DBSAT – Erfahrungsbericht

Thorsten Grebe
twg-it
Berlin

Schlüsselworte
DBSAT, Database Security, EU-DSGVO, GDPR, Security-KPI

Einleitung

Oracle hat mit dem Database Security Assessment Tool (DBSAT) ein Werkzeug bereitgestellt, das komfortabel und umfassend den Sicherheitsstatus eines Datenbankservers ermitteln kann. Es analysiert nicht nur sicherheitsrelevante Einstellungen innerhalb der Datenbank, sondern auch Einstellungen von Listener, Datei- und Betriebssystem. Insgesamt können von DBSAT zurzeit über 80 Parameter begutachtet werden. Das Ergebnis wird in vier alternativen Formaten bereitgestellt (CSV, HTML, TXT, JSON). Zusätzlich erstellt DBSAT eine Management-taugliche Übersicht, die als Messlatte verwendet werden kann, um Verbesserungen oder Verschlechterungen im Sicherheitsstatus einer einzelnen Datenbank oder einer gesamten Datenbanklandschaft quantifizieren zu können.

Die erste Version von DBSAT wurde im Mai 2016 zunächst ohne weitere Marketingoffensiven veröffentlicht. Das Freigabedatum der Version 1.0.0 fällt nicht zufällig auf den Monat, in dem die neue Datenschutzgrundverordnung der EU (EU-DSGVO, engl. GDPR) in Kraft trat. Den meisten Administratoren entging dieses neue Werkzeug vermutlich für mindestens ein Jahr. Erst zum Ende 2017 begann Oracle für sein neues Werkzeug zu werben. Bei der DOAG-Konferenz in Nürnberg, bei Regionalveranstaltungen und bei speziellen Customer Events für Endkunden.

Dieser Erfahrungsbericht versucht die Frage zu beantworten, ob und wie DBSAT mit seinen unterschiedlichen Modulen beim gesetzeskonformen Absichern sensibler Oracle Datenbanken unterstützen kann.

Oracles Motivation zur Entwicklung von DBSAT

Die ursprüngliche Motivation zur Entwicklung von DBSAT erwähnt Pedro Lopez, der Product Manager für den Bereich *Oracle Database Security*, in einem Interview (youtube.com/watch?v=XsPuiCPcyA0): Innerhalb Oracle wurde in den Jahren vor der Entwicklung von DBSAT festgestellt, dass weltweit in unterschiedlichen Teams von Oracle unabhängig voneinander individuelle Skriptsammlungen und Hilfsprogramme entwickelt wurden, um den Sicherheitsstatus von Kundendatenbanken auf *Good Practice* Vorgaben zu prüfen. In Deutschland ist aus einem solchen Einzelengagement das 2013 veröffentlichte Sicherheitsbuch „Oracle Security in der Praxis“ von Carsten Mützlitz hervorgegangen, das bis heute in seiner umfassenden und praxisbezogenen Sicht auf den Sicherheitsstatus einer Datenbank konkurrenzlos ist. Offenbar wollte Oracle die unterschiedlichen, redundanten Anstrengungen zusammenführen und statt zahlreicher Einzellösungen, ein gemeinsames Werkzeug entwickeln, das die Erfahrungen und das *Know How* vieler erfahrener Sicherheitsexperten vereint.

In der Dokumentation wird die Motivation zur Bereitstellung von DBSAT etwas knapper formuliert: Oracle möchte seinen Kunden helfen.

In den Ergebnisberichten von DBSAT wird auf die zahlreichen Sicherheitsprodukte von Oracle hingewiesen, die fast ausnahmslos eine Enterprise Edition voraussetzen. Verweise auf Artikel der EU-

DSGVO stimmen besorgt, ob Verstöße gegen Auflagen der neuen, bußgeldgewaltigen Datenschutzregelung nachgewiesen werden könnten.

Die Motivation des Datenbank Administrators zur Verwendung von DBSAT

Für den DBA, der die sichere Konfiguration einer Datenbank gewährleisten soll, stellt DBSAT eine enorme Erleichterung dar. Zwar kann man selbst Skripte und Routinen schreiben, die auf sichere Konfigurationen prüfen. Jedoch ist der initiale Einarbeitungs- und Entwicklungsaufwand hierfür beträchtlich. Das Thema ist umfangreich und komplex. Schlimmer noch: Die in Eigenproduktion geschriebenen Routinen veralten. Sie können aus eigener Kraft kaum so aktuell und umfassend sein, wie es DBSAT derzeit vormacht. Hier liegt die Stärke von DBSAT. Es kann als externes, geprüftes und robustes Modul in eigene Reporting-Routinen eingearbeitet werden. Oracle kümmert sich um die Aktualisierung und die fehlerfreie Ausführung. Dem DBA wird eine Sicherheits-Todo-Liste in die Hand gegeben, die er nur noch abarbeiten muss.

Die Motivation des Security Administrators zur Verwendung von DBSAT

Der Security Administrator interessiert sich nicht für die hoch aufgelösten Details und Handlungsanweisungen, die DBSAT dem Datenbank Administrator zur Verfügung stellt. Der Security Administrator möchte einen verlässlichen Überblick, er interessiert sich für aggregierte Zusammenstellungen oder Scoring-Werte. Verbessert sich der Sicherheits-Status einer Datenbank oder einer kompletten Datenbankumgebung, stagniert er oder verschlechtert er sich sogar? Wichtig für ihn ist, dass Scoring-Werte reproduzierbar, nachvollziehbar und mit geringem Aufwand aktualisierbar sind. Genau hier kann DBSAT auftrumpfen. Die Scoring-Matrizen, die DBSAT für einzelne Datenbanken erstellt, lassen sich aufsummieren (allerdings nicht automatisch) und als Basis zur Berechnung eines aggregierten Security Key-Performance-Indikators für alle Oracle Datenbanken verwenden.

Aggregieren von DBSAT-Ergebnissen

DBSAT aggregiert keine Daten. Man erhält Einzelberichte, je ein Bericht pro Datenbank. Das Zusammenführen der Daten muss zurzeit in Eigenleistung erbracht werden. Am besten eignen sich hierzu die JSON-Dateien. Sie lassen sich per SQL*Loader in eine Monitor-Datenbank laden und von dort per SQL weiterverarbeiten. Auf diese Weise ist es möglich, einen Key-Performance-Indikator für die eigenen Oracle Datenbanken komplett automatisiert zu ermitteln und zu aktualisieren.

Wie sind das Potential und der Nutzen des DBSAT Discoverers einzuschätzen?

Der DBSAT Discoverer sucht in der Oracle Datenbank nach sensiblen, vertraulichen Daten. Dazu vergleicht er Namen und Kommentare von Tabellenspalten mit einer editierbaren Liste von regulären Suchausdrücken, die auf schützenswerte Inhalte deuten.

Was auf den ersten Blick wie eine gute Idee klingt, erweist sich in der Praxis jedoch als kaum sinnvoll umsetzbar. Wie unbeholfen sich das Suchen von sensiblen Daten in der Praxis gestalten kann, zeigt eine kurze Betrachtung von Fallbeispielen, in denen der Discoverer eine große Anzahl von Falsch-Positiven und – schlimmer noch – eine nicht abschätzbare Anzahl von Falsch-Negativen Befunden produziert.

Fazit

Das Collector/Reporter Duo von DBSAT erweist sich als wertvolle Ergänzung im Administrationsalltag. Einmal eingerichtet, hilft es dabei, einen etablierten Sicherheitsstandard für die von einem Team verantworteten Oracle Datenbanken aufrecht zu erhalten. Die Scoring Tabelle ist hervorragend als

Grundlage für eine vollautomatisierte KPI Erfassung geeignet. Großartig wäre es, wenn er für eigene Abfragen geöffnet werden könnte oder wenn er um optionale Tests erweiterbar wäre.

Ob man sich mit dem Discoverer auseinander setzen möchte, bleibt Geschmacksache. Er kann sehr viel Zeit kosten, ohne einen Mehrwert zu liefern. Findet der Discoverer etwas, muss geprüft werden, ob der Treffer Falsch-positiv ist. Findet er keine sensiblen Daten, heißt das längst nicht, dass es keine gibt. Allein diese Einschränkung lässt ihn als verlässliches Werkzeug durchfallen.

Wünschenswert wäre, dass der Collector für die weitere Entwicklung mehr Fokus erhält, der Discoverer weniger.

Kontaktadresse:
Dr. Thorsten Grebe
twg-it Datenbankberatung
Geisenheimer Straße 6
D-14197 Berlin

Telefon: +49 (0) 176 3140 3337
E-Mail Thorsten.Grebe@twg-it.de
Internet: www.twg-it.de