Database Activity Monitoring

- Was'n das?! -

Sebastian Kilchert

Hamburg

Schlüsselworte

DAM, Database Activity Monitoring, Firewall, Audit

Einleitung

Das Thema Sichert ist in aller Munde. Es werden viele Maßnahmen in den Firmen getroffen, jedoch wird meistens das eigentliche System der Aufbewahrung von unseren Daten vergessen. Die Datenbank. Vielen Firmen ist nicht bewusst, dass die gemäß Bundesdatenschutzgesetzt bzw. auch DSGVO bei System mit personenbezogenen Daten gewisse Dinge protokollieren müssen.

Was ist ein DAM (Database Activity Monitoring genau?

Ein DAM ist ein spezielles Monitoring, das zusätzlich zu dem normalen und in der Regel eingesetzten Standard Monitoring betrieben wird. Beim normalen Monitoring, dass wie in dem folgenden Bild, z.B. den Füllstand des Tanks bzw. Tablespaces überwacht oder den Motor bzw. die Instanz, ob die Prozesse laufen, fehlt etwas Gravierendes. Die Überwachung und Kontrolle der Leitungen, in dem Beispielbild, die Benzinleitung. Bei einer Datenbank wäre das die Vielzahl an Datenströme.

Abbildung 1: Überwachung

Ein Activity Monitoring unterstützt Sie noch bei viel mehr, als nur der Datenstromüberwachung.

- Kombiniert Auditing (Protokollierung) und Firewall/Alerting für die Datenbank
- Sichtbarkeit und aufdecken von Auffälligkeiten oder Angriffe

- Aktives Einwirken möglich
- Zugriff auf Objekte für alle Benutzerarten einschränken
- Abgrenzung von Verantwortungsbereichen möglich
- Auswertung/Reporting bzw. Analysemöglichkeiten
- Zusätze Sicherheitsprüfungen möglich

Wo sind die Unterschiede zu anderen Sicherheitstools?

Database Activity Monitoring	Syslog-Server	Wep-Application Firewall
Kann Angriffe mitbekommen, bevor sie in der Datenbank ausgeführt werden	Bekommt die Informationen erst wenn Sie passiert sind	Sitzt zw. Client und Applikationsserver
Kann aktiv einwirken und ggf. Session beenden oder ins Leere laufen lassen	Kann nicht direkt Angriffe verhindern	Firewall für Webanwendungen – Nicht für Datenbanken
Kann Konfigurationen gegen einen „Standard“ prüfen (Compliance)	-	Für statische Request geeignet
Zieht Daten direkt über den Agent und/oder im Netzwerk ab. Braucht größtenteils keine/wenig extra Mechanismen	Oftmals müssen extra Logging etc. eingeschaltet werden	
Dient dem revisionssicherem Protokollieren		
Versteht die SQL-Sprache und kann somit verdeckten Angriffen zuvor kommen		

Abbildung 2: Unterschiede zu Sicherheitstools

Wie man sieht, hat jedes Tool seine Stärken. Am besten wirken die Tools zusammen z.B. WAF und DAM. Je nachdem ob in der jeweiligen Firma ein SIEM oder ein SYSLOG-Server genutzt wird, kann dieser natürlich auch mit eingebunden werden.

Im folgenden Bild kann man sehr gut sehen, wo die jeweiligen Tools ansetzen und entsprechenden Schutz bewirken.

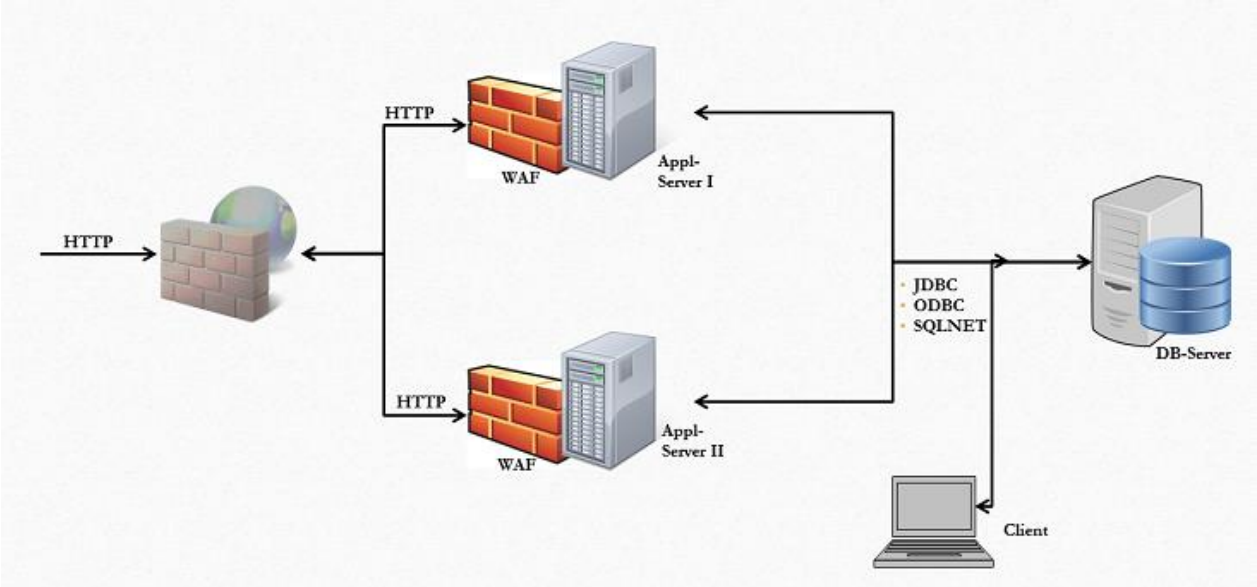

Abbildung 3: WAF vs. DAM

Vorteile ein DAMs

- DAM ist Auditing und Alerting mit Weiterleitungsfunktion an einem SIEM und/oder Syslog-Server
- DAM wertet das Ergebnis des Execution Plans aus bzw. versteht SQL → sieht somit, was wirklich passiert

Beispiel:
select * from SYNONYM;
Das Synonym zeigt auf eine VIEW und die VIEW auf eine TABLE.
Wenn eine Monitoring Regel SELECT auf die TABLE monitoren soll, dann tut sie das eben auch,
wenn, wie hier im Beispiel ein SYNONYM verwendet wird (oder direkt die VIEW).
Auch Verschleierung der Zugriffe mit dynamischem SQL hilft dem Angreifer hier nicht weiter. Netzwerkbasierte Lösungen können dies nicht erkennen.

- DAM bietet einen direkten Schutz der Datenbanken, während Firewalls und Network Security die Infrastruktur schützen. DAM kann als "letzte" Verteidigungslinie betrachtet werden.
- Minimierung des Risikos der Haftbarkeit, in dem man Angriffe sofort erkennt.
- Eigene Compliance-Regeln können erstellt werden, DBs werden dagegen geprüft
- Im Zweifel fachgerechte Beurteilung und Eingreifen durch den DBA statt im Nachgang durch die Security-Abteilung.
- DBA‘s und andere User können von den Applikationsdaten ferngehalten werden
- Absicherung der DBAs durch die Protokollierung (Auditing)
- unerlaubte Zugriffe auf die Applikationsdaten können protokolliert werden

- geringer Einfluss auf die Performance
- einfache Formulierung der Monitoring Regeln
- hunderte mögliche Regeln können definiert werden
- umfangreiche Reporting Möglichkeiten
- große Infrastrukturen werden unterstützt (skalierbar)
- DAM kann mit weiteren Komponenten aufgestockt werden ergänzt werden
- schwache Kennwörter können entdeckt werden

Unterschiede zwischen den Herstellern

	McAfee Together is power.	IMPERVA	ORACLE
Oracle	✓	✓	✓
MySQL	✓	✓	✓
Microsoft SQL Server	✓	✓	✓
DB2	✓+	✓+	✓+
SYBASE	✓	✓	✓
TERADATA	✓	✓	
Maria DB	✓	✓	
PostgreSQL	✓	✓	
Progress OpenEdge		✓	
IBM Informix, Netezza		✓	
SAP HANA	✓	✓	

Abbildung 4:Unterschiede zw. den Herstellern

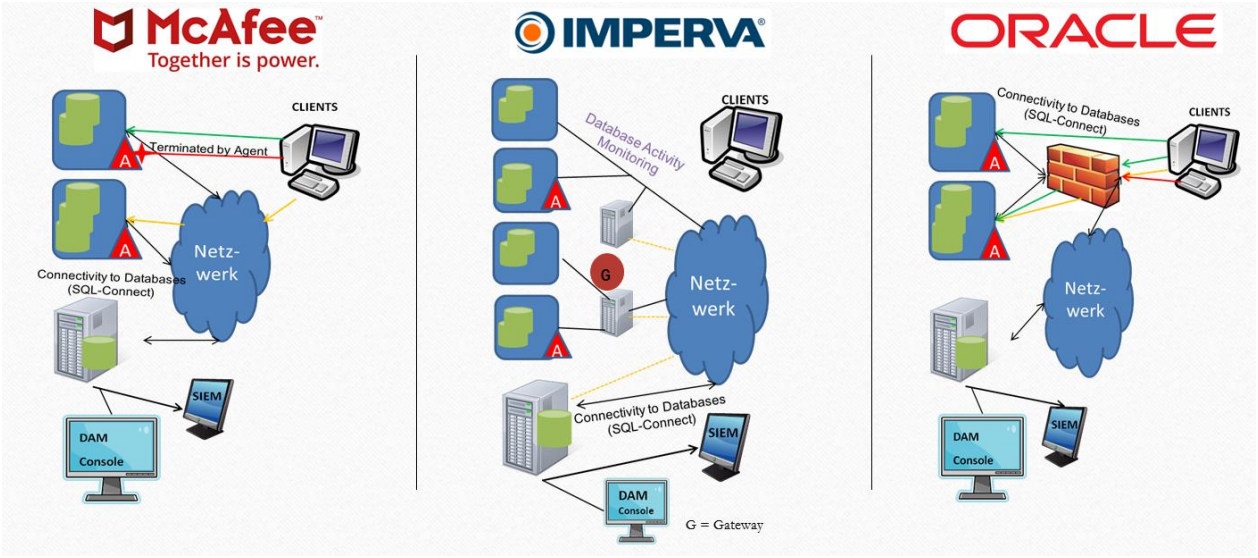

Abbildung 5: Architekturunterschiede

Überlegungen für einen Einsatz eines DAMs

- Definieren Sie die Systeme / Datenbanken die geschützt werden sollen
- Definiere Sie die Plattformen für Betriebssystem / Datenbank
- Prüfen Sie die Voraussetzungen für Compliance Checks
- Definieren Sie Reports- und Analyseanforderungen
- Prüfen Sie Anforderungen aus Datenschutzgesichtspunkten / Sicherheitsanforderungen
- Definieren Sie Prozessuale Abläufe zwischen DBA, Sicherheits-Admin und Sicherheitsabteilung

Kontaktadresse:

Sebastian Kilchert

MAIL: doag@kilchert.net

LinkedIn: https://www.linkedin.com/in/sebastian-kilchert-542a4937/

XING: https://www.xing.com/profile/Sebastian_Kilchert