

Hit Me Baby Three More Time

Live Hacking SQL Server



Zur Person

■ Bernd Jungbluth

- Freiberuflicher Berater, Entwickler und Coach
 - Access und SQL Server
 - SQL Server Administration und Datenbankentwicklung
 - Datawarehouse-Systeme, Integration Services, Reporting Services
 - Azure SQL Database
 - Informationssicherheit, Datensicherheit und Datenschutz
- Zertifizierter Datenschutzbeauftragter und Zertifizierter IT-Grundschutz-Praktiker (BSI)

■ Agenda

- The First Cut Is The Deepest
- Kuckuck, Kuckuck, ruft's aus dem Wald
- Let Me In

Fall 1

The First Cut Is The Deepest

Cat Stevens - 1967

Fall 1

■ Sicherheitslücken

- Verbindung vom Client zum SQL Server über SQL Server-Anmeldung sa
- Access-Applikation nicht verschlüsselt
- Kennwort zur SQL Server-Anmeldung sa lesbar

■ Sicherheitsmaßnahmen

- Keine Verbindung vom Client zum SQL Server über SQL Server-Anmeldung sa
- Zugang über eigens erstellte SQL Server-Anmeldung
- Zugang der Applikation auf die Zieldatenbank begrenzen
- Protokollieren der Anmeldevorgänge mit der SQL Server-Anmeldung sa
- SQL Server-Audit mit Ziel Windows-Ereignisprotokoll
- Besser: Deaktivieren der SQL Server-Anmeldung sa

Fall 2

Kuckuck, Kuckuck, ruft's aus dem Wald

Traditional

Fall 2

■ Sicherheitslücken

- SQL-Injection durch dynamisches erzeugte SQL-Anweisungen
- Anmeldung als Datenbank-Benutzer in Datenbankrolle db_owner

■ Sicherheitsmaßnahmen

- Vermeiden der Datenbankrolle db_owner
 - Nutzen der Systemdatenbankrollen db_datareader und db_datawriter
- Besser: Dedizierte Rechtevergabe nach Least Privilege
 - Zugang zur Datenbank per Windows-Authentifizierung der Mitarbeiter und Mitarbeiterinnen
 - Datenbankrollen pro Aufgabe mit Zugriffsrechten an den Objekten zur Aufgabe
 - Beispiel: Zugriffsrechte an Tabelle Mitarbeiter für die Datenbankrolle Personal
- Vermeiden von dynamisch erzeugten SQL-Anweisungen
 - Verwenden von Suchbegriffen als Parameter von Gespeicherten Prozeduren

Fall 3

Let Me In

Beatsteaks - 2002

Fall 3

■ Sicherheitslücke

- Dienst SQL Server VSS Writer und SQL Server-Anmeldung NT SERVICE\SQLWriter
 - Erforderlich zum Sichern der Datenbankdateien durch Sicherungssoftware

■ Sicherheitsmaßnahmen

- Sicherung der Datenbanken nur durch Datenbanksicherung per BACKUP-Befehl
 - Keine Sicherung der Datenbankdateien mit Sicherungssoftware
 - Deaktivieren des Diensts SQL Server VSS Writer
 - Entfernen der SQL Server-Anmeldung NT SERVICE\SQLWriter aus Serverrolle sysadmin
 - Deaktivieren der SQL Server-Anmeldung NT SERVICE\SQLWriter
- Protokollieren von Änderungen in der Serverrolle sysadmin
 - SQL Server-Audit mit Ziel Windows-Ereignisprotokoll
- Informieren der Systemadministratoren über die Protokollierung – zur Abschreckung

Fazit

■ Fall 1 – Anmeldung sa

- Der Klassiker ... Leider immer noch
- Keine Verbindung vom Client zum SQL Server über SQL Server-Anmeldung sa
- Dedizierte Rechtevergabe nach dem Prinzip Least Privilege

■ Fall 2 – SQL-Injection

- Alt, effektiv ... und leider immer noch verbreitet
- Ausführen von Gespeicherten Prozeduren anstelle generierter SQL-Anweisungen
- Dedizierte Rechtevergabe nach dem Prinzip Least Privilege

■ Fall 3 – Ein Admin ist ein Admin

- Kein kompletter Ausschluss von System-Administratoren im SQL Server möglich
- Überwachen der Aktivitäten der System-Administratoren rund um und im SQL Server

Danke

**Heute ist nicht alle Tage.
Das Thema kommt wieder.
Keine Frage.**

Frei nach „Paulchen Panther“

Danke

Noch Fragen?

✉ *info@berndjungbluth.de*

Vielen Dank für die Aufmerksamkeit.