssel
    - Asymmetrische Schlüssel
    - Zertifikate
  - Objekte in einer Datenbank
- Möglichkeiten
  - Daten mit T-SQL und »Always Encrypted«
  - Datenbanken mit »Transparent Data Encryption« – TDE
  - Netzwerkübertragung
  - Datenbanksicherungen

- T-SQL
  - T-SQL-Befehle zum Ver- und Entschlüsseln von Daten
    - Per Symmetrischem Schlüssel mit `ENCRYPTBYKEY` und `DECRYPTBYKEY`
    - Per Asymmetrischem Schlüssel mit `ENCRYPTBYASYMKEY` und `DECRYPTBYASYMKEY`
    - Per Zertifikat mit `ENCRYPTBYCERT` und `DECRYPTBYCERT`
    - Per Zeichenfolge mit `ENCRYPTBYPASSPHRASE` und `DECRYPTBYPASSPHRASE`
  - Performanceverlust durch Ver- und Entschlüsseln

- Access und per T-SQL verschlüsselte Daten
  - Kein Ver- und Entschlüsseln der Daten beim Zugriff auf eingebundene Tabellen
  - Ver- und Entschlüsseln der Daten nur mit entsprechenden T-SQL-Befehlen
    - Datenzugriff per Pass Through-Abfragen
    - Mit entsprechenden T-SQL-Befehlen – oder besser mittels Gespeicherter Prozeduren

- Demo
  - Symmetrischen Schlüssel anlegen
  - Daten per T-SQL verschlüsseln und entschlüsseln

- »Always Encrypted«
  - Automatisches Ver- und Entschlüsseln der Daten einzelner Spalten einer Tabelle
  - Nur möglich mit Zertifikat aus externem Zertifikatsspeicher
  - Erlaubt das Trennen der Datenbesitzer von den Datenverwaltern
  - Lesen und Ändern der Daten nur mit den dafür vorgesehenen Applikationen
  - Verhindert Lesen und Ändern der Daten durch Administratoren

- Access und »Always Encrypted«
  - Automatisches Ver- und Entschlüsseln der Daten beim Zugriff auf eingebundene Tabellen
  - Erfordert »ODBC Treiber 13 für SQL Server« und höher
  - Aktivieren der ODBC-Eigenschaft *Spaltenverschlüsselung*
  - Erweitern der Verbindungszeichenfolge mit `ColumnEncryption=Enabled`
  - Benötigt Zugriffsrechte auf das Zertifikat

- Demo
  - Access und »Always Encrypted«

Agenda

- Datenschutz
  - Sicherheit der Verarbeitung
  - Datenschutz durch Technikgestaltung
- Zugriffsschutz
  - Sicherheitsarchitektur des SQL Servers
  - Berechtigungskonzepte mit SQL Server
- Verschlüsselung
  - Verschlüsselungsmethoden
  - Verschlüsselung mit SQL Server
- Zusammenfassung und Fazit

Zusammenfassung und Fazit

- Maßnahmen zur Sicherheit der Verarbeitung
  - Pseudonymisieren und Verschlüsseln
  - Sicherstellen der Vertraulichkeit und Integrität der Systeme und Dienste
  - Sicherstellen der Verfügbarkeit und Belastbarkeit der Systeme und Dienste
  - Sicherstellen einer schnellen Wiederherstellung der Systeme und Dienste
  - Prüfen, Bewerten und Evaluieren der Wirksamkeit der Maßnahmen
- Verschlüsselung
  - Ver- und Entschlüsselung von Daten mit T-SQL-Befehlen
  - Automatische Verschlüsselung einzelner Spalten einer Tabelle mittels »Always Encrypted«
  - Verschlüsselung gesamter Datenbanken mittels »Transparent Data Encryption«
  - Verschlüsselte Netzwerkübertragung
  - Verschlüsselte Datenbanksicherungen

Zusammenfassung und Fazit

- Vertraulichkeit und Integrität
  - Rechtevergabe auf Ebene der SQL Server-Instanz und auf Ebene der Datenbanken
  - Berechtigungskonzepte per Datenbankrollen und Schemata
  - Konfiguration der SQL Server-Dienste mit wirksamen Dienstkonten
  - Sichere Firewall-Einstellung durch eigens definierte Ports
- Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit
  - Ausfallsicherheit mit AlwaysOn, Datenbankspiegelung und Transaktionsprotokollversand
  - Vollsicherung, differenzielle Sicherung und Transaktionsprotokollsicherung von Datenbanken
- Kontrolle der Maßnahmen
  - Überwachung mit SQL Server-Audit, Anmeldeüberwachung und XEvents
  - Sicherheitsrisikobewertungen und Richtlinienverwaltung in SQL Server

- Seminar »Datenschutz mit SQL Server«
  - Aktiver Datenschutz – realisiert mit Funktionen vom SQL Server
  - Konfiguration der SQL Server-Dienste und der Firewall
  - Klassifizieren von Daten, Zugriffsberechtigungen und Verschlüsselung
  - Überwachung mittels Richtlinien und SQL Server-Audits
  - 2-tägiges Seminar
- Termin, Ort, Preis und Anmeldung
  - 27. und 28. November 2018
  - Hotel Ebertor in Boppard am Rhein
  - 799 Euro zzgl. MwSt.
  - 25 Euro Rabatt für AEK-Teilnehmer
  - Anmeldung per E-Mail an *workshop@berndjungbluth.de*

Danke

Noch Fragen?

Vielen Dank für die Aufmerksamkeit.

Quellenangaben

(1) Artikel 25 Abs. 1 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung – DSGVO
(2) Artikel 25 Abs. 2 – EU-Verordnung 2016/679 – Datenschutz-Grundverordnung – DSGVO
(3) Quelle unbekannt
(4) www.wikipedia.de – Artikel *Volkszählungsurteil*