Im Mai 2010 hat Oracle die britische Firma Secerno gekauft. Das von Secerno bis zur Version 4.2 entwickelte Produkt DataWall wurde nach einigen Änderungen und Erweiterungen unter dem neuen Namen „Database Firewall Version 5.0" Anfang 2011 von Oracle zum Einsatz bei Kunden freigegeben. Dieser Artikel beschreibt die Komponenten und die Funktionsweise des neuen Oracle-Produkts.

Brandschutz für (fast) alle: Oracle Database Firewall

Heinz-Wilhelm Fabry, ORACLE Deutschland B.V. & Co. KG

Die Hersteller von Datenbank-Systemen verweisen seit Jahrzehnten darauf, dass wichtige Unternehmensdaten nicht direkt in Dateien der Betriebssysteme gespeichert werden sollen, sondern in ihren Datenbanken. Inzwischen ist das auch völlig selbstverständlich. Damit können aber auch Kriminelle sicher sein, dass sie wichtige Daten genau dort suchen müssen. Der Data Breach Investigations Report der Firma Verizon für das Jahr 2010 belegt, dass etwa 92 Prozent der weltweit gestohlenen Datensätze aus Datenbanken stammen (http://www.verizonbusiness.com/go/2010databreachreport/). Darüber hinaus bezeichnet der Report SQL-Injection als das effektivste Mittel, Daten aus Datenbanken zu stehlen – laut Verizon wurden 89 Prozent der Datensätze unter Verwendung von SQL-Injection gestohlen. Der Einsatz der Oracle Database Firewall kann SQL-Injection und andere Angriffe auf Datenbanken von Oracle und anderen Anbietern erkennen und abwehren.

Übersicht

Abbildung 1 zeigt eine schematische Übersicht über die Funktionsweise der Oracle Database Firewall. Die Firewall funktioniert wie eine Bridge, die verschiedene Segmente eines Netzwerks verbindet. Der gesamte Netzwerkverkehr von der Anwendung zur Datenbank läuft nach der Installation der Firewall über diese Bridge. Die Firewall erlaubt unterschiedliche Reaktionen auf die durch die Anwendungen generierten SQL-Befehle. Diese Befehle können folgende Aktionen erfahren:

- Die Firewall passieren
- Protokolliert werden
- Einen Alarm auslösen
- Durch einen anderen Befehl ersetzt werden
- Abgeblockt, das heißt an der Weiterleitung zur Datenbank gehindert werden

Das Blocken erfordert den Einsatz spezieller Netzwerkkarten. Eine Liste darüber stellt Oracle zur Verfügung.

Die Liste der Datenbanken, die mit der Firewall geschützt werden können, macht deutlich, dass sich die Oracle Database Firewall auch ideal zum Einsatz in einer heterogenen Datenbank-Landschaft eignet:

- Oracle von Version 8*i* bis Version 11*g*
- Microsoft SQL Server 2000, 2005 und 2008
- Sybase ASE 12.5.3 bis 15 und SQL Anywhere 10.0.1
- DB2 Version 9 auf den Betriebssystemen Linux, Unix und Windows

Weitere Datenbanken werden folgen. So ist zum Beispiel die Unterstützung von MySQL in einem der nächsten Releases der Firewall geplant.

Wie in Abbildung 1 angedeutet, verfügt die Database Firewall in ihrem Lieferumfang bereits über eine üppige Berichtsbibliothek. Sie enthält über 130 Berichte und ist zusätzlich um eigene Berichte erweiterbar. Dazu eignet sich ein beliebiger Berichtsgenerator, der auf Oracle-Datenbanken zugreifen kann.

Da alle gespeicherten Informationen um sensitive Daten (wie zum Beispiel Kreditkartennummern) bereinigt werden können, sind sie auch in den Berichten nicht sichtbar: Selbst das berechtigte Lesen der Berichte kann sensitive Daten nicht kompromittieren.

Aus der Sicht von Auditoren stellen neben der Schutzfunktion der Firewall die Berichte sicherlich den größten Wert des Produkts dar. Durch sie wird einerseits das Einhalten von Compliance-Richtlinien dokumentierbar und andererseits im Problemfall eine forensische Analyse erleichtert. Dieser forensische Aspekt wird zusätzlich unterstützt durch die Integration der Oracle Database Firewall mit der Web

Abbildung 1: Übersicht Oracle Database Firewall

Application Firewall der Firma f5 Networks Inc. sowie mit dem ArcSight Security Event Management System, einem zentralen System für das Logging, das Management und die Analyse von Syslog-Informationen aus unterschiedlichsten Systemen. Beide Systeme gehören nicht zum Lieferumfang der Database Firewall.

Unersetzlich: die Genauigkeit

Entscheidend für die Effektivität einer Database Firewall ist ihre Fähigkeit, berechtigte Aktivitäten von unberechtigten zu unterscheiden. Vergleichbare Produkte am Markt verwenden zu dieser Unterscheidung die Analyse der Zeichenketten der SQL-Befehle. Die Oracle Database Firewall geht einen völlig anderen Weg. Das eingesetzte Verfahren wurde an der Universität Oxford in Großbritannien entwickelt und ist unter der Bezeichnung „SynoptiQ Engine“ patentiert. Ausgangsbasis des Patents war die Erkenntnis, dass SQL über Zeichenketten-Vergleiche eben nicht ausreichend exakt interpretierbar ist. Das zeigt folgendes Beispiel: Ein SQL-Befehl, der eine unsinnige WHERE-Bedingung enthält, ist grundsätzlich suspekt und als Gefahr einzustufen. Bei SQL-Injection-Angriffen wird nämlich unter anderem davon Gebrauch gemacht, den WHERE-Bedingungen von SQL-Befehlen eine eigene Bedingung der Form „OR 1=1“ anzuhängen. Da die Auswertung dieser Bedingung den Wert „TRUE“ liefert, werden zum Beispiel im Falle eines SELECT-Befehls alle Datensätze der betroffenen Tabellen angezeigt.

Selbst einfachste Firewall-Implementierungen können in einem SQL-Befehl durch einen Zeichenketten-Vergleich die Bedingung „1=1“ als Gefahr identifizieren. Allerdings sind die drei folgenden Bedingungen selbst durch ausgefeilte Zeichenkettenvergleiche nicht als gefährlich zu erkennen:

- SQRT(49) = (9 - 2) / 1
- SUBSTR(‚catastrophe‘, 1, 3) = ‚cat‘
- ‚maus‘ <> ‚katze‘

Die unzureichende Eignung von Zeichenketten-Vergleichen hat für den EDV-Alltag Konsequenzen: Einerseits werden Zeichenketten-Vergleiche immer wieder dazu führen, dass SQL-Befehle zu Unrecht als gefährlich eingestuft werden. Setzt man etwa eine minimale Fehlerquote von nur 0,0001 Prozent in einem System mit 300 Transaktionen pro Sekunde voraus, ergeben sich bei 2,6 Millionen Transaktionen pro Tag täglich 26 fälschlich als gefährlich gemeldete SQL-Befehle. Die EDV muss jedem dieser Befehle auf den Grund gehen – ein arbeitszeitintensives Ärgernis. Zum anderen wird ein solches System immer wieder auch Befehle als harmlos einordnen, die in Wirklichkeit SQL-Injection-Angriffe sind – eine potenzielle Gefahr für das Unternehmen.

Systemkomponenten

Ein Oracle-Database-Firewall-System besteht immer aus mindestens drei Komponenten: einer oder mehrerer Firewalls, einem oder zwei sogenannter „Management Server“ und einem Werkzeug namens „Analyzer“.

Die eigentliche Funktion der Firewall übernimmt die gleichnamige Produkt-Komponente, die wie eine Bridge in das Netzwerk eingebaut ist. Der gesamte Datenverkehr zu einer Datenbank wird über diese Bridge geleitet und dort analysiert. Dies geschieht nahezu in Echtzeit. Wird die Last für eine Firewall zu hoch oder um eine höhere Verfügbarkeit zu erreichen, können auch mehrere Firewalls parallel zum Einsatz kommen. Als vager Anhaltspunkt für den möglichen Durchsatz kann dabei pro dedizierter CPU von einer Leistungsfähigkeit von etwa 5.000 SQL-Befehlen pro Sekunde ausgegangen werden.

Standardmäßig führt der Ausfall einer Firewall dazu, dass die Datenbank nicht mehr erreichbar ist (fail-close). Das ist im Interesse der Sicherheit wünschenswert. Häufig ist die Sicherheit einer Datenbank zwar wichtig, noch wichtiger ist mitunter jedoch die Verfügbarkeit. Daher kann es sinnvoll sein, sogenannte „Network-Bypass-Karten“ einzusetzen. Mit diesen Karten kann auch bei einem kompletten Ausfall einer Firewall der Netzwerk-Verkehr zur Datenbank aufrechterhalten werden kann (fail open).

Die Komponente „Management-Server“ hat zwei Funktionen. Erstens ist sie für die Administration einer oder mehrerer Firewalls zuständig. So sind hier auch die Regeln hinterlegt, die das Verhalten der Firewalls steuern. Zweitens dient der Management-Server als Repository für alle Informationen, die die Firewalls über den von ihnen kontrollierten Datenfluss sammeln. Der Umfang der Informationssammlung ist konfigurierbar und unterliegt den gleichen Überlegungen, wie sie auch im Rahmen jedes Auditing angestellt werden müssen: Man sollte nicht alles sammeln, sondern sich auf relevante Daten beschränken. Das reduziert die zu speichernde – und noch wichtiger – die im Bedarfsfall zu analysierende Datenmenge. Als Faustregel für den benötigten Speicherplatz kann man übrigens pro Log-Eintrag von etwa 650 Bytes ausgehen. Diese Log-Einträge sind die Basis für die oben bereits erwähnten Berichte. Die Informationen sind signiert und dadurch gegen Manipulationen geschützt.

Der Management-Server wird über eine Browser-Schnittstelle verwaltet und konfiguriert, die sogenannte „Administration Console“. Aus dieser können auch die Berichte angestoßen werden. Abbildung 3 zeigt den Eingangsbildschirm der Administration Console.

Durch Hinzufügen eines zweiten Management-Servers ist auch hier eine höhere Verfügbarkeit erreichbar. Das zweite System ist stets auf dem gleichen Stand wie das erste, läuft aber ansonsten passiv. Nur wenn der erste Management-Server ausfällt, übernimmt der zweite die Rolle des aktiven Servers.

Die dritte Komponente des Systems ist der Analyzer. Es handelt sich um eine grafische Oberfläche, über die die Regeln konfiguriert werden, nach denen die Firewalls SQL-Befehle analysieren. Dazu greift der Analyzer auf die Informationen zurück, die von den Firewalls im Management-Server abgelegt werden.

Installation

Sowohl Firewall als auch Management-Server sind als Appliances konzipiert. Allerdings muss der Kunde dazu die

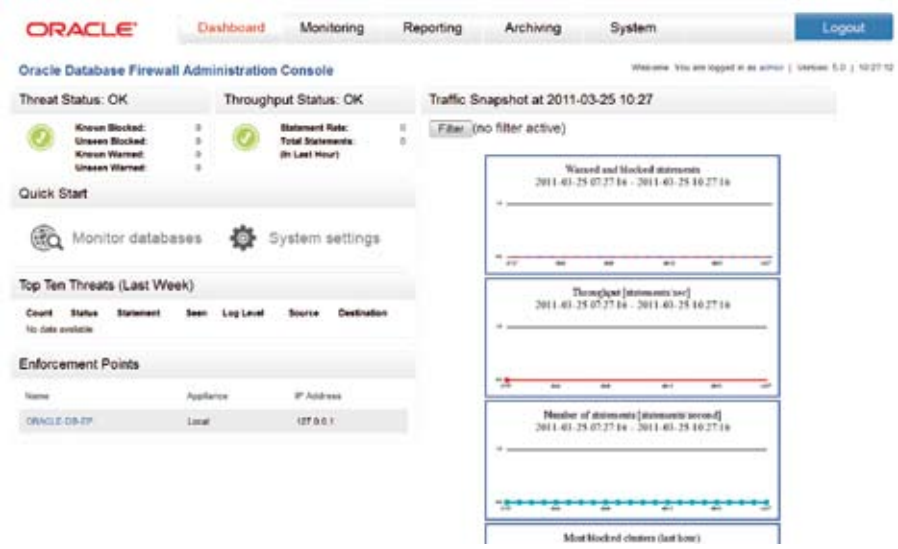

Abbildung 3: Administration Console

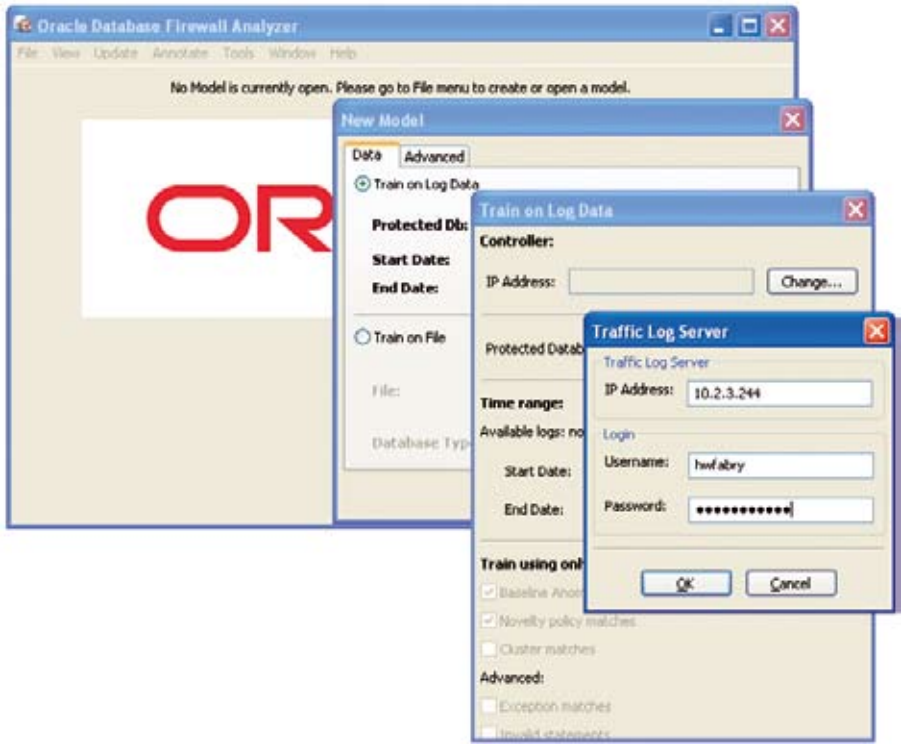

Abbildung 4: Arbeiten mit dem Analyzer

Hardware zur Verfügung stellen: Für jede Komponente wird ein X86-Rechner mit mindestens 1 GB Arbeitsspeicher und 80 GB Festplattenspeicher benötigt. Oracle hätte nach der Akquisition von Sun zwar auch die entsprechende Hardware als Teil des Produkts liefern können. Aber die Trennung von Hard- und Software nimmt Rücksicht darauf, dass viele Kunden in ihren Rechenzentren ausschließlich Systeme eines einzigen Anbieters verwenden.

Auf den von den Kunden gestellten Rechnern wird in einem Installationsgang zunächst ein angepasstes und gehärtetes Oracle Enterprise Linux installiert und dann die Software für die Firewall beziehungsweise für den Management-Server. Das Ergebnis ist ein Appliance, das der Kunde in keiner Weise verändern darf. Alle Änderungen an dem Firewall-System dürfen ausschließlich über von Oracle gelieferte Patches vorgenommen werden. Verändert ein Kunde eigenmächtig das Appliance in irgendeiner Form, droht ihm der Verlust des Supports.

Als letzte Komponente wird der Analyzer auf einem Windows-XP- oder Vista-System installiert. Windows 7 oder andere Betriebssysteme werden zurzeit nicht unterstützt.

Konfiguration für Zugriffe über das Netzwerk

Die Firewall muss konfiguriert werden, damit sie ihre Aufgaben erfüllen kann. Am einfachsten geschieht das, indem man die Fähigkeit der Firewall nutzt, selbst zu lernen: Man lässt sich eine Positiv-Liste (Whitelist) erstellen, das heißt eine Liste aller Aktionen, die keine Gefahr darstellen. Abbildung 4 zeigt den Eingangsbildschirm zum Anlegen einer solchen Liste.

Dazu lässt sich der gesamte Netzwerk-Verkehr zu einer Datenbank im sogenannten „Monitor-Modus“ aufzeichnen. Alternativ kann man auch nur die Aktivitäten einer bestimmten Anwendung aufzeichnen. Ist man sich sicher, dass die Aktionen des Beobachtungszeitraums keine Gefahr darstellen, kann man die Firewall zum Beispiel anweisen, unter Berücksichtigung festgelegter Tageszeiten oder IP-Adressen diese und – extrem wichtig – alle vergleichbaren Aktionen zuzulassen sowie alle anderen Aktionen abzublocken und zu protokollieren. Die Firewall schickt dann die Protokolldaten zur Speicherung und weiteren Bearbeitung an den Management-Server.

Diese Konfigurationsvariante ist ausgesprochen bequem und sehr flexibel. Man kann die Konfiguration aber auch über Negativ-Listen (Blacklists) vornehmen. Diese Listen können zum Beispiel den Zugriff auf festzulegende Objekte verbieten. Auch hier können Faktoren aus der Umgebung des Benutzers einfließen. Das Erstellen der Negativ-Listen ist offensichtlich aufwändiger als das Arbeiten über Positiv-Listen. Außerdem ist nie auszuschließen, dass potenziell gefährliche Aktionen übersehen wurden.

Konfiguration für die lokalen Zugriffe

Nicht alle Zugriffe auf zu schützende Datenbanken erfolgen über das Netzwerk. Gerade Administratoren melden sich lokal auf den Servern an und greifen direkt mit eigenen Werkzeugen auf die Datenbanken zu. Eine Firewall, die auf der Analyse des Netzwerk-Verkehrs beruht, kann das nicht verhindern. Ein Abblocken oder das Ersetzen von Statements ist in diesem Fall nicht möglich. Stattdessen bietet die Firewall für ein Subset der unterstützten Datenbanken die Möglichkeit, die lokalen Aktionen zu protokollieren – also eine Art Audit-Funktion. Im Jargon der Firewall spricht man vom sogenannten „local Monitoring". Innerhalb der überwachten Datenbank sind in einer Tabelle die lokal initiierten Aktionen festgehalten. Aus dieser Tabelle bedient sich dann eine Firewall und leitet die daraus gelesenen Informationen an einen Management-Server weiter. Dort können sie wie gewohnt ausgewertet werden oder auch Alarme auslösen.

Für den Schutz einer Oracle-Datenbank wird man das lokale Monitoren allerdings nicht verwenden. Das Oracle-Auditing bietet bereits vergleichbare eigene Möglichkeiten. Für Datenbanken anderer Hersteller, die auf das lokale Monitoren angewiesen sind, stellt sich möglicherweise zusätzlich das Problem, dass die Tabelle, in der das Protokoll geführt wird, gegen Manipulationen durch die Benutzer geschützt werden muss, für deren Überwachung sie eigentlich angelegt wurde.

Database Firewall und Netzwerk-Verschlüsselung

Abschließend muss noch darauf hingewiesen werden, dass die Firewall zurzeit Datenbank-Zugriffe über verschlüsselte Datenleitungen nur pauschal verhindern kann. Das betrifft sowohl verschlüsselte Zugriffe über SQL Net (Oracle Advanced Security) als auch über andere Verfahren. Die SQL-Net-Netzwerk-Verschlüsselung soll jedoch schon im nächsten Major Release der Firewall integriert sein. Die noch fehlende Unterstützung verschlüsselter Datenübertragung kann man jedoch dazu nutzen, die Firewall stufenweise einzuführen: Zunächst schützt man Systeme, auf die unverschlüsselt zugegriffen wird oder auf die ohnehin nur unverschlüsselt zugegriffen werden kann – zum Beispiel auch die Standard-Edition-Oracle-Datenbanken. So gewinnt man erste praktische Erfahrungen in der Arbeit mit der Oracle Database Firewall. Sobald die Verschlüsselung unterstützt wird, bindet man dann die übrigen Systeme ein.

Heinz-Wilhelm Fabry
ORACLE Deutschland B.V. & Co. KG
heinz-wilhelm.fabry@oracle.com