SQL Server Datenbanken Verschlüsselung unter der Beachtung der Datenschutz-Grundverordnung mit DbDefence

Kathegorie
SQL Server

Simon
Schlaipfer

In diesem Beitrag wollen wir uns mit einem der wichtigsten, aber oft außer Acht gelassenem, Thema der Informatik widmen, dem **Datenschutz**. 90% aller Daten dieser Welt sind in den letzten zwei Jahren entstanden und es werden jeden Tag mehr und mehr. In einer Zeit, in der das Wachstum einer gigantischen Ansammlung an Daten, die meistens unternehmenskritische Informationen enthalten, kein Ende kennt und sich stetig fortsetzt, ist der Schutz dieser Daten von essenzieller Bedeutung.
Aus diesem Grund hat die Europäische Union die sogenannte Datenschutz-Grundverordnung (**DSGVO**) erlassen, die ab dem 25. Mai 2018 angewendet wird.

Bei der **DSGVO** handelt es sich um eine Verordnung mit der die Regeln zur Verarbeitung personenbezogener Daten durch die meisten Datenverarbeiter, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.
Die **DSGVO** gilt hierbei nicht nur für große Unternehmen in der EU, sondern für jedes Unternehmen, das Geschäfte in der EU macht – auch wenn diese nur über eine einzelne, sehr kleine SQL Server Datenbank verfügen.

Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612

Basierend auf den Bestimmungen in den Artikeln 23 und 30, in denen allgemeine Praktiken zum Schutz von Kundendaten, zum Löschen und zum Zugriff des Kunden auf die Daten beschrieben sind, kann bei Nichteinhaltung der **DSGVO** mit sehr hohen Busgeldern gerechnet werden.
Doch auch über die **DSGVO** und potentielle Geldstrafen hinaus ist es sehr ratsam, die eigenen Daten zu schützen. Beispielsweise sollten Kundendaten auch unabhängig von der **DSGVO** geschützt sein, um so auch ein gewisses Vertrauen zu dem eigenen Kundenstamm aufzubauen. Doch auch bei eigenen, unternehmensinternen Daten, sollte die Wichtigkeit eines guten Schutzes nicht außer Acht gelassen werden. Stell dir vor, Du vertraust einer Organisation Deine Informationen an, die anschließend von dieser nicht gut geschützt werden. Dies hätte direkte Auswirkungen auf Dich und Dein Unternehmen und könnte fatale Folgen nach sich ziehen.

Was kannst Du also tun, um gegen solche Szenarien bestmöglich geschützt zu sein? Wir wollen uns in diesem Beitrag auf den Schutz von Online-Kundendaten auf SQL Server beschäftigen.

Mögliche Verschlüsselungsmethoden mit SQL Server und ihre Hürden

SQL Server bietet hier eine Reihe von Möglichkeiten zum Verschlüsseln und Schützen der eigenen Daten. Eine dieser Optionen ist die

Verschlüsselung auf Spaltenebene.

Eine zweite Möglichkeit ist die sogenannte

Transparente Datenverschlüsselung.

Da für die Verschlüsselung auf Spaltenebene Programmieränderungen zum Ver- und Entschlüsseln der Daten vorgenommen werden müssen, entspricht sie nur dann einer praktikablen Lösung, wenn nur wenige Spalten geändert werden müssen und der gesamte Datenzugriff über **stored procedures** erfolgt.

Die transparente Datenverschlüsselung ist nur in der Enterprise Edition von SQL Server verfügbar, wodurch die Upgrade-Zeit und die damit verbunden Lizenzkosten bei zahlreichen Installationen von Standard- und Express-Editionen von SQL Server schnell unerschwinglich werden.
Weiterhin stellt das Finden und Filtern aller vertraulichen Daten innerhalb eines Unternehmens, die dringend geschützt werden müssen, eine gewisse Herausforderung dar. Auch wenn Du viele Datenbanken, Tabellen und Spalten kennst die Dein Unternehmen zum Speichern von wichtigen Kundendaten verwendet, kannst Du Dir nicht sicher sein, dass Du Dir wirklich über alle Daten bewusst bist. Beispielsweise können sich auch in Notizfeldern und Kommunikationsprotokollen oder in Tabellenspalten, in der diese vielleicht nicht erwartet werden, kritische Kundendaten befinden.
Wie kannst Du Dir also sicher sein, dass Du wirklich alle Daten kennst die Schutz brauchen und wie kannst Du diese finden, ohne akribisch alle Felder innerhalb einer Datenbank zu untersuchen? Wäre es nicht optimal eine einzige Verschlüsselung auf einem gesamten SQL Server anwenden zu können, um so Online-Datenbanken und Sicherungen zu schützen?

Hier kommt nun **DbDefence** ins Spiel. Hierbei handelt es sich um von **Activecrypt** entwickelte Software die seit dem Jahre 2011 im Einsatz ist und sich auf die Verschlüsselung ganzer SQL Server Umgebungen konzentriert. Die aktuellste Version **7.3** bietet folgende Funktionen:

- **1 Button 128-Bit- oder 256 Bit-AES Verschlüsselung**
  Einfache Schnittstelle zum Konfigurieren, Verschlüsseln und Entschlüsseln von Datenbanken mit einer FIPS 140-2-validierten Lösung
- **Keine Anwendungsänderungen**
  Echte transparente Datenverschlüsselung für alle Editionen (Standard, Express, Web, LocalDB, Enterprise) und Versionen (2019, 2017, 2016, 2014, 2012, 2008 R2, 2008, 2005) von SQL Server
- **Automatisierung**
  Umfassende T-SQL-API zur Verwaltung der Verschlüsselung einer SQL Server-Datenbank zur Automatisierung des Prozesses
- **Leistung**
  Schnelle Ver- und Entschlüsselung für SQL Server-Datenbankobjekte und -daten mit minimalem Overhead
- **Anpassung**
  Möglichkeit, die Verschlüsselung für bestimmte Tabellen, Anmeldungen und Anwendungen anzupassen

Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612

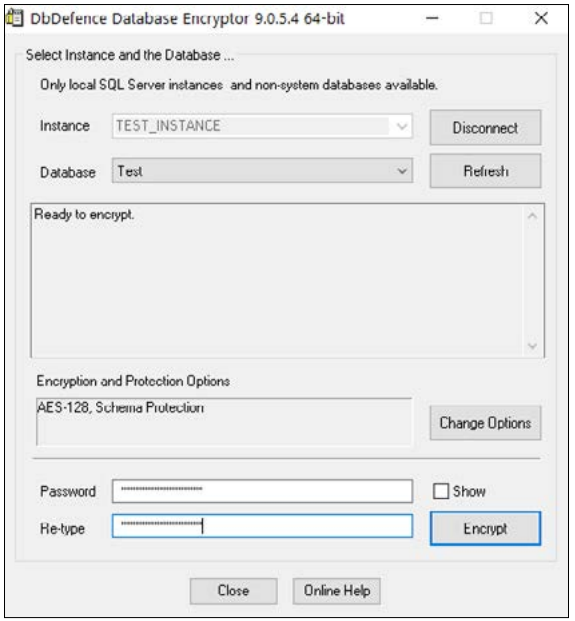
- **Anmelde- oder Anwendungsbeschränkungen**
  Möglichkeit, den Zugriff auf die Datenbank so einzuschränken, dass nur bestimmte Anmeldungen unabhängig von ihren SQL Server-Serverrollen oder Anmeldeberechtigungen auf die Datenbank zugreifen können
- **Anwendungsbeschränkungen**
  Möglichkeit, bestimmte Anwendungen (einschließlich Profiler) oder IIS-Anwendungspools auf den Zugriff auf die Datenbank zu beschränken, um sich vor internen und externen Bedrohungen zu schützen
- **Schutz**
  Zertifikatsbasierte Verschlüsselung zum Schutz der Datenbank online und aller Sicherungen
- **Hochverfügbarkeit**
  Möglichkeit zum Übertragen von Zertifikaten zwischen Servern zur Unterstützung von Protokollversand-, Replikations- und Verfügbarkeitsgruppen
- **Mehrschichtschutz**
  Möglichkeit, eine Lizenz an einen Client zu binden, sodass eine Datenbank ohne die Client-Lizenz nicht wiederhergestellt werden kann, um beim Wiederherstellen der Datenbank eine weitere Schutzschicht hinzuzufügen

Bei der Verwendung von **DbDefence** muss lediglich der Verschlüsselungsschlüssel für die gewünschte Datenbank geschützt und verwaltet werden, um die Datenbank zu sperren und zu entsperren. Abhängig von der Größe der Datenbank kann innerhalb einer Stunde die gesamte Datenbank verschlüsselt werden.

Schauen wir uns nun mal an einem Praktischen Beispiel **DbDefence** genauer an.

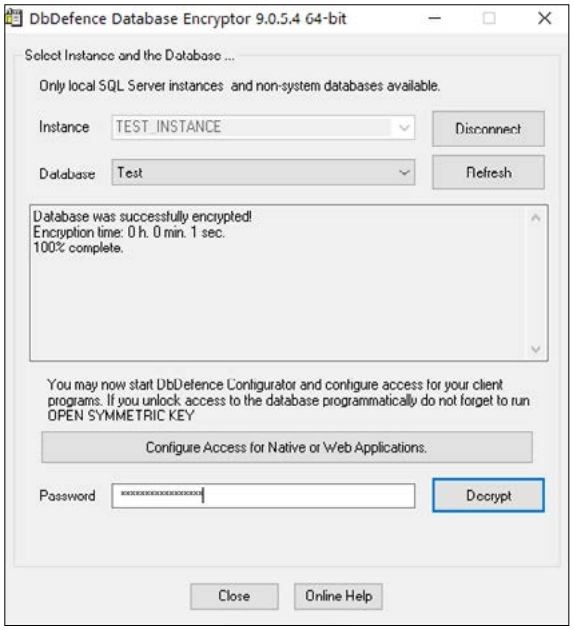
SQL Server mit DbDefence für eine Datenbank Verschlüsselung konfigurieren

Um mit der Verschlüsselung der Datenbank zu beginnen, installieren wir zunächst **DbDefence**, was hier heruntergeladen werden kann. Nachdem wir die Installation abgeschlossen haben, starten wir **DbDefence** und wählen die Instanz und die Datenbank aus, die wir verschlüsseln wollen. Wir verwenden in diesem Beispiel eine SQL Server 2019 Instanz mit dem Namen **TestInstance**. Nach der Authentifizierung können wir den Verschlüsselungsschlüssel in Form eines Passworts festlegen und anschließend auf den Verschlüsselungs-Button Klicken. Je nach Größe der Datenbank kann die Verschlüsselungszeit von wenigen Sekunden bis zu einer Stunde dauern. Diese Verschlüsselungsstufe gilt für alle Standardparameter.



Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612

Um die Datenbank nun wieder zu entschlüsseln, müssen wir nun Verschlüsselungsschlüssel, den wir vor dem Verschlüsseln festgelegt haben, eingeben:



Um Anpassungen vorzunehmen, können wir nun die Datenbank entschlüsseln und anschließend auf den Button **change options** Klicken. Unter der Registerkarte **Encryption** können wir nun die verschlüsselten Objekte und Schemas anpassen, die AES-Verschlüsselungstufe ändern und die Daten verwalten, die der SQL Server Profiler anzeigen kann.

(siehe Bild A)

Unter dem Reiter **Key Storage** kannst Du konfigurieren, ob die durch die Windows-Datenschutz-API geschützten Schlüssel im Dateisystem oder in Windows-Interna speichert sind. Weiterhin besteht die Möglichkeit, Schlüssel in PKCS# 11 – kompatiblen Hardwaregeräten speichern.

(siehe Bild B)

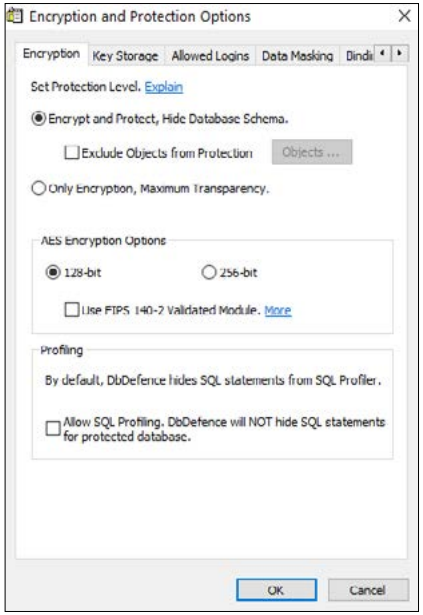


Bild A

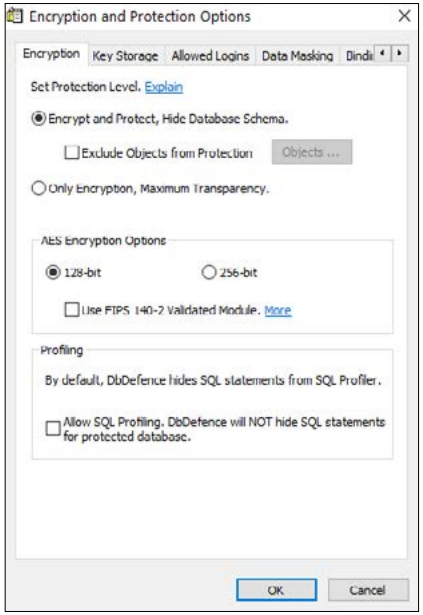
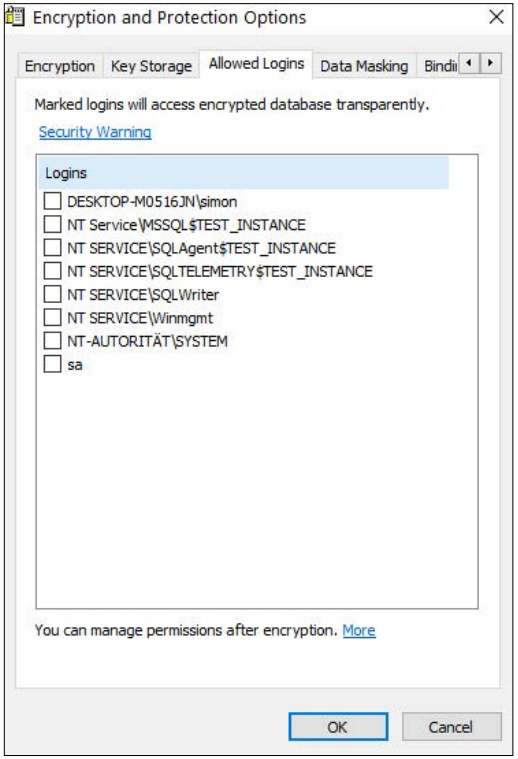


Bild B

Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612

Anwendungszugriff mit DbDefence beschränken

Neben den Verschlüsselungsoptionen bietet **DbDefence** auch die Möglichkeit, den Zugriff auf eine SQL Server Datenbank durch Anmeldung zu beschränken. Über die Registerkarte **Allowed Logins** kann der Zugriff auf eine Datenbank eingeschränkt werden. Hierbei ersetzen die neu konfigurierten Einschränkungen die SQL Server Anmelde- und Serverrollenberechtigungen.



SQL Server Backup-Verschlüsselung mit DbDefence

SQL Server Datenbanksicherungen können mit einem einfachen Texteditor geöffnet und die enthaltenen Daten im Klartext angezeigt werden. **DbDefence** beseitigt diese "Sicherheitslücke". Ein Backup einer mit **DbDefence** verschlüsselten Datenbank ist auch offline verschlüsselt und die Daten können nicht eingesehen werden.

Fazit

DbDefence ist ein sehr vielseitiges und mächtiges Tool, um SQL Server Datenbanken sicher zu verschlüsseln. Der Schutz von wichtigen Daten, sowohl geschäftlich als auch privat, ist ein wichtiger Schritt den man, zumindest im Produktionsbereich eines Unternehmens, ernst nehmen und verfolgen sollte. Probiere **DbDefence** doch einfach mal selbst aus, und schaue, ob es Deinen Vorstellungen und Ansprüchen entspricht.

Mainzer Datenfabrik GmbH
Rotterdamer Platz 2, 55120 Mainz
info@madafa.de
madafa.de
+49 6131 3331612