Nabídka řešení Database Security

McAfee Data Center Security Suite for Databases

Zabezpečuje organizacím real-time přehled o aktivitách, které probíhají v jejich databázích a chrání citlivá data, která jsou v těchto databázích uchována. Ochraňuje databázový systém před vnějšími i vnitřními hrozbami a nabízí možnost provádění hloubkových auditů v databázích a navíc zabraňuje proniknutí do databáze, ukončením spojení porušujícího bezpečnostní politiky společnosti.

Hrozby pro databázové systémy mohou být zpřístupněny přes samotnou síť, od místního uživatele připojeného na server, nebo i přímo z databáze samotné přes uložené procedury. McAfee Database Activity Monitoring dokáže pomocí softwarových senzorů, které jsou umístěny k jednotlivým databázím, zachytit všechny výše zmíněné hrozby. Záznamy o incidentech je poté možno využít pro audity systému, či pro jeho další vylepšení.

Integrace s McAfee ePO

McAfee Data Center Security Suite for Databases se spravuje pomocí softwaru McAfee ePolicy Orchetrátor a nabízí tak komplexní správu a přehled o zabezpečení databáze, podnikové bezpečnosti a dodržování shody pro end-to-end viditelnost bez slepých míst. Dále nabízí i integraci nejen s produkty McAfee, ale díky Security Innovation Aliance, je možné Data Center Security Suite integrovat i s produkty třetích stran.

Klíčové charakteristiky:

- **Ochrana před hrozbami ze sítě, od uživatelů a přímo z databáze.**
- **Provádí monitoring v reálném čase.**
- **Integrace s dalšími McAfee nástroji, např. centrální správou McAfee ePO nebo McAfee Vulnerability Manager for Databases .**
- **Využití služeb Global Threat Intelligence, které účinně napomáhájí s detekcí hrozeb.**
- **Možnost Virtuálního patchovaní.**
- **Ukončení rizikových relací**
- **Využití pro audity systémů**
- **Detekuje a chrání proti nelegálním průnikům do databáze (v reálném čase), bez nutnosti odstávky databáze.**

McAfee Database Activity Monitoring

Monitorování se zaměřuje se na tři klíčové oblasti:

- **Aktivity**: Prověřuje přihlašování a odhlašování uživatelů, změny hesel, práva uživatelů, atd.
- **Změny schémat:** Vytváření a úprava tabulek, indexování, atd.
- **Změna dat:** Vkládání, mazání a úprava citlivých dat v databázi

Výsledky lze později využít, k určení kdo, kdy a jak provedl danou změnu pro případnou forenzní analýzu, kde tyto informace mohou mít zásadní význam pro určení, zda byla změna korektní, či ne. V neposlední řadě je třeba uvést, že monitoring databáze má minimální nároky na výkon celé infrastruktury

Identifikace hrozeb a snižování rizik

Na rozdíl od jednoduchých nástrojů pro audity a sběr logů, McAfee Database Activity Monitoring v průběhu analýzy v reálném čase dokáže odhalit narušení sítě a relaci ukončit dříve než dojde ke vzniku škod. Alerty o takové události jsou zasílány obsluze s kompletními informacemi o porušení zásad tak, aby mohla být učiněna patřičná opatření v co nejkratším možném čase.

Virtuální patchování

V případě, že existuje aktuální riziko pro databáze a nebyl vydán nový patch, McAfee Database Active Monitoring se na tuto slabinu zaměří a v případě útoku přes toto slabé místo relaci ukončí, či zašle report o probíhajícím útoku a to vše v reálném čase. Druhou výhodou je, že po vydání nového patche není nutné patch ihned nasadit, což sebou nese velké nepříjemnosti spojené s restartem databáze.

Nasazení McAfee Database Activity Monitoring – agent based řešení včetně ukončení rizikových relací

McAfee Database Active Monitoring je softwarové řešení, které nepotřebuje žádný speciální hardware, či další server. Jednotliví agenti běží přímo na databázích, což vede k přesnému aplikování bezpečnostních politik. McAfee Database Activity Monitoring provádí skenování sítě zcela automaticky, uživateli poskytuje šablony pro rychlejší specifikaci potřeb konkrétní sítě a vytváření vlastních bezpečnostních politik vedoucích ke splnění požadavků na audity. Bezpečnostní politiky lze jednoduše distribuovat k jednotlivým senzorům běžícím na databázových serverech, díky tomu lze řešení nasadit i v největších společnostech.

Klíčové charakteristiky:

- **Umožní flexibilní vytváření vlastních politik, tak aby byly s souladu s předpisy**
- **Nabízí log přístup k citlivým datům, včetně transakčních detailů (pro účely auditu)**
- **Ukončí relaci při porušení zásah**
- **Možnost umístění do karantény podezřelých uřivatelů.**
- **Ukončení rizikových relací**
- **Využití pro audity systémů**

COMGUARD
security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

Nabídka řešení Database Security

McAfee Vulnerability Manager for Databases

Dnešní svět je plný hrozeb zaměřených na databázové systémy, a proto McAfee přichází s nástrojem, který umožňuje administrátorům na základě provedeného skenování určit zranitelnosti databázových systémů. Zároveň umožňuje určit, která ohrožení jsou kritická, resp. která jsou méně či vůbec relevantní. Díky tomu je možné zaměřit se na kritická místa systému a zamezit potenciálním útokům. Díky spolupráci se systémem globální inteligence je systém skenován vždy na aktuální hrozby, tím získáme přehled, jak si naše databáze stojí v porovnání s hrozbami reálného prostředí.

McAfee Vulnerability Manager for Databases kontroluje více jak 3000 zranitelností, mezi něž například patří:

- **Zranitelnost hesel**
- **Úroveň patchovaní**
- **Configuration baselining**
- **Backdoor detection**
- **Sensitive data discovery (PII, SSN, etc)**
- **Vulnerable PL/SQL code**
- **Unused features**
- **Custom checks**

Klíčové charakteristiky:

- **Vulnerability scanner pro databáze**
- **identifikace patch levelů a nezabezpečeného PL/SQL kódu**
- **nalezení slabých hesel**
- **nalezení pokusů o SQL injections a databázových rootkitů a stop malware**
- **Podrobné reporty**
- **Integrace s dalšími McAfee nástroji, např. centrální správou McAfee ePO.**
- **Nízké nároky na výkon**
- **BEZ AGENTŮ**

Informace o jednotlivých zranitelnostech systému jsou uchovány a my můžeme sledovat, jestli byla sjednána náprava (například nainstalováním záplaty nebo změnou hesla, atd.). To nám zajistí přehled o vývoji zranitelností naší databáze.

Nasazení McAfee Vulnerability Manager for Databases – nevyžaduje agenty na databázích

Tento softwarový nástroj se instaluje na server běžící v datovém centru a odtud jsou prováděny skeny jednotlivých databází. Služba běží na serveru a z něj je prováděna kontrola z pohledu útočníka, na jednotlivé zranitelnosti. Získáme tedy kompletní přehled o stavu zabezpečení našich databází.

McAfee Virtual Patching for Databases

S Virtual Patching pro databáze si mohou organizace být jisti, že mají aktuální zabezpečení databáze. Virtual Patching skenuje stav zabezpečení databáze v reálném čase a pomáhá chránit citlivé informace společností tím, že vyhledává dostupné aktualizace vydané i pro Systém řízení báze dat (SŘBD). Nasazení a testování vydaných aktualizací (main release) je náročný a kontinuální proces, který má za následek časová okna a možnost zranitelnosti systému. McAfee Virtual Patching chrání databáze před nebezpečím neaktualizovaných zranitelností pomocí detekce a prevence vniknutí, včetně terminování session na databázově orientované hrozby založené na známých zranitelnostech směřujících na nepatchované databázové servery zahrnující obvyklé „zero-day" útoky. K dispozici je množina pravidel pro virtuální patchování (nelze vytvářet uživatelská pravidla).

Klíčové charakteristiky:

- **Updatuje a chrání citlivá data v databázi, aniž by musela být v režimu offline**
- **Nevyžaduje znalosti struktury databáze**
- **Automatická distribuce aktualizací**
- **Soulad s normami PCI DSS, HIPAA atd.**
- **Ochrana databáze i mezi aktualizacemi**

McAfee Virtual Patching je plně integrovatelný se ePolicy Orchestrator a nabízí centralizovaný reporting a souhrnné informace o všech databázích na jednom jediném přehledném dashboardu.

Systémové požadavky

Podporované OS pro DBM

- Redhat Linux or SUSE Machine
- Sun Solaris
- AIX
- HPUX
- Windows Machine

Browsers (for management Acces)

- Firefox 2.0 or later
- Microsoft Internet Explorer 7.0 or later
- Microsoft Edge
- Chrome

Podporované databáze

- Oracle version 8.1.7 or later, running on Sun Solaris, IBM AIX, Linux, HP-UX, Microsoft Windows, including Oracle RAC and Oracle Exadata
- Teradata 12, 13, 13.10, 14,15, and 15.1 on Linux
- MySQL 5.1, 5.5, 5.6 and 5.7 on Linux
- Microsoft SQL 2000, 2005, and 2008 on any supported Windows platform
- IBM DB2 Z/OS, iSeries(AS/400)
- PostogreSQL 9.2 or later (Linux)
- MariaDB version 5.5 (Linux)
- SAP HANA SPS 09, Revision 91 or later
- Sybase ASE 12.5 or later on all supported platforms

COMGUARD security & networking

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz