Schutz der GoldMine KDM Datenbank mit DbDefence

1.0 , 1. Juni 2013

Einführung

Als das Rückgrat eines jeden digitalen Unternehmens sind Datenbanken für das Funktionieren von Organisationen, ob es sich nun um große Kapitalgesellschaften oder kleine Firmen, die von zu Hause aus geleitet werden, handelt, unentbehrlich. Aus diesem Grund ist es äußerst wichtig, dass Datenbanken geschützt werden. Dieses Informationsblatt erklärt Ihnen, wie das zu tun ist, selbst wenn Sie mit der Datenbank-Administration und -Programmierung nicht vertraut sind.

GoldMine ist eine beliebte Kundendienst-Management-Lösung, die bereits weltweit im Einsatz ist und häufig für die Speicherung vertraulicher Daten verwendet wird. Mit dem jährlichen Anstieg der digitalen Kriminalität war die Verschlüsselung zum Schutz Ihrer Datenbanken und der darin enthaltenen Daten noch nie so wichtig wie heute.

Für die Zwecke dieses Informationsblattes haben wir die kostenlose, dreißig Tage Probeversion von GoldMine benutzt, die unter anderem Daten zur Demonstration und zu Testzwecken enthält, um es potentiellen Kunden zu ermöglichen, die Software auch ohne Eingabe ihrer eigenen Daten auszuprobieren, um zu sehen, wie sie funktioniert. Es ist außerdem eine kostenlose Version von DbDefence erhältlich, die mit Datenbanken von bis zu 200 MB arbeiten kann. Auf der anderen Seite kann die zahlungspflichtige Version von DbDefence für dreißig Tage ausprobiert werden. Bitte wenden Sie sich an support@dbdefence.com. DbDefence ist zum Herunterladen von deren Webseite www.dbdefence.com/ erhältlich. Wenn Sie an unserem Produkt interessiert sind, können wir Ihnen eine Reihe verschiedener Preisoptionen anbieten, die abhängig von der Größe Ihrer Datenbank sind. Die Preise beginnen bei $698 pro Server.

Transparente Verschlüsselung

Für den Fall, dass jemand unbefugt in Ihren Server eindringt, hätte dieser keine Probleme damit, die Daten in der Datenbank zu lesen oder sie sogar komplett zu stehlen, da der Inhalt sich in einem klaren, gut lesbaren Format befände, das lediglich durch die Verbindung der Datenbank zu einem SQL-Server angeschaut werden könnte.

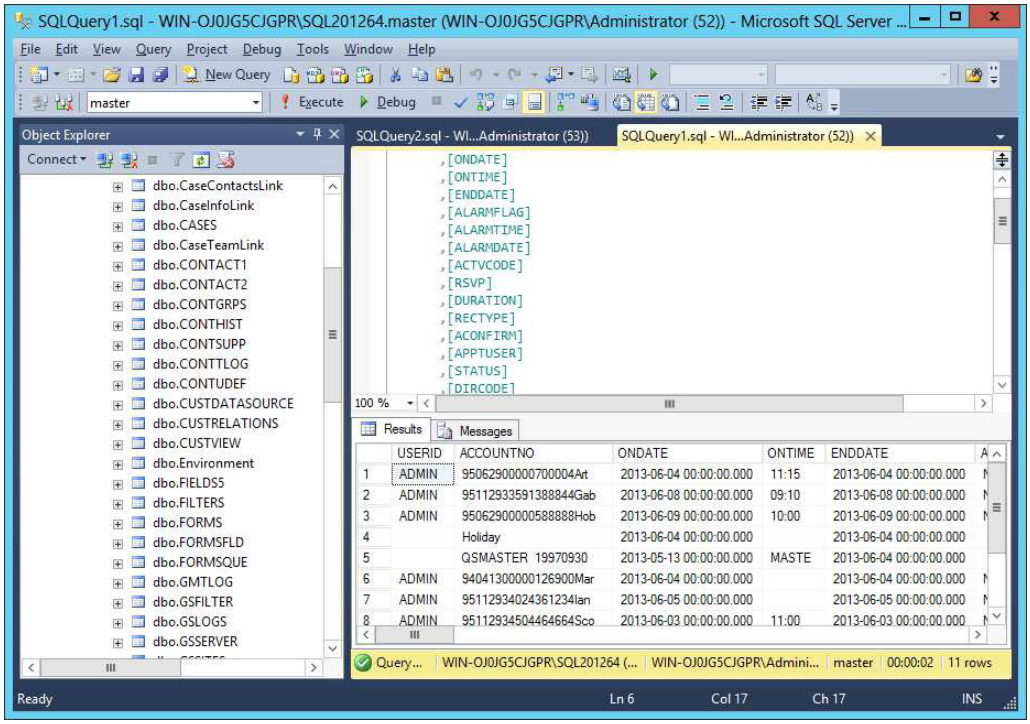

Abb. 1 - Wie eine SQL-Server Management-Konsole aussieht, wenn sie dabei ist, Daten zu erfragen. Ein SQL-Administrator hat Zugriff auf den gesamten Inhalt der Datenbank.

DbDefence hat die Fähigkeit, jede Instanz eines SQL-Servers mit transparenten Verschlüsselungs-Funktionen zu versorgen – einschließlich der modernen Versionen – ohne die Notwendigkeit, die Anwendungen zu ändern, die Sie verwenden, um auf besagte Datenbank zuzugreifen. Dieses Informationsblatt erläutert, wie DbDefence verwendet werden muss, um diesen Effekt zu erreichen.

Es gibt eine ähnliche Funktion, transparente Daten-Verschlüsselung (TDE - Transparent Data Encryption) genannt, die in der SQL-Server Unternehmens-Version zur Verfügung steht. Der Preis der Unternehmens-Version macht diese Lösung für kleinere Unternehmen jedoch eher unrealistisch.

Installation

Erst einmal müssen Sie DbDefence installieren [Abb. 2]. Wenn Sie es nicht bereits getan haben, laden Sie die dreißig Tage Testversion von www.dbdefence.com herunter. DbDefence muss auf demselben Computer installiert werden, von dem aus der SQL-Server arbeitet. Die Installation selbst ist sehr einfach, aber wir werden Sie durch die einzelnen Schritte hindurch begleiten.

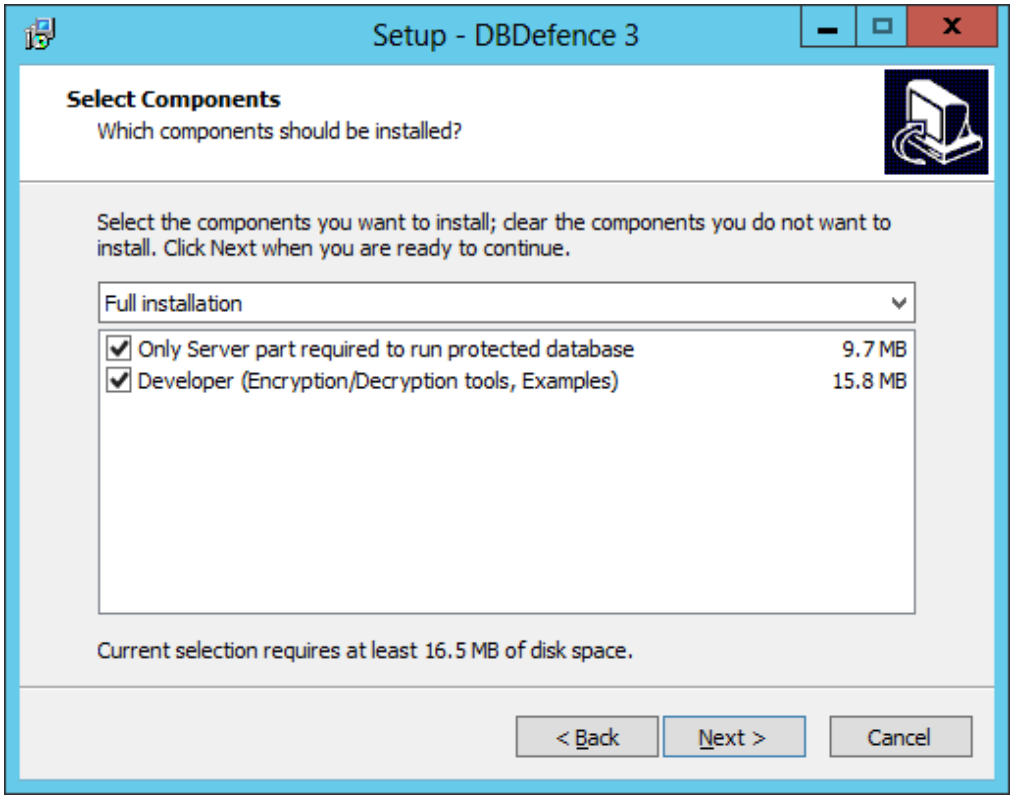

Abb. 2 - DbDefence Installations-Bildschirm „Komponenten wählen“

Die Installation wird Sie bitten, sich bei einem SQL-Server anzumelden [Abb. 3] und Ihnen eine Liste mit allen lokal-installierten SQL-Servern zur Auswahl anbieten. Sie müssen sich nur bei dem SQL-Server anmelden, den Sie schützen möchten. Sie müssen sich als Administrator anmelden, so dass dem DbDefence Installationsprogramm voller Zugriff gewährt wird.

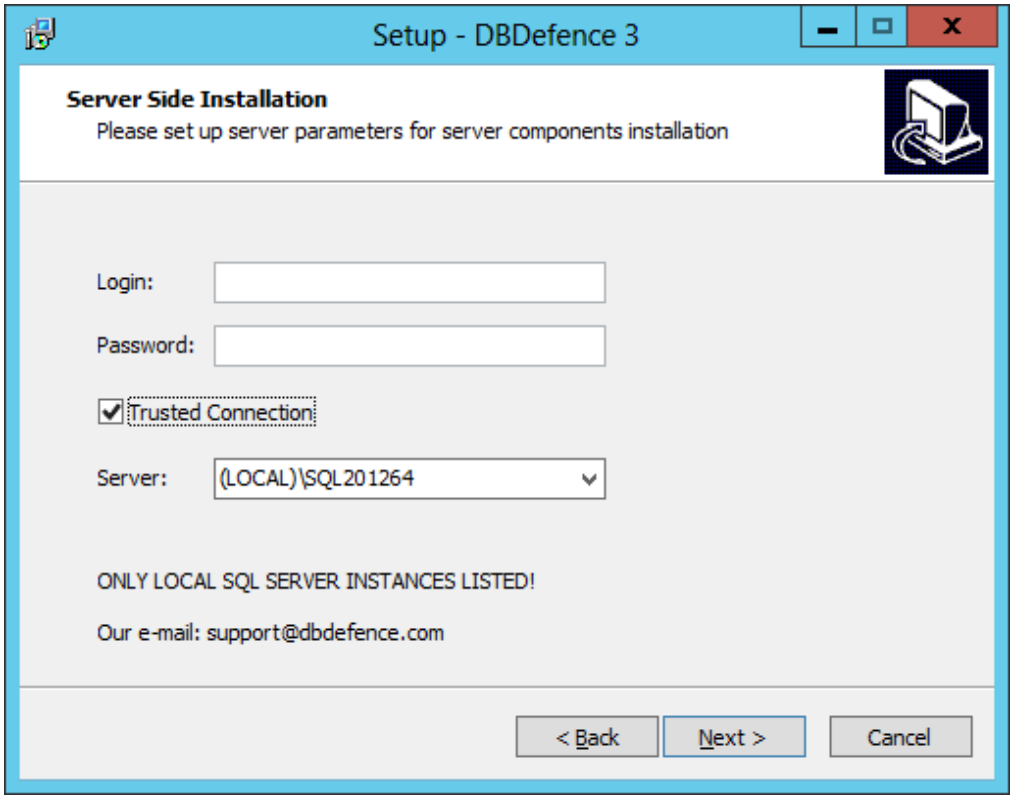

Abb. 3 - DbDefence Installation - Anmeldung beim Ziel-SQL-Server

Nachdem Sie sich bei dem Ziel-SQL-Server angemeldet haben, ist während des Installationsvorganges keine weitere Konfiguration notwendig. Klicken Sie einfach auf Weiter, und die Installation wird fortgesetzt. Sobald sie abgeschlossen wurde, wird Ihnen ein letzter Bildschirm angezeigt [Abb. 4], der Sie darüber informiert, dass die Installation erfolgreich war (oder dass die Installation fehlgeschlagen ist). Klicken Sie einfach auf Fertigstellen, um das Installationsprogramm zu schließen.

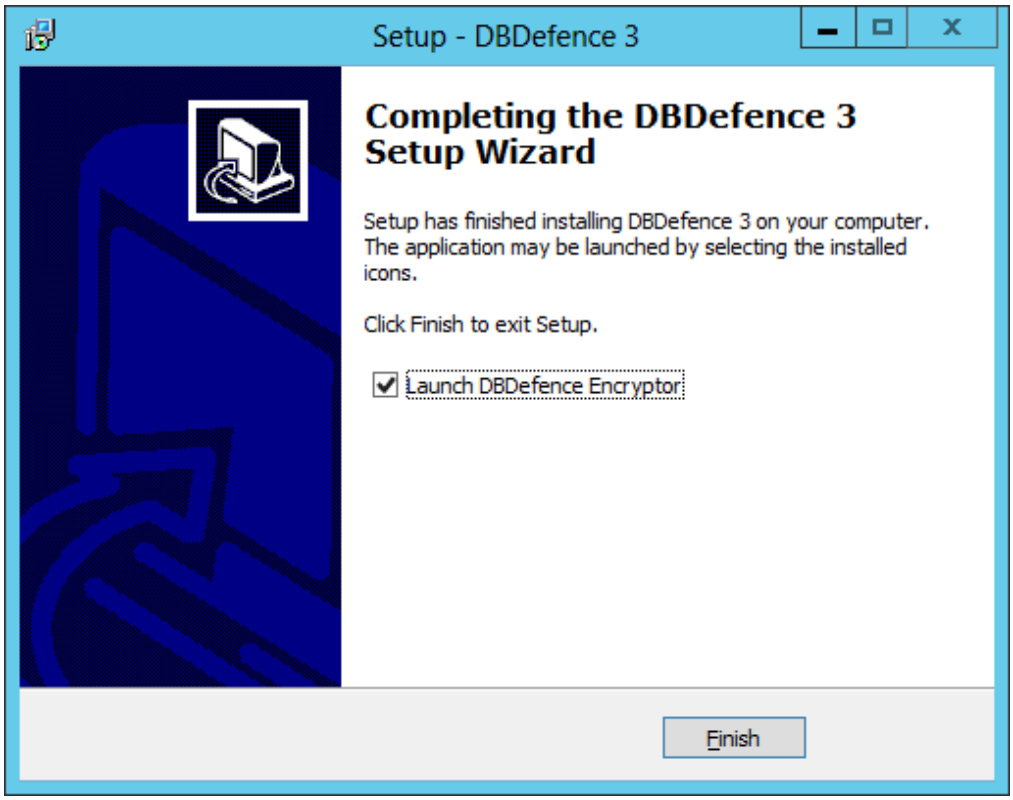

Abb. 4 - DbDefence Installation – letzter Bildschirm. Sie können DbDefence unmittelbar nach Schließen des Installationsprogrammes starten, indem Sie des Kontrollkästchens anklicken.

Sobald die Installation beendet ist, müssen Sie den DbDefence-Verschlüsseler aktivieren. Wenn Sie auf dem letzten Bildschirm des Installationsvorganges die Option „DbDefence-Verschlüsseler starten“ gewählt haben [Abb. 4], wird die Software automatisch gestartet, sobald des Installationsprogramm geschlossen ist. Ansonsten klicken Sie einfach auf die Schnelltaste in Ihrem Startmenü.

Verschlüsselung und Entschlüsselung

Sobald der DbDefence-Verschlüsseler aktiv ist, verbinden Sie ihn mit der Instanz des SQL-Servers, mit der Sie arbeiten möchten und Ihnen werden einige Informationen aufgezeigt [Abb. 5]. Denken Sie daran, dass die kostenlose Version des DbDefence-Verschlüsselers nur Datenbanken von bis zu 200 MB unterstützt. Aber, da dieses Informationsblatt dazu gedacht ist, Ihnen dabei zu helfen, den Vorgang in den Griff zu bekommen, wäre es ratsam, am Anfang nur mit einer kleinen Test-Datenbank zu arbeiten. Der Vorgang ist einfach und nimmt nicht viel Zeit in Anspruch. Es wird Ihnen also leicht fallen, die folgenden Schritte für die Datenbank, die Sie verwenden möchten, zu wiederholen.

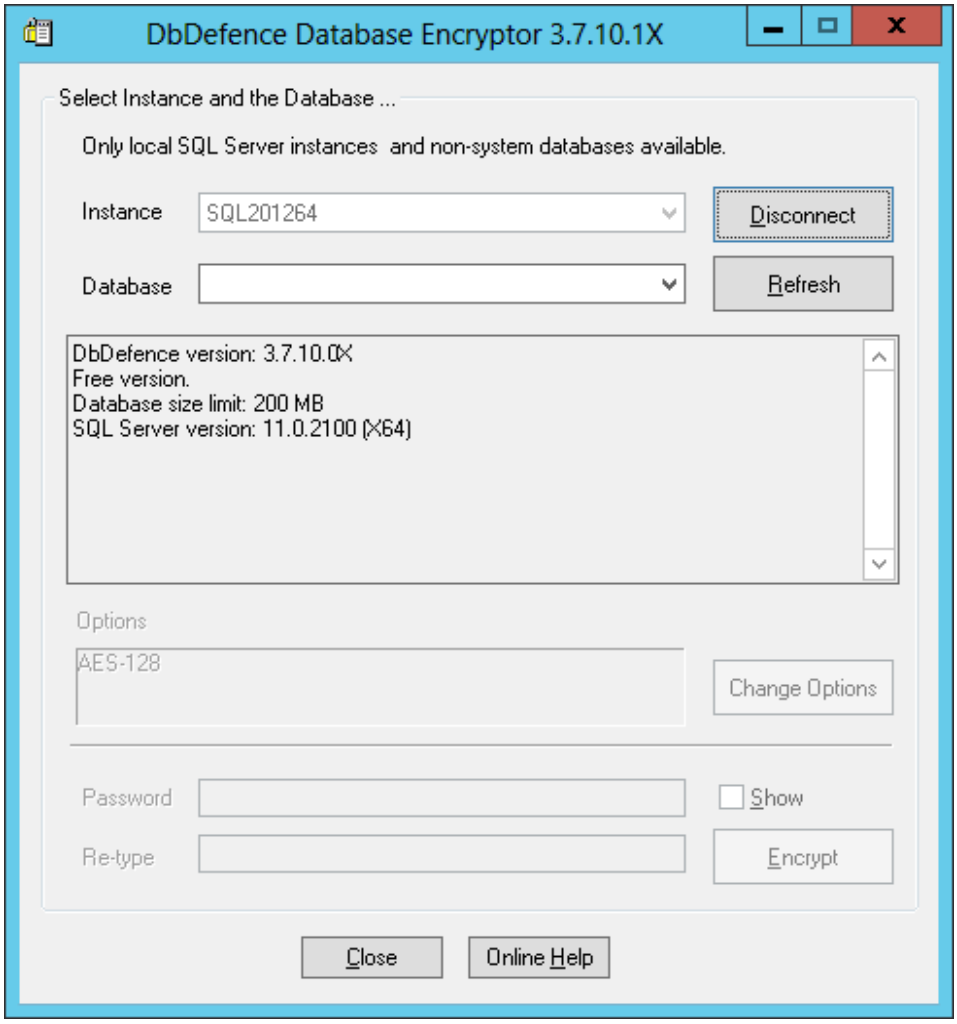

Abb. 5 – DbDefence-Verschlüsseler Bildschirm „Instanz wählen“. Hier wählen Sie die Instanz der Datenbank aus, mit der Sie arbeiten möchten. (Bei Benutzung der kostenlosen Version muss die Datenbank kleiner als 200 MB sein.)

Nach Auswahl der entsprechenden Instanz des SQL-Servers, die Sie verschlüsseln möchten, müssen Sie die Datenbank aus dem entsprechenden Drop-down-Menü auswählen, welches sich direkt unter dem Drop-down-Menü befindet, aus dem Sie die SQL-Server-Instanz gewählt haben [Abb. 6]. Die Standardverschlüsselungsmethode ist AES 128-Bit, wobei AES der Verschlüsselungsstandard in den USA ist, der dort häufig eingesetzt wird. Die Abkürzung steht für „Advanced Encryption Standard“. In den meisten Fällen ist die 128-Bit-Verschlüsselung ausreichend. Wenn jedoch eine stärkere Verschlüsselung notwendig ist, wird die 256-Bit-Verschlüsselung ebenfalls unterstützt. Sie können die Verschlüsselung durch Klicken auf die Schaltfläche „Optionen ändern“ anpassen. Diese befindet sich direkt unter dem Informationsfeld [Abb. 6]. Dieses wird das Dialogfenster Verschlüsselungs-Optionen anzeigen. Am oberen Rand des Fensters stehen zwei Möglichkeiten zur Auswahl (128-Bit und 256-Bit). Wählen Sie einfach die gewünschte Alternative, und klicken Sie auf OK. Es gibt in diesem Dialogfenster noch weitere Optionen, die wir aber erst später nähern erläutern werden.

Schließlich müssen Sie noch ein Passwort eingeben. Dieses Passwort ist der Schlüssel für den Zugriff auf die Datenbank. Sobald diese verschlüsselt wurde, ist es wichtig, dass Sie Ihr Passwort nicht vergessen – die Funktion „Passwort zurücksetzen“ existiert bei der Verschlüsselung nicht. Es ist außerdem wichtig, dass Sie ein sicheres Passwort wählen, nicht nur aus Sicherheitsgründen, sondern auch, weil die SQL-Server-Richtlinien (abhängig vom Betriebssystem) die Annahme von Passwörtern, die als zu schwach angesehen werden, verweigern können. Ein kraftvolles Passwort sollte sowohl Groß- als auch Kleinbuchstaben sowie mindestens eine Zahl und ein Symbol enthalten.

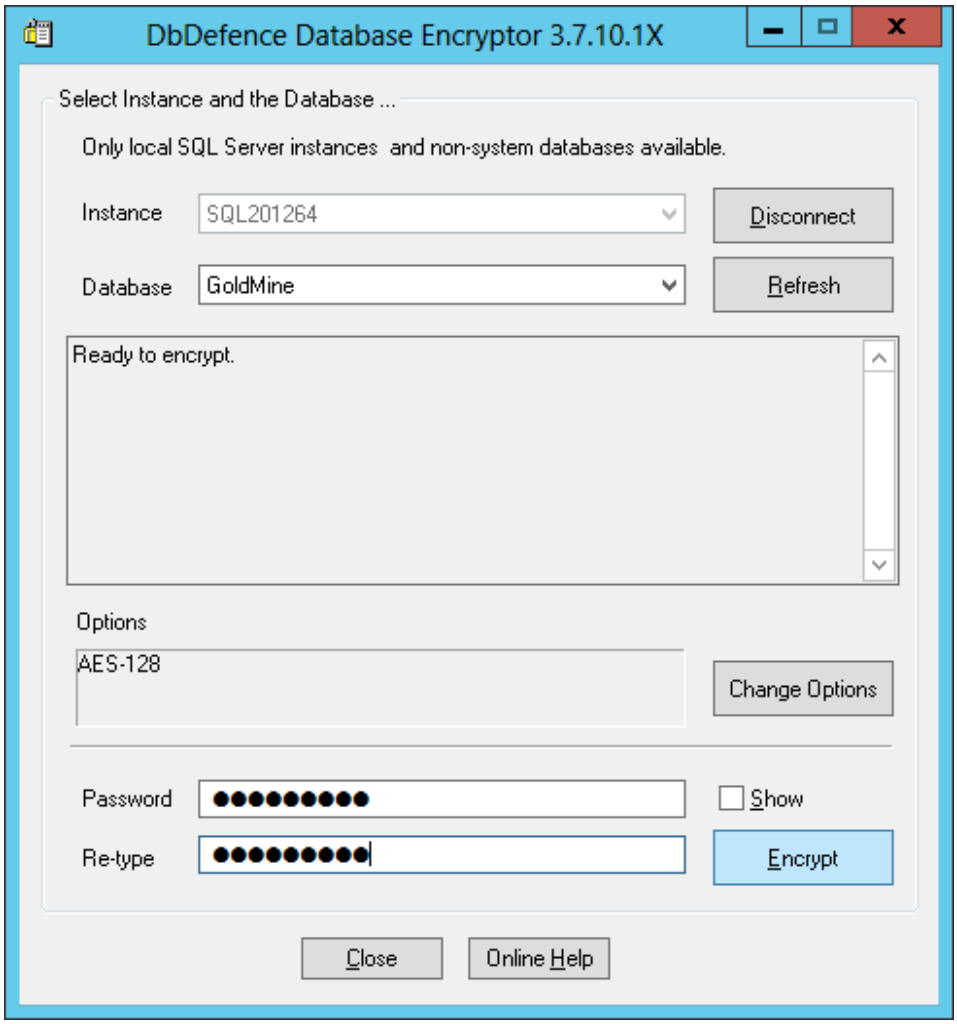

Abb. 6 – Noch einmal der Bildschirm „Instanz wählen“, dieses Mal komplett mit allen Informationen.

Heutzutage werden Verschlüsselungsroutinen, die für moderne Prozessoren optimiert wurden, von modernen Maschinen besonders gut verarbeitet, was bedeutet, dass sie auf neuen Computer sehr schnell sind. Eine Datenbank mit 40 GB zum Beispiel kann in etwa zehn Minuten verschlüsselt werden. Nach Abschluss ist die Datenbank einschließlich Protokolldatei komplett verschlüsselt. Von diesem Punkt an ist der Zugriff auf die Datenbank ohne das Verschlüsselungs-Passwort praktisch unmöglich (es ist möglich, eine Verschlüsselung zu „knacken“, aber es ist sehr, sehr schwierig und erfordert eine Menge Zeit und Ressourcen).

Durch Verwendung des gleichen Dialogfensters wie zum Verschlüsseln Ihrer Datenbank wird Ihnen die Möglichkeit gegeben, eine Datenbank zu entschlüsseln, wenn eine bereits verschlüsselte Datenbank ausgewählt wurde. Dieses kann leicht getan werden. Geben Sie einfach das Passwort ein, das Sie in dem vorherigen Schritt festgelegt haben, und klicken Sie auf Entschlüsseln [Abb. 7]. DbDefence wird die Datenbank dann entschlüsseln und in ihren ursprünglichen Zustand zurückversetzen.

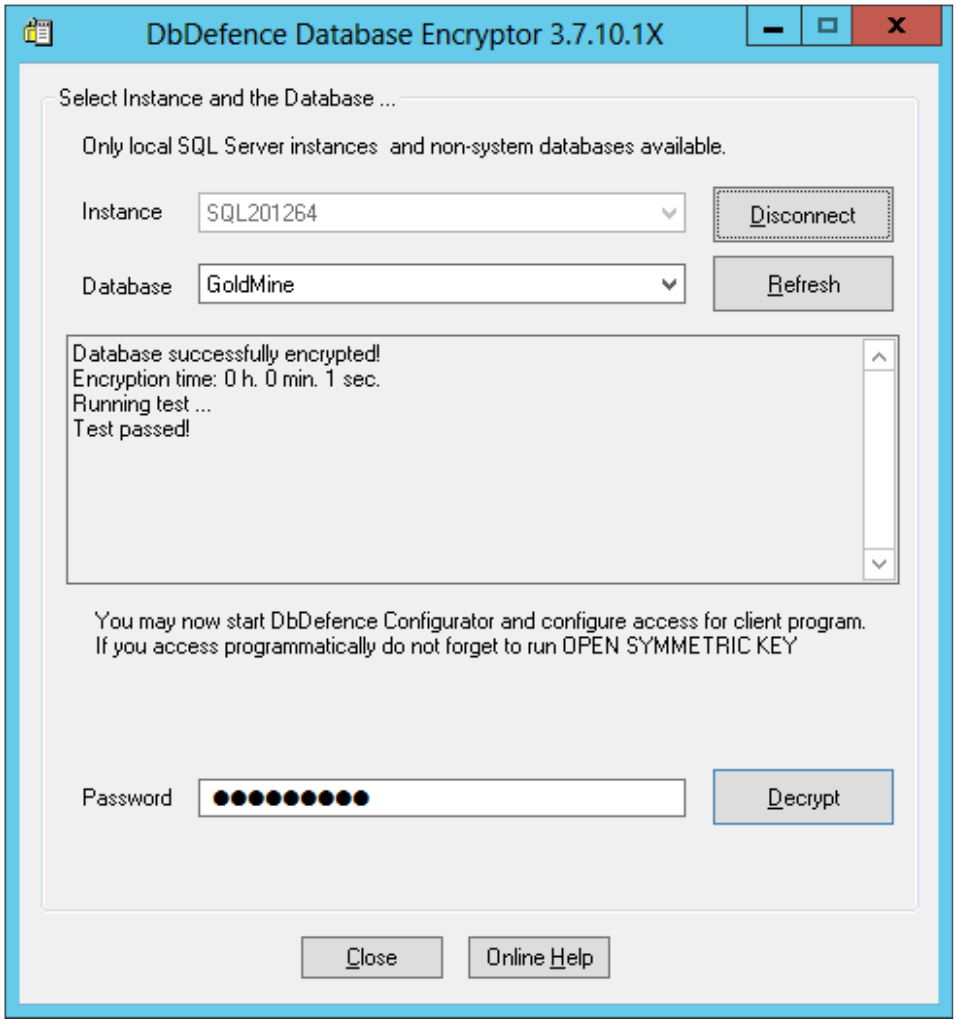

Abb. 7 – DbDefence bestätigt, dass die Datenbank erfolgreich verschlüsselt wurde.

Eine verschlüsselte und geschützte Datenbank verwenden

Jetzt, da Ihre Datenbank verschlüsselt ist, ist der Zugriff auf die Anwendungen und Dienstleistungen beschränkt, die das korrekte Passwort liefern können. Dieses beinhaltet alle Anwendungen, die versuchen, auf die Datenbank zuzugreifen, und sogar die Datenbank Administratoren. Das Öffnen der Datenbank selbst mit den Rohdaten wird lediglich verstümmelten, nicht mehr zu entziffernden Code offenbaren. Der Versuch, den Inhalt der Datenbank ohne das korrekte Passwort anzuschauen, führt zu der Anzeige einer Fehlermeldung [Abb. 8].

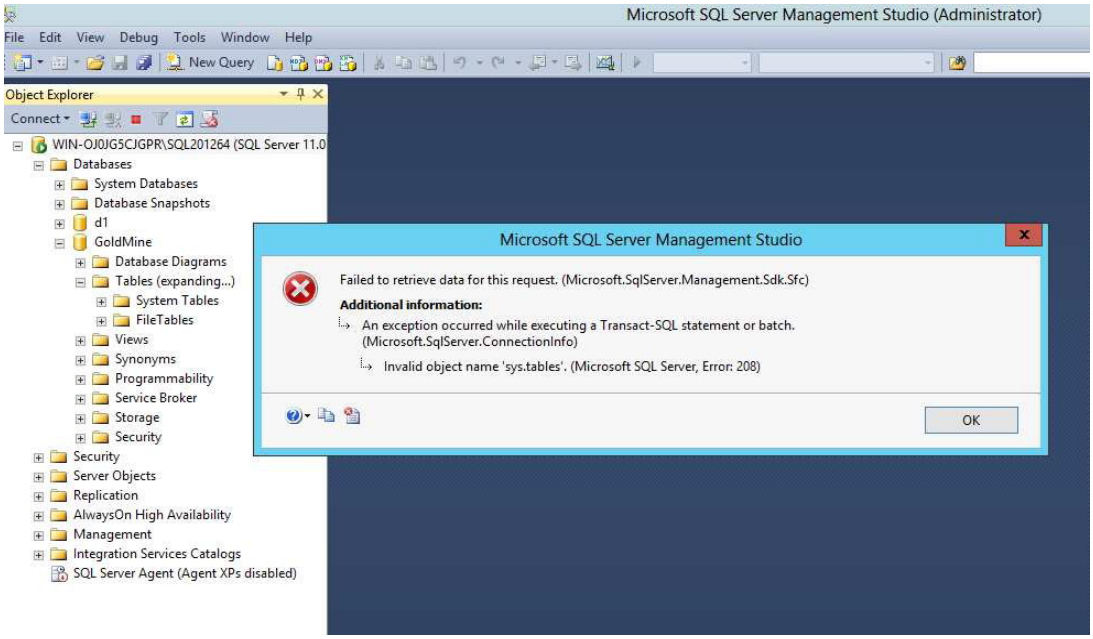

Abb. 8 – Wenn Sie versuchen, den Inhalt einer verschlüsselten Datenbank ohne das richtige Passwort anzuschauen, wird eine Fehlermeldung generiert.

Wenn Ihre Datenbank verschlüsselt wurde und Sie GoldMine wie gewohnt starten, sollten Sie eine Fehlermeldung erhalten, die Ihnen mitteilt, dass die Anmeldung aufgrund einer leeren BENUTZER Tabelle nicht erfolgreich war [Abb. 9]. Dieses passiert, da GoldMine ohne das Verschlüsselungspasswort nicht in der Lage ist, die Daten zu verstehen.

Abb. 9 –Von GoldMine generierte Fehlermeldung bei versuchter Anmeldung nach Verschlüsselung der Datenbank.

Die Datenbank befindet sich allerdings immer noch in einem voll funktionsfähigen Zustand, und autorisierte Anwendungen werden mit der Datenbank weiterhin ordnungsgemäß funktionieren, aber DbDefence muss wissen, welche Anwendungen erlaubt sind, so dass es die Datenbank für diese entschlüsseln kann.

Wir werden nun die GoldMine-Anwendung autorisieren müssen, um auf die Daten innerhalb der verschlüsselten Datenbank zugreifen zu können. Wenn Sie ein Programmierer sind, würde dieser Schritt lediglich eine einzige SQL-Anweisung im Code erfordern. Da dieses Informationsblatt jedoch für Nicht-Programmierer verfasst wurde, die eine Anwendung wie zum Beispiel GoldMine höchstwahrscheinlich benutzen, gehen wir davon aus, dass Sie kein Programmierer sind.

Passwort Eingabeaufforderung

Starten Sie zuerst die DbDefence-Konfiguration. Im linken Bereich finden Sie *Kunde Programm-Konfiguration*; klicken Sie dieses mit der rechten Maustaste an. In dem textabhängigen Menü, welches eingeblendet wird, wählen Sie „Programm hinzufügen“ [Abb. 10]. Von hier aus kann jedes beliebige Desktop-Programm hinzugefügt werden, für unser Beispiel werden wir aber GoldMine verwenden.

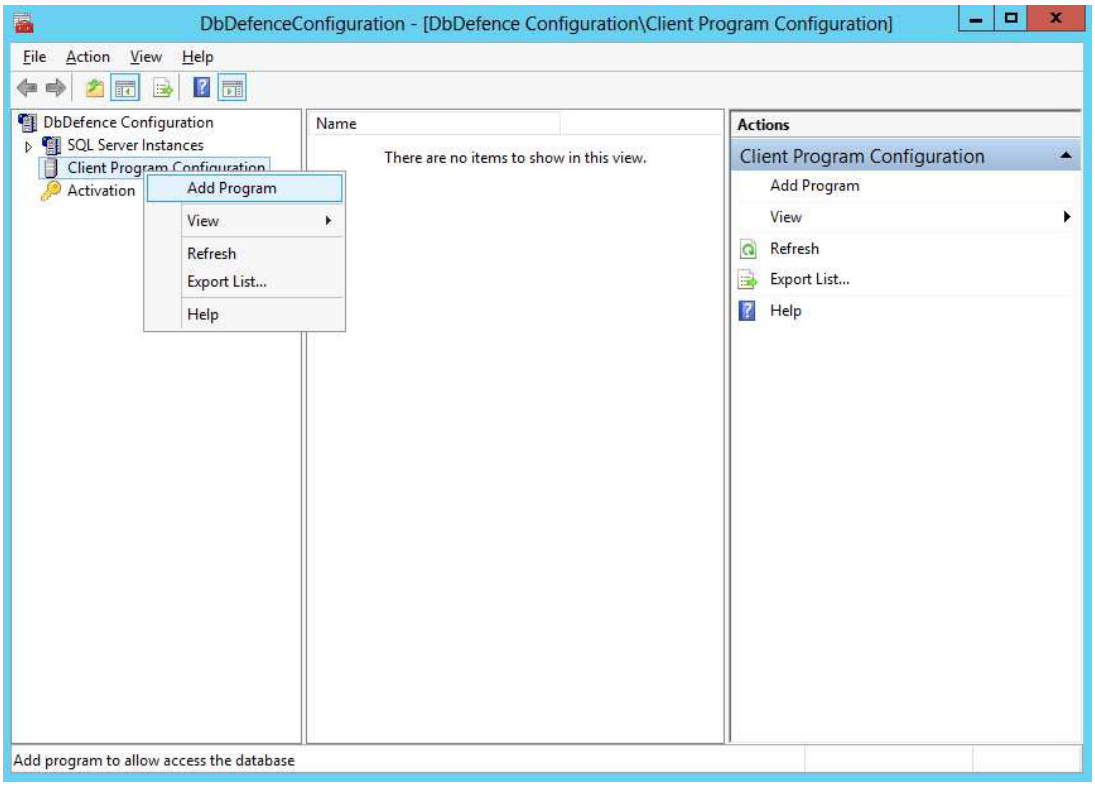

Abb. 10 – DbDefence Konfigurations-Fenster. Klicken Sie mit der rechten Maustaste auf „Kunde Programm-Konfiguration“ und dann „Programm hinzufügen“."

Wechseln Sie im Fenster *Öffnen* zum GoldMine Installations-Ordner. Dies ist der Ordner, in dem die GoldMine Programmdateien installiert wurden. Die Adresse wird in der Regel etwa so aussehen „C:\Programmdateien\GoldMine\“. Sobald Sie den Ordner geöffnet haben, sollten Sie eine Datei namens *gmw* sehen. Wählen Sie diese Datei aus. Sie ist die wichtigste ausführbare Anwendungsdatei für GoldMine. Sobald Sie sie ausgewählt haben, klicken Sie auf „Öffnen“.

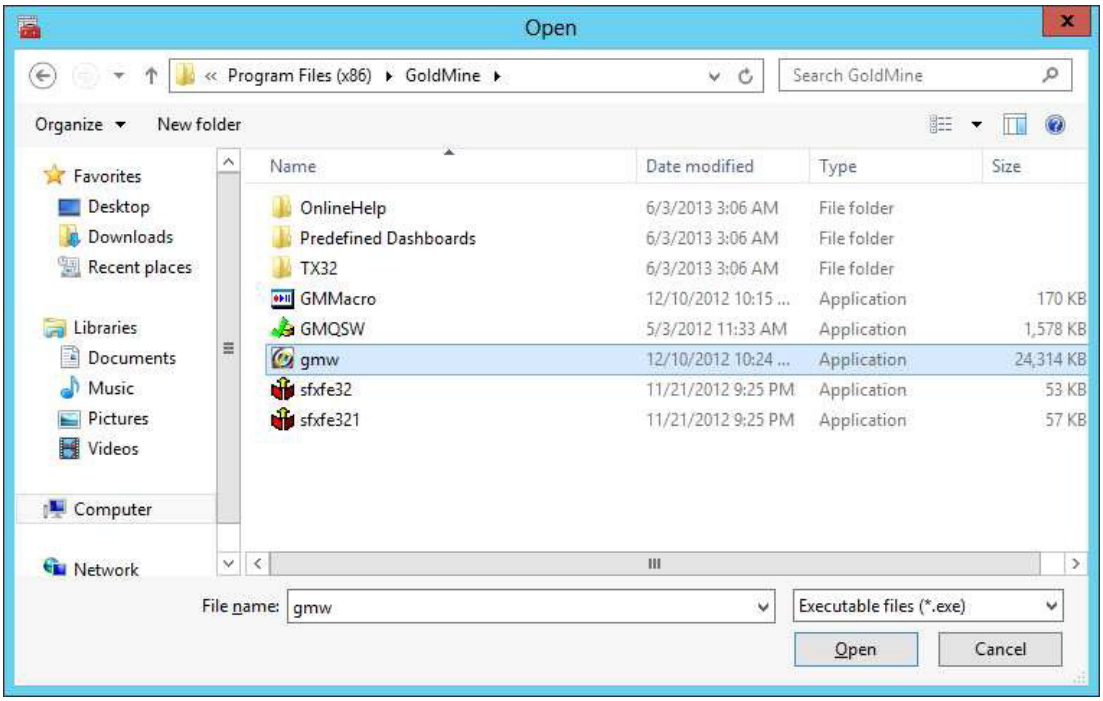

Abb. 11 – Das Fenster „Öffnen“, in der die GoldMine ausführbare Datei ausgewählt wurde.

Nachdem Sie *gmw.exe* ausgewählt und geöffnet haben, wird Ihnen innerhalb des DbDefence Konfigurations-Fensters eine neue Dialogbox präsentiert [Abb. 12]. Von hier aus können Sie die Einstellungen so ändern, dass GoldMine automatisch das Verschlüsselungs-Passwort eingibt, wann immer es versucht, auf die Datenbank zuzugreifen, indem Sie den Namen der Datenbank und das Passwort in die entsprechenden Felder eintragen. Wir werden dieses Verfahren später in diesem Informationsblatt noch genauer erläutern.
Für die Zwecke dieser Beschreibung ignorieren Sie diesen Punkt einfach, und ticken Sie nur das Kontrollkästchen „Passwort Dialogbox anzeigen“. Dann klicken Sie *Start!*, um mit GoldMine zu beginnen.

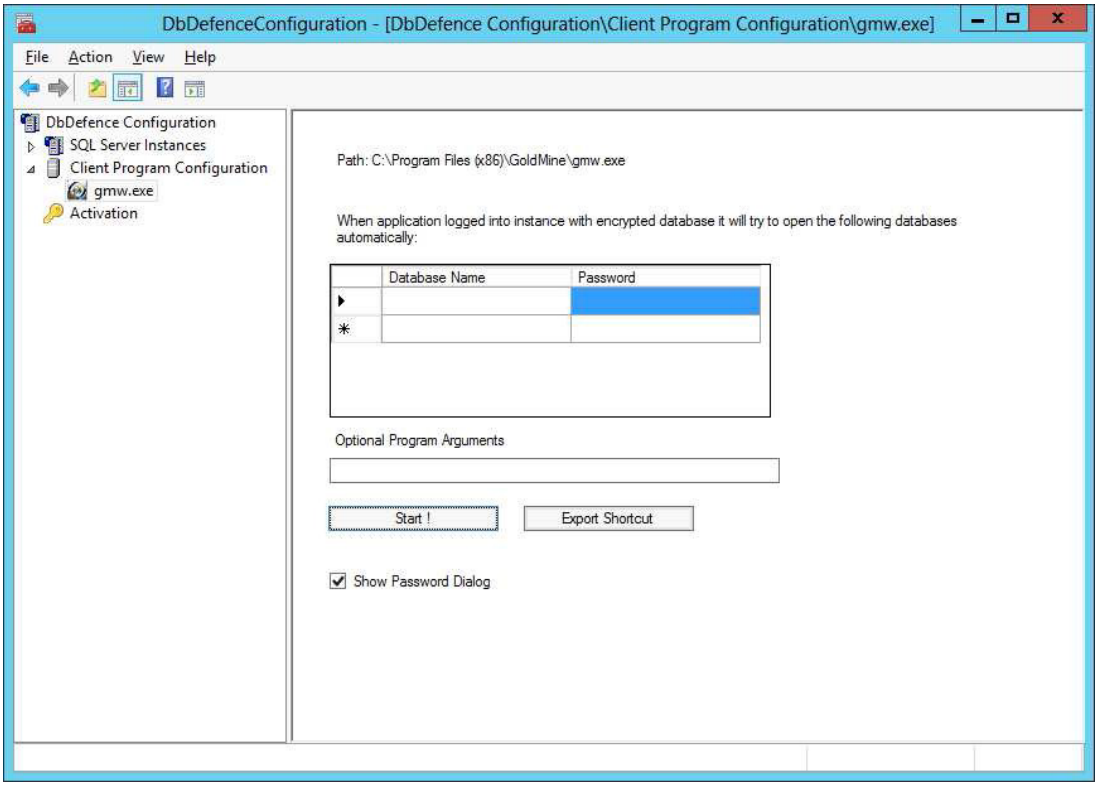

Abb. 12 – Wählen Sie, wie GoldMine auf die verschlüsselte Datenbank zugreifen soll – automatisch oder nach Aufforderung.

Nun, wenn GoldMine gestartet wird und es versucht, eine Verbindung zu Ihrer verschlüsselten Datenbank herzustellen, öffnet DbDefence eine Passwort Dialogbox [Abb. 13]. Vergewissern Sie sich, dass die richtige Datenbank ausgewählt wurde, und geben Sie in dem Feld unter der Drop-down Box das Passwort ein.

Abb. 13 – Sobald GoldMine genehmigt wurde, wird die DbDefence Passwort Dialogbox eingeblendet, wenn GoldMine versucht, auf die Datenbank zuzugreifen.

Wenn die richtige Datenbank ausgewählt und das korrekte Passwort eingegeben wurden, klicken Sie auf Freischalten. Da GoldMine nun berechtigt ist, wird es die Datenbank ganz normal laden und den Inhalt genauso anzeigen, als würde es mit einer unverschlüsselten Datenbank arbeiten [Abb. 14]. Wenn wir in der Zwischenzeit versuchen, gleichzeitig mit der SQL-Server Management-Konsole auf die Datenbank zuzugreifen, erhalten wir eine Fehlermeldung, die uns zeigt, dass der Zugriff verweigert wurde [Abb. 15], denn SSMS erhielt von DbDefence nicht die Berechtigung, auf die Datenbank zuzugreifen.

Abb. 14 – GoldMine arbeitet wie gewohnt mit der nun verschlüsselten Datenbank.

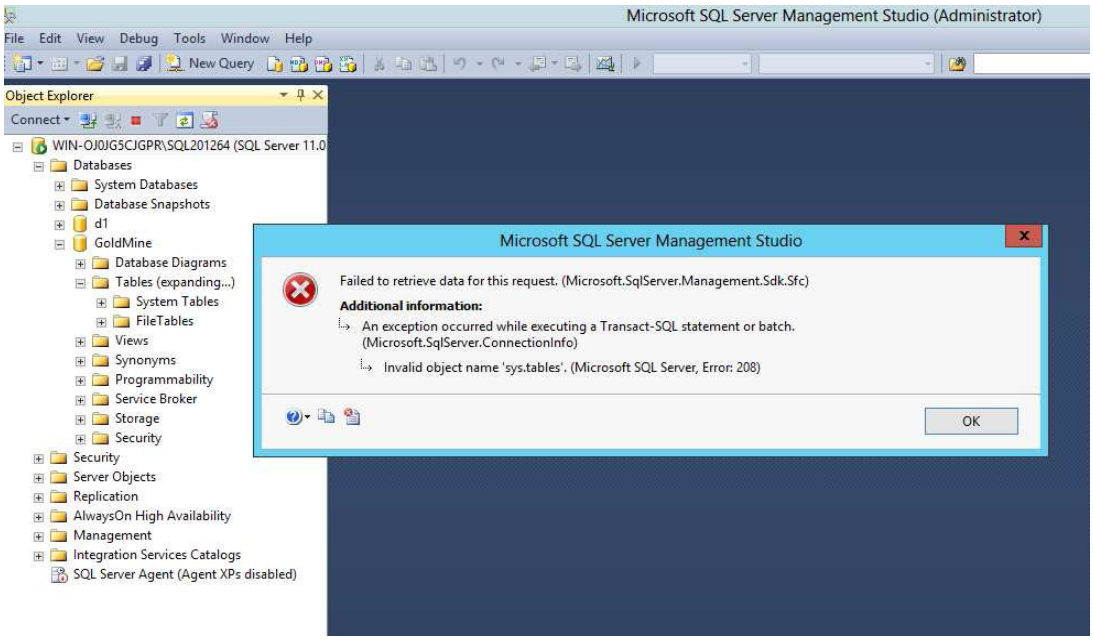

Abb. 15 – Solange GoldMine auf die verschlüsselte Datenbank zugreift, wird SQL DBA der Zugriff verweigert.

Automatische Anmeldung

Wenn Sie von einem sicheren System aus arbeiten, könnten Sie es als unnötig ansehen, jedes Mal Ihr Kennwort eingeben zu müssen, wenn Sie auf die Datenbank zuzugreifen möchten. Wie bereits erwähnt, können Sie DbDefence glücklicherweise so einstellen, dass es bestimmte Anwendungen erkennt und das Passwort bei jedem Versuch, auf die verschlüsselte Datenbank zuzugreifen, automatisch eingegeben wird.

Um dieses zu tun, müssen Sie zurück zu der DbDefence-Konfiguration gehen. In der linken Leiste finden Sie Kunde Programm-Konfiguration. Die *gmw.exe* sollte sich darunter befinden. Wenn Sie die gmw.exe nicht sehen können, klicken Sie auf Kunde Programm-Konfiguration, um die Auswahl zu erweitern. Sie sollten nun den gleichen Bildschirm sehen können wie zu Beginn dieses Abschnitts dargestellt, aber dieses Mal brauchen Sie *gmw.exe* nicht zu suchen und der Liste hinzufügen, da Sie das bereits getan haben.

Dieses Mal werden wir die Anmeldedaten in die entsprechenden Felder der Tabelle in der Mitte der rechten Leiste einfügen [Abb. 16]. Sie müssen den Namen der Datenbank (höchstwahrscheinlich GoldMine) und Ihr Verschlüsselungspasswort eingeben. In den Fällen, in denen Sie mehrere verschlüsselte Datenbanken haben, zu denen Sie den Zugriff gestatten möchten, können Sie in diesem Feld mehrere Datenbank-Namen und Passwörter eintragen. Sobald Sie fertig sind, entfernen Sie das Häkchen für „Passwort Dialogbox anzeigen“, so dass Sie beim nächsten Mal, wenn Sie versuchen, über GoldMine auf die Datenbank zuzugreifen, nicht wieder aufgefordert werden, Ihr Kennwort einzugeben.

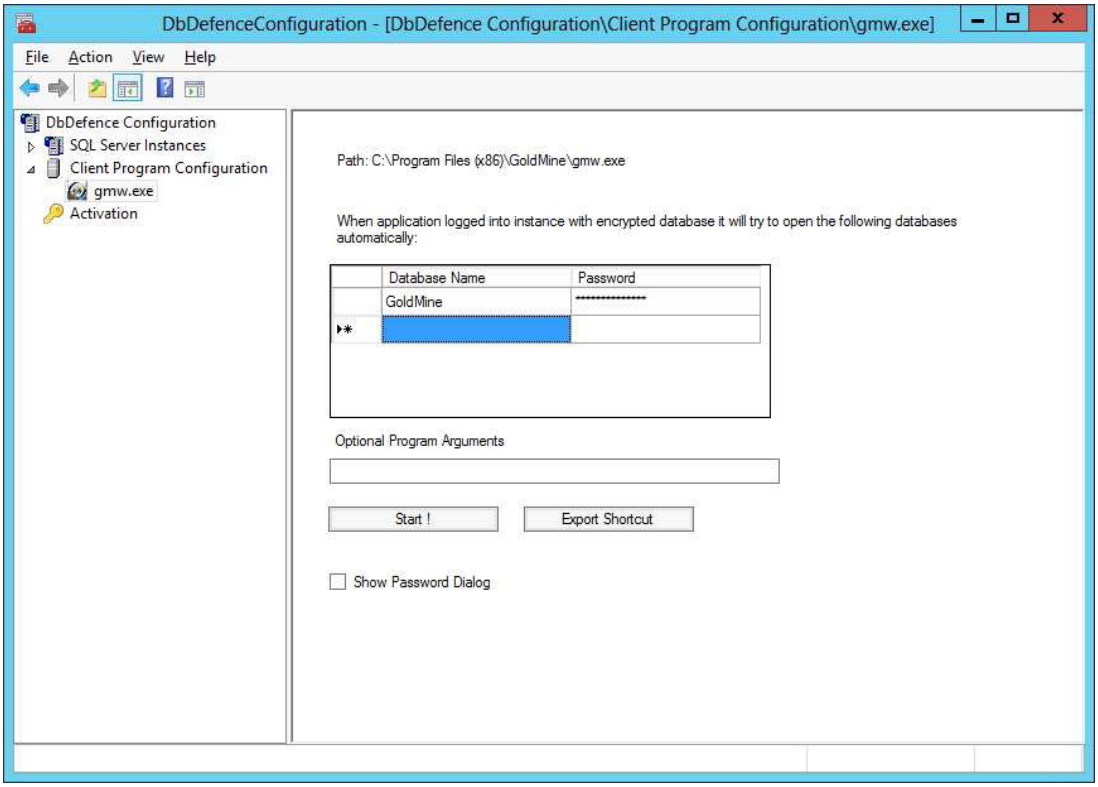

Abb. 16 – Eingabe des Passwortes, so dass autorisierte Anwendungen automatisch Zugriff auf die Datenbank erhalten.

Wenn Sie GoldMine nun durch Klicken von *Start!* in dem Konfigurationsfenster öffnen, wird es wie gewohnt starten, ohne dass Sie das Verschlüsselungspasswort eingeben müssen, um Zugriff zu erhalten.

Erstellen einer Verknüpfung

Falls Sie es vorziehen, nicht jedes Mal die DbDefence Konfiguration öffnen zu müssen, wenn Sie Zugriff auf Ihre verschlüsselte Datenbank haben möchten, können Sie eine Verknüpfung erstellen [Abb. 17], die dann auf Ihrem Desktop erscheint. Momentan wird noch das Passwort angezeigt, wenn Sie diese Verknüpfung erstellen, aber das wird in zukünftigen Versionen verbessert werden. Es ist außerdem wichtig, sich zu vergewissern, dass die Position der Verknüpfung im Hinblick auf andere Benutzer sicher ist. Wenn Sie die Verknüpfung mit Ihrer Datenbank auf dem Desktop eines gemeinsam genutzten Computers, welcher auch von Personen genutzt wird, die *keinen* Zugriff auf die Datenbank haben sollten, platzieren, können diese einfach auf die Verknüpfung klicken, um Zugriff zu erhalten. Stellen Sie zumindest sicher, dass Ihre Verknüpfung sich wenigstens in Ihrem eigenen Passwort-geschützten Benutzerbereich befindet, wenn schon nicht auf einem sicheren System, zu dem nur Sie Zugriff haben.

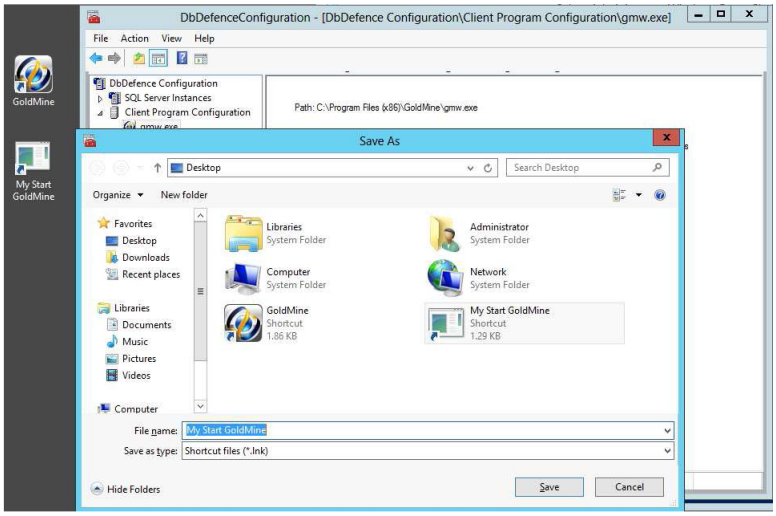

Abb. 17: - Speichern einer Verknüpfung auf dem Desktop, um zu vermeiden, dass DbDefence jedes Mal geöffnet werden muss, wenn Sie auf Ihre verschlüsselte Datenbank zugreifen möchten.

Der Zugriff auf die verschlüsselte Datenbank auf diese Weise ist der gleiche wie der Zugriff über die DbDefence-Konfiguration, ohne den Aufwand, die DbDefence-Konfiguration öffnen zu müssen. Der Prozess ist für die Anwendung (in diesem Fall GoldMine) vollkommen transparent.

Das Hinzufügen einer anderen Anwendung neben GoldMine ist genau so einfach. Alles, was Sie wissen müssen, sind der Name und der Speicherort der ausführbaren Hauptdatei. Wiederholen Sie dann die oben beschriebenen Schritte, und tauschen Sie *gmw.exe* mit der ausführbaren Datei der Anwendung, die Sie hinzufügen möchten, aus. SQL Server Management Studio von SQL Server 2012 befindet sich in der Regel in dem Ordner „C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\ssms.exe“, SQL Server Management Studio von SQL Server 2008 in „C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\VSShell\Common7\IDE\ssms.exe“.

Verschlüsselung von Datenbanken ohne Schutz

Es gibt Anlässe, bei denen Sie zwar Datenbankdateien verschlüsseln möchten, aber nicht den Zugriff von oder durch eine Anwendung oder Web-Service verhindern wollen. Zum Glück bietet DbDefence eine Funktion an, die dies erreichen kann.

Mit Hilfe dieser Funktion können Sie festlegen, auf welche Teile der Datenbank der Zugriff ohne das Verschlüsselungspasswort erlaubt ist. Dies geschieht, bevor die Datenbank verschlüsselt wird, und zwar in demselben Dialogfenster, das bereits am Anfang dieses Informationsblattes erwähnt wurde, welches Sie benutzen würden, um zwischen einer 128-Bit und einer 256-Bit Verschlüsselung zu wählen.

In dem Bildschirm „Instanz wählen“ [Abb. 6] klicken Sie auf *Optionen ändern*. Dieses wird die Dialogbox „Verschlüsselungs-Optionen“ anzeigen [Abb. 18]. Markieren Sie hier *„Zugriff ohne Verschlüsselungspasswort erlauben“*.

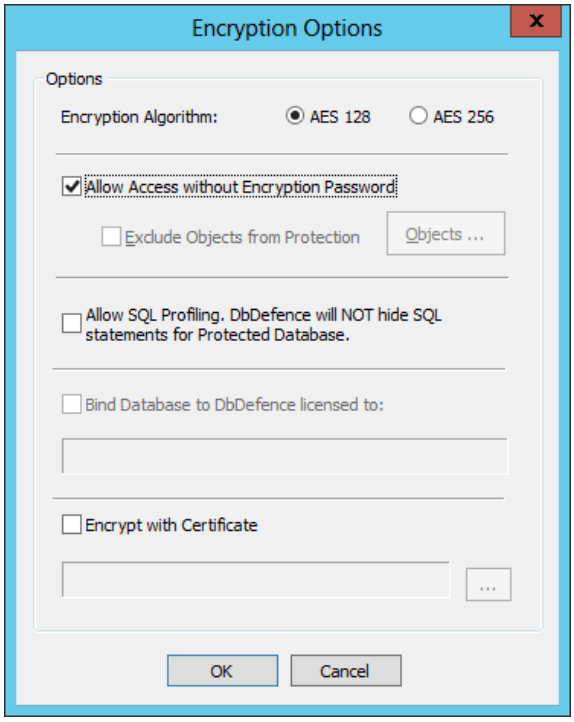

Abb. 18 – Die Dialogbox „Verschlüsselungs-Optionen“.

Sobald Sie Ihre Datenbank mit dieser Option verschlüsselt haben, wird der Zugriff auf die Datenbank ohne das Verschlüsselungspasswort für jede Anwendung möglich sein. Die Datenbankdatei hingegen *wird* verschlüsselt, was bedeutet, dass, wenn jemand (zum Beispiel ein Hacker) versuchen sollte, den Inhalt der Datenbank durch Blick auf die Rohdaten anzuschauen, wäre er ohne das Verschlüsselungspasswort erfolglos.

Fazit

Die Bedeutung, die dem Schutz Ihrer Daten zukommt, darf heutzutage auf keinen Fall unterschätzt werden. Der Wert von Informationen in allen möglichen Formen steigt exponentiell an, was aber nicht heißt, dass der Schutz Ihrer wertvollen Informationen schwierig sein muss. Mit unserer Software können Sie sicher sein, dass Ihre Datenbanken oder die Ihres Unternehmens vollkommen sicher sind, ohne dass Sie langjährige technische Erfahrung und/oder Programmierkenntnisse besitzen müssen.

Wenn Sie an unserem Produkt interessiert sind, können wir Ihnen eine Reihe verschiedener Preisoptionen anbieten, die abhängig von der Größe Ihrer Datenbank sind. Die Preise beginnen bei $698 pro Server.

Wir hoffen, dass dieses Informationsblatt hilfreich war. *Vielen Dank für Ihre Zeit!*