

Schwachstellen in Datenbanken erkennen

Mit FortiDB lanciert Fortinet eine Serie wegweisender Security-Appliances, die den erhöhten Schutzbedarf im Datenbankbereich adressieren. Sie erkennen und reporten Schwachstellen sowie mögliche Angriffspunkte.

Datenbanken bilden das «intellektuelle Herzstück» jeder Unternehmung. Sie beinhalten wichtige, vertrauliche und in aller Regel erfolgskritische Daten – und geraten als Folge davon oft ins Visier krimineller Machenschaften. Vor diesem Hintergrund ist die Suche und das Erkennen von Schwachstellen bei Passwörtern, Zugriffsberechtigungen und Datenbank-Konfigurationen eine unabdingbare Notwendigkeit. Mit den von Fortinet lancierten Security-Appliances FortiDB sind nun leistungsfähige «Database Vulnerability Assessment»-Lösungen

erhältlich, die diesem Bedürfnis Rechnung tragen.

Hüter der Daten – in heterogenem Umfeld

FortiDB ist eine automatisierte und zentralisierte Sicherheitslösung, die Datenbankapplikationen stabilisiert (härtet), indem sie potenzielle Angriffspunkte aufdeckt. Sie erkennt Probleme bei Passwörtern, Zugriffsberechtigungen und Konfigurationen und schickt bei deren Vorhandensein entsprechende Warnungen an den Systemadministrator. Zudem bietet die innovative Appliance konkrete Korrekturhilfen an.

Ergänzend zur Schwachstellenanalyse erkennt FortiDB Abweichungen im Nutzerverhalten (z. B. «Change Control», Monitoring privilegierter User), wobei auch Zugriffe von nur scheinbar legitimierten Nutzern erkannt werden. Entsprechende Vorkommnisse protokolliert die Appliance nahtlos und alarmiert die verantwortliche Stelle.

Mit FortiDB erhalten Firmen jeder Grösse eine VA-Appliance (Vulnerability Assessment), die sich komfortabel in heterogenen Umgebungen einsetzen lässt und den Arbeitsaufwand der Datenbankadministratoren nachhaltig reduziert. Unterstützt werden unter anderem Oracle, DB2, Sybase und SQL Server – bis zu 60 parallele DB-Instanzen pro Appliance.

Dank dem umfangreichen Funktionsset bieten die FortiDB-Appliances einen weitreichenden Schutz gegen den internen und externen Datendiebstahl – ganz egal, ob es sich dabei um firmeneigene oder persönliche Daten handelt. Allen Systemen gemeinsam ist die kontinuierliche Überwachung der Datenbankaktivitäten (7 x 24), umfangreiche Datenbank-Audits sowie gründliche Vulnerability Assessments. Diesen automatisierten Test- und Überwa-



FortiDB ermöglicht eine zentralisierte Datenbank-Security in heterogenen Netzwerken. Die VA-Appliance ist auch als reine Software-Lösung erhältlich.

chungsprozeduren liegen DB-spezifische Best-Practice-Policies zugrunde sowie regelmässige Updates bestehender Richtlinien. Diese sorgen dafür, dass neue Bedrohungen wirksam angegangen und dass regulatorische sowie branchenspezifische Anforderungen jederzeit erfüllt werden (z. B. SOX, Basel II oder GLBA). Hinsichtlich Compliance ebenso bedeutsam ist die Implementierung sogenannter «separation of duty»-Funktionen. Diese ermöglicht eine rollenbezogene Administration

FortiDB – Auszug aus dem Leistungskatalog

Zentralisierte Appliance

Vereinfachte Implementierung und Durchsetzung firmenweiter Datenschutz-Richtlinien.

Vulnerability-Management

Sicherheitsschwächen werden erkannt, entsprechende Warnungen und konkrete Korrekturvorschläge automatisch übermittelt.

Aufzeichnung von DB-Aktivitäten (inkl. DDLs und DCLs)

Sicherheits-relevante Aktivitäten werden dokumentiert.

Unterstützung virtualisierter Umgebungen

Gewährt Policy-Compliance in virtualisierten und Standard-Umgebungen.

Reporting und Dokumentation

Konform mit internen Richtlinien sowie mit externen Regulatorien wie PCI-DSS, SOX, Basel II, GLBA und HIPPA.

Kontakt

BOLL Engineering AG

Jurastrasse 58, 5430 Wettingen,
Tel. 056 437 60 60
info@boll.ch, www.boll.ch