Franz Hüll
Brad Wilkinson
McAfee GmbH
Ohmstrasse 1
85716 Unterschleißheim

Schlüsselworte

Datenbank Sicherheit Database Security Monitoring Scanning Protecting
Angriff Verteidigung Attack Defense Auditing Compliance

Einleitung

Bei der geplanten Session handelt es sich nicht um eine Präsentation im eigentlichen Sinne. Es werden nur wenige Slides gezeigt. Dadurch ist dann aureichend Zeit für die geplante Live Demo vorhanden. Es wird erläutert, wie ein Angreifer gegen die Datenbank vorgehen könnte und welche Spuren er dabei hinterlässt. Sehr wichtig in diesem Zusammenhang ist auch, ab wann die ersten Anzeichen des Angriffes feststellbar sind. Wie können diese aussehen und was kann man dagegen tun. Zum Einsatz kommt SQL-Injection und die Eskalierung von Privilegien,

Aus Sicht des Angreifers ist der folgende Satz ausnahmesweise nicht gültig:

„Der Weg ist das Ziel“

Stattdessen gilt:

„Die Daten(bank) am Ende des Weges ist das Ziel“

Der Angriff wird auch aus zwei unterschiedlichen Sichten gezeigt: Zum einen aus Sicht des Angreifers, zum anderen aus Sicht des Verteidigers bzw. aus Sicht der Datenbank.

DieVoraussetzungen

Zwei Systeme sind an der Demo beteiligt:

Der Rechner des Angreifers und der Datenbankserver mit Datenbank (Oracle 11) und Monitoring Software (Database Activity Monitoring by McAfee).

Damit das für die Zuhörer gut nachvollziebar ist, werden die beiden Sichten zeitgleich über zwei Beamer dargestellt.

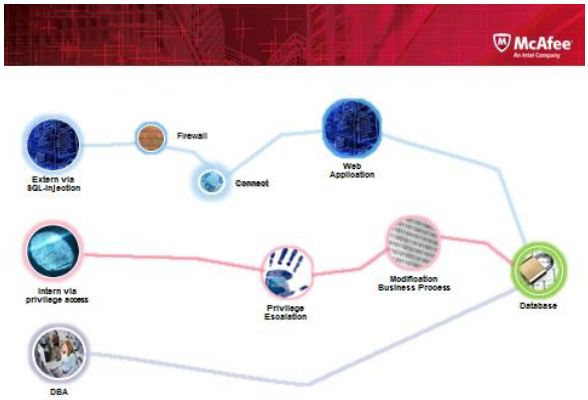

Abb. 1: Drei Angrifsszenarien

Die Szenarien:

Es werden drei Szenarien durchgespielt:

1. Angriff über eine lückenhaft programmierte Webanwendung. Mittels SQL-Injection werden in der Datenbank zusätzliche Informationen aufgespürt mit deren Hilfe dann über die Eskalierung von Privilegien vertrauliche Daten abgezogen werden können.

2. Angriff durch Innentäter. Ein Mitarbeiter (oder Consultant) der Firma verwendet seinen Account um einen Exploit zu starten mit dem Ziel, DBA zu werden. Damit ist der Abzug vertraulicher Daten kein Problem mehr.

3. Zugriff durch den DBA (oder eines anderen, ähnlich hoch privilegierten Nutzer). Dieser Nutzer muss keine Exploits mehr ausnutzen, er kann natürlich direkt auf alle Daten zugreifen. Zusätzlich versucht er noch Loginformationen der Anwendung zu manipulieren.

Die Angriffe werden Schritt für Schritt durchgeführt, dadurch bleibt auch die Zeit Varianten zu diskutieren. Es wird gezeigt, wie sich die ersten Spuren eines bevorstehenden Angriffes zeigen, wie der Angriff erkannt wird und wie letztendlich erfolgreich Gegenmaßnahmen getroffen werden können.

Kontaktadressen:

Franz Hüll
Telefon: 0171/7677475
Mail: franz_huell@mcafee.com

Brad Wilkinson
0151/16893640
brad_wilkinson@mcafee.com