NETWORKWORLD
The Leader In Network Knowledge
www.networkworld.com November 6, 2013

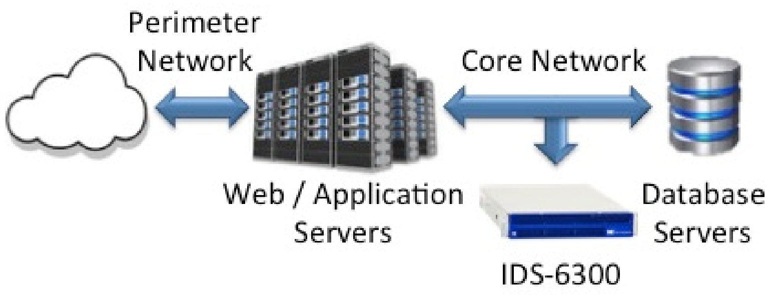
DB Networks' new core IDS aims to stop SQL injection attacks

By Linda Musthaler, Principal Analyst with Essential Solutions Corp.

For several years now, "injection" flaws have topped the list of software security issues as identified by the Open Web Application Security Project (OWASP). The non-profit organization, which is dedicated to improving the security of software, defines the problem this way:

"Injection flaws, such as SQL, OS and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing unauthorized data."

Of course the problem we hear about most is SQL injection, and it's used to attack data driven applications. SQL injection is known as an attack vector for Web sites, but can be used to attack any type of SQL database. Attacks using this vector are growing in frequency, which is especially bad news considering that about 90% of the data records stolen in the past 10 years have been attributed to this technique.



Despite the fact that there are Web application firewalls (WAFs) and other technologies aimed at stopping these types of attacks, hackers have become adept at using obfuscation techniques that manage to skirt the perimeter protections. For example, any technology today that depends on signatures is bound to fail because attackers are staying ahead of the vendors' abilities to create and update signatures. Therefore, the trend today is toward using behavioral analysis to detect attack attempts.

DB Networks (www.dbnetworks.com) has just announced a new solution it calls a next-generation core intrusion detection system (IDS). Rather than sitting at the perimeter in front of the Web or application servers, this IDS sits in the core between the Web and app servers and the database server. The device is not inline; it is passively attached, connecting via a tap or span port. The product today handles the two most dominant databases – Oracle and Microsoft SQL Server – and the company says it will add more databases over time.

DB Networks uses behavioral analysis to scrutinize the structured query language code accessing the database. The vendor claims to have the ability to accurately detect SQL injection attacks real-time. "We ensure the integrity of sensitive data so if there are unauthorized attempts at modifying data or getting data out, any kind of SQL injection attempts are identified and an alarm procedure is invoked," says Brett Helm, chairman and CEO of DB Networks.

DB Networks claims to have some unique features in its IDS. For example, the company says the solution gives deep visibility to the database tier. When the product is installed, it automatically detects databases and an administrator can choose which ones to protect. Sometimes the IDS will detect databases that no one knew about and that probably aren't protected.

Hackers either create or go after these rogue databases and use cross credentials to attack other targets because quite often databases trust each other. If an attacker is able to get system privileges on a database that is vulnerable, then he walks across laterally to attack the database that he's really after. For example, it's possible for a hacker to utilize an unprotected printer database to gain peer status with more important databases. DB Networks can detect these rogue databases so the organization can choose to remove or protect them.

Another product feature is the ability to identify flaws in the legitimate SQL statements that are generated by applications. This shows the app developer exactly where they need to fix their flawed code.

Sometimes organizations must operate their applications with a known vulnerability. Having a vulnerability doesn't necessarily mean an attack is imminent, but the situation does require monitoring. The DB Networks IDS can monitor the vulnerability so if someone does get close to exploiting it, an alert can be sent so that extra precautionary measures can be put in place.

Helm describes an occasion when a customer knew of an application vulnerability that had not yet been mitigated because the company was still testing a fix. When the IDS sent an alert that there was activity that was challenging the vulnerability, the organization was able to put its database in read-only mode until it got a better handle on the situation.

When the DB Networks IDS identifies a SQL injection attack, it automatically sends an alert showing the context of where the attack was and how it was done. The alert is sent through traditional emails, syslogs or a SIEM. From there it's up to the organization to decide what action to take: quarantine the activity, stop it or even let it go.

DB Networks claims to have unprecedented SQL injection accuracy, which the vendor attributes to its behavioral-based approach. "When an attack gets to us and we see it, it is unobfuscated," says Helm. "We catch zero-day attacks because we don't operate on signatures. It could be the first time ever that something is attacked on the system and their application and we catch it. We have extraordinarily low false-positives." The IDS basically learns the behavior of the legitimate applications and can detect attacks based on the SQL and the application working together.

Network World recognized DB Network's IDS in the Product of the Week roundup at the end of October.

DB NETWORKS.

5909 Sea Lion Place
Suite H
Carlsbad, CA 92010
Phone - 1- 800 - 598 - 0450
www.dbnetworks.com