

## Experten: Horrende Sicherheitslücken bei Datenbanken

Von Armin Barnitzke

28. November 2007

„Grauenhaft“ stehe es in der Praxis um die Sicherheit von Datenbanken, berichten Experten. Doch der Schutzbedarf für sensible Informationen wächst. Für Unternehmen bieten sich daher spezielle Security-Produkte an, denn die in den Databases direkt eingebauten Sicherheitsfunktionen schlucken viel Ressourcen.

Einen Schub für das Thema Auditing und Echtzeitschutz bei Datenbanken beobachtet Forrester-Analyst Noel Yuhanna. Stand dabei früher vor allem im Fokus, die Richtigkeit von Finanzdaten nachzuweisen, gehe es heute eher um den Schutz personenbezogener Daten oder Kreditkarten-Infos.

Neben Compliance-Vorgaben in Sachen Datenschutzgesetz oder [Kreditkartenrichtlinie PCI-DSS](#) treibt Firmen die Furcht vor peinlichen Datenverlusten. So konnten Cyberdiebe beim US-Handelskonzern TJX über ein [unsicheres Filial-WLAN](#) in das Firmennetz einbrechen und dann über Monate hinweg in aller Seelenruhe Kreditkartendaten abziehen.

„Ein verhaltensabhängiges Softwaremonitoring hätte gewarnt, dass ein User fortlaufend auf alle Kreditkartentransaktionen des Konzerns zugreift“, sagt Mark Bregman, Cheftechnologe bei Symantec. Grundsätzlich gibt es für eine solche Kontrolle der Datenbank-Zugriffe zwei Ansätze:

Siehe dazu auch:

- [CZ Zone Managed Security Services](#)
- [CZ Zone Security Corner](#)
- [Nur ein integriertes Vorgehen sorgt für eine hohe Sicherheit](#)

Zum einen bauen Datenbank-Anbieter selbst solche Auditing-Funktionen ein. Am weitesten sei hierbei Oracle, so Forrester. „Allerdings schalten die wenigsten Anwender die Auditing-Funktionen an, da sie extrem viel Rechenleistung schlucken“, so Stefan Strobel, Chef des Beratungshauses Cirosec.

Das öffnet das Feld für Spezialanbieter, die meist mit einer Hardwareappliance vor der Datenbank agieren und dort „die SQL-Statements im Netz analysieren“, wie der Oracle-Sicherheitsspezialist Alexander Kornbrust von Red Database Security verdeutlicht.

Neben vielen kleinen Anbietern tummelt sich hier auch Symantec. Der Security-Riese ist mit seiner in den eigenen Labs entwickelten Symantec Database Security (SDS) zwar relativ spät in den Markt eingestiegen, biete aber ein gutes Set an Funktionen und Features, so Forrester. In der überarbeiteten Version 3.0 bringt Symantec etwa eine heuristische Lernfähigkeit, die automatisch SQL-Verhaltensmuster empfiehlt.



cirosec GmbH  
Edisonstraße 21  
74076 Heilbronn  
Tel: 07131 / 59455-0  
Fax: 07131 / 59455-99  
info@cirosec.de  
[www.cirosec.de](http://www.cirosec.de)

Strobel betont aber, dass die meisten Produkte nur Datenverkehr protokollieren und bei Verdacht alarmieren. Aktiv einschreiten und wie eine Firewall Angriffe tatsächlich stoppen könnten nur Imperva, Guardium und SQL Block.

Kornbrust hält ohnehin relativ wenig von solchen Security-Produkten, da sie aus seiner Sicht relativ einfach umgangen werden können. Strobel hält dem entgegen, dass normale Datenbank-Angreifer kein ausgefeiltes Hacker-Know-how haben: Das seien eher Vertriebsmitarbeiter, die beim Jobwechsel mal schnell noch ein paar Kundendaten abziehen wollen.

Strobel: „Insofern steigert ein Datenbank-Schutzprodukt – egal welches – die Sicherheit in jeden Fall dramatisch“. Denn um die Datenbank-Sicherheit sei es in der Praxis „grauenhaft“ bestellt. „Wir finden bei Überprüfungen stets hunderte von Schwächen. Sei es, weil keine aktuellen Patches eingespielt sind oder weil noch die Default-Passwörter verwendet werden.“

Auch der Chef von NGS-Software, David Litchfield, bestätigt die [horrenden Sicherheitslücken](#) bei Datenbanken. Er geht weltweit von etwa einer halben Million Datenbank-Server aus, die direkt über das Internet zugänglich seien. Vor zwei Jahren waren es erst 350 000. Litchfield: „Wir alle verfolgen zwar die Schlagzeilen über die vielen Datendiebstähle – aber es scheint niemanden zu kümmern.“

Zudem zeigt seine Studie, dass viele dieser ungeschützten Datenbanken nicht up-to-date sind und mit alter unsicherer oder ungepatchter Software laufen.

***computerzeitung.de 28.11.2007***