



# Secerno DataWall

Nico Zinner . Consultant . 18.06.2010

**Oracle gab am 20.05.2010 bekannt, dass sie die Firma Secerno aufgekauft haben, um ihre Palette von Datenbank-Sicherheitsprodukten zu erweitern. Secerno ist ein Softwareanbieter mit Niederlassungen in Oxford und New York, der sich mit dem Produkt DataWall auf die Überwachung und den Schutz von Datenbanken spezialisiert hat. Dieser Artikel soll eine Übersicht über Secerno's DataWall geben.**

## 1. Einsatzbereich

DataWall ist eine heterogene Datenbank Firewall, die den Datenbank-Sicherheitsbereich von Oracle erweitern soll. Neben Oracle werden auch weitere Datenbanken unterstützt wie der SQL-Server von Microsoft oder DB2 von IBM. Secerno liefert ein umfassendes Schutzschild, das in Echtzeit alle SQL-Befehle verfolgt, analysiert und wenn nötig blockiert. Es wird dadurch ein Schutz sowohl gegen externe als auch interne Angreifer garantiert.

Durch seine Fähigkeit, Auswertungen und Berichte zu erstellen, hilft es Unternehmen einen Überblick darüber zu erhalten, wie auf Daten zugegriffen wird und ob die Anforderungen für Vorschriften, Regularien und Gesetze wie SOX, J-SOX, PCI DSS, Basel II oder HIPAA eingehalten werden.

## 2. Funktionsweise

DataWall erfüllt hauptsächlich zwei Aufgaben: Überwachen und Schützen. Secerno's Produkt zeichnet sich dabei durch die SynoptiQ Engine aus, welche die SQL Befehle nicht nur nach Schlüsselwörtern durchsucht, sondern die Anfragen wirklich wie die Datenbank selbst versteht. Die SynoptiQ Engine erkennt also genau, welche Anfragen die gleiche Intension haben und welche aus dem Muster der üblichen ausbrechen. Im Überwachungsmodus kann sie alle SQL Befehle analysieren und zu Gruppen von validen Anfragen mit ähnlichem Verhalten zusammenfassen. Dadurch können automatisiert Positivlisten mit den erlaubten Anfragen erstellt werden. Erkennt die DataWall nun eine Anfrage, die ein anderes Verhalten aufweist als das derer in den Positivlisten, kann sie die Anfrage blockieren, noch bevor sie die Datenbank erreicht. Zur Bewertung ob eine Anfrage erlaubt ist oder nicht, werden mehrere Fakten berücksichtigt. Dazu zählen: WER versucht auf Daten zuzugreifen, WELCHE DATEN sollen angesprochen werden, von WO und WANN findet der Zugriff statt. Die DataWall kann dann entsprechend der festgelegten Regeln auf verschiedene Weisen reagieren. Autorisierte SQL-Anweisungen gelangen ungehindert zur Datenbank. Bei nicht autorisierten Anfragen kann sie einen Alarm auslösen oder die Anfrage blockieren. Darüber hinaus ist die DataWall, auf Grund der Tatsache, dass sie SQL wirklich versteht, auch in der Lage, Anfragen umzuschreiben. Secerno's DataWall erzeugt keine zusätzliche Last auf die Datenbank. Es besteht somit keine Beeinflussung der Performance.



### 3. Integration

Man kann die DataWall grundsätzlich auf zwei Wege in seine bestehende Systemlandschaft integrieren. Entweder als eine Art „Wächter“ im Netzwerk oder als Software auf dem Datenbankserver.

Der „Wächter“ kann ein dediziertes Gerät von Secerno (Appliance), eine Software auf einem Server des Kunden, in einer VMware oder auf einem Bladeserver sein. Die Wächter-Implementationsart ermöglicht es, unerwünschte Anfragen über die Standard Netzwerkverbindung abzufangen, noch bevor sie die Datenbank erreichen.

Ein Nachteil dieser Möglichkeit ist aber, dass man die Datenbank so nicht vor dem Zugriff von Administratoren schützen kann, die keine Standard Netzwerkverbindung nutzen, sondern sich über die Konsole oder via SSH direkt an der Datenbank anmelden.

Für diesen Fall gibt es einen Softwaremonitor, der auf dem Datenbankserver installiert wird und alle Anfragen überwacht. Wenn nun ein Administrator, beispielsweise bei Wartungsarbeiten, Befehle direkt an die Datenbank richtet, wird er zwar nicht blockiert, aber alle Aktivitäten können aufgezeichnet werden und bei unerlaubten Aktionen kann ein Alarm ausgelöst werden. Es ist somit jederzeit überprüfbar, wer etwas getan hat und was genau er getan hat.

### 4. Fazit

Oracle erhält mit der DataWall eine Datenbank Firewall, die eine einfache Handhabung, eine hohe Zuverlässigkeit und keine Beeinträchtigung der Performance verspricht. Wünschenswert wäre vielleicht ein besserer Schutz vor einem Administrator, denn was nützt ein Alarm, wenn bereits alle sensiblen Daten auf eine CD gebrannt und außer Landes geschafft wurden, bevor man auf den Alarm reagieren konnte.

Da aber in der IT nie eine hundertprozentige Sicherheit erreicht werden kann, gilt es zumindest möglichst viele Hindernisse zu schaffen, die es einem Angreifer erschweren, sein Ziel zu erreichen. Die DataWall scheint dabei ein sehr gutes Hindernis zu sein.

Dieser Artikel sollte einen ersten Überblick über das Produkt geben. Wir werden es noch weiter intensiv testen - und dann weiter über unsere praktischen Erfahrungen berichten.

Viel Erfolg beim Einsatz von Trivadis-Know-how wünscht Ihnen

Nico Zinner

Trivadis GmbH

Industriestraße 4

D-70565 Stuttgart

Internet: [www.trivadis.com](http://www.trivadis.com)

Tel: +49-711-903 63 230

Fax: +49-711-903 63 259

Mail: [info@trivadis.com](mailto:info@trivadis.com)



## Literatur und Links...

[www.trivadis.com](http://www.trivadis.com)

[www.secerno.com](http://www.secerno.com)