Flexible und automatisierte Reaktionen auf Sicherheitsvorfälle

Franz Hüll
McAfee GmbH
Ohmstraße 1

85716 Unterschleißheim

Schlüsselworte
Database Security
Database Activity Monitoring
Virtual Patching for Databases
Vulnerability Manager for Databases

Einleitung

McAfee Database Activity Monitoring ist ein regelbasiertes System zur Überwachung der Zugriffe auf Datenbanken verschiedener Hersteller in Echtzeit. Ein Monitoring Sensor überprüft die SQL-Statements, die zur Ausführung an die Datenbank geschickt werden. Wenn ein Statement den in den Regeln hinterlegten Bedingungen entspricht, wird die mit dieser Regel assoziierte Aktion ausgeführt. (Event speichern, Mail verschicken, Weiterleitung via syslog oder SNMP, Archivierung in Archiv oder Datei). In gravierenden Fällen kann die Datenbanksitzung abgebrochen werden.

Durch Nutzung von Automatismen und die Einbindung in eine Sicherheitsinfrastruktur, kann die Flexibilität des Systems gesteigert und der Nutzen erhöht werden.

Im Vortrag wird an Hand von Beispielen in Theorie und Praxis aufgezeigt, wie das funktioniert.

Alle diese Beispiele funktionieren automatisiert, einmal eingestellt, sind keine weiteren Interaktionen eines Security Administrators erforderlich.

Security Connected

Unter dem Stichwort Security Connected hat McAfee hier eine Lösung geschaffen, die den Austausch von Informationen verschiedener Sicherheitsprodukte untereinander ermöglicht. Von zentraler Bedeutung sind dabei zwei Systeme:

McAfee ePolicy Orchestrator (McAfee ePO): McAfee ePO ist eine extrem erweiterbare und skalierbare Software für zentrales Sicherheits-Management. McAfee ePO fasst die Sicherheitsverwaltung auf einer offenen Plattform zusammen und vereinfacht sowie verbessert dadurch das Risiko- und Compliance-Management für Organisationen jeder Größe. Als Grundlage der Sicherheits-Management-Plattform von McAfee ermöglicht McAfee ePO Kunden die Verbindung branchenführender Sicherheitslösungen mit ihren jeweiligen Unternehmensinfrastrukturen, um die Transparenz und die Effizienz zu steigern und den Schutz zu stärken.

McAfee Enterprise Security Manager (ESM): ESM arbeitet mit der Geschwindigkeit und liefert die Kontextinformationen, die für die Erkennung kritischer Bedrohungen, die schnelle Reaktion darauf und die Unterstützung von Compliance-Anforderungen notwendig sind. Die fortlaufend gesammelten Daten zu globalen Bedrohungen und Unternehmensrisiken ermöglichen ein adaptives und autonomes Risiko-Management, das die Behebung von Bedrohungen sowie die Erstellung von Compliance-Berichten innerhalb von Minuten statt Stunden erlaubt.

Ausgangssituation:

In jedem Unternehmen sind eine Vielzahl von Security Produkten im Einsatz. Möglicherweise kommen alle von einem Hersteller, aber in meisten Fällen sind Produkte verschiedener Hersteller installiert. Beispiele sind Virenschutz, Firewall Software, Mail- und Web-Gateway Produkte, Intrusion Detection/Protection Systeme (IDS/IPS), Data Leakage Prevention (DLP), Security Incident and Event Management Systeme (SIEM) und - natürlich - Datenbank Sicherheitslösungen.

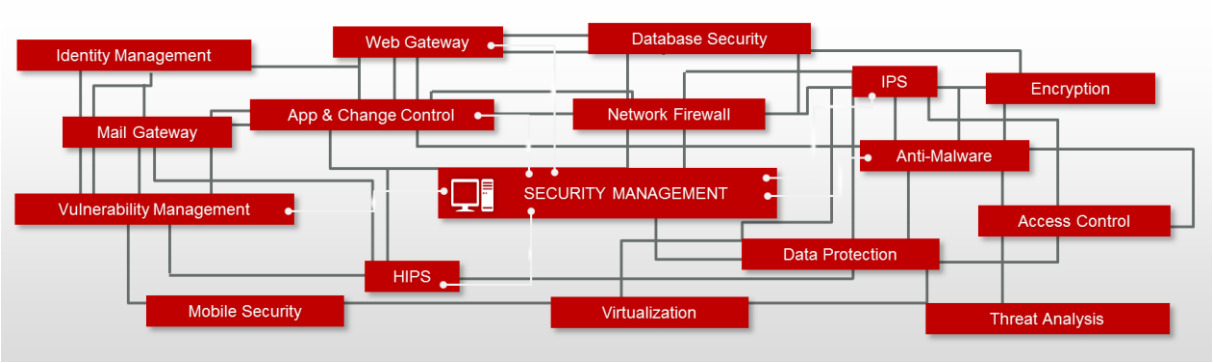

Abb. 1: Security Produkte

Wenn man sich jetzt einen typischen Angriff vor Augen führt, dann sind bei einer im Sinne des Angreifers „erfolgreichen“ Attacke immer mehrere Systeme betroffen. Angreifer von außen müssen die Firewall überwinden und gehen unter Umständen über mehr als eine Station bis das Zielsystem erreicht ist.

Angreifer von innen haben es da oft wesentlich einfacher, da für sie die Wege kürzer sind. Sie verfügen in den meisten Fällen auch über detailliertere Kenntnis der IT Infrastruktur und besitzen bereits Accounts zu den verschiedenen Systemen. Häufig besteht der Angriff von Innentätern darin, vorhandene Privilegien zu eskalieren um Zugriff auf sensible Daten zu erhalten.

Das Ziel eines Angreifers sind immer die Daten, die auf File Servern, Mail Servern und natürlich auf den Datenbank Servern gespeichert sind.

Die Vorbereitung eines Angriffes auf die Datenbanken hinterlässt dabei bereits Spuren. Das kann eine bestimmte Schadsoftware auf dem Arbeitsplatzrechner sein, aber auch der Zugriff auf eine sogenannte Honeypot Tabelle in einer Datenbank. Es kann der Versuch sein, eine gepatchte oder ungepatchte Datenbank mit einem Exploit anzugreifen, oder auch der Versuch, sich mit unerlaubten Tools gegen die Datenbank zu verbinden. Selbst der Zugriff auf eine Webseite, von der ein Exploitcode herunter geladen wird, kann bereits als Vorbereitung eines Angriffes interpretiert werden. Wird der Aufruf einer entsprechenden URL entdeckt, kann ein Benutzer, eine IP-Adresse oder eine Workstation für den Zugriff auf alle Datenbanken gesperrt werden.

Letztendlich geht es darum, Informationen über Sicherheitsvorfälle, die an einer Stelle der Infrastruktur entstehen, an anderer Stelle und durch andere Produkte weiter zu verwenden. McAfee hat hier eine Kommunikationsschnittstelle entwickelt, die den Informationsaustatsch verschiedener Security Produkte ermöglicht.

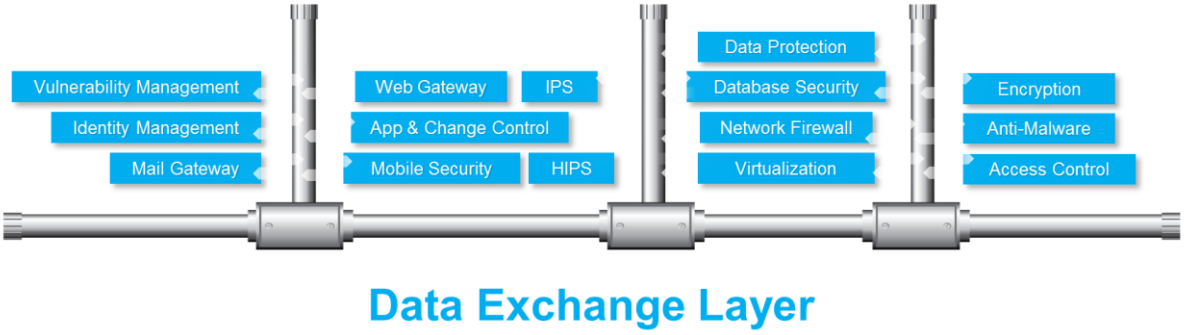

Abb. 2: DXL Data Exchange Layer

Duch das Zusammenspiel verschiedener Komponenten und der Kommunikation untereinander ergeben sich vielfältige Möglichkeiten. Bezogen auf die Sicherheit der Datenbanken können beispielsweise folgende Szenarien realisiert werden.

1. In der Datenbank wird ein Account mit DBA Rolle gefunden, der NICHT in der Liste der bekannten und zugelassenen DBAs enthalten ist. Jede Datenbankaktivität dieses Benutzers soll unterbunden werden.

2. Ein Anwender greift auf Daten zu, verwendet aber nicht das dafür vorgesehene Programm oder kommt von einer unzulässigen Quelle (IP, Hostname...). Ab sofort sollen ALLE Aktivitäten dieses Anwenders auditiert werden.

3. Ein im Unternehmen eingesetztes SIEM Tool erkennt aufgrund von eingegangenen Meldungen, dass ein Angriff stattfindet, da die Datenbanken in Gefahr sind wird die IP-Adresse für den Zugriff auf alle Datenbanken gesperrt.

4. Ein Benutzer surft auf Webseiten, die Exploitcode anbieten. Informationen über den Nutzernamen und/oder IP-Adresse und/oder Rechnernamen können von Database Activity Monitoring verwendet werden, um alle Zugriffe dieses Benutzers zu auditieren.

5. Ein Benutzer greift auf eine sogenannte Honeypot Tabelle zu. Ab diesem Zeitpunkt werden alle Aktivitäten dieses Benutzers für eine bestimmte Zeit protokolliert. Das soll auch für Accounts gleichen Namens in anderen Datenbanken gelten.

6. Ein Benutzer hat versucht, einen Exploit Code auf einer Datenbank auszuführen. Der Benutzer ist auf allen Datenbanken zu sperren.

Verwendete Tools in der Demo:

a) McAfee ePolicy Orchestrator

b) Database Activity Monitoring

c) McAfee Virtual Patching for Databases

d) McAfee Vulnerability Manager for Databases

e) ESM – Enterprise Security Management (SIEM)

Kontaktadresse:
Franz Hüll
McAfee GmbH
Ohmstraße 1
85716 Unterschleißheim

Telefon: +49.89.3707-1666
Mobile: +49.171.7666475
E-Mail franz_huell@mcafee.com